Successful Applications of Risk-Informed Decision-Making for Operating and New Reactors

Shilp Vasavada

Chief, PRA Licensing Branch C

Division of Risk Assessment, Office of Nuclear Reactor Regulation

Shilp.Vasavada@nrc.gov

Approval of NuScale's Risk-Informed EPZ Sizing Methodology

- Achieved a globally impactful and seminal risk-informed regulatory decision
  - Demonstrated the value of risk-informed decision-making in balancing safety and flexibility
  - Demonstrated the value of an integrated multi-disciplinary team spanning three Offices
  - Expanded the applicability of risk-informed decision-making
- Solved significant technical issues while maintaining fidelity with EPZ fundamentals
  - Present day risk assessment and dose consequence tools applied to EPZ sizing fundamentals (NUREG-0396) using the principles of risk-informed decision-making
  - Licensing and design ≠ EPZ spectrum of accidents
- Developed technology-inclusive and reproducible approaches
  - Event screening, including seismic events, for EPZ sizing
  - Dose-distance acceptance criteria

Use of Risk Insights to Support the NuScale SDAA Review

- Collected design-specific risk information and insights during pre-application engagement
- Shared insights with reviewers and senior management
- Discussions and decisions on challenge areas for acceptance review started with relevant risk insights
- Level of effort for different FSAR chapters graded (H, M, L) with support from risk insights
- Continued use and communication of risk insights for challenging technical issues
  - Integrated teams spanning multiple technical disciplines

Risk-Informed Process for Evaluations (RIPE)

- RIPE is a streamlined NRC-review process for addressing low safety significance license amendment and exemption requests
  - Focus resources and attention on safety significant issues
  - Rooted in principles of risk-informed decision-making
  - Leverages existing regulations and risk-informed initiatives
- Application
  - Applied to a first-of-a-kind exemption request
  - Process exercised for efficient review and approval (approximately 100 staff review hours)
  - Feedback from staff resulted in enhanced guidance

Open Phase Condition (OPC) Resolution

- Open Phase Isolation System (OPIS) installed by several licensees as part of industry initiative on OPC
- Spurious actuations were observed during the monitoring phase of OPIS implementation resulting in need to identify and evaluate options
- Resolved spurious actuations issue at approximately 65% of plants using a risk-informed approach by implementing manual OPC isolation
- Comparison of risk from OPIS and the manual OPC isolation determined to be small
- Risk-informed approach balanced safety and operational flexibility

Key Takeaways

- ✓ NRC staff continues to apply the principles of risk-informed decision-making across business lines
- ✓ Tangible successes demonstrate progress and provide opportunities to further expand applications

Palo Verde RIPE Exemption Success

Removal of the Diverse Auxiliary Feedwater Actuation System

Matthew Cox

Department Leader, Nuclear Regulatory Affairs

September 12, 2023

PaloVerde™ GENERATING STATION

RIPE Exemption Application

- 10 CFR 50.12 partial exemption from 10 CFR 50.62(c)(1)

  … must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, **to automatically initiate the auxiliary (or emergency) feedwater system** *and initiate a turbine trip under conditions indicative of an ATWS…*

- Removed the Diverse Auxiliary Feedwater Actuation System (DAFAS) from the PVNGS licensing basis
- Addressed equipment obsolescence

Journey

Identification of low-risk application for the new RIPE process

	CDF	LERF
Increase in risk between Baseline & DAFAS Sensitivity	3.2×10^{-9}	5.9×10^{-11}
NEI 21-01 RIPE Acceptance Guidelines	$< 1.0 \times 10^{-7}$	$< 1.0 \times 10^{-8}$

Resources associated with maintaining or replacing DAFAS was not commensurate to its safety significance, which represented an undue hardship

Journey

- Reviewed NRC and NEI guidance for RIPE exemptions
- Challenge board with industry including NEI
- Initial NRC pre-submittal meeting
- Integrated Decision-making Panel (IDP) observed by NRC
- Second NRC pre-submittal meeting
- Submitted January 2022 and approved March 2022

Challenges

- Interpreting the new process
- Ensuring adequate technical detail and addressing defense-in-depth
- Developing RIPE-IDP procedure, training, and qualification
- Managing increased observations
- Importance of a high quality submittal
  - Request for additional information (RAI) exits RIPE and enters the traditional exemption process

Success

- Timely NRC approval within the 13 week guidelines
- DAFAS removed from the licensing basis, bypassed by operations, and plant modification in progress to physically remove the system
- Open communication from a seek to understand perspective
- ADAMS References
  - Submittal dated 1/14/2022 – ML22014A415
  - Acceptance review dated 1/31/2022 – ML22032A031
  - Response to RCI dated 2/22/2022 – ML22053A212
  - Approved exemption dated 3/23/2022 – ML22054A005

Aircraft Radio Altimeters and 5G C-Band Deployment in the United States

NRC's 2023 Risk Forum

September 12, 2023 | Rockville, MD

Presented by:

Chris Hope, Deputy Director (A), Office of Safety Standards, FAA Flight Standards Service

FCC R&O and the RTCA Report

- **The FCC Report and Order dated February 28, 2020, established a new and unknown operating environment for aircraft operating in areas where 5G (3.7-3.98 GHz C-Band) emissions will be present**
  - Under the FCC rules, the wireless C-Band deployment was to start on December 5, 2021 in the lower 100 MHz (3700-3800 MHz) in only 46 markets
  - Phase 2 of the deployment included 19 additional license holders and would allow deployment in CONUS (ex: HI and AK) in the full band (3.7-3.98 GHz)
- **Results from RTCA testing published in October 2020 indicated a major risk that 5G C-Band telecommunications system will cause harmful interference to RADALT of all types of civil aircraft**
- **The RTCA report, public comments to the RTCA report, and analyses from radio altimeter manufacturers and aircraft manufacturers were used in support of the safety risk determination and development if the AD published in Dec 2021**

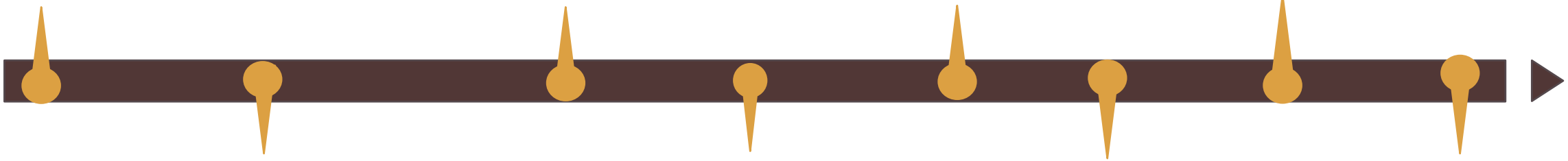
Radio Altimeter Airworthiness Directives

FAA issued two ADs in December 2021 prohibiting certain operations in the presence of 5G (3.7-3.98 GHz C-Band) emissions

- One AD addresses transport category airplanes and the other helicopters
- The Unsafe condition is defined as unreliable radio altimeters in the presence of 5G C-Band
- Notices to Air Missions* (NOTAM) have been issued to limit the impact of the AD to areas and airports where 5G C-Band will be deployed

- These ADs are interim actions. As FAA obtains additional data, we may issue additional ADs to address aircraft specific hazards or choose to revise these ADs
- FAA regulations and advisory guidance allows anyone to propose to the FAA an alternative method of compliance (AMOC) or a change in the compliance time, if the proposal provides an acceptable level of safety
  - An AMOC provides an acceptable level of safety for a different way, other than the one specified in the AD, to address the unsafe condition
- 12 additional aircraft specific ADs published

Timeline of 5G Deployment in the U.S.



2015

- Mobile C-Band Allocations are Proposed at World Radio Communications Conference
- ICAO Job Cards Created

2017

- U.S. Initiates Procedures to Allocate C-Band for 5G
- Aviation Submits Comments Expressing Concerns

2019-20

- Testing by Aviation Demonstrates Potential Interference
- RTCA Report Published in 10/2020

2020

- U.S. Completes Allocation of C-Band Spectrum for 5G

2021

- FCC Auctions 5G C-Band Spectrum

2021

- U.S. Government Interagency Discussions
- FAA Issues Safety Mitigation Actions including Airworthiness Directives Restricting Low Visibility Landings

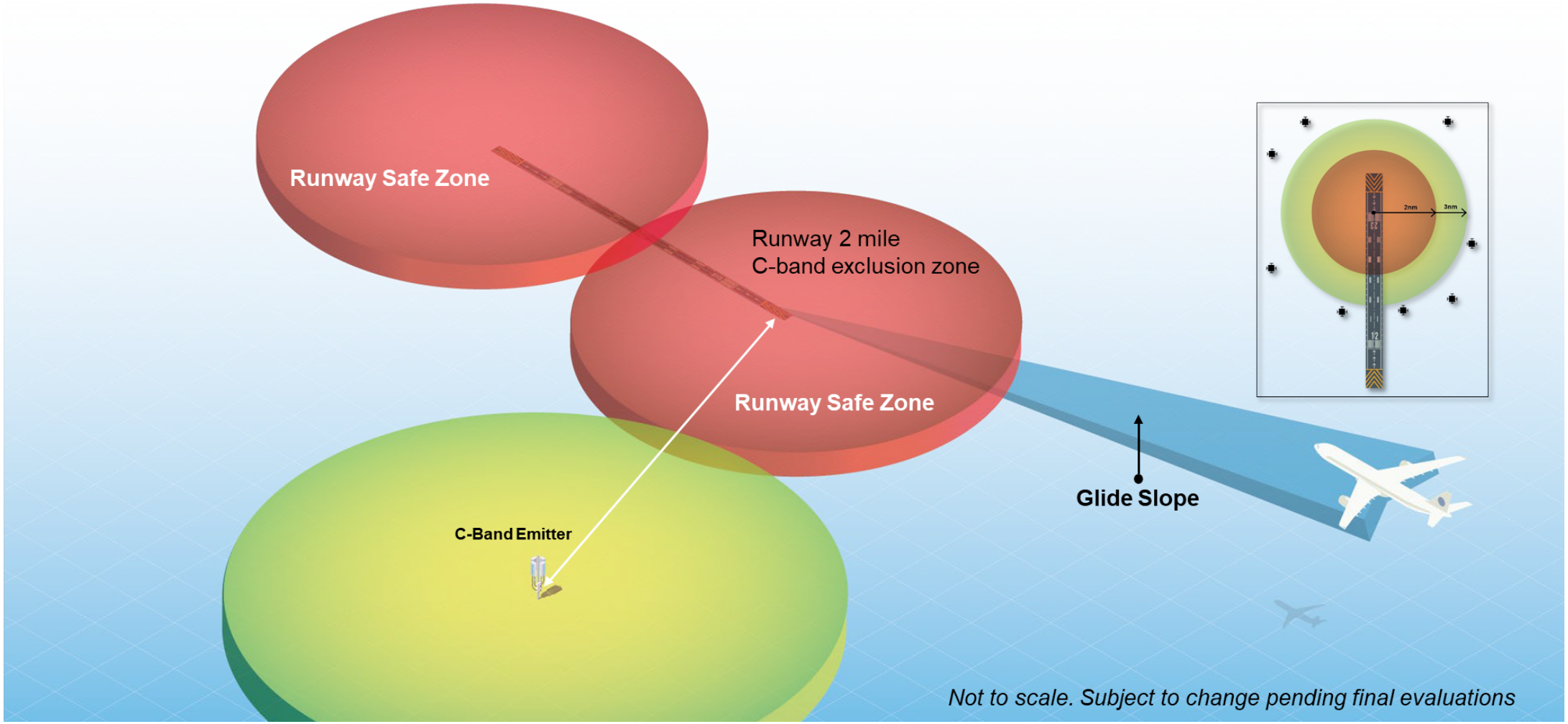
2022

- Verizon and AT&T Begin Deploying 5G C-Band Services in the U.S.
- FAA brokers Cross-Industry Information Sharing to Manage Operational Impacts

2022

- FAA Issues Additional Airworthiness Directives Mitigating Airplane-Specific Safety Risks

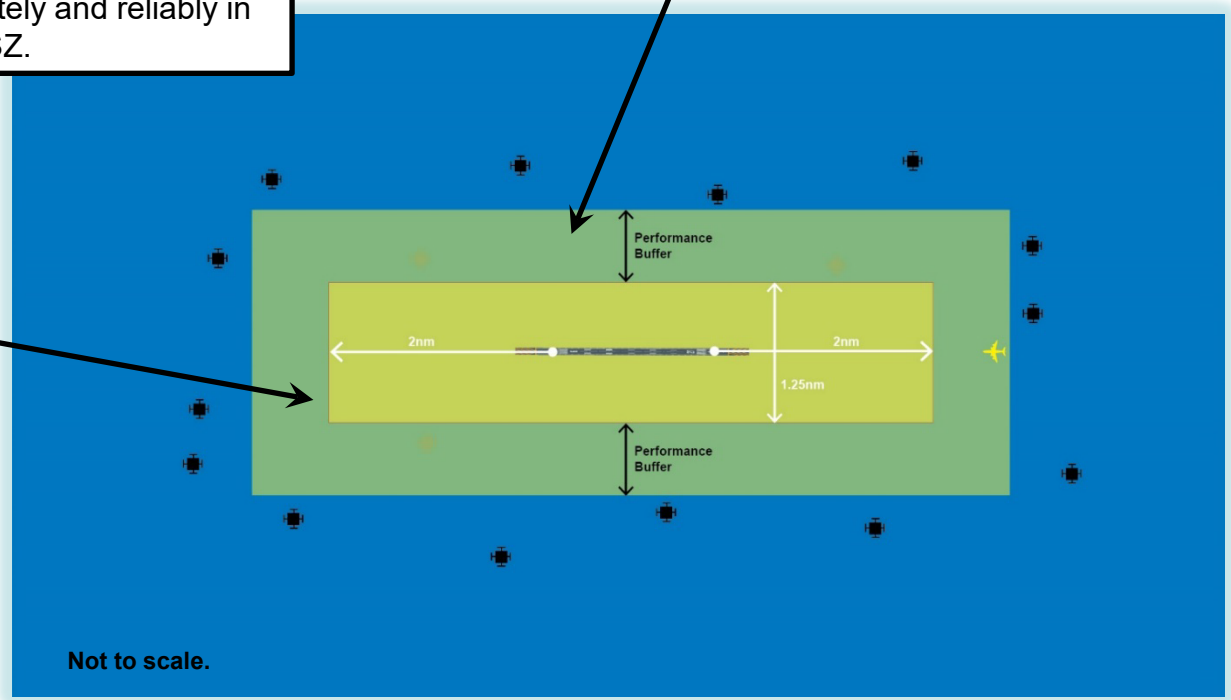
Runway Safety Zone (v1.0) with Performance Buffer



Runway Safety Zone (v2.0) with Performance Buffer

Performance Buffer (PB)
– FAA AMOCs are issued based on the performance capabilities of the Radio Altimeter.

Runway Safety Zone (RSZ)
– The Radio Altimeter must function accurately and reliably in 100% of the RSZ.



FAA's method for performing this evaluation has evolved several times since January 2022

5G C-Band Real World Measurement

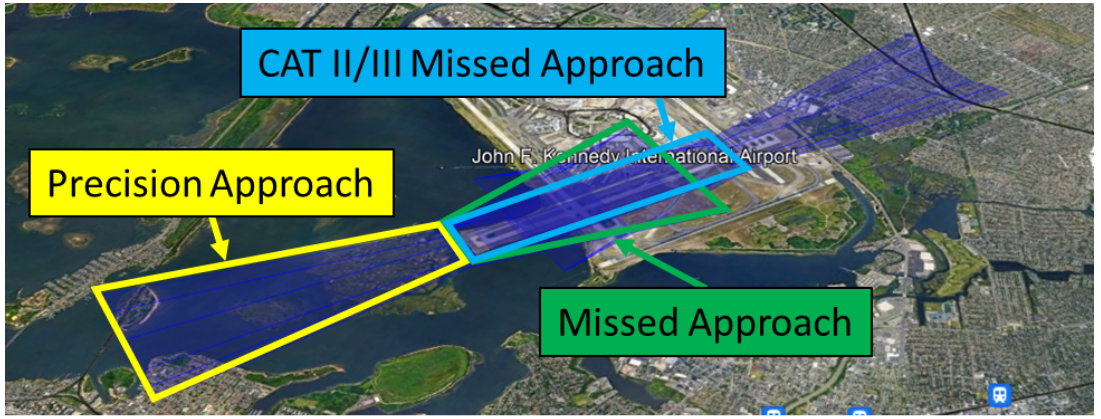
Understanding 5G Signal Levels in an “airspace”

- We now know the RA Failure modes and levels of signal that cause it
- We needed to know the actual signal levels in real world environment
- Historical approach to FAA modeling of RF propagation uses the maximum regulatory limits of a system as operating assumptions:
  - For 5G C-Band - that modeling showed no path to safe coexistence (see R&O)
  - New method needed to have confidence in the level of signal on the aircraft:
    1. Model the Radio Frequency (RF) predicted environment
       - FAA worked with wireless to understand their in-house RF modeling tools predicting 5G signal propagation using as-built characteristics
       - With those wireless models – they showed that the signal levels were high enough to cause impacts to altimeters
    2. Measure the actual RF environment
       - Need to empirically assess realistic encounterable 5G signal levels in the airspace
       - FAA coordinated a series of flight measurements in partnership with AT&T and Verizon to measurement ambient 5G signal levels

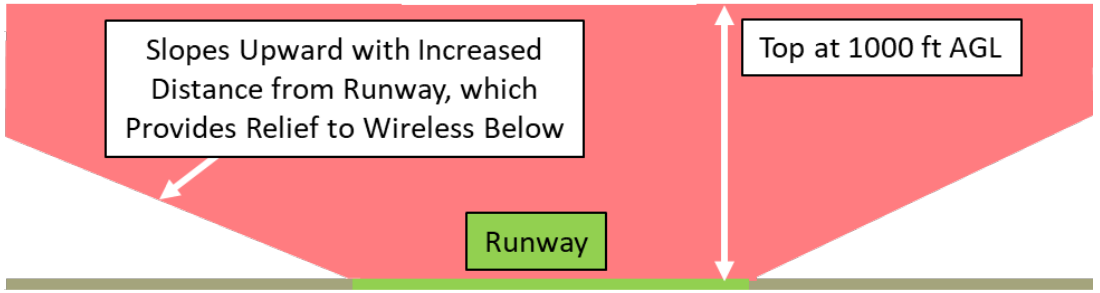
5G C-Band Real World Measurement

Signal-in-Space Basics

- **Runway Safety Zone:** Area around an airport that represents a 3D volume of space where normal operation of a radar altimeter is critical to aviation safety
- **Power Thresholds:** The maximum amount of fundamental and spurious 5G signal levels that radar altimeters can experience before producing erroneous results
- **Predictive Model:** The mathematical formulas that convert 5G base station locations into 5G SIS power level predictions throughout the Runway Safety Zone (discussed on previous slides)
- FAA assesses the compatibility of the base stations against the applicable **Power Thresholds** inside the **Runway Safety Zone** using the **Predictive Model** to predict the signal levels



Satellite View



Typical Profile View

Key Safety Systems Affected by RadAlt

- **Terrain Awareness and Warning System (TAWS)**
  - Alerts and prevents controlled flight into terrain (CFIT)
  - Looks ahead and downward
  - Introduced 1998--mandatory since 2002
- **Traffic Collision Avoidance System (TCAS)**
  - Alerts the presence of nearby traffic and cooperates among airplanes
  - Introduced 1988--mandatory from 2003
- **Windshear (Reactive) Warning and Guidance**
  - Alerts aircrew to windshear
  - Measures ground clearance during escape maneuver (Inhibited above 2500 feet)
  - Mandatory since 1991

Key Safety Systems, historical examples

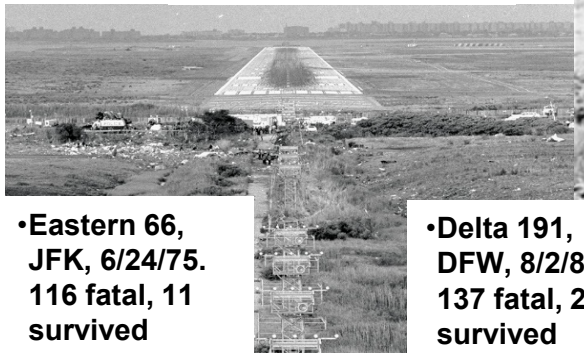
Precipitants of TAWS

- Alaska 1866, Juneau, 9/4/71. 111 fatal
- American 965, Cali, 12/20/95. 151 fatal, 4 survived

TCAS

- PSA 182, San Diego, 9/25/78. 144 fatal
- Aeromexico 498, LAX, 8/31/86. 82 fatal

Windshear



- Eastern 66, JFK, 6/24/75. 116 fatal, 11 survived

- Delta 191, DFW, 8/2/85. 137 fatal, 26 survived

Managing Cumulative Fleet Risk

Source: ICAO Safety Management Manual (SMM) (Doc 9859)

Safety Risk		*Severity*				
Probability		*Catastrophic A*	*Hazardous B*	*Major C*	*Minor D*	*Negligible E*
Frequent	5	5A	5B			5E
Occasional	4	4A	4B	4C	4D	4E
Remote	3			3C	3D	3E
Improbable	2	2A	2B			2E
Extremely improbable	1	1A	1B	1C	1D	1E

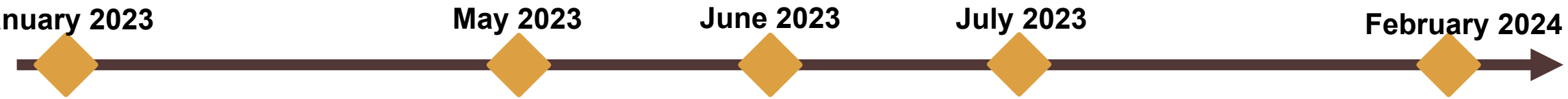
Major / Minor

Hazardous / Catastrophic

Major / Minor

- FAA ADs mitigate risks of hazardous/catastrophic outcomes
- Numerous major/minor hazards are not addressed by current ADs
- Expanded 5G deployments will increase the rate of major/minor events
- Residual risk is accumulating globally; FAA, EASA, TCCA, ANAC are discussing how to harmonize our approach to global risk management

5G / RA Coexistence Timeline



January 2023

- FAA issues Notice of Proposed Rulemaking (NPRM) Airworthiness Directive (AD) establishing retrofit requirements for all airplanes
- Retrofits underway

May 2023

- FAA issues NPRM ADs confirming additional airplane-specific restrictions

June 2023

- FAA issues Final Rule ADs confirming NPRM requirements

July 2023

- 5G C-band deploys nationwide in the 3.7 to 3.98 GHz frequency band at increased power levels
- Low visibility landings and airplane-specific restrictions apply nationwide for aircraft that are not retrofit

February 2024

- AD requires all commercial airplanes to meet retrofit requirements

Operator SMS

- **Associated Systems**
  - RA systems such as autoflight, TAWS, TCAS, HUD, FD, Anti-ice, etc
- **Possible System Hazards**
  - Erroneous indications/annunciations, inoperable systems, takeoff and landing wind limitation hazards, loss of windshear guidance, etc
- **Aircraft-Level Hazards (Consequences)**
  - Accidents
    - Runway excursion/overrun
    - Hard landing
    - Tail strike: fuselage drags on contact with pavement
    - Loss of control inflight
    - Midair collision
  - Long-term effects
    - Desensitization to flightcrew alerts from increased nuisances
- **Controls**

Enabling Coexistence Long Term (e.g., beyond July 2023)

- **Focus will remain on getting remainder of aircraft modified to meet February 2024 requirement**
- **All 21 3.8-3.98 GHz licensees have advised FCC that they voluntarily agree to:**
  - Delay widespread use of these higher frequencies
  - Limit spurious (out of band) emissions
  - Implement antenna “down tilt” nationwide
  - Reduce power near airports
- **Sunset date of these agreements is five years with “midterm” check in**
- **Buys aviation community time to develop and implement more robust RAs**

Lessons Learned Summary

- U.S. approach is an example of safe integration—other countries have also had success
- New generation of performance standards are needed to ensure future technology evolutions won't disrupt coexistence
- Government and industries need to work together
- Industry and Safety Management System (SMS)

NRC’s 2023 Risk Forum

September 12, 2023 | Rockville, MD

Discussion

Risk-Informed Program Benefits

Suzanne Loyd

Senior Manager, Constellation Risk Management

12 September 2023

Long Standing Risk-Informed Programs at Constellation

Surveillance Frequency Control Program

- Used to extend surveillance intervals
- Equipment with good test history
- Multi-disciplined panel used for decision-making

Benefits:
- Focus on important SSC surveillances
- **Divisional outage planning**
- **Reduced half-trips**
- Reduced labor for testing

MSPI

- Measures difference in system unavailability and unreliability
  - High-pressure systems, RHR, Emergency AC, Cooling Water

Benefits:
- Focus on risk significant SSCs
- **Encouraged plant improvements to reduce MSPI vulnerability**

Maintenance Rule

- Configuration Risk Management and Maintenance Rule (a)(4)
  - Planned and emergent work
- Component risk ranking

Benefits:
- Focus on risk significant SSCs
- **Balance of plant availability and reliability through maintenance practices**

Constellation

RICT Program Benefits

Avoid emergent shutdowns

- Instant use of approved RICT procedures/Risk Monitor tool instead of seeking NOED/LAR
- Extend very short AOTs
  - Inverter replacement
  - Extended 2hr AOT

Plan large design changes & modifications

- Eliminate one-time LAR(s)
- Transformer work
- Avoid complex offsite power re-alignments
  - Avoided potential human errors

Move routine work from outage to online

- Work performed during less stressful times
- Large power transformers
- Common equipment at multi-unit sites
  - Preclude dual unit shutdown

Lower organizational stress

- Contingency/What-if RICT calculations/preparations
- Possible relaxation of 24/7 requirements
- Less urgency for contingency vendor support and parts
- “Friday” spin-ups

Constellation

10CFR50.69 Program Benefits Projected Savings with Alternative Treatments at Limerick

- Cost avoidance from PM extensions
  - ~ $375k/year Materials and Labor
- IST - Projected savings for descoping RISC-3 components from supplementary position indication
  - ~ $200k(one time procedures savings)
  - ~ $15k/year (App J reduction)
- ISI – Reduction in weld exams and pressure testing
  - $17k/yr.

SLC relief valve test/replacement

- Extending from 8 to 15 years gives annualized savings of ~$30k/year

SLC EQ PMs for squib valve and level transmitter

- Retiring Replacement PMs gives annualized savings of ~$21k/year

PCIG relief valve test & replacement

- Extending from 8 to 15 years gives annualized savings of ~$16k/year

Drywell HVAC motor

- Condition-based monitoring, extending PM (previously EQ) ~ $260k/year

Radiation Monitor recorders

- 50% savings in parts; Lead time changed from 12 weeks to “In stock”

Constellation

10CFR50.69 Case Study – Limerick RHR Service Water Spray Pond Piping – July 2019

Spray network piping corrosion

RHR Service Water categorized as RISC-3 using the 50.69 program

Successful replacement in September 2019

Prompt resolution of a significant material condition issue

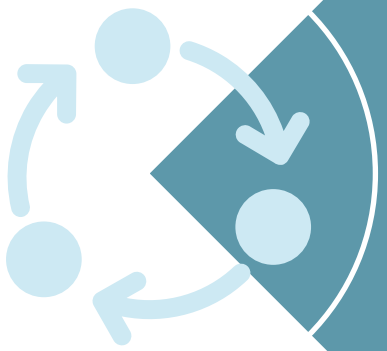
- One header of two for each unit of RHR Service Water unavailable
- Entry into Action Statements for both units required to repair

- Reduced cost using approved alternative treatment'
- RICT to perform piping replacement without dual-unit shutdown

- Fast lead time and turnaround
- Manufacturing safety-related piping would have required delays due to conversion to manufacture safety related piping
- Would have caused additional delays in other orders, impacting supply chain
- Overall savings ~ $1M considering materials, labor, QA/QC, etc.

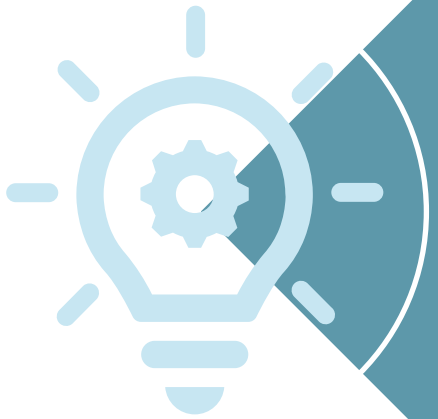
Constellation

Lessons Learned from 10CFR50.69 Program Implementation



Benefits from 50.69 are not just money saved

- Quicker turnaround on material procurement
- Prompt resolution of material condition problems
- Prompt restoration of systems
- Focus on safety-related systems



Innovative risk-informed applications take time

- Experience creates new ideas/innovation
- Realizing some early “wins” builds plant confidence

Constellation

Risk-Informed Initiative Success Stories – Oversight

Julio Lara, Director
Division of Operating Reactor Safety, Region III

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Oversight

Regional Offices have responsibility for Reactor Oversight

- Increased focus on implementation of risk informed initiatives
- Modernizing internal processes to enable staff to better integrate risk insights
- Focus on risk-informed decision-making

Risk Informed Completion Times

- Inspector tabletops as RICT amendment requests approved
- SRAs proactively engage inspectors in RICT reviews
- Safety and operational flexibilities

PRA Configuration Control

- Operating experience smart sample that will verify that PRA configuration control programs
- Verify that PRA models remain technically adequate, reflecting the as-built, as operated plant to ensure confidence in the use of PRA results

Risk Focused Inspections

- 10 CFR 50.69 Risk-informed categorization and treatment of components
- Maintenance Rule
- Outage risk management

Managing Uncertainty: The Role of Safety Margins and Performance Monitoring

Sunil Weerakkody

Senior Level Advisor, PRA

Division of Risk Assessment

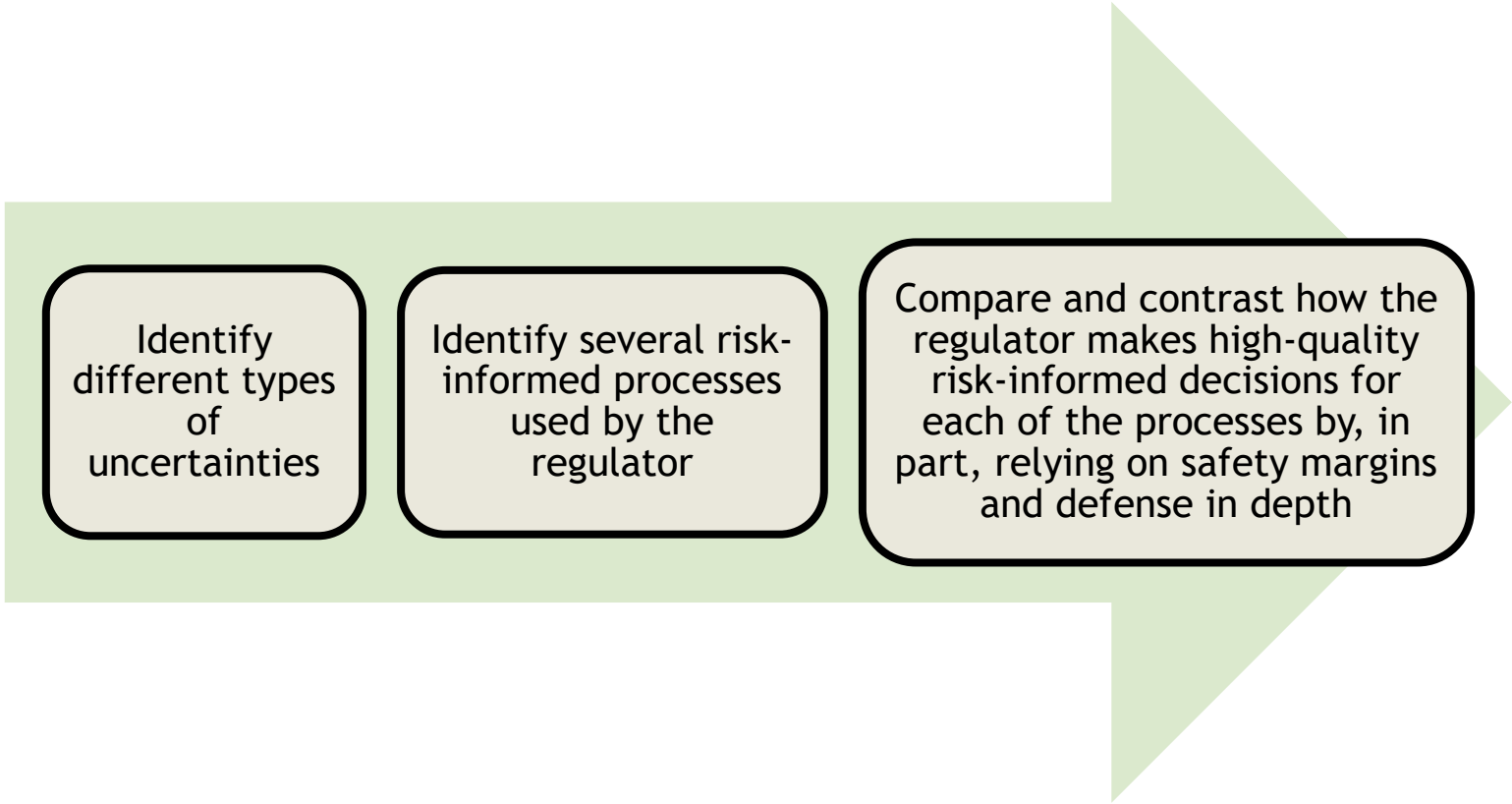
Office of Nuclear Reactor Regulation

US Nuclear Regulatory Commission

KEY QUESTION

Is NRC making high-quality risk-informed decisions that ensure adequate protection of public health and safety by appropriately treating uncertainties?

OVERVIEW OF THE PRESENTATION



What is aleatory uncertainty?

(NUREG-1855): “Aleatory uncertainty is based on the randomness of the nature of the events or phenomena and cannot be reduced by increasing the analyst’s knowledge of the systems being modeled. Therefore, it is also known as random uncertainty or stochastic uncertainty.”

(Oxford English Dictionary): “[Uncertainty] dependent on uncertain contingencies; left to or resulting from a chance process.”

(Mariam Webster Dictionary): “[Uncertainty] dependent on an uncertain event or contingency as to both profit and loss; Deriving from the Latin noun *alea*, which refers to a kind of dice game, *aleatory* was first used in English in the late 17th century to describe things that are dependent on uncertain odds, much like a roll of the dice. ”

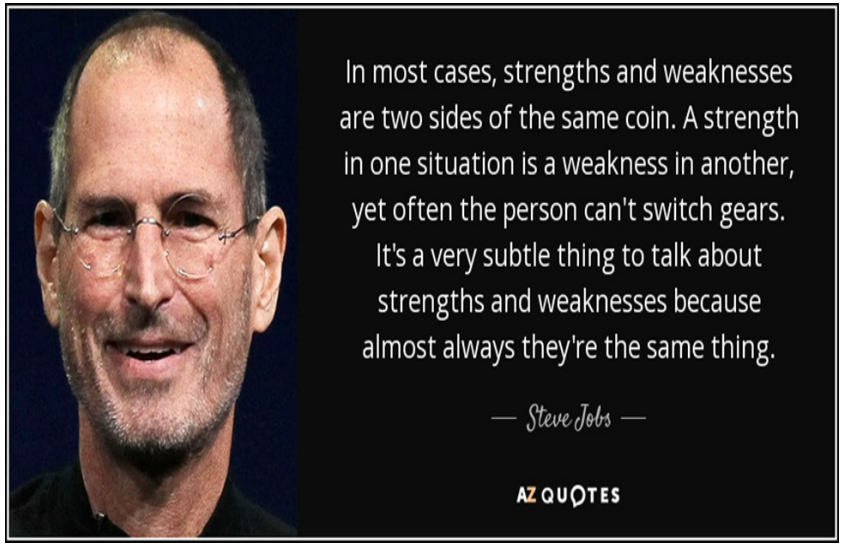
What is epistemic uncertainty?

NUREG-1855: “Epistemic uncertainty is the uncertainty related to the lack of knowledge about or confidence in the system or model and is also known as state-of-knowledge uncertainty (Includes Parametric uncertainty, Completeness uncertainty, Model uncertainty)”

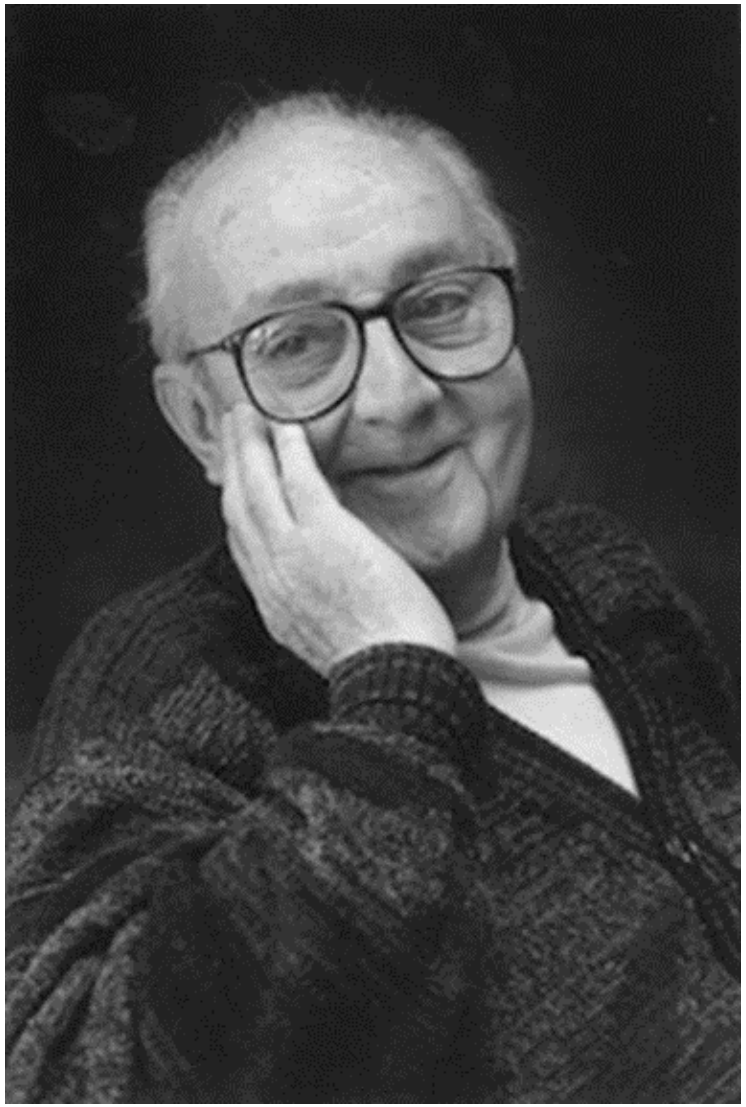
Oxford English Dictionary: “[uncertainty] Of or relating to knowledge, or to its extent, linguistic expression, or degree of validation.”

Mariam Webster Dictionary: “[uncertainty] of or relating to knowledge or knowing; Wherever it is used, *epistemic* traces back to the knowledge of the Greeks; It comes from *epistēmē*, Greek for "knowledge." That Greek word is from the verb *epistanai*, meaning "to know or understand," a word formed from the prefix *epi-* (meaning "upon" or "attached to") and *histanai* (meaning "to cause to stand")”

Are PRA models cause or the solution to uncertainties?



- What are the contributors to aleatory uncertainty?
- How do the PRA models enable NRC address aleatory uncertainties?
- Do the PRA practitioners introduce epistemic uncertainties during the modeling process ?
- Does NRC have appropriate processes appropriately consider epistemic uncertainties introduced during the modeling process in risk-informed decisionmaking?



"All models are wrong, but some are useful… Fortunately to be useful, a model does not have to be perfect."

- George E. P. Box
- University of Wisconsin
- (1919-2013)

Risk-Informed Regulatory Processes

Description of the regulatory process	Key Characteristics that could influence the rigor required to manage uncertainty.
Improve the design of a nuclear plant using PRA insights	Use insights from PRAs to identify and eliminate potential risk outliers and improve the design.
Review acceptability of a permanent change to the licensing basis (e.g., change to design, accident analysis, technical specifications)	If approved, change will be permanent.
Review acceptability of a temporary change (weeks, months) to the licensing basis (e.g., changes to design, accident analysis, technical specifications)	If approved, change will be temporary.
Determine appropriate regulatory actions that must be taken based on an emerging issue with limited data which requires timely regulatory actions	Regulator chooses prompt or longer-term actions that must be taken to ensure public health and safety based on the risk significance of the issue.
Determine whether the licensee may operate outside of approved technical specifications for a few hours or days	If approved, the licensee will be allowed to operate for a few days or hours while outside of conditions imposed by technical specifications.
Determine the risk significance assigned to a performance deficiency that will be corrected.	The regulatory decision has the potential have a significant impact on the follow-up resources required by both the regulator and licensee and affects licensee's reputational risk.
Determine the magnitude of inspection resources that must be expended to follow-up an event or a degraded condition at a nuclear plant.	The regulatory decision has the potential have a significant impact on the follow-up resources required by both the regulator and licensee and on enterprise risk.

Managing Uncertainty: The Role of Safety Margins and Performance Monitoring

Purpose & Relevant Guidance	Remarks
Improve the design a nuclear plant using PRA insights {AEA SSG-3, SRP 19.0 (ML#15089A068), RG NEI 18-04 (ML#19241A472)\RG 1.233 (ML#20091L698)}	These documents provide guidance on how defense-in-depth, safety margins, and safety analyses must be considered in designing commercial nuclear plants and discusses, in some situations, how reliability of non-safety related risk significant systems must be monitored
Review acceptability of a permanent change to the licensing basis (e.g., changes to design, procedures, technical specifications) {(RG 1.174 (ML#20164A034), RG 1.77 (ML#17317A256), NUREG-1855 (ML#20164A034))}	Section C.2.5 of RG 1.174 (~4 pages) discusses in detail how uncertainties must be considered and documented by the licensee to address all three components of epistemic uncertainties and refers to NUREG-1855 Rev. 1 for additional guidance.
Review acceptability of a permanent change to the licensing basis (e.g., changes to design, accident analysis, technical specifications) (RG 1.174, NUREG-1855)	Section C.2.5 of RG 1.174 (~4 pages) discusses in detail how uncertainties must be considered and documented by the licensee to address all three components of epistemic uncertainties and refer to NUREG-1855 Rev. 1 for additional guidance.

Managing Uncertainty: The Role of Safety Margins and Performance Monitoring

Purpose & Relevant Guidance	Remarks
Determine appropriate regulatory actions that must be taken based on an emerging issue with limited data which requires timely regulatory actions (LIC-504, ML#19253D401).	LIC-504 requires consideration of "facility-wide safety margin" and defense-in-depth. Section 4.1 of LIC 504 provides guidance on treatment of uncertainty. Since issues reviewed under LIC-504 are "emerging," there is usually limited information available to perform risk analysis. Therefore, normally, there is a relatively high reliance on performance measurement strategies that can be used to re-visit regulatory decisions.
Determine whether the licensing may operate outside of approved technical specifications for a few hours or days (Appendix F, "Notices of Enforcement Discretion," to NRC ML#19193A023)	Regional senior reactor analysts and NRR risk analysts in collaborations with NRC subject matter experts consider defense-in-depth and safety margins and uncertainties during the review process.
Determine the magnitude of inspection resources that must be expended to follow-up an event or a degraded condition at a nuclear plant (IMC0309, ML#111801157)	Regional senior reactor analysts and NRR risk analysts in collaborations with NRC subject matter experts consider defense-in-depth and safety margins and uncertainties during the review process.
Determines the risk significance that must be assigned to a performance deficiency that will be corrected. (IMC 0308 Attachment 3, ML#21271A120)	Section 0308-03-07 of IMC 308 discusses how uncertainties must be treated. Significant efforts are expended by senior reactor analysts and NRR risk analysts to perform sensitivity analyses and uncertainty analyses if necessary to make informed judgements, and present results NRC's decisionmakers.

Matt Forsbacka

Director of Mission Assurance Standards and Capabilities Division
Office of Safety and Mission Assurance
National Aeronautics and Space Administration

10:40 AM Session

Managing Uncertainty: The Role of Safter Margins and Performance Monitoring

NRC's 2023 Risk Forum

Managing Uncertainty: The Role of Safety Margins and Performance Monitoring

NRC's 2023 Fall Risk Forum

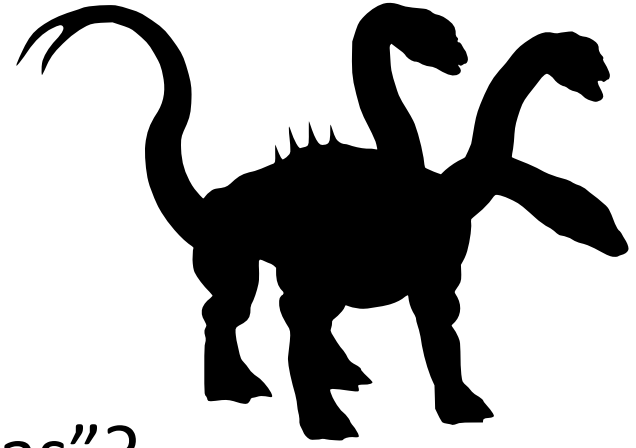
Fernando Ferrante
Program Manager,
Risk & Safety Management

EPRI
September 12, 2023

Conservatism, Margins, Uncertainties and other Creatures

What do we mean when we say…

- "Conservatism"?
- "Margins"?
- "Uncertainty"?
- "Defense-in-Depth"?
- "Realism"?
- "Best Estimate"?, "Reasonable"?, "Bias"?…



More importantly, in what context are we saying it?

- "What is the level of conservatism in your analysis?"
- "Do we have appropriate/sufficient safety margin?"
- "How were the uncertainties addressed in the model?"
- "Was there an impact to the level of defense-in-depth?"

These Words Matter…

"The program was operating too close to too many ***margins***"
— Report on *Columbia Shuttle Disaster*

"…***margins*** need to be sufficiently large to address… high level of ***uncertainty***…"

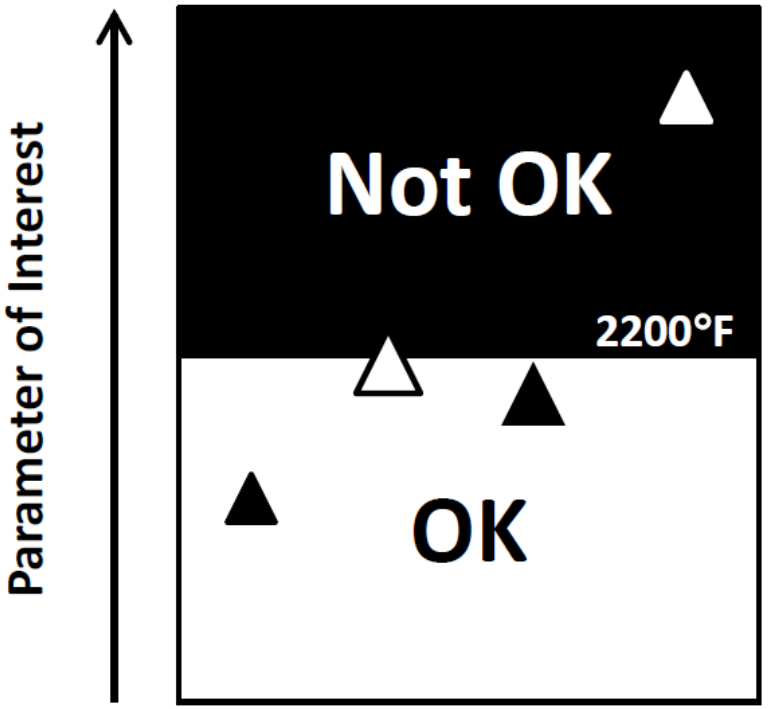
"…failure to provide sufficient means of protection at each level of ***DID***"

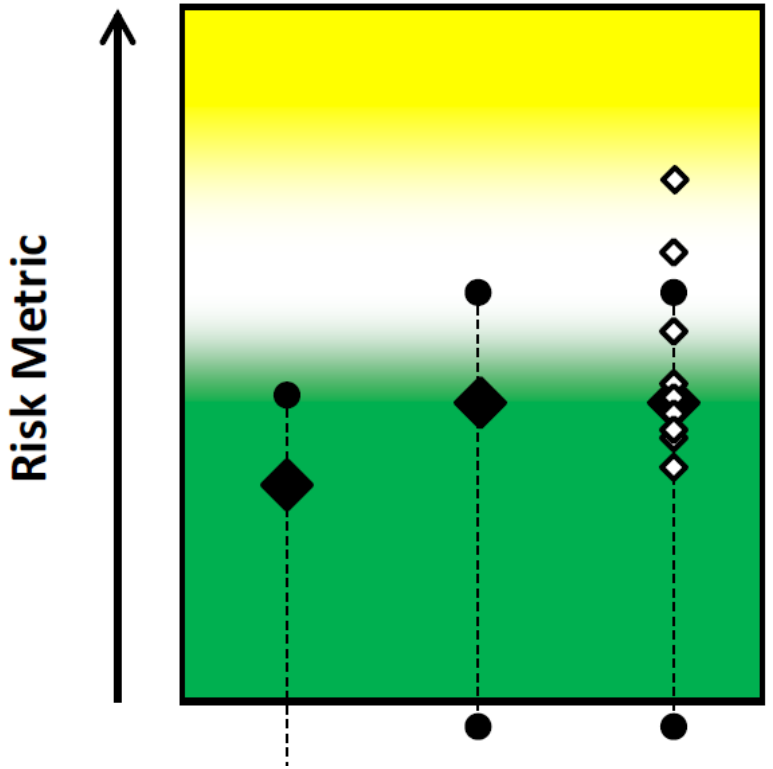
"…site did not know how the accident would progress… significant ***uncertainty***…"
— *Fukushima Daiichi* Accident Report by the IAEA

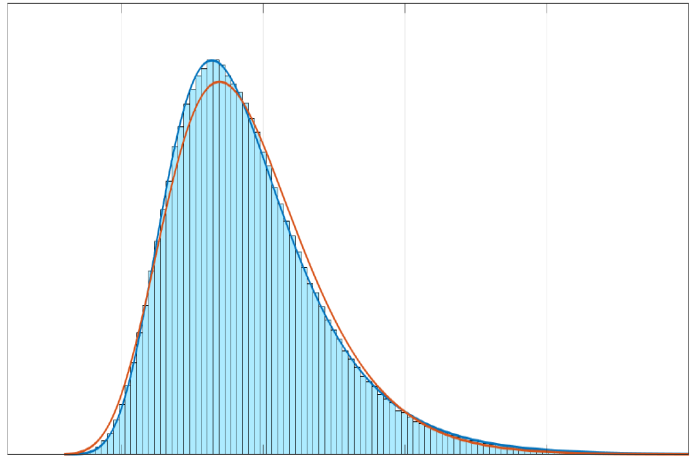
"It's not just as ***conservative*** as would have been the norm in the old Boeing" — Former *Boeing* flight-controls engineer

A word about Safety Margins and Uncertainty (in general)

Need to be careful when mixing deterministic/probabilistic "Margin"



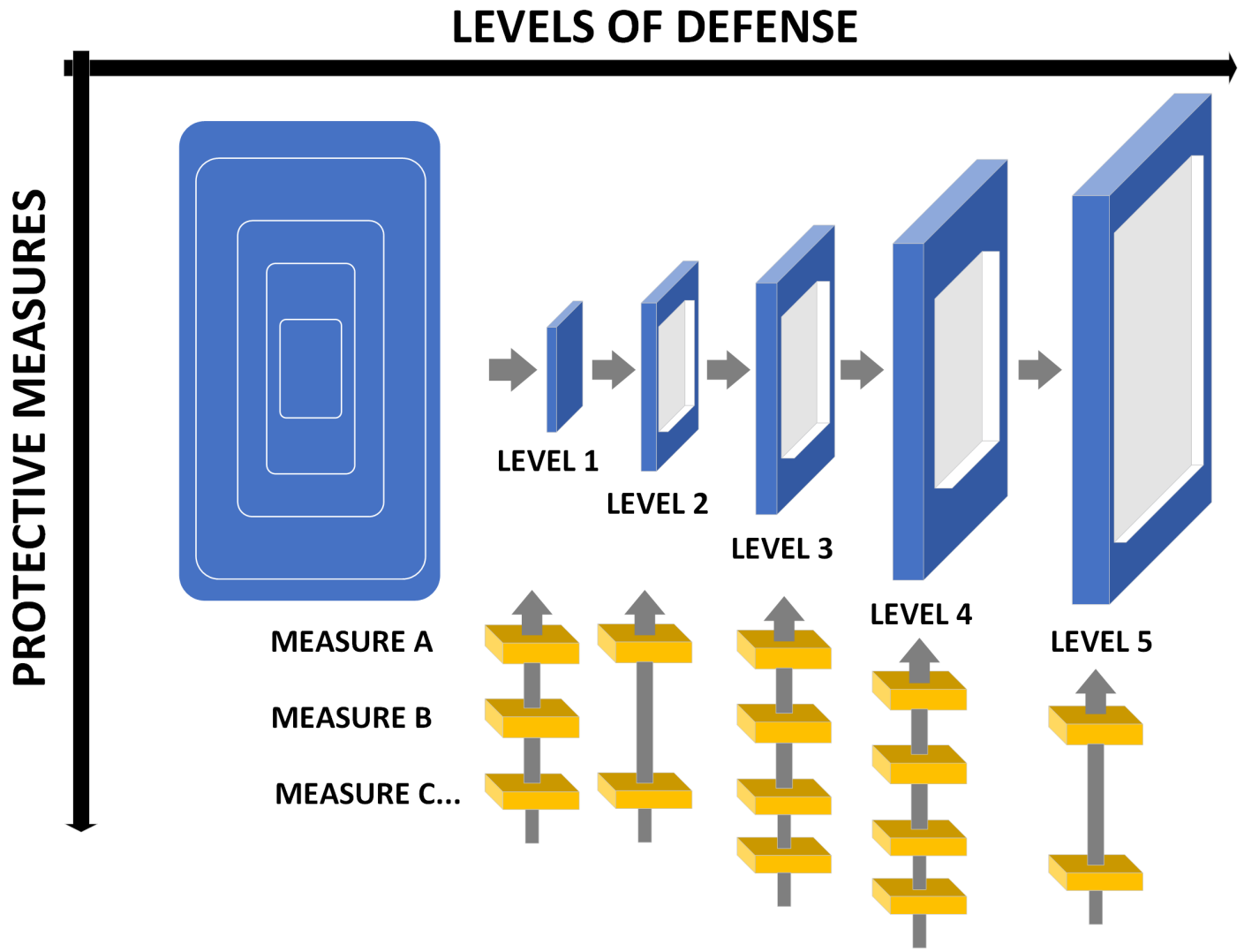




Too often, "Uncertainty" is viewed as a quantification exercise

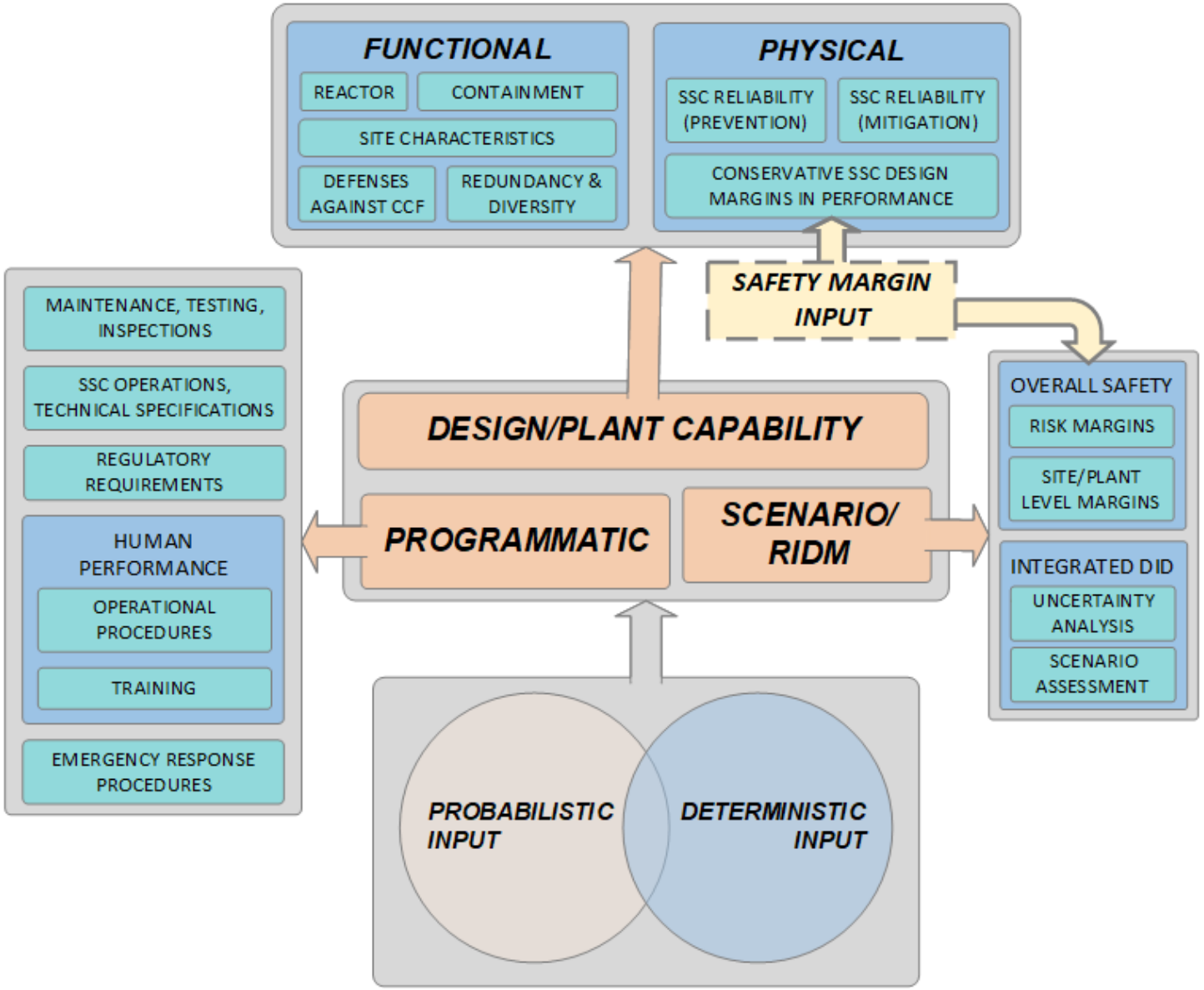
Reframing Defense-in-Depth (DID)/Safety Margin (SM)

EPRI 3002020763 Consideration of DID and SM in RIDM: Practical Guidance



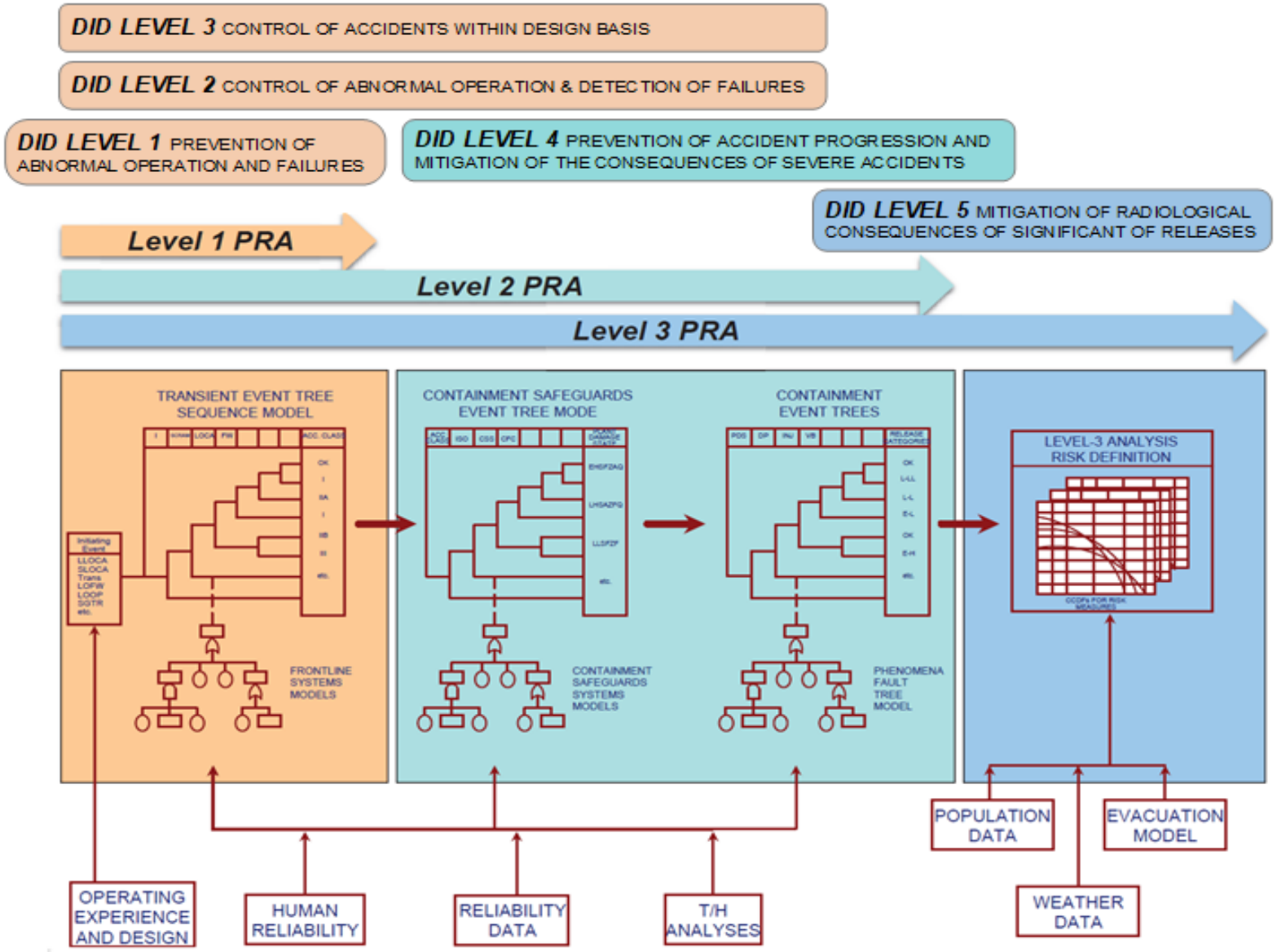
- Solution MUST include BOTH deterministic and probabilistic inputs
- Suggested approach is to include aspects from
  - DESIGN DID
  - PROGRAMMATIC DID
  - SCENARIO DID
- Consider SM as DID input
  - Localized SM impacts
  - Globalized DID impacts
- Integrate risk in DID/SM

Reframing Defense-in-Depth (DID)/Safety Margin (SM)



- Redefined framework for DID and SM built upon recent efforts for Advanced Reactor Design Licensing
- Goal is to bring together DESIGN DID, PROGRAMMATIC DID, SCENARIO DID
- But also to place SM in a better context with better guidance
- PRA insights are one input into the overall framework
- Goal is to provide better understanding, justification

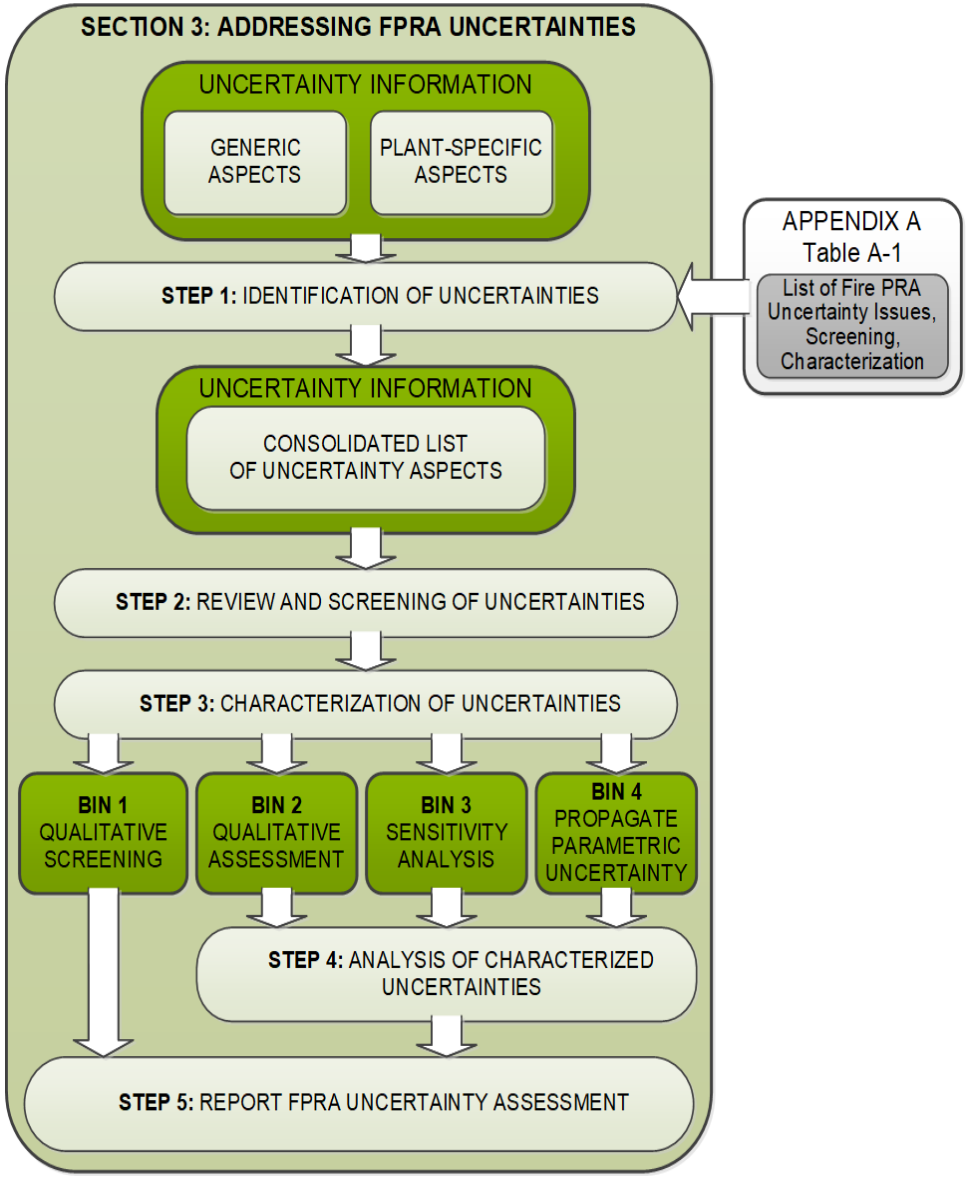
What is the Role of Risk in terms of DID/SM/Uncertainty?



- Several deterministic inputs into DID are inputs for PRA
- Key scenarios considered for DID in licensing of NPPs are part of PRA
- Hence, PRA overlaps significantly with DID and SM
- PRA can explicitly consider what we know and don't know
- But role of PRA is not to "quantify" DID
  - Using PRA to "quantify" DID would be a misuse of PRA
  - But not using PRA insights would also misinform DID

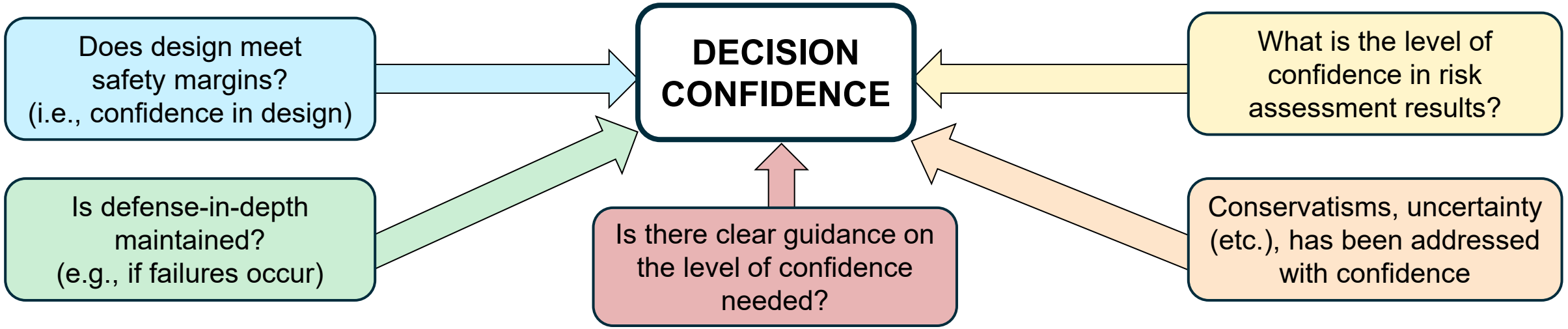
Reframing Fire Uncertainty – EPRI 3002018268

- Simply saying "there is uncertainty, we need to be conservative" is not enough
  - Where is the uncertainty coming from?
  - How can one better understand it?
  - Can something be done about it?
  - Where does it matter (or doesn't)?
- Guidance is detailed, but basic direction is:
  - Use a structured approach
    - Identify, review and screen, characterize, disposition, continue to monitor
    - Relate to margin, DID, within RIDM
- Don't overfocus on quantification for the sake of adding more complexity



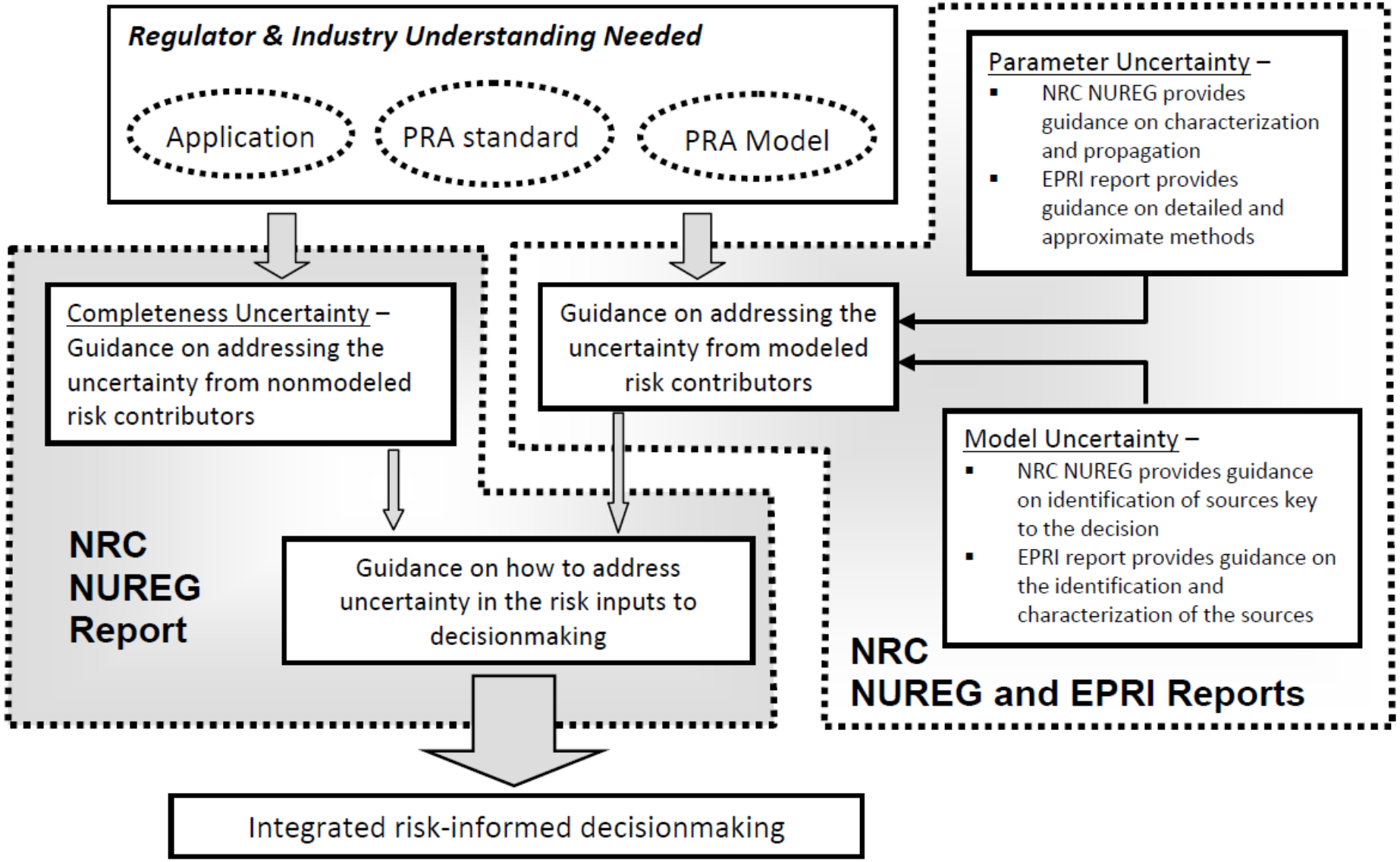
Some additional thoughts, for further discussion/debate

- Risk assessment (like any other engineering tool) will always have conservatisms and simplifying assumptions – need to move on
- "Best estimate", "realism", "bias", "reasonable", … if subjective, not useful
- "Margins", "conservatism", "uncertainty" all speak towards having sufficient confidence in the results, given what we know, regarding a decision:
  - Do we understand factors that could change our decision given available information?
  - If so, do we know what needs to be done in order to gain confidence in the decision?

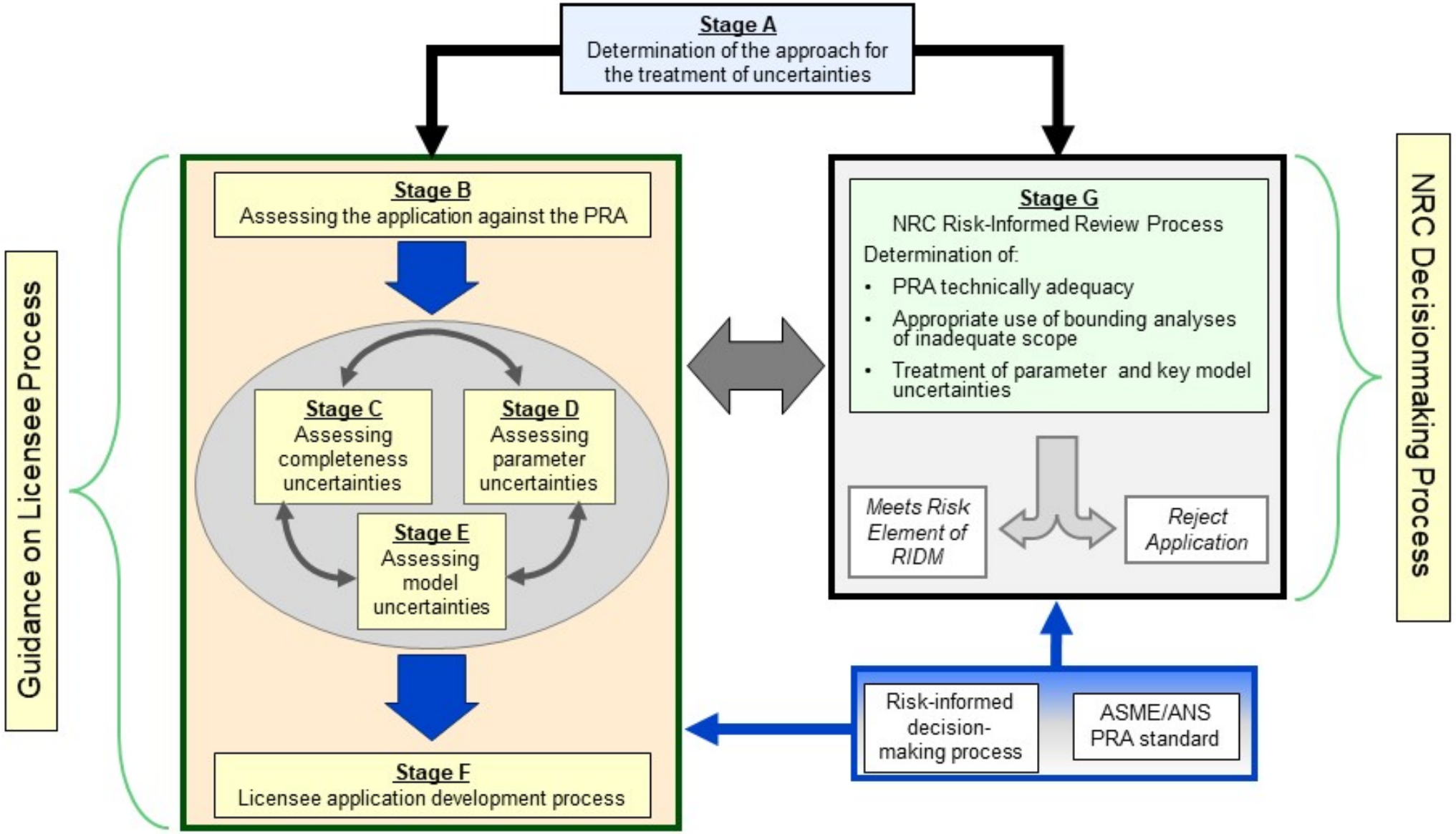


BACKUP SLIDES

Treatment of Uncertainty – NUREG-EPRI Guidance



Treatment of Uncertainty – Structured Approach



Reframing Defense-in-Depth (DID)/Safety Margin (SM)

- EPRI 3002020765 discusses reframed context in multiple areas:


- Internal events


- Internal fire


- Internal flooding


- Seismic Events


- External Flooding


- Multi-unit accidents


- Spent Fuel Pool (SFP)


- Dry Cask Storage


- Digital Instrumentation & Control


- Shutdown Risk


- Periodic Safety Reviews

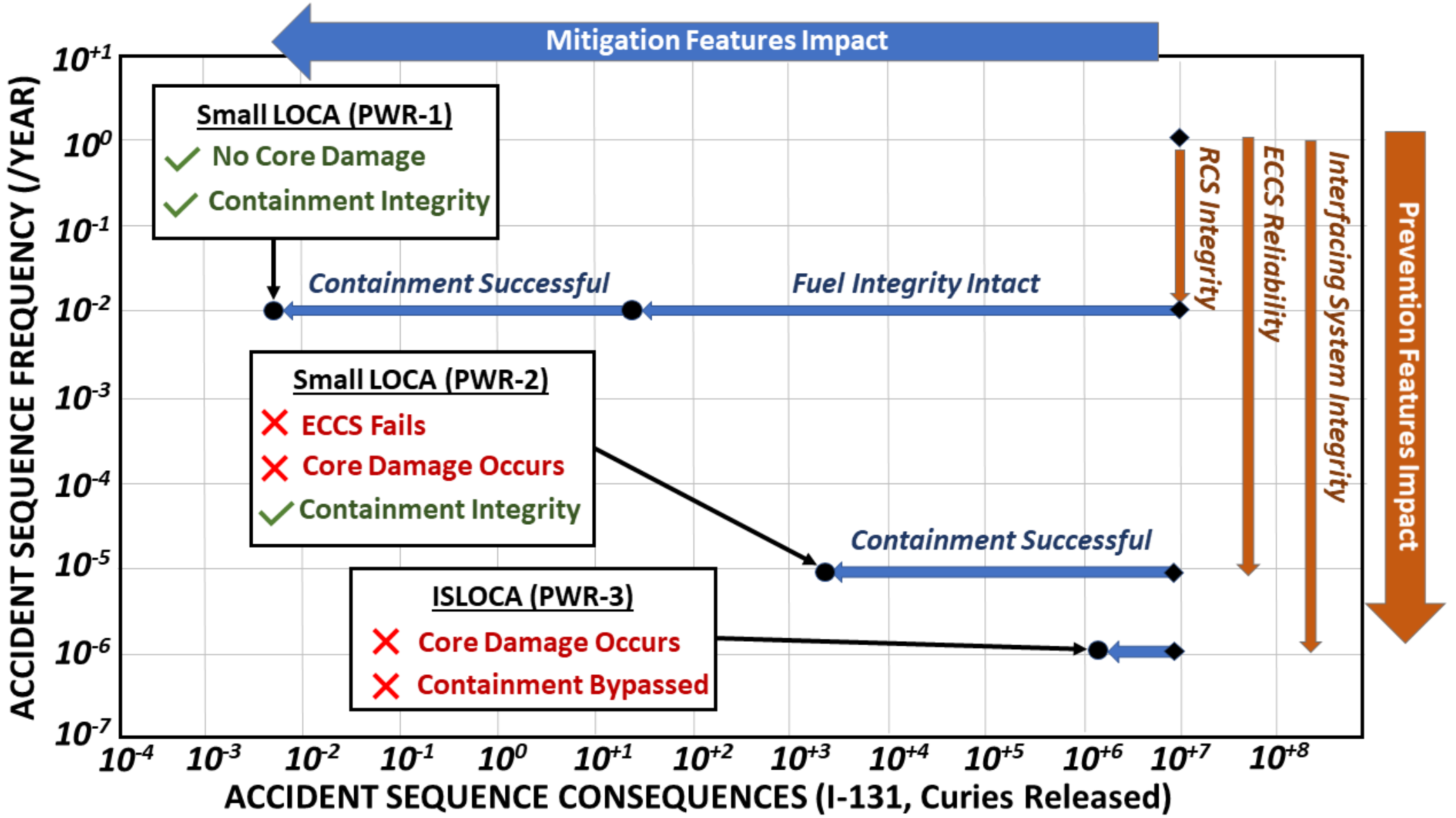

- Physical Security


- Portable Equipment

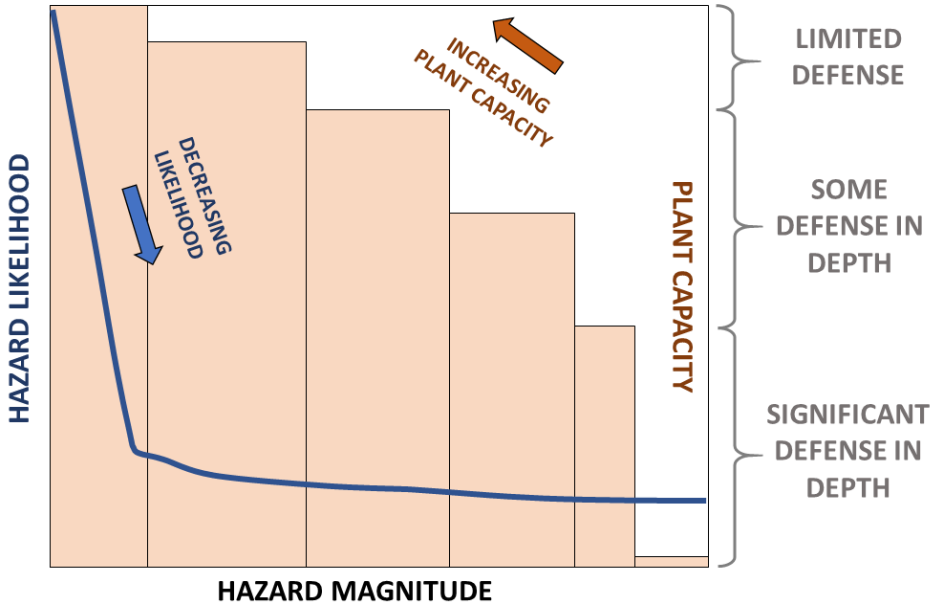

- Risk-Informed Applications

- **Note** that purpose is not how PRA can be used in all these areas, but how DID/SM can be better understood in RIDM (risk insights are leveraged, along with design/programmatic/scenario information)

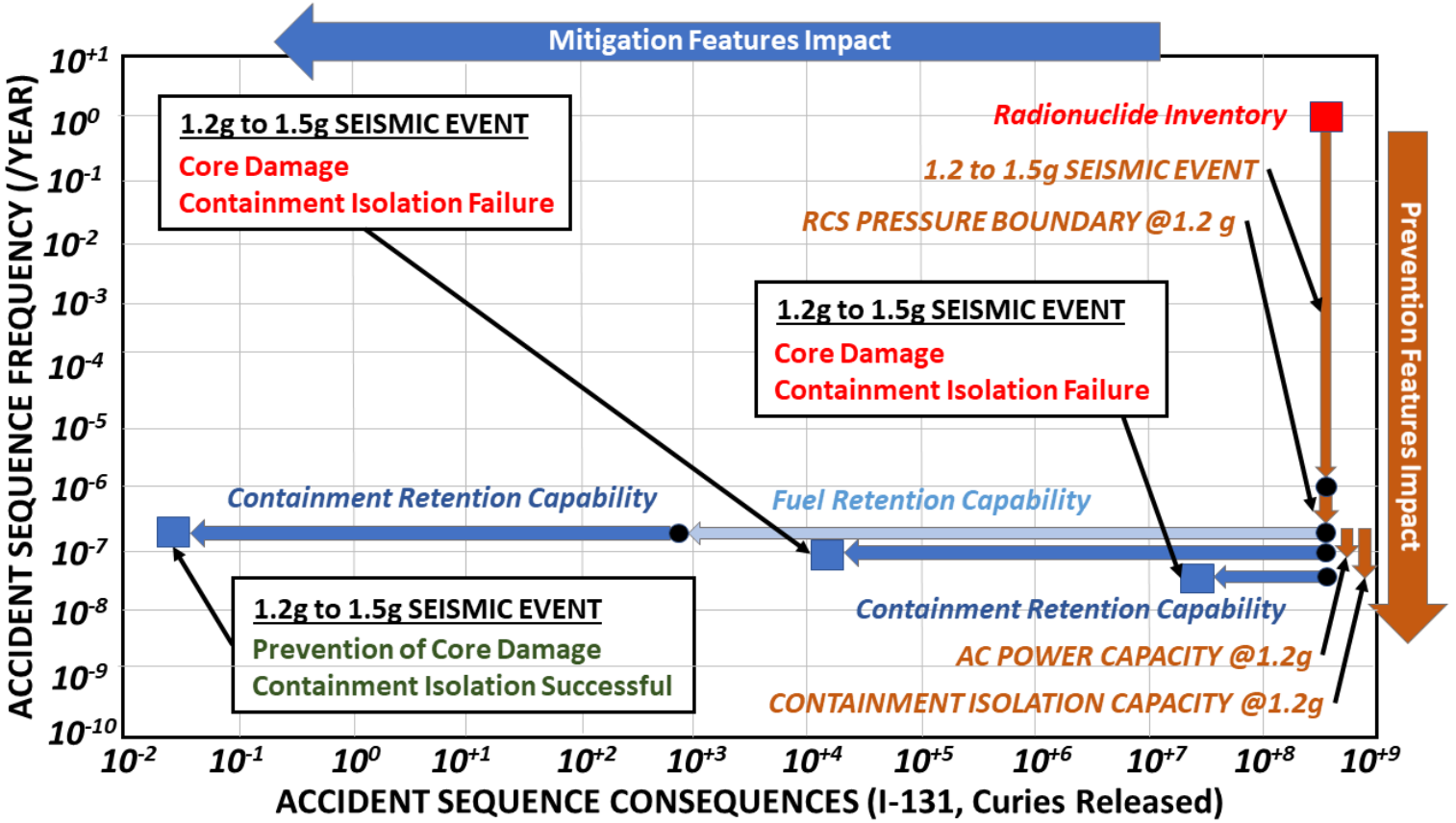
Role of Risk Insights in DID/SM for RIDM Purposes



Role of Risk Insights in DID/SM for RIDM Purposes



- Account for DID/SM in different hazards
- Include consideration of varying DID with scenario-specific inputs into DID/SM



- Risk results can be used as an insight, along with design and programmatic
- Intent is NOT to "measure" DID but to assess effectiveness

Managing Uncertainty: The Role of Safety Margins and Performance Monitoring

Jennifer Varnedoe, Lead Engineer
Duke Energy

DUKE ENERGY®

BUILDING A **SMARTER** ENERGY FUTURE®

The many flavors of uncertainty

- PRA standard requires identification and characterization of model uncertainties
- Parameter Uncertainty
  - State-of-Knowledge
  - Initiating Event frequencies
    - Combining different sources of data (generic experience + plant specific operating events)
  - Component failure probabilities
  - Human error probabilities
  - Calculated probability distributions for the results of the PRA
- Modeling Uncertainty
  - Some component failure affects are unknown
  - Identifying and quantifying operator errors is complex
  - Common cause failures
- Completeness Uncertainty
  - Some phenomena, failure mechanisms or other factors may be omitted due to negligible contribution

Defining “Key” Sources of Uncertainty and Assumptions

- Early 10 CFR 50.69 applications worked through RAIs to gain understanding of “key”
  - RG 1.200 Revision 2
  - NUREG-1855 Rev 1
  - Related references (EPRI 1016737, 1013491, and 1026511)
- Evaluation of generic hazard specific issues from EPRI reports
- Evaluation of Plant-Specific Assumptions and Uncertainties

Compensatory Measures

- Dispositioning “key” sources of uncertainties and assumptions for the application

- Compensatory Measures
  - Application specific sensitivity for each categorization
  - Application specific bounding sensitivity to show no impact to the decision (HSS/LSS)
  - 50.69 sensitivity (e.g. HFE’s to 5th and 95th) addresses the issue
  - 50.69 sensitivity for reliability – addresses unknown impact of relaxing special treatments

Performance Monitoring

- 50.69 Periodic Review
  - Validates reliability sensitivity remains appropriate
  - Validates impacts from alternative treatment on reliability are appropriate
- 805 Performance Monitoring
  - Programmatic – Fire Brigade Response time
  - Equipment – Detection and Suppression System Performance
- Maintenance Rule
  - Reliability and Unavailability
- Risk Informed Completion Times (TSTF-5050)
  - RG 1.177, Revision 1, and RG 1.174, Revision 3, establish the need for an implementation and monitoring program to ensure that extensions to TS CTs do not degrade operational safety over time and that no adverse degradation occurs due to unanticipated degradation or common cause mechanisms
  - Intended to ensure that the impact of the proposed TS change continues to reflect the availability of SSCs impacted by the change
  - Cumulative Risk calculated at least once per cycle (in reality it is calculated in real time as RICTs are used) to ensure change in risk is small

Decision-Making

- Goal of assessing PRA model uncertainty is to establish the level of confidence that can be placed in a decision or conclusion based on a quantitative assessment of risk.

- The treatment of uncertainties can many times consist of recognition of the uncertainties and the acknowledgment that the decisions are made based on the realistic, best-estimate values from the probabilistic models coupled with margin designed into the acceptance guidelines and with the defense-in-depth deterministic inputs.

Changes to the Plant

- A wide variety of types of applications introduce a wide variety of uncertainties
  - Timing of actions
    - Differences in empirical vs academic approaches
      - How long could it really take to fix a component?
    - Simulator runs vs procedure reviews; Engineering vs Operations
  - Impacts of changes that are not directly represented in the PRA model
    - 50.69 Opportunities - These do not always increase risk!
      - Using different code requirements or materials
      - Using different NDE techniques
      - Differing maintenance strategies
      - Buying industrial components
- Recall these applications introduce small changes with very small changes in overall plant risk

All the other controls…

- The layers of programmatic oversight for component / system performance and changes to the plant are significant
  - Design control (design, fabrication, testing)
  - Supply Chain control (documentation, receipt, etc.)
  - 10 CFR 50.59 requirements
  - Safety Analysis
  - Testing and Maintenance
    - Tech Spec driven surveillances
    - Preventive Maintenance that prevents “Run-to-Failure”
    - Code Driven Testing (In-Service Testing, In-Service Inspection)
    - License Renewal for Aging affects
    - Raw Water Program
    - Buried Pipe Program
    - Flow Accelerated Corrosion
    - And the list goes on and on…

Conclusion

- Risk-informed, not risk-based, decision making
  - Small uncertainties in tiny numbers have small impacts on risk margin
- The decision is integrated…not based solely on a number
- An application may change one part of how we operate the plant, but we must consider all of the other requirements that remain unchanged.

Uncertainties addressed via reasonable compensatory actions and performance monitoring

Coupled with a robust problem identification and resolution program

Provide a reasonable way to utilize risk-insights to optimize resources.

*BUILDING A **SMARTER** ENERGY FUTURE ®*

Developing and Maintaining Risk-Informed Decision Making as Part of Your Organizational Culture

1:00 PM Session

NRC's 2023 Risk Forum

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- Mirela Gavrilas, NRC Director of the Office of Nuclear Security and Incident Response
- Cheryl Gayheart, Director of Risk Informed Engineering & Safety Analysis at Southern Nuclear
- Homayoon Dezfuli, NASA Technical Fellow for System Safety
- Mark Steinbicker, Acting Director of the Office of Safety Standards, Flight Standards Service at FAA

- NRC Facilitator: Brett Klukan, Regional Council, Region I-Office of the Regional Administrator

ANSI/ANS-30.3-2022, *Light Water Reactor Risk-Informed, Performance-Based Design*

N. Prasad Kadambi (Risk-informed, Performance-based Principles and Policy Committee Chair) and Kent B. Welter (ANS-30.3 Working Group Chair)

NRC Risk Forum – September 12, 2023

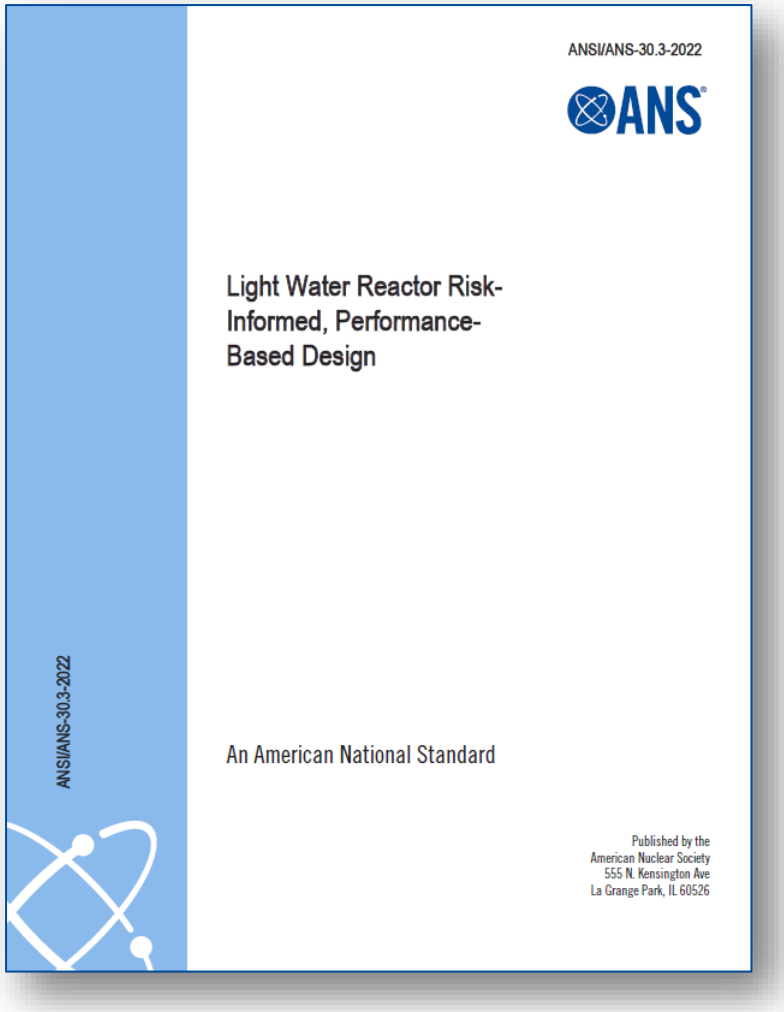
ANS®
American Nuclear Society

Outline

- What is ANS-30.3?
- How does ANS-30.3 address risk-informed decision-making?
- How does ANS-30.3 address risk-informing licensing basis events?
- What significance does ANS-30.3 have for ANS and other voluntary consensus standards?

What is ANS-30.3?

- Establishes a minimum set of requirements for the designer to follow in order to appropriately combine deterministic, probabilistic, and performance-based methods during LWR design development.
- A distinction is made between the safety design of a reactor product and the overall set of design activities that necessarily includes economic, environmental, and other considerations.
- A further distinction is made between the processes associated with safety design and licensing of the product, but the standard does not cover all the licensing matters that may arise.



ANS

What is ANS 30.3? (Continued)

- **<u>Requirement</u> to establish a formal decision analysis process**.
  - Without a formal RIPB decision analysis process, decisions made over the evolution of a design may become ambiguous, conflicting, or inefficient.
- **<u>Requirement</u> to employ requirements management** for establishing requirements, evaluate options, identify acceptable options, and track integration of requirements into the reactor product.
- Describes a decision-making structure within which requirements associated with the processes described meet specified acceptance criteria and thereby achieve the standard's outcome objectives in a formal way.
  - A substantial part of the value of ANS-30.3 as a voluntary consensus standard is on account of this formal decision-making structure.

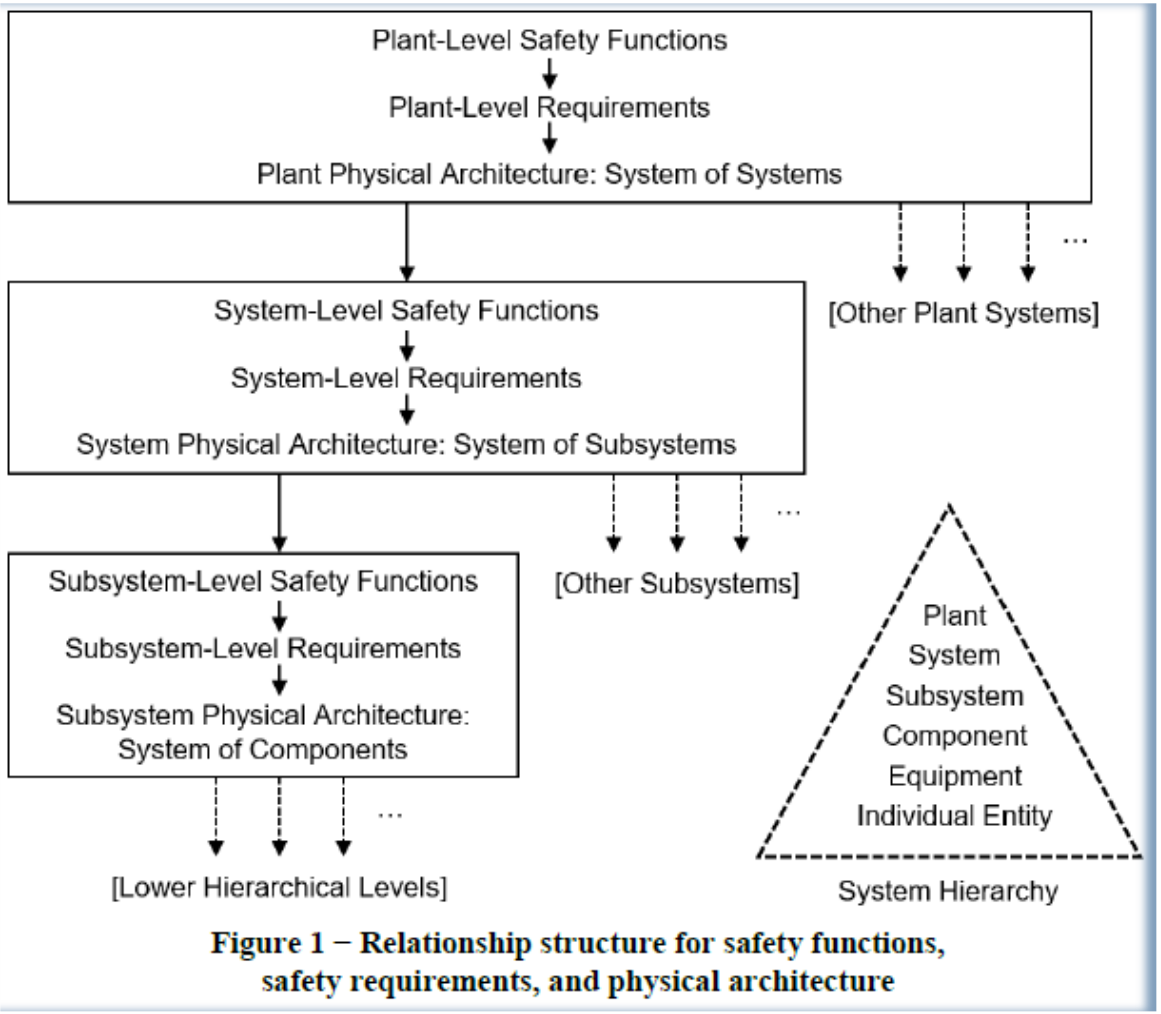


Figure 1 – Relationship structure for safety functions, safety requirements, and physical architecture

How does ANS-30.3 address risk-informed decision-making (RIDM)?

- Although not explicitly called out in ANS-30.3, it is implicit to the particular topics offered in the standard that a framework exists within which design and licensing can proceed efficiently to accomplish overall objectives for the reactor product.
  - The framework needs to incorporate the necessary and sufficient needs of the design and licensing aspects for gaining regulatory approval.
  - The decision-making structures associated with design and licensing necessarily overlap to a considerable extent.

- Framework as applied here is taken to mean one or more decision-making structures. A decision-making structure may be considered as a “scaffolding” that holds together various processes within a logical architecture that expresses relationships and dependencies among the various elements.

- ***The RIDM aspect of ANS-30.3 is embedded and nested within the iterative and recursive processes provided in the standard.***

How does ANS-30.3 address RIDM? (Continued)

- ANS-30.3 takes its cue from the Nuclear Energy Innovation and Modernization Act (NEIMA) and the defined attributes of a technology-inclusive regulatory framework as evidenced by the following:

  > "Technology-inclusive regulatory framework—The term "technology-inclusive regulatory framework" means a regulatory framework developed using methods of evaluation that are flexible and practicable for application to a variety of reactor technologies, including, where appropriate, the use of risk-informed and performance-based techniques and other tools and methods."

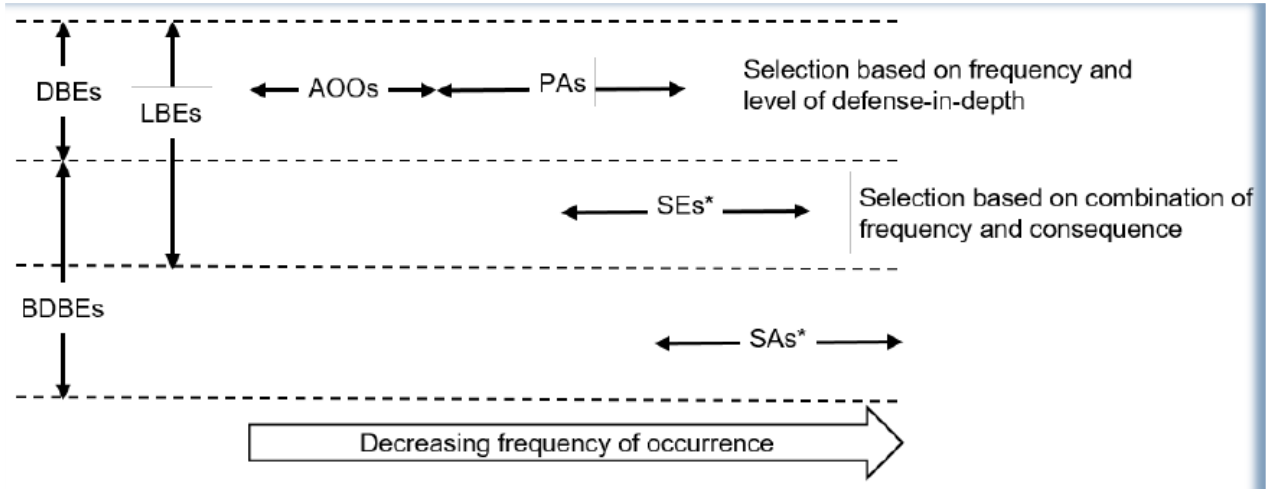
- NEIMA focuses on NRC and regulation, but ANS-30.3 focuses on the LWR design process.

How does ANS-30.3 address risk-informing LBEs?

- The starting point for the user of ANS-30.3 is expected to be a well-defined set of outcome objectives which necessarily need to be supported by technically defensible LBEs.
- These outcome objectives are accomplished by using this standard taking into account the needs of reactor safety and licensing of the reactor.
- The outcome objectives, which would be explicitly called out in the framework discussed above, provide the context for specific performance objectives associated with a specific LWR design.

How does ANS-30.3 address risk-informing LBEs? (Cont'd)

- A designer using ANS-30.3 is expected to use accepted engineering practices to specify the limiting conditions associated with scenarios that impose design basis challenges on affected systems.
  - Such scenarios are generally defined by plant responses to postulated initiating events including coincident equipment failures and malfunctions that could challenge plant safety.
- In this context, "requirements management," as part of a set of systems engineering best-practices, involves identifying and specifying such events with a formality that enables discussions regarding LBEs in relation to regulatory needs.
- ANS-30.3 provides for a range of options that a designer may invoke given current U.S. regulatory practices in which combinations occur of conventional, risk-informed, and performance-based requirements.
  - Specified under the definitions that the Commission provided in SRM-SECY-98-144.
- Given that the development of ANS-30.3 was motivated and significantly resourced by the successful deployment of an LWR SMR, the applicability is specifically focused on LWR technology.
- ***A key outcome objective for ANS-30.3 is achievement of a successful design and not just success at licensing.***



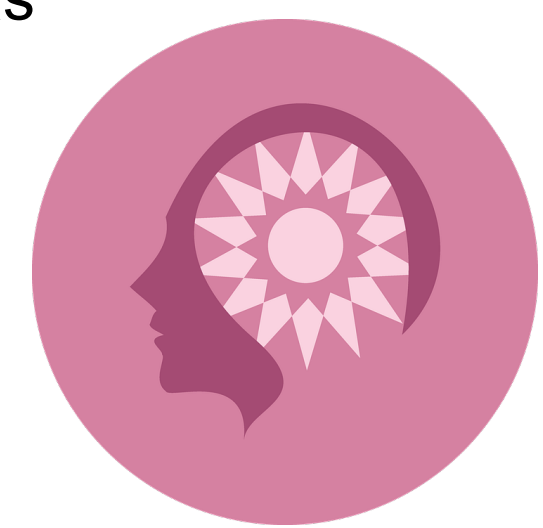
AOO: anticipated operational occurrence
BDBE: beyond-design-basis event
DBE: design-basis event
LBE: licensing-basis event
PA: postulated accident
SE: special event
SA: severe accident

*NOTE: NRC guidance necessitates specification of a core damage event for design-basis dose evaluations. These are often called special events (See Sec. 6.4).

Figure 2 – Selection of LBEs

Significance of ANS-30.3 for ANS and other voluntary consensus standards?

- ANS-30.3 is a transitional, voluntary consensus standard that bridges the gap between design practices that have provided the solid basis for demonstrating the viability of LWRs as a well-known technology.
- ANS views ANS-30.1*, 30.2, and 30.3 as being a suite of interrelated standards which can help make progress on efforts such as the North American Advanced Reactor Roadmap.
- Additionally, ANS sees opportunities for working with ASME on standards such as Section III, Division 5, and Section XI, Division 2.



*ANS-30.1 is now being prepared as an ANS guidance standard, **not** as an ANSI consensus standard.

Enabling the Use of Industry's Licensing Modernization Project (LMP) Methodology

Marty Stutzke
Senior Technical Advisor for PRA
Division of Advanced Reactors and Non-Power Production and Utilization Facilities
Office of Nuclear Reactor Regulation

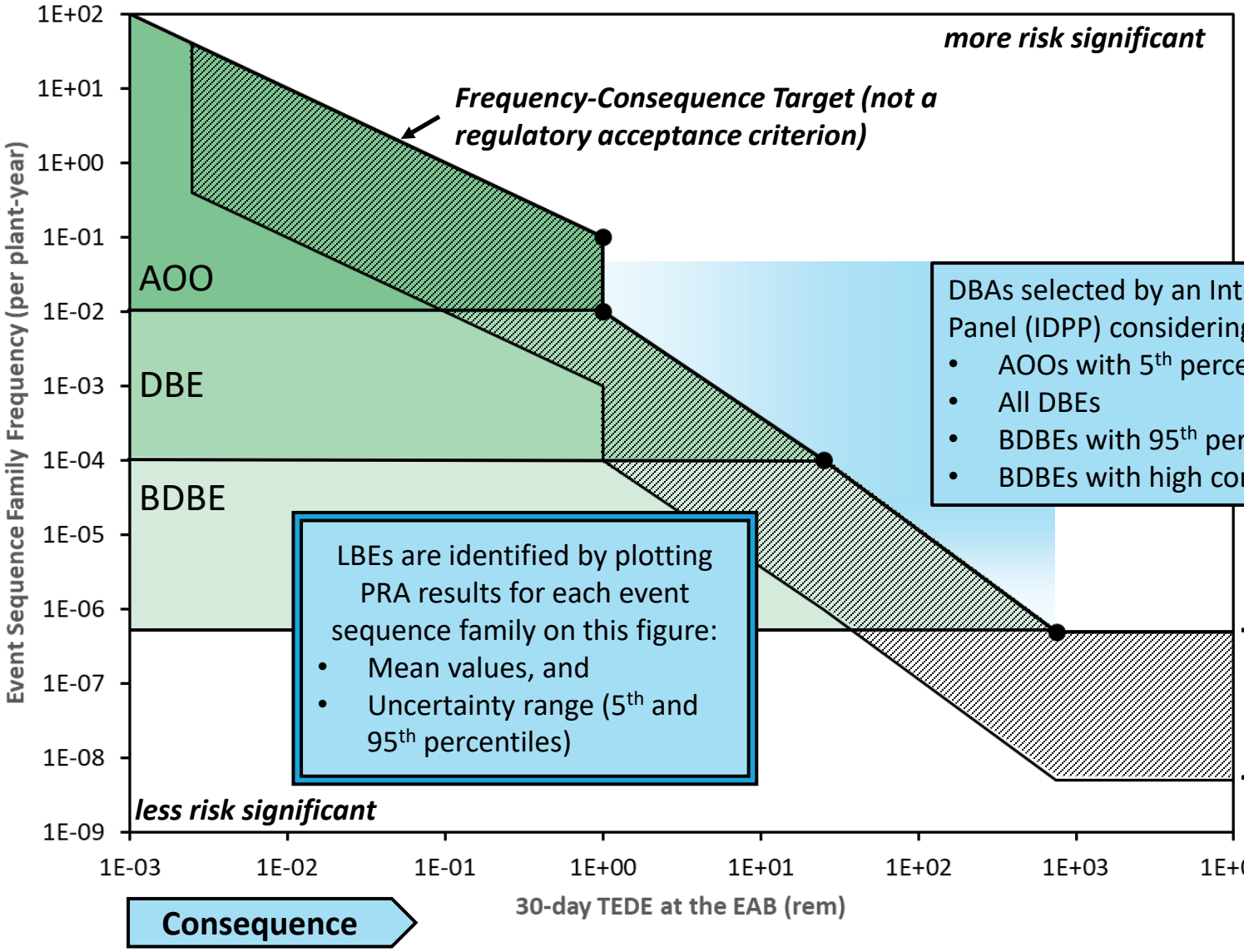
NRC Fall Risk Forum
September 12, 2023

Industry's Licensing Modernization Project (LMP)

The idea: Use the PRA up-front to help define the licensing basis, rather than after-the-fact to confirm the acceptability of a design that has been developed using the traditional, deterministic approach.

- Origins
  - Original concepts developed in late 1980s for the modular high-temperature gas-cooled reactor (MHTGR) (Ref. 1)
  - NUREG-1860, December 2007 (Ref. 2)
  - Next Generation Nuclear Plant (NGNP) Licensing Strategy, 2006-2013 (Ref. 3)
- Industry initiative (beginning in 2017):
  - Lead by Southern Company
  - Cost-shared with Department of Energy (DOE)
  - Coordinated with Nuclear Energy Institute (NEI)
- Scope
  - Licensing basis event (LBE) selection
  - System, structure, and component (SSC) safety classification
  - Defense-in-depth evaluation
- Methodology and Endorsement
  - NEI 18-04, Rev. 1, August 2019 (Ref. 4)
  - SECY-19-0117, December 2, 2019 (Ref. 5)
  - SRM-SECY-19-0117, May 26, 2020 (Ref. 6)
  - RG 1.233, June 2020 (Ref. 7)
- Applicability
  - Non-light-water reactors
  - Part 50 construction permit (CP) and operating license (OL) applications
  - Part 52 standard design certification (DC), standard design approval (SDA), manufacturing license (ML), and combined license (COL) applications

LMP Methodology: Licensing Basis Event Selection



LBEs selected according to event sequence frequency (not initiating event frequency)

DBAs selected by an Integrated Decision-Making Process Panel (IDPP) considering:

- AOOs with 5th percentile frequency < 1E-2/plant-year
- All DBEs
- BDBEs with 95th percentile frequency > 1E-4/plant-year
- BDBEs with high consequences (> 25 rem)

LBEs are identified by plotting PRA results for each event sequence family on this figure:

- Mean values, and
- Uncertainty range (5th and 95th percentiles)

Use of absolute (not relative) risk significance to identify risk-significant LBEs

LMP Implementation Guidance

Clean sheet approach!

Industry's Technology-Inclusive Content of Application (TICAP): NEI 21-07, Rev. 1

1. General Plant Information, Site Description, and Overview
2. Methodologies and Analyses and Site Information
3. Licensing Basis Event (LBE) Analysis
4. Integrated Evaluations
5. Safety Functions, Design Criteria, and SSC Safety Classification
6. Safety Related SSC Criteria and Capabilities
7. Non-safety related with special treatment SSC Criteria and Capabilities
8. Plant Programs

Applies to:

- Non-LWRs
- Part 50 CP and OL applications
- Part 52 DC and COL applications

NRC's TICAP Endorsement
DG-1404, Rev. 1 (proposed new RG 1.253)

ARCAP Roadmap: DANU-ISG-001

Additional SAR Content Outside the Scope of TICAP

2. Site Information: DANU-ISG-002
9. Control of Routine Plant Radioactive Effluents, Plant Contamination, and Solid Waste: DANU-ISG-2022
10. Control of Occupational Doses: DANU-ISG-2022-004
11. Organization and Human-System Considerations: DANU-ISG-2022-005
12. Post-construction Inspection, Testing and Analysis Programs: DANU-ISG-2022-006

Additional ARCAP Guidance

- Risk-informed Inservice Inspection and Inservice Testing: DANU-ISG-007
- Risk-informed Technical Specifications: DANU-ISG-008
- Fire Protection for Operations: DANU-ISG-009

NRC's Advanced Reactor Content of Application (ARCAP) Project

Additional contents of application may exist only in the SAR, may be in a separate document incorporated into the SAR, or may exist only outside the SAR.

Acronyms and Initialisms

AOO	anticipated operational occurrence
ARCAP	Advanced Reactor Content of Application
BDBE	beyond design basis event
DBA	design basis accident
DBE	design basis event
DOE	Department of Energy
LBE	licensing basis event
LMP	Licensing Modernization Project
MHTGR	modular high temperature gas-cooled reactor
NEI	Nuclear Energy Institute
Non-LWR	non-light-water reactor
PRA	probabilistic risk assessment
SSC	systems, structures, and components
TICAP	Technology-Inclusive Content of Application

References

1. Nuclear Regulatory Commission (NRC), “Draft Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor,” NUREG-1338, March 1989, (Agencywide Documents Access and Management System (ADAMS) Accession No. ML05278049)
2. NRC, NUREG-1860, “Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing,” December 2007.
3. Idaho National Laboratory, INL/EXT-10-19521,“Next Generation Nuclear Plant Licensing Basis Event Selection White Paper,” September 2010. (ML102630246)
4. Nuclear Energy Institute (NEI), NEI 18-04, “Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development,” August 2019.
5. NRC, SECY-19-0117, “Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors,” December 2, 2019.
6. NRC, SRM-SECY-19-0117, “Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors,” May 26, 2020.
7. NRC, RG 1.233, “Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors,” June 2020.

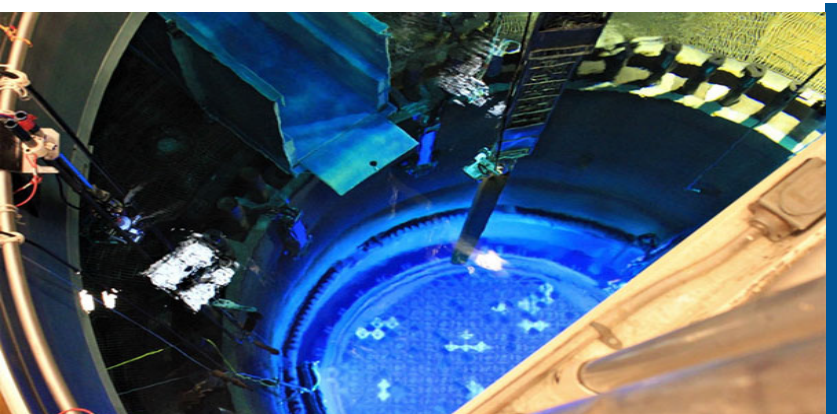
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Risk-Informing Licensing Basis Events for Operating and New Reactors

NRC Fall Risk Forum

September 12, 2023

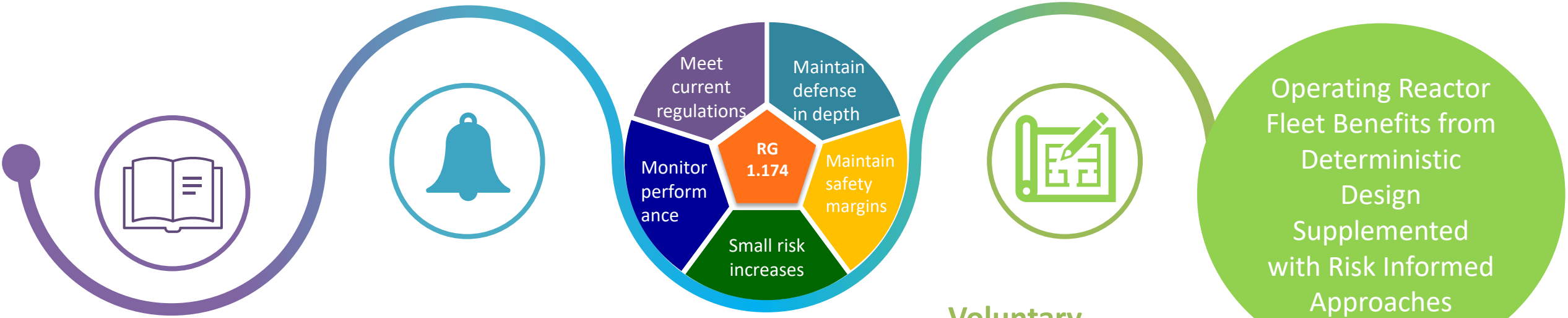
Mihaela Biro
Division of Risk Assessment
Office of Nuclear Reactor Regulation



Licensing Basis Events under Parts 50 and 52

- Design basis events (§ 50.2 definition of safety-related SSCs; § 50.49 specifies four subcategories):
  - Anticipated operational occurrences (AOOs)
  - Design basis accidents (i.e., postulated accidents)
  - External events
  - Natural phenomena
- Non-DBA (§ 50.2, definition of safe shutdown, for Station Blackout (SBO) only)
- Beyond design basis events (BDBEs)
- Anticipated Transients Without Scram (ATWS)
- Station Blackout

Operating Fleet Risk-Informed Journey



10 CFR 50

Plants designed and licensed under 10 CFR 50 are not required to perform PRAs.

Policy Statements and Risk Studies

WASH-1400, 1975

Safety Goal Policy Statement, 1986

PRA Policy Statement, 1985

…

Risk Informed Regulatory Guides

RG 1.174 Risk-informed Changes

RG 1.200 PRA Technical Acceptability

Voluntary Programs

NFPA 805 Risk Informed Performance Based Fire Protection

Risk Informed Technical Specifications (TSTF-505 & 425)

50.69 Risk-Informed Categorization and Treatment

Inservice Inspection

Operating Reactor Fleet Benefits from Deterministic Design Supplemented with Risk Informed Approaches

Note: The proposed revision to 10 CFR 50 aligns PRA requirements for 10 CFR 50 with PRA requirements for 10 CFR 52 (SECY 22-0052)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

10 CFR Part 52

Motivation for the Required Use of PRA in Review of Reactor Designs and Licensing

- WASH-1400, "Reactor Safety Study" (1975)
- Three Mile Island Accident (1979)
- Severe Reactor Accidents Regarding Future Designs and Existing Plants (50 FR 32138; August 8, 1985)
- Safety Goals for the Operation of Nuclear Power Plants (51 FR 28044; August 4, 1986, as corrected and republished at 51 FR 30028; August 21, 1986)
- Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities (60 FR 42622; August 16, 1995)
- Regulation of Advanced Nuclear Power Plants (59 FR 35461; July 12, 1994)
- The Policy Statement on the Regulation of Advanced Reactors (73 FR 60612; October 14, 2008)

Plant designs approved (**10 CFR 52.47(a)(27)**) and licensed (**10 CFR 52.47(a)(46)**) under part 52 are required to perform PRAs

for all operating modes in areas for which NRC-endorsed consensus standards exist at the time of the application for the construction permit or combined license (10 CFR 50.71(h) references to 10 CFR 52).

During design and certification stages, PRA is used to **identify/address potential design features** and **operational vulnerabilities** and to **reduce/eliminate** the **significant risk contributors**.

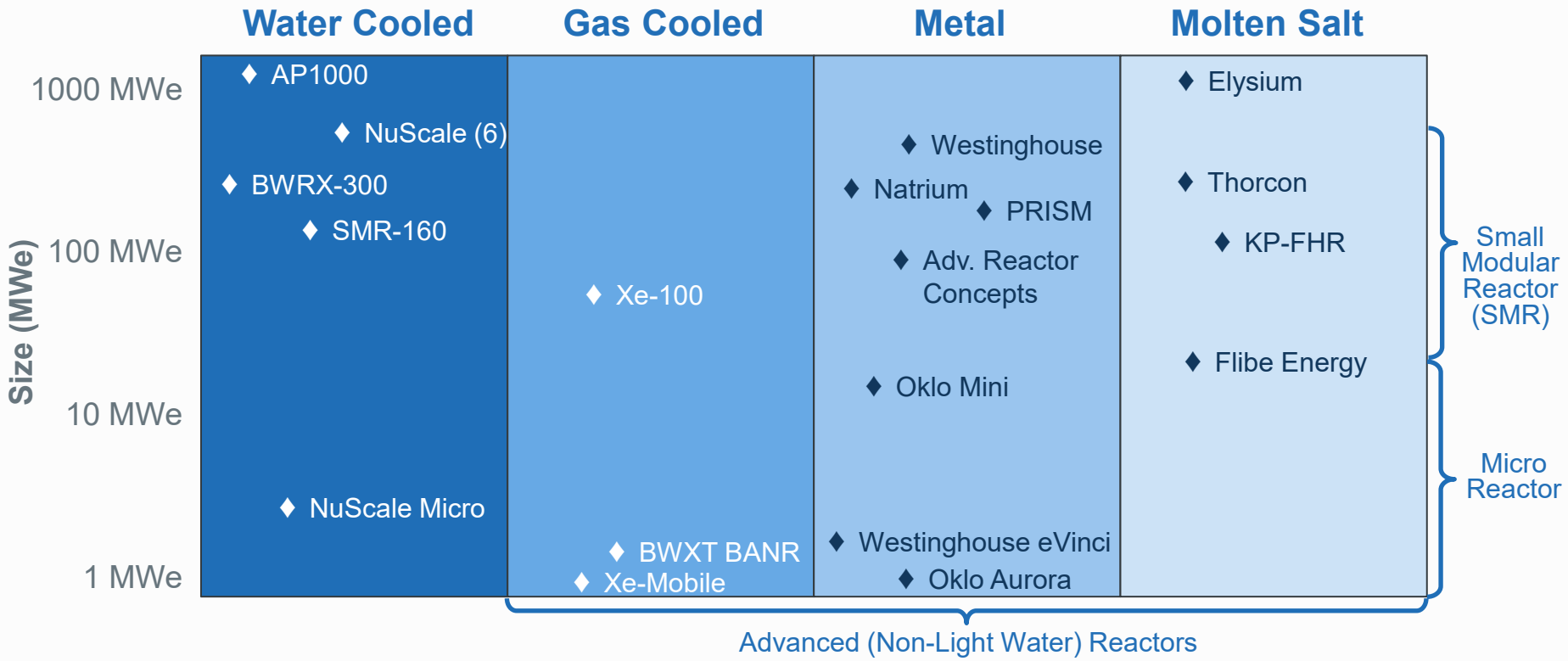
NUCLEAR ENERGY INSTITUTE

Risk-Informed Licensing for New Nuclear Applications: NRC Fall Risk Forum

September 12th, 2023

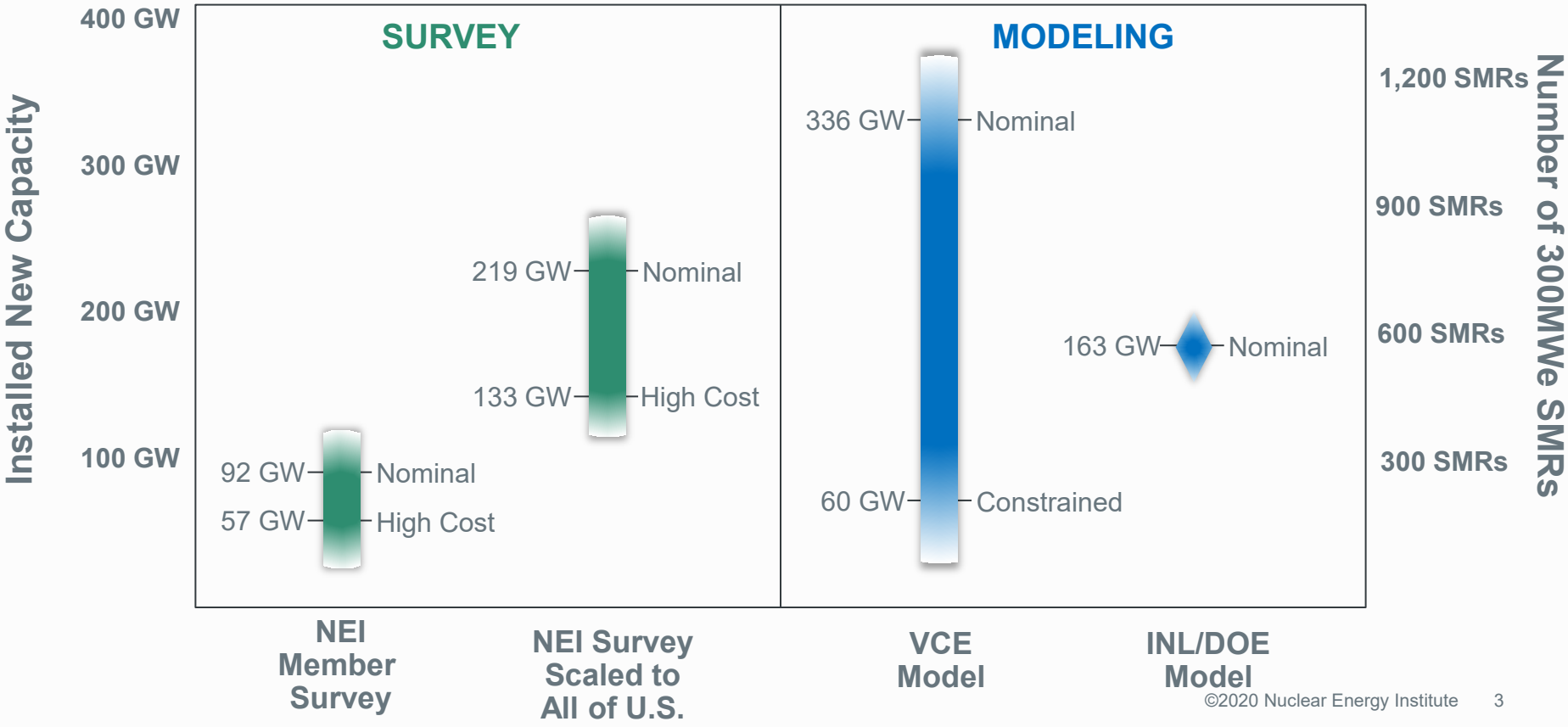
Ben Holtzman
Director, New Nuclear

Advanced Nuclear Technologies*



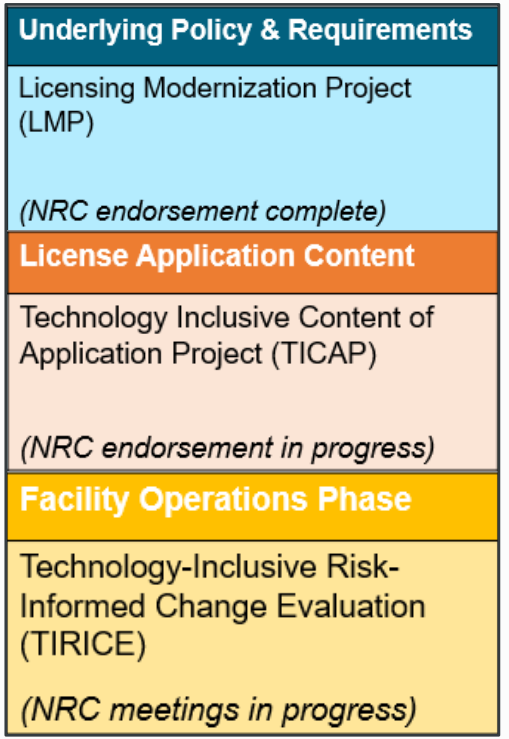
* - partial list of technologies

Triangulating New Nuclear Demand – Grid Only



Risk-Informed Regulatory Efforts

- Problem: existing regulations and guidance designed for large light water reactors
- Solution: risk-inform and modernize the regulatory framework such that it can be applied to any technology
  - Developing adaptations of light water reactor (LWR) based regulations for advanced non-LWRs
  - Establishing risk-informed performance-based NRC license application content and review criteria guidance
  - Establishing risk-informed regulatory approaches for key parts of the plant operations phase



INL

Questions?

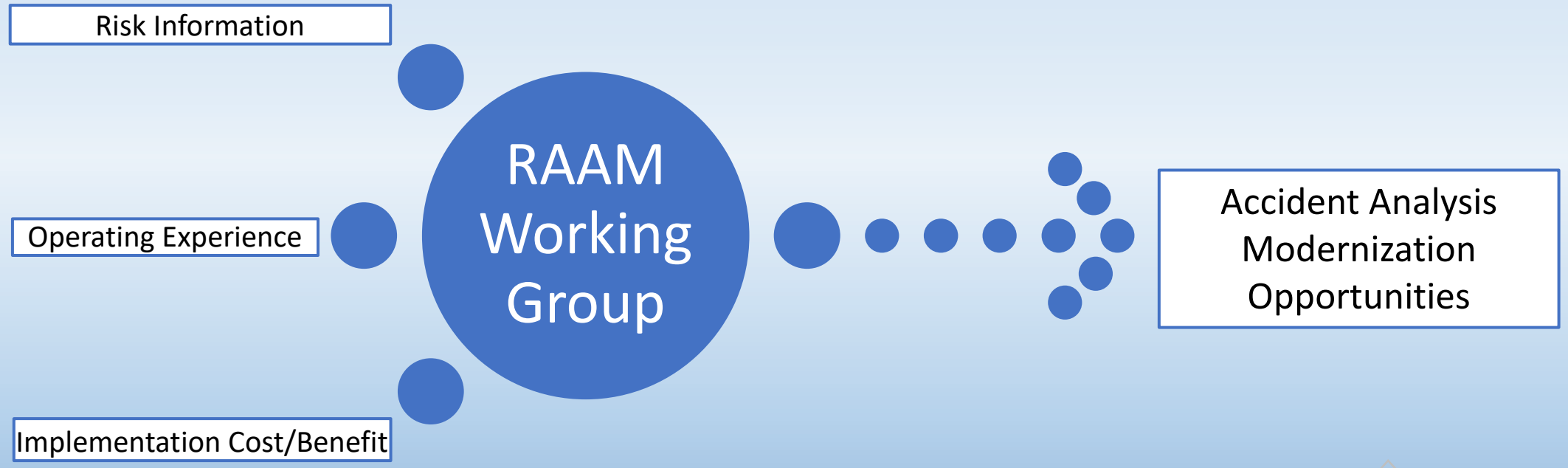
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Reactor Accident Analysis Modernization (RAAM)

Christopher Van Wert

Senior Technical Advisor for Reactor Fuel, Division of Safety Systems, NRR

What is RAAM?

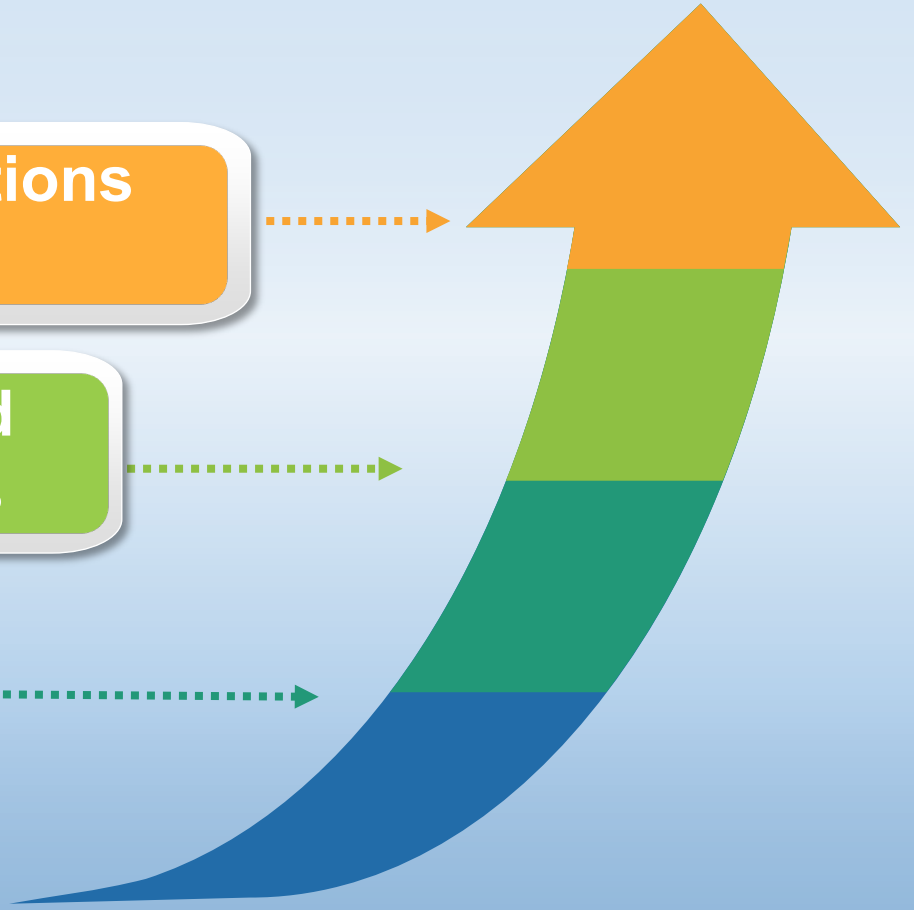

Risk Information
Operating Experience
Implementation Cost/Benefit
RAAM Working Group
Accident Analysis
Modernization
Opportunities

RAAM Tasks

Development of Recommendations Report to Management

Identification of Considerations and Development of Recommendations

Identification of Scope and Development of Charter



NRC's 2023 Fall Risk Forum
September 12, 2023

NRC's Approach to Risk-Inform the Policy for Addressing Digital Instrumentation and Controls Common-Cause Failures

Samir Darbali
Long-Term Operations and Modernization Branch
Division of Engineering and External Hazards
Office of Nuclear Reactor Regulation

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NRC's Approach to Risk-Informing the CCF Policy

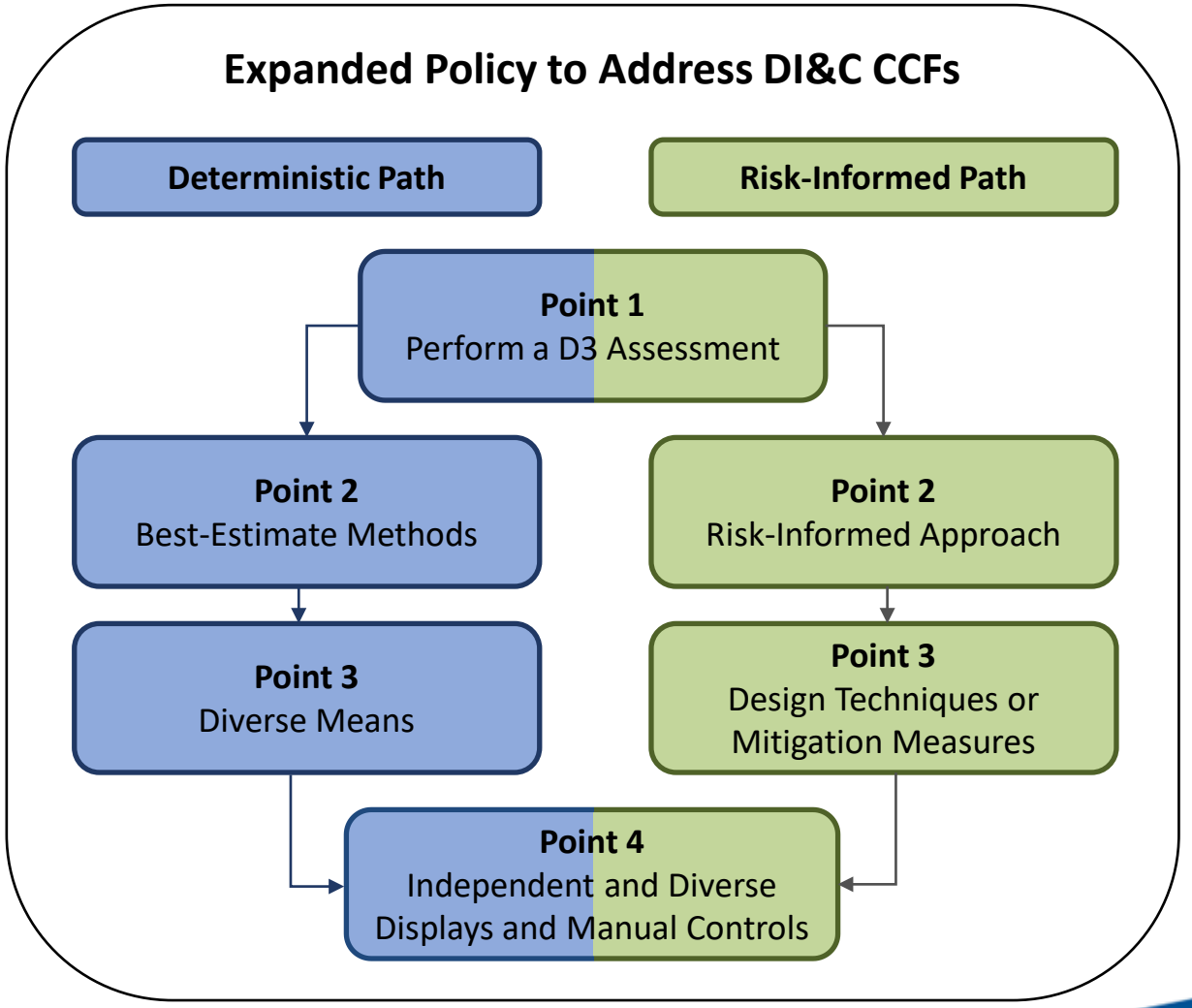
- Nuclear power plants continue to install digital I&C (DI&C) technology
  - increased reliability and safety benefits
  - can introduce new types of potential systematic, nonrandom, concurrent failures of redundant elements (i.e., common-cause failures (CCFs))
- NRC's policy for addressing DI&C CCFs goes back 30 years
  - first established in SRM-SECY-93-087
  - has been effectively used to license DI&C systems in nuclear power plants
  - requires a diverse means of actuation if a CCF could disable a safety function
- The NRC staff recognized the opportunity to further risk-inform the policy to address DI&C CCFs for high safety significance systems

NRC's Approach to Risk-Informing the CCF Policy

- In August 2022, the staff issued SECY-22-0076 – "Expansion of current policy on potential common-cause failures in digital instrumentation and control systems"
  - requests that the Commission expand the DI&C CCF policy to allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth
  - this may include not providing any diverse automatic actuation of safety functions
- The staff's goals:
  - the current policy will continue to remain a valid option for licensees and applicants
  - the acceptance criteria for risk-informed approaches for DI&C CCFs will be consistent with established NRC practices and guidance for risk-informed decision-making
  - provide more flexibility in addressing the DI&C CCF challenge while continuing to ensure safety

NRC's Approach to Risk-Informing the CCF Policy

The deterministic path requires the use of best-estimate methods for performing the defense-in-depth and diversity (D3) assessment, and the use of diverse means to address a potential DI&C CCF



The risk-informed path allows for the use of risk-informed approaches for performing the D3 assessment, and the use of design techniques or mitigation measures other than diversity to address a potential DI&C CCF

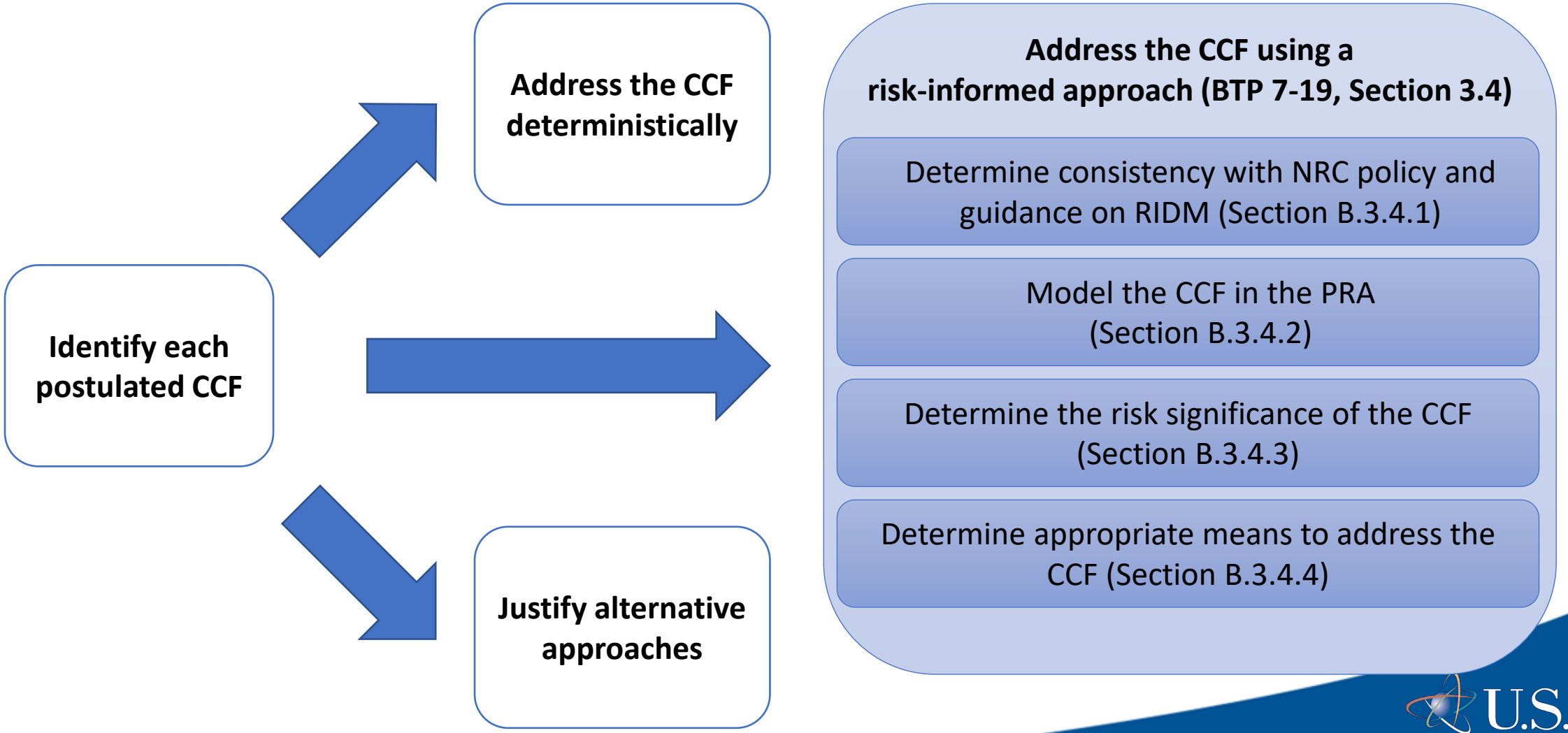
NRC's Approach to Risk-Informing the CCF Policy

- In May 2023, the Commission approved in SRM-SECY-22-0076 the staff's recommendation to expand the existing policy
- The Commission directed the staff to:
  - clarify in the implementing guidance that the new policy is independent of the licensing pathway selected by reactor licensees and applicants
  - complete the final implementing guidance within a year from the date of the SRM
- To meet the Commission direction, the staff evaluated what updates were necessary to existing guidance for addressing DI&C CCFs
  - guidance for operating light-water reactor (LWR) DI&C licensing reviews
  - guidance for non-LWR DI&C licensing reviews

Guidance for LWR Digital I&C Licensing Reviews

- The existing guidance is found in Standard Review Plan (SRP) Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense in Depth and Diversity to Address Common-cause Failure Due to Latent Design Defects in Digital Safety Systems," Revision 8
- BTP 7-19, Revision 8 explicitly addresses the CCF policy in SRM-SECY-93-087 (i.e., use of only best-estimate methods and requirement of diverse means)
- The staff is currently working on a draft Revision 9 to BTP 7-19
  - allows the staff to review risk-informed applications
  - may result in use of design techniques or mitigation measures other than diversity
  - focuses the edits on the expanded policy

Risk-Informed D3 Assessment Process



Guidance for non-LWR DI&C Licensing Reviews

- RG 1.233 includes specific acceptance criteria on risk significance, frequency-consequence targets, and defense-in-depth as part of the systematic risk-informed and performance-based approach
- NRC staff review of DI&C design is performed in a risk-informed and performance-based manner using the Design Review Guide (DRG)
- RG 1.233 and the DRG can be used to address potential CCFs in a risk-informed and performance-based manner that meets the overall intent of SRM-SECY-22-0076
- The staff will continue to engage the stakeholders through pre-application engagement and ongoing advanced reactor I&C workshops

Guidance for non-LWR DI&C Licensing Reviews

- The staff will update RG 1.233 and the DRG in the future, as appropriate, to reflect the lessons learned from the staff and industry stakeholders
  - based on the use of these guidance documents during the initial licensing reviews of the near-term applications
  - input received from the stakeholders during the ongoing advanced reactor I&C public workshops
- These updates to RG 1.233 and the DRG will also reflect SRM-SECY-22-0076

Next Steps

- The staff is planning to issue draft BTP 7-19, Revision 9 for public comment in October 2023
- The public comment period is expected to end in November 2023
- The staff is planning to issue the final BTP 7-19, Revision 9 in May 2024

THANK YOU!

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Acronyms

BTP	Branch Technical Position
CCF	Common Cause Failure
CDF	Core Damage Frequency
D3	Defense-in-Depth and Diversity
DAS	Diverse Actuation System
DI&C	Digital Instrumentation and Control
DRG	Design Review Guide
ESFAS	Engineered Safety Features Actuation System
I&C	Instrumentation and control
LERF	Large Early Release Frequency
LMP	Licensing Modernization Project
LWR	Light-Water Reactor
NRC	Nuclear Regulatory Commission
PRA	Probabilistic Risk Assessment
RG	Regulatory Guide
RIDM	Risk-Informed Decision-Making
RPS	Reactor Protection System
SECY	Commission Paper
SRM	Staff Requirements Memorandum
SRP	Standard Review Plan

References

- SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” April 1993 (ML003708056)
- SRM-SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” July 1993 (ML18145A018)
- SECY-18-0090, “Plan for Addressing Common Cause Failure in Digital Instrumentation and Controls,” September 2018 (ML18179A066)
- BTP 7-19, Revision 8, “Review of NUREG-0800, Branch Technical Position 7-19, “Guidance for Evaluation of Defense in Depth and Diversity to Address Common Cause Failure Due to Latent Design Defects in Digital Safety Systems,” Revision 8,” December 2020 (ML20339A647)
- SECY-22-0076, “Expansion of Current Policy on Potential Common Cause Failures in Digital Instrumentation and Control Systems,” August 2022 (ML22193A290)
- Supplement to SECY-22-0076, “Expansion of Current Policy on Potential Common Cause Failures in Digital Instrumentation and Control Systems,” January 2023 (ML22357A037)
- SRM-SECY-22-0076, “Expansion of Current Policy on Potential Common Cause Failures in Digital Instrumentation and Control Systems,” May 2023 (ML23145A181 and ML23145A182)
- RG 1.200, Revision 3, “Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities,” December 2020 (ML20238B871)
- RG 1.174, Revision 3, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” January 2018 (ML17317A256)
- RG 1.233, “Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors,” June 2020 (ML20091L698)
- Design Review Guide (DRG): Instrumentation And Controls for Non-light-water Reactor (Non-LWR) Reviews, February 2021 (ML21011A140)

EPRI Digital Systems Engineering Framework

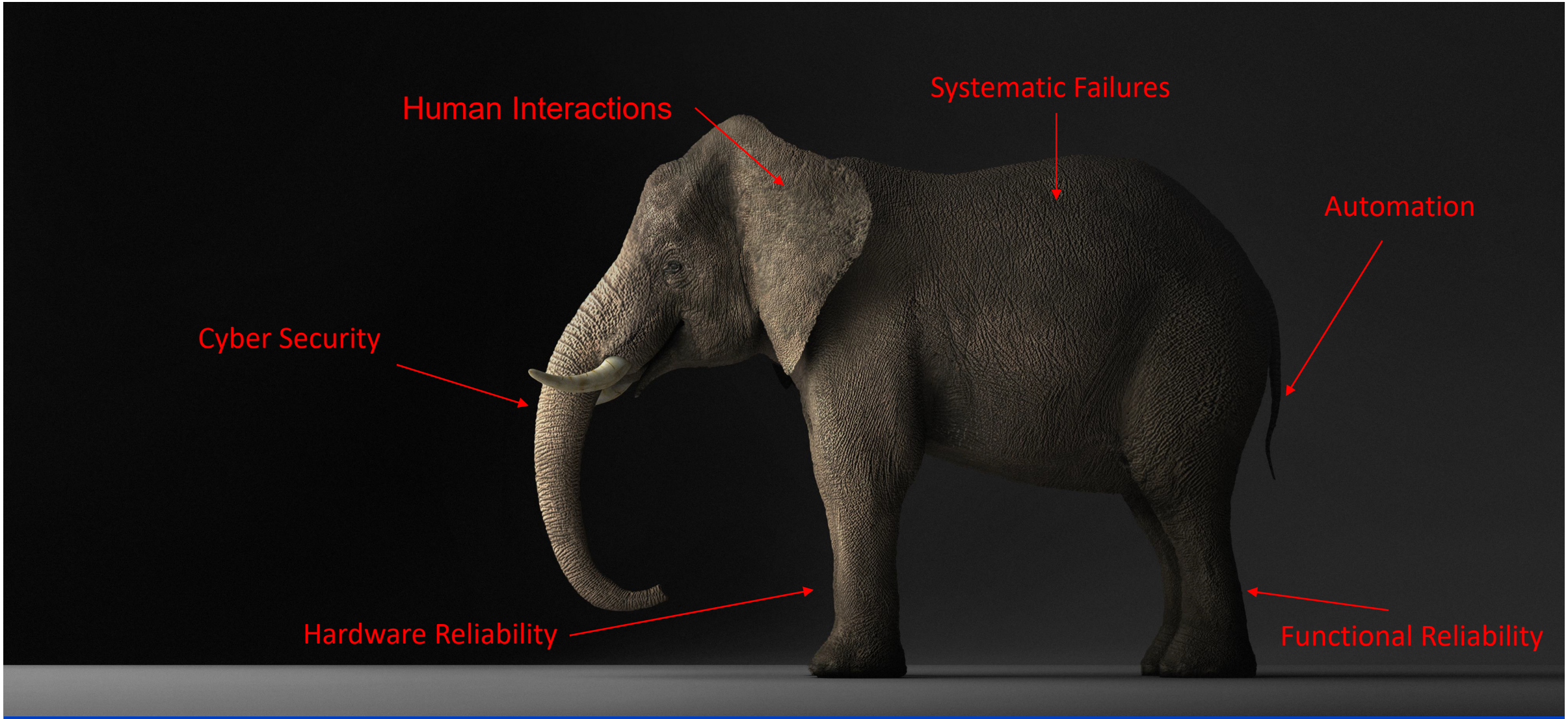
A Modern Approach

Matt Gibson-Technical Executive
EPRI

NRC's 2023 Risk Forum- Digital CCF Panel
NRC Headquarter
North Bethesda , Maryland

September 12th , 2023

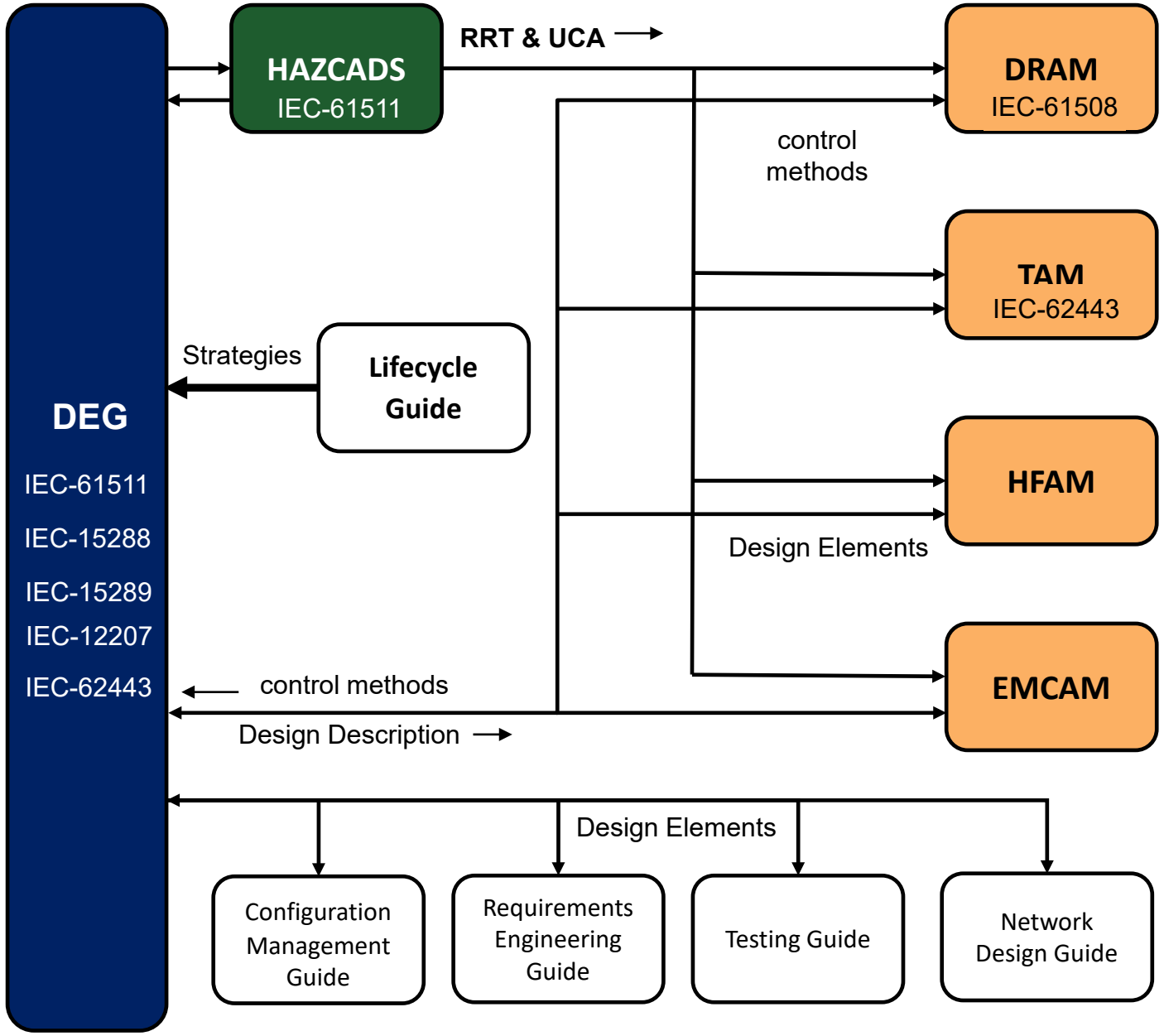
Looking at the Whole Elephant



How to address design requirements, risks, and hazards from various sources in one integrated process

Framework Highlights

- Systems Engineering Based- Single Process
  - ✓ Addresses all elements of new and modified I&C designs
  - ✓ Usable for both new reactor and legacy plant upgrades
  - ✓ Risk-Informs: Digital Reliability, Cyber Security, Human Factors
  - ✓ Achieves requirement completeness via hazards analysis, iteration and validation. Systems Theoretic Process Analysis (STPA) is a key tool
  - ✓ **Fully addresses technical common cause failure (CCF) concerns**
  - ✓ Provides feedback to the PRA/PSA process to close the loop on risk determinations
- Developed over 8 ears using blind studies, comparative analysis, usability exercises, and insights from other industries.
- Dramatically reduces Design and Implementation Uncertainty



DEG –Synthesizes the Systems Engineering framework from IEC-15288. Includes all relevant Lifecycle topics. Takes strategic input from the Lifecycle guide

HAZCADS –Uses STPA/FTA to identify hazards and associated UCA . FTA and Risk Matrices develop a Risk Reduction Target (RRT) which informs the downstream processes. Implements a PHA/LOPA from IEC-61511.

DRAM – Identifies Hardware and Software reliability vulnerabilities and develops loss scenarios. Develops and Scores protect, detect , and respond/recover control methods using the RRT

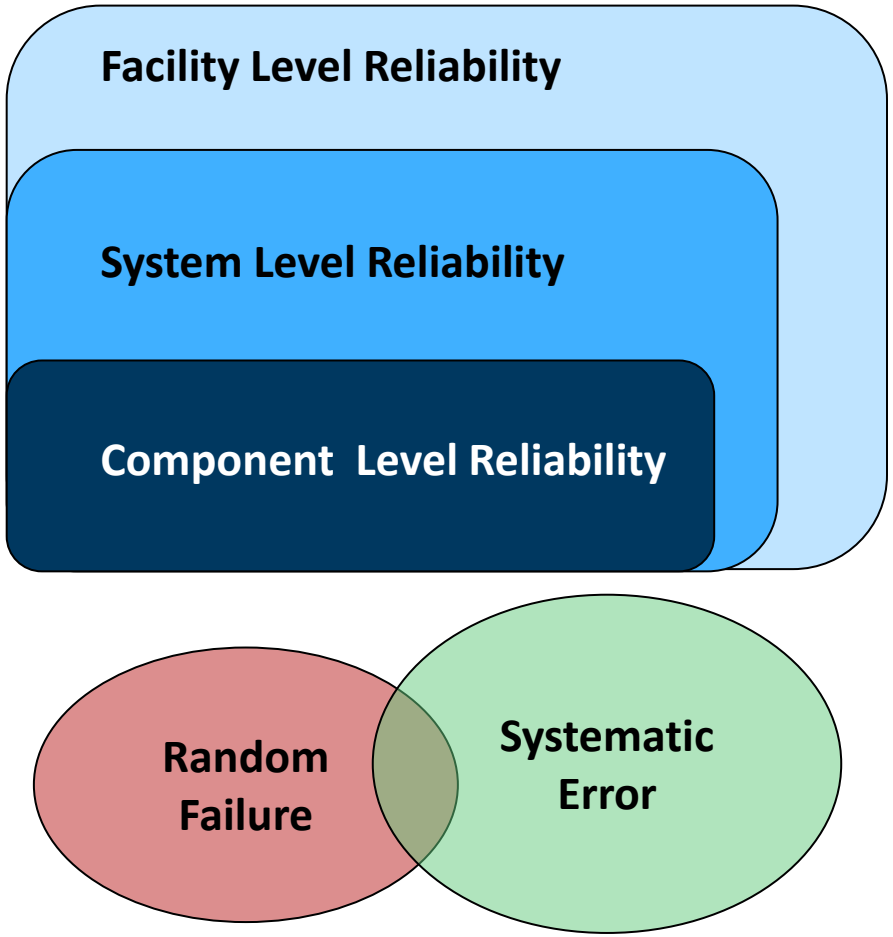
TAM –Identifies cyber security vulnerability classes. Develops Exploit Sequences. Develops and Scores protect, detect , and respond/ recover control methods using the RRT

HFAM – Develops human actions and interfaces. Identifies and scores Human Reliability using the RRT

EMCAM – Identifies EMC vulnerability classes. Develops and scores protect, detect , and respond/ recover control methods using the RRT

RRT= Risk Reduction Target
UCA= Unsafe Control Action
STPA=System Theoretic Process Analysis
FTA= Fault Tree Analysis
LOPA= Layers of Protection Analysis
EMC= Electromagnetic Compatibility

Digital Reliability Model



Reliability Axioms

- Common Cause Failures must **first** have a failure or systematic error (including emergent behavior)
- Achieved Systematic and Random Reliability is inversely proportional to the likelihood of a CCF
- Reliability is best achieved via a cost, likelihood, and consequence equilibrium
- Net Functional Reliability is the prime objective (at the system/facility level)
- Focused Models can provide actionable reliability Insights (FTA, STPA, Relationship Sets)

- **Functional Reliability is an Equipment Level Challenge**
- **Functional Reliability is a Lifecycle Challenge**

Use of Models for Engineering within the Framework

The Digital Engineering Framework Currently leverages seven distinct focused models:

Model	Question to be Answered
Systems Engineering	What are the key systems elements, the functional allocation of those elements, and what is the reliability of those elements? (DEG)
Fault Trees	What are the Risk Sensitivities within a Dependency Scope? (HAZCADS,PRA)
STPA	What are the Systematic Hazards and Pathways? (HAZCADS, DRAM, TAM, HFAM,EMCAM)
Relationship sets	What are the system element dependencies and degree of independence across multiple relationships? (DEG)
HRA	What is the reliability of Human Actions? (HFAM)
Exploit Sequences	What are the exploit objectives, pathways to those objectives, and the method of exploit? (TAM)
Reliability Analysis	What are the failure frequencies/errors that impact Probability of Failure on Demand-PFD? (DRAM)

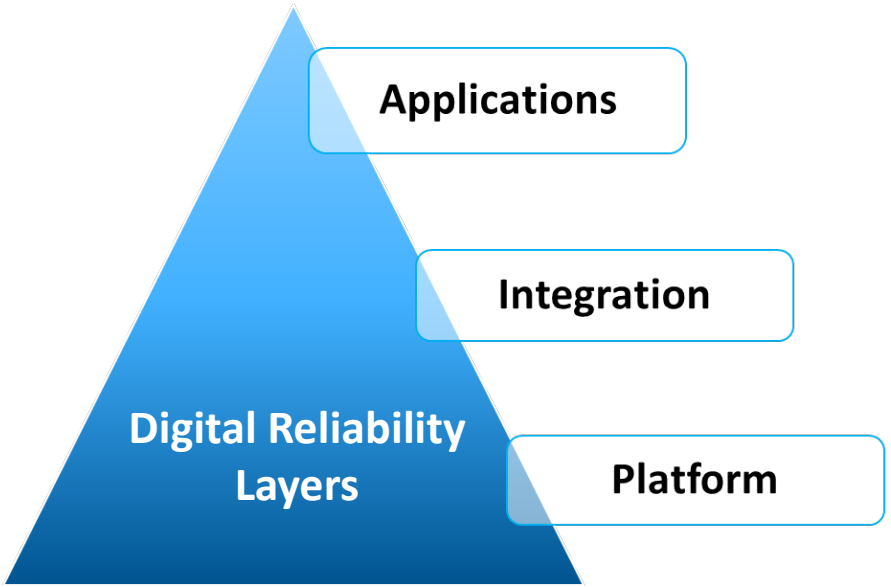
- EPRI continues to leverage or develop additional models as the “questions” become better defined.
- Performance based design requires the design questions to be defined and bounded.

To be useful, a model must answer a key question

Safety Integrity Level (SIL) efficacy for Nuclear Power

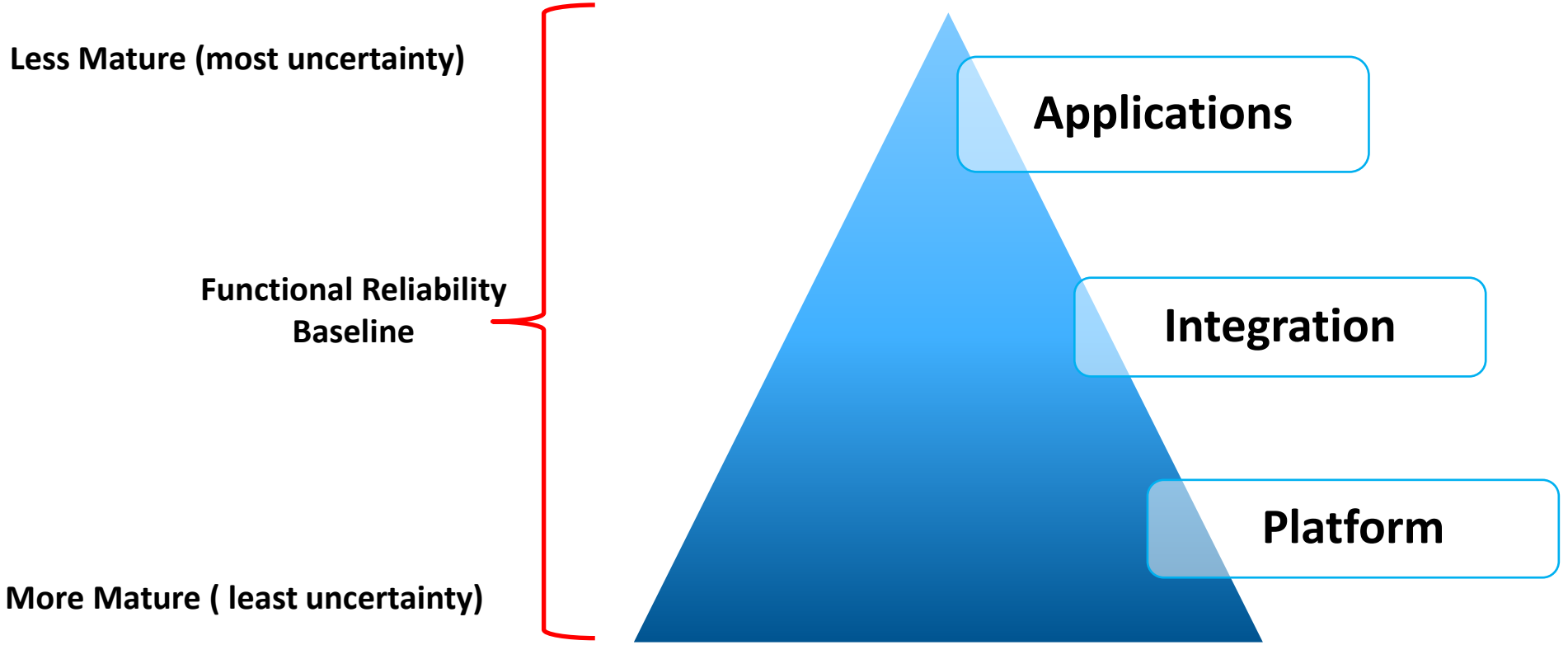
- EPRI research on field failure data from SIL certified logic solvers revealed no ***platform level*** Software Common Cause Failures (SCCF) after over 2 billion combined hours of operation for IEC-61508 SIL certified PLC's (3002011817)
- Indicates that using existing SIL certifications, at the ***platform level***, has a high efficacy for use as surrogates for some existing design and review processes.
- **Leveraged for NEI 17-06/RG-1.250 and NEI 20-07 in US**

- Correlates well with EPRI review of global OE (Korea, France, China, etc.) that indicates:
  - Safety related software is no more problematic than other CCF contributors when subjected to deliberate safety and reliability design processes.
  - There have been no events where diverse platforms would have been effective in protecting against SCCF



Reliability Layers

Functional Reliability, which includes software, hardware, and human elements should be segmented by layers: *platform, integration, and application*.
Then Considered Separately



Production Data and OE Quantity and Quality Dive Maturity and Reliability

Relationship Sets

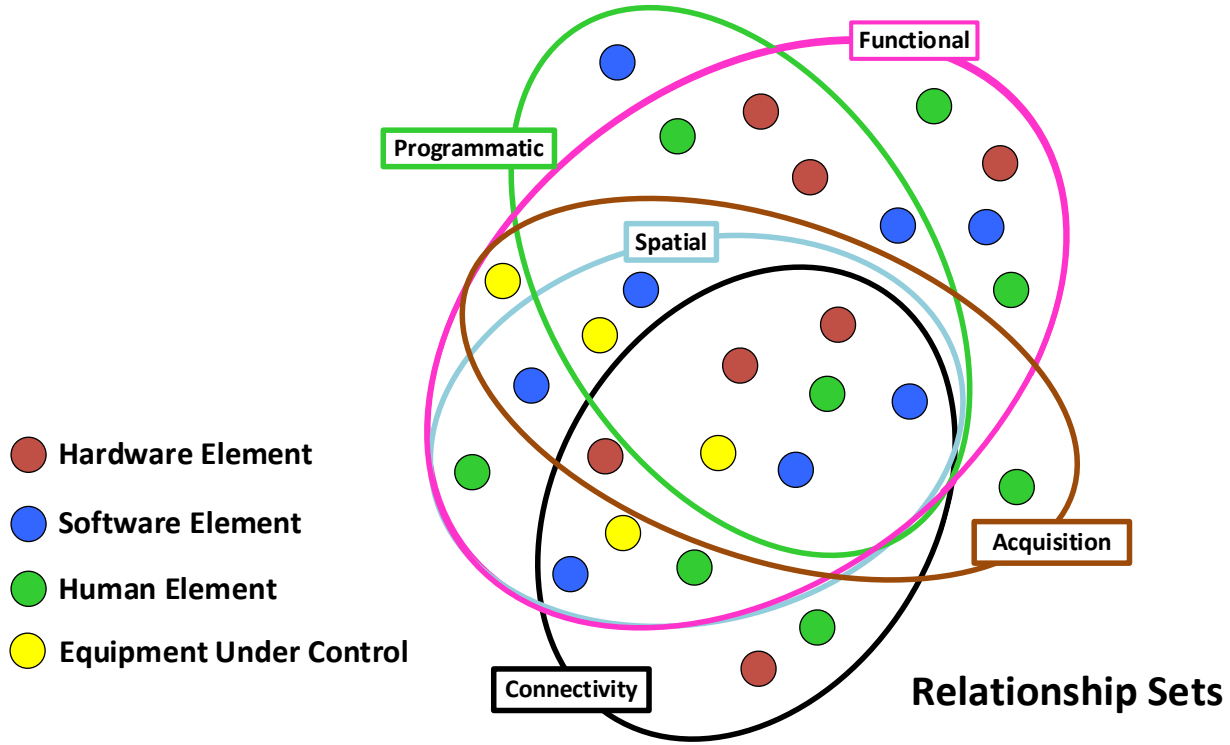
Relationship sets are an architecture view and contain all system elements scoped within the new design or design change.

There four of system elements

- Hardware
- Software
- Human
- Equipment Under Control

There are five relationship set types:

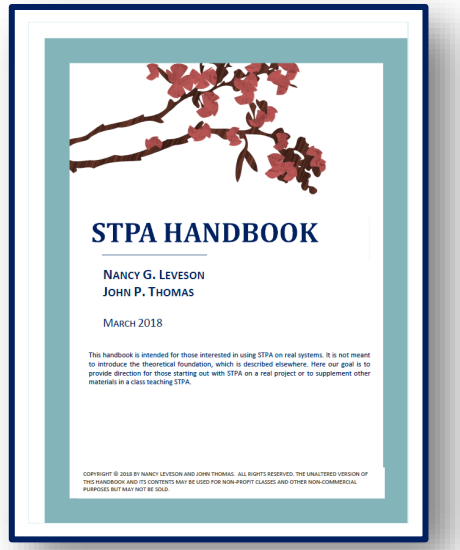
- Functional
- Connectivity
- Spatial
- Programmatic
- Acquisition



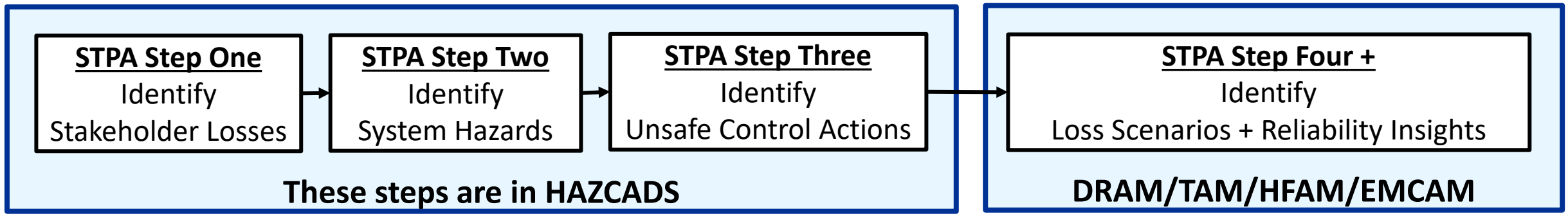
Models the Relationship/Dependencies Between System Elements

HAZCADS Basis: Hazard Analysis via STPA

- IEC Std. 61508-1 requires a determination of hazards of the Equipment Under Control (EUC) and the EUC control system, and "***consideration shall be given to the elimination or reduction of the hazards***."
- System Hazards are Challenges to Critical (Safety) Functions
- Risk and Reliability analysis extend the STPA Process

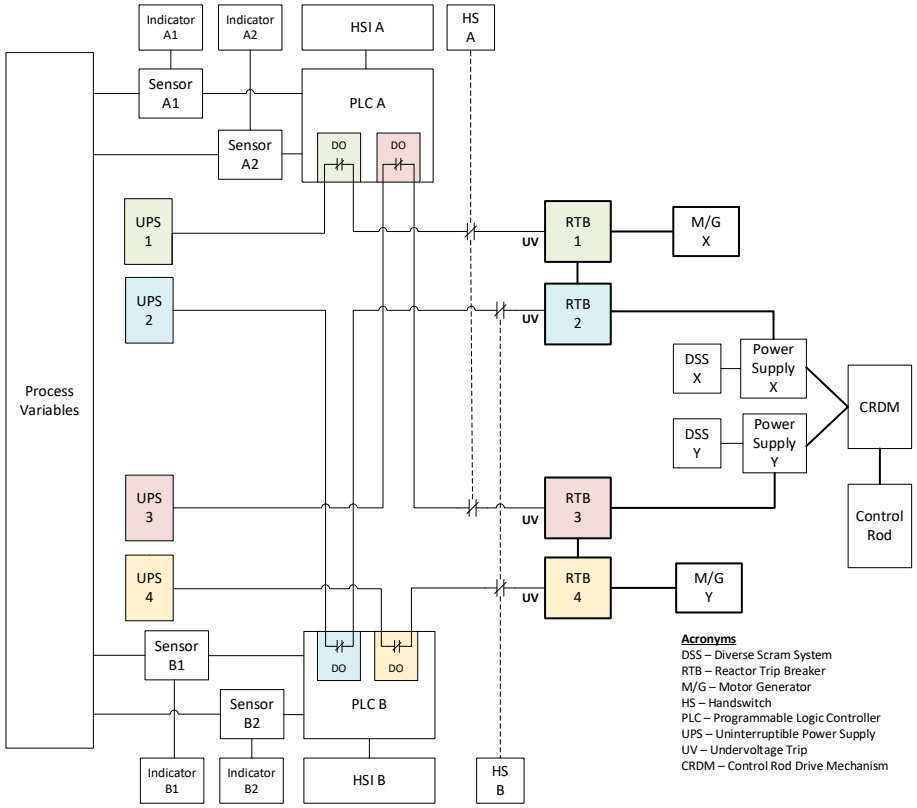


For the determination of hazards and their causes, HAZCADS and DRAM/TAM/etc. apply the four-part Systems Theoretic Process Analysis (STPA). Insights from this diagnostic process are pipelined back to the DEG for aggregation and requirements updates.

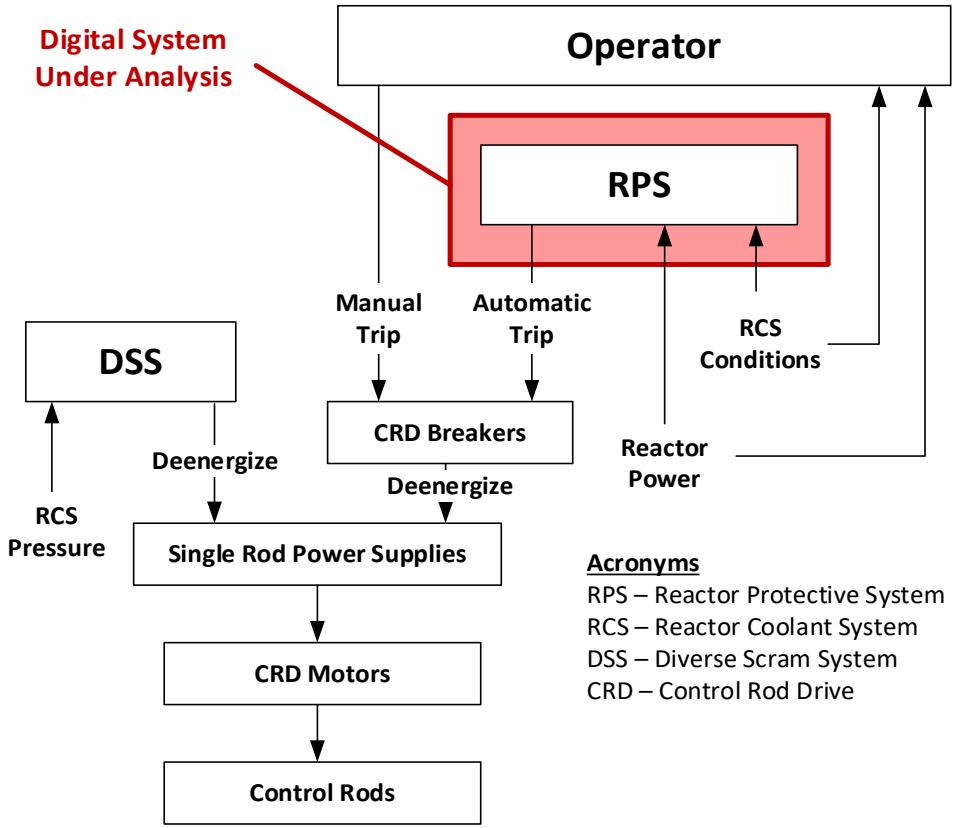


Systems and STPA

Notional 1oo2 RPS Concept



STPA Control Structure



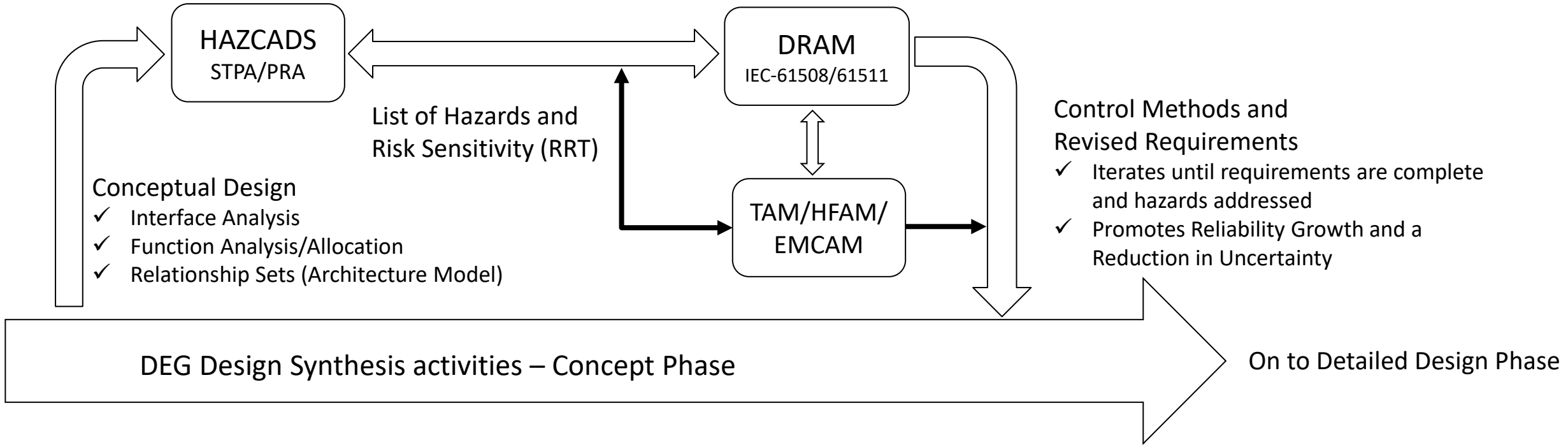
The STPA Control Structure is a Diagnostic Model

Workflow- Conceptual Phase

Diagnostic Process to Identify Digital Hazards & Risk Sensitivities and Refine Requirements

Models System and Plant level Hazards and criticality (Risk Sensitivity)

Identifies Hardware, Software, and Human Reliability Vulnerabilities and Mitigations associated with Hazards



Integrating Design Insights into the PRA/LMP/PSA

- Research in progress
  - Collecting/developing examples and use cases to test proposed approach
  - Re-look at the data, existing guidance and lessons from HAZCADS
  - Ensure consistency with RIDM framework
  - Ensure plant reflects “as built, as operated”, including change management

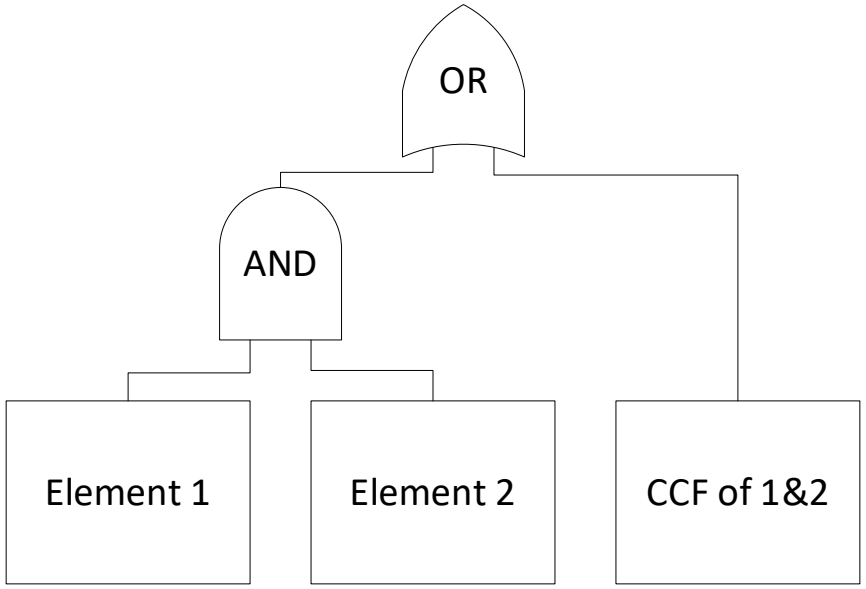
- Incorporation of the design into the PRA should
  - Be consistent in insights from the design process
  - Be consistent with overall PRA modelling approach
  - Continue to reflect the “as-built, as-operated” plant

Integrating Design Insights into the PRA/LMP/PSA (cont.)

- Digital systems should be modeled at a reasonable level of detail adequate to support decision making
  - Over decomposition introduces unnecessary modeling complexity
  - Modeling level should match boundary conditions of collected data
  - Software should not be separated from hardware (all software is implemented through a hardware system) → *Functional Reliability*

- Fundamental Assumption: **Control Methods** implemented through the design process reduces the risk to *acceptably low levels of risk*
  - Both for functional reliability and common cause failures
  - Qualitative analysis reflects the best state of knowledge (best-estimate); this is key for consistency between design and assessment phases

Capturing Consequence of Digital Failures* in the PRA



Cause and Effect Relationship

- The cause-effect relationship of potential unsafe control actions (UCAs) that survived to final design should be retained in the PRA or documentation:
  - UCAs with non-unique consequences should be mapped to existing basic events for documentation
  - UCAs with unique consequences can be included explicitly in the model
- Logic reassessed as the PRA evolves to reflect the as-built, as-operated plant

*Can be hardware, software or human error; systematic or random.

EPRI's Digital Framework Elements

EPRI's ***high-quality engineering process*** uses the same modern methods and international standards used in other safety related industries to reduce implementation cost

Utilize Industry Standards	Use the same proven design and supply chain structures that non-nuclear safety related industries use (IEC-61508/61511/62443). This leverages the economies-of-scale achieved in other industries.
Use of Systems Engineering	Use of a modern, high performance, single engineering process that leverages systems engineering in the transition to team-based engineering for conception, design, and implementation(IEC-15288,IEC-15289, IEC-12207,STPA).
Risk Informed Engineering	Making effective engineering decisions via hazards and risk analysis to integrate all digital engineering topics into a single engineering process (STPA,FTA)

Capable Workforce

Modern Methods to Support Nuclear Fleet Sustainability and Advanced Reactor Design

Supplemental Funded:
Digital Systems Engineering User Group - 3002022140

A forum for information sharing of digital specific material

- ✓ Operational Experience
- ✓ Lessons Learned
- ✓ Interactive community
- ✓ Common Design Packages
- ✓ Cyber Security Evaluations
- ✓ Member Feedback

Fall Meeting 2023
September 19th & 20th

Current Members to Date

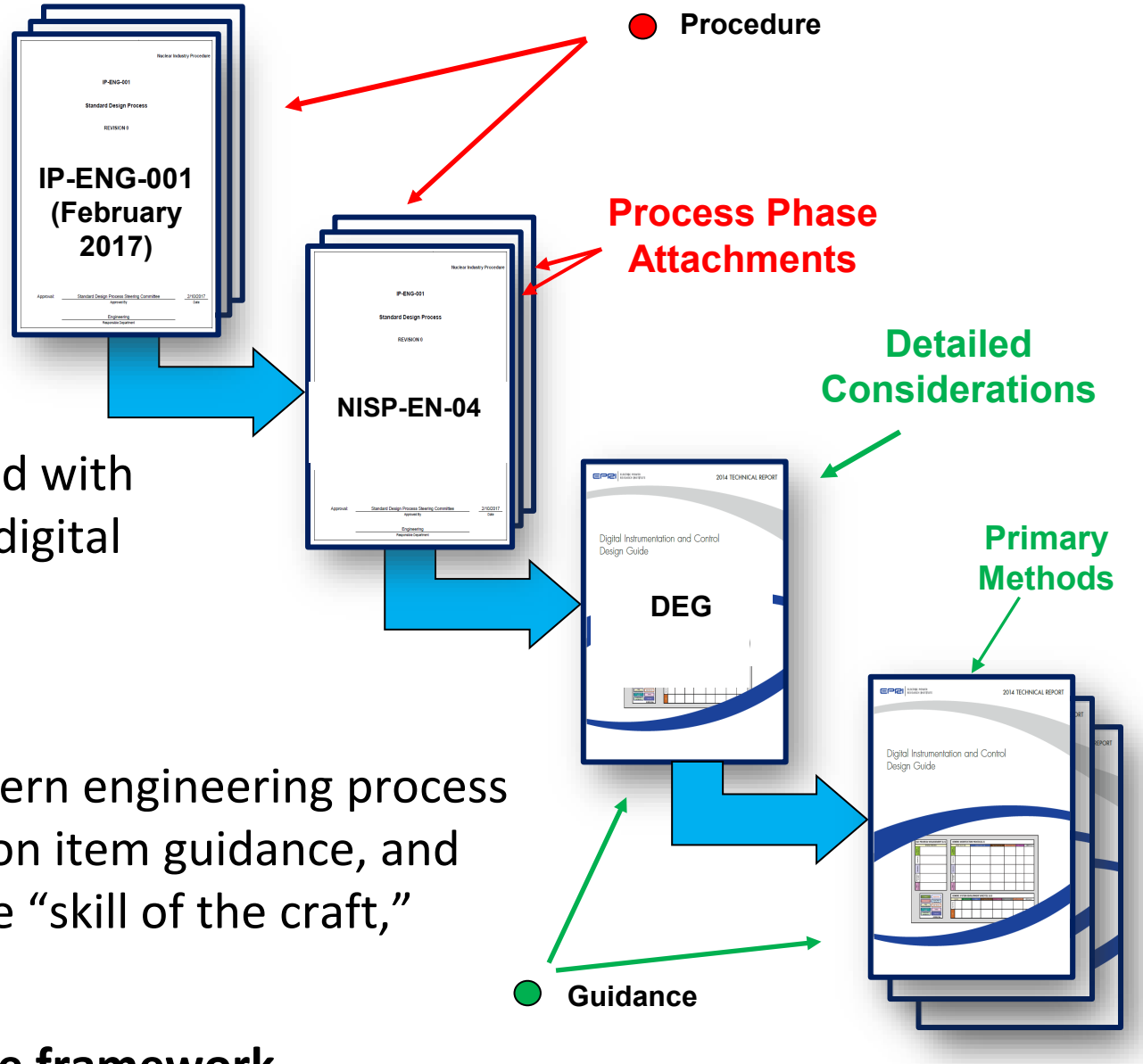
Framatome
Constellation Energy
Dominion Energy South Carolina, Inc.
Dominion Energy, Inc.
Duke Energy Corp.
Entergy Services, Inc.
Evergy Services (Wolf Creek)
Callaway (Ameren)
Palo Verde
Sargent & Lundy Engineers
Southern Company
Tennessee Valley Authority (TVA)
Vistra Corp. (Comanche Peak)
Westinghouse Electric Company, LLC
Xcel Energy
PSEG (Salem/Hope Creek)
South Texas Project (STP)
NPPD (Cooper)
Enercon Services
Curtiss Wright
Bruce Power

Current Activities:

- ✓ Harmonization of the DEG,HAZCADS,DRAM,TAM,EMCAM,HFAM, and Digital Lifecycle Strategy Guide. Improves coordination between products and updates with current OE.
- ✓ Roll out of the member sharing website.
- ✓ Nuclear Digital Project Experience Baseline 2022 published. Updated annually, members of this supplemental can download EPRI Technical Report 3002023748. This report provides a baseline of installed digital equipment across members.

US DEG Implementation

- IP-ENG-001 (Standard Design Process)- Main Procedure
- NISP-EN-04 is the Digital Specific Addendum to the SDP under the same mandatory Efficiency Bulletin (EB 17-06)

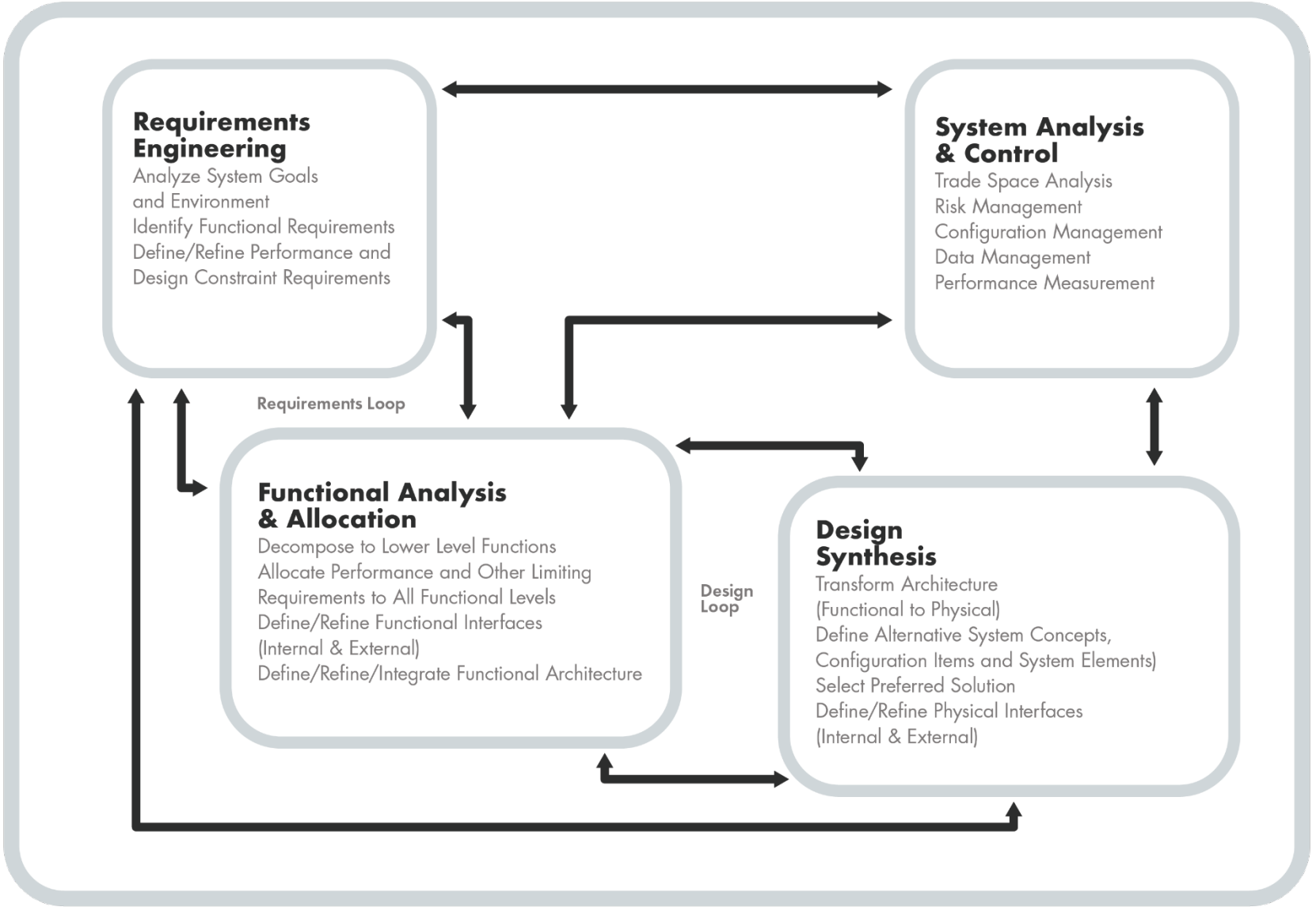


- Same process phases as IP-ENG-001, tailored with DEG-specific supplemental information for digital implementations. **Including Cyber Security**.
- Provides the user with **"what to do"**

- DEG provides detailed guidance using a modern engineering process with digital design considerations, information item guidance, and division of responsibility methods to improve "skill of the craft,"
- Provides the user with **"How to Do"**
- **Digital Training/Tech Transfer completes the framework**

Systems Engineering - Discovery, Iterations & Refinements

- Systems Thinking is the key skill required to use Systems Engineering
- It is multidisciplinary and requires teamwork
- Requires ability to see system relationships in a holistic manner
- Ability to communicate across disciplines
- Ability to understand complexity



Risk-Informed Forum

Alan Campbell, PE

September 12, 2023

NUCLEAR ENERGY INSTITUTE

Common Cause Failure Policy

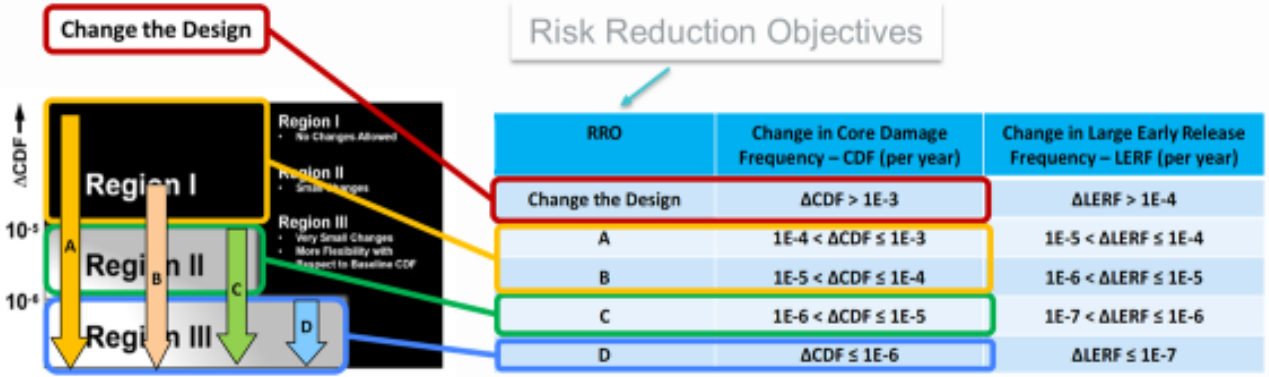
- Previous policy requires a Diversity and Defense-in-Depth (D3) analysis:
  - For each UFSAR Chapter 15 events, postulate a complete failure of RPS/ESFAS systems and analyze coping mechanisms
  - Any loss of a safety function will require a diverse means of achieving that safety function
- Impact of new, expanded policy:
  - Specifies defense-in-depth of the facility, not the proposed system
  - Allows for risk-informed approaches

Software Reliability Limitations

- Due to challenges modeling Digital I&C software reliability in PRA:
  - The absolute risk impact of software reliability cannot be quantitatively measured without substantial uncertainties
  - The effectiveness of applied design techniques cannot be quantitively measured without substantial uncertainties
  - There are no means of comparing design techniques to using diversity without substantial uncertainties

How Can We Use Risk Insights?

- NEI 20-07 utilizes Fault Tree Analysis to assess the risk sensitivity of each loss scenario
- The result of the sensitivity analysis is mapped to the CDF/LERF regions and used in a graded approach to apply control measures



RRO	Change in Core Damage Frequency – CDF (per year)	Change in Large Early Release Frequency – LERF (per year)
Change the Design	ΔCDF > 1E-3	ΔLERF > 1E-4
A	1E-4 < ΔCDF ≤ 1E-3	1E-5 < ΔLERF ≤ 1E-4
B	1E-5 < ΔCDF ≤ 1E-4	1E-6 < ΔLERF ≤ 1E-5
C	1E-6 < ΔCDF ≤ 1E-5	1E-7 < ΔLERF ≤ 1E-6
D	ΔCDF ≤ 1E-6	ΔLERF ≤ 1E-7

NEI 20-07, Rev. E

- Leverages EPRI Digital Engineering Guideline, HAZCADS, and DRAM processes to demonstrate that CCF has been adequately addressed
- HAZCADS:
  - Hazards analysis methodology that identifies stakeholder losses, system hazards and unsafe control actions
  - Provides risk insights based on PRA sensitivity analysis
- DRAM:
  - Reliability assessment that identifies loss scenarios and applies control methods

NEI 20-07, Rev. E

- Why are we using HAZCADS and DRAM?
  - DEG is adopted into the Standardized Design Process via NISP-EN-04.
  - Efficacy studies demonstrate that underlying methodologies are compatible (i.e., limit weaknesses)
  - Technology agnostic
  - Accounts for the defense-in-depth of the facility
  - Improves overall reliability of the system by addressing credible and likely sources of systematic failures (including poor requirements, latent design errors, etc.)

LWRS
LIGHT WATER REACTOR SUSTAINABILITY

2023 NRC Fall Risk Forum

Han Bao
Idaho National Laboratory
09/12/2023

LWRS Program Research on Risk Assessment of Safety-related Digital I&C Systems

Light Water Reactor Sustainability (LWRS) Program

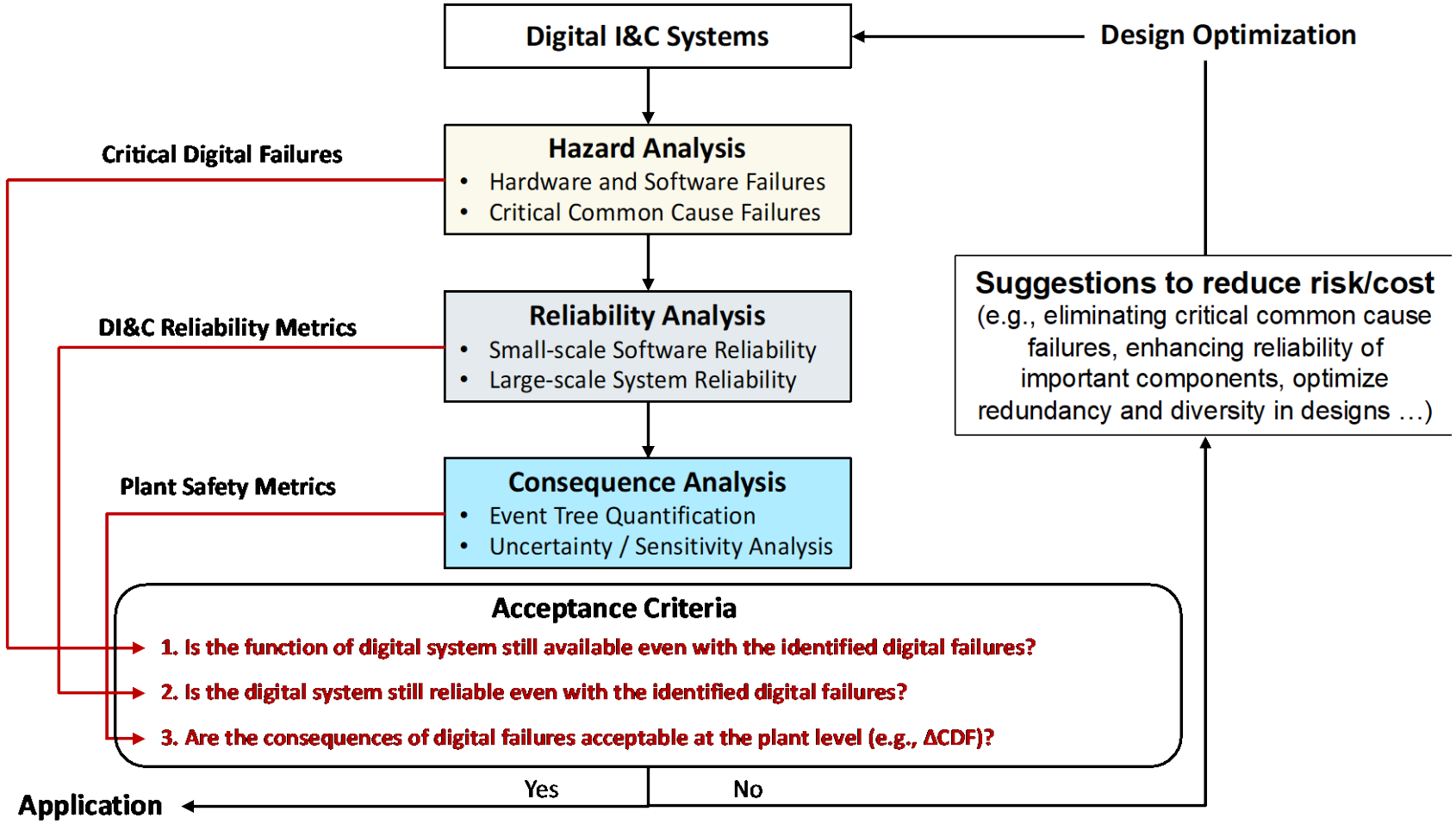
LWRS Goal

Enhance the safe, efficient, and economical performance of our nation's nuclear fleet and extend the operating lifetimes of this reliable source of electricity

Plant Modernization	Enable plant efficiency improvements through a strategy for long-term modernization
Flexible Plant Operation & Generation	Enable diversification and increase revenue of light water reactors by extracting electrical and thermal energy to produce non-electrical products
Risk Informed System Analysis	**Develop risk assessment methods and tools to optimize the safety, reliability, and economics of plants**
Materials Research	Understand and predict long-term behavior of materials in nuclear power plants
Physical Security	Develop technologies and the technical bases to optimize physical security postures

Goals of LWRS-RISA Efforts on DI&C Risk Assessment

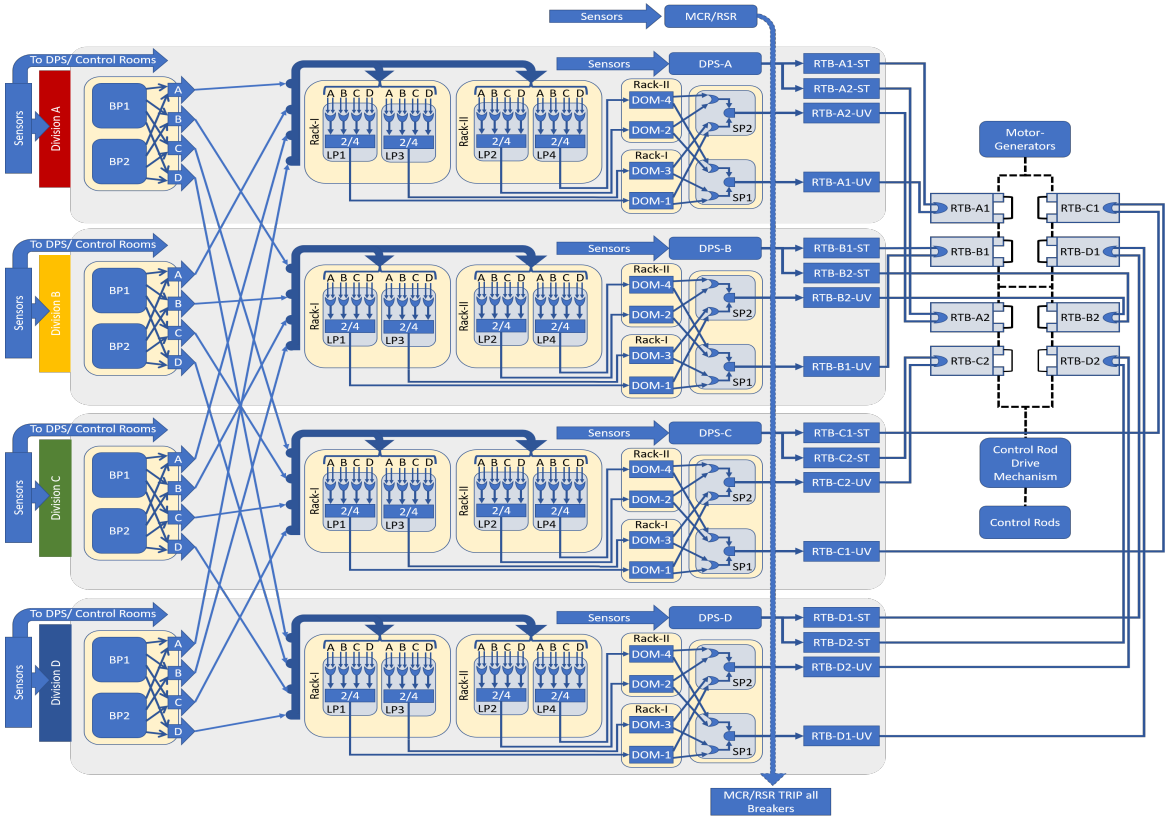
- **Offer a capability of design architecture evaluation** of various DI&C systems to support system design decisions on **diversity and redundancy applications**;
- Develop approaches to **address CCFs and estimate corresponding failure probabilities** for DI&C technologies;
- **Support existing risk-informed DI&C design guides** by providing quantitative risk-informed evidence.



Value Proposition

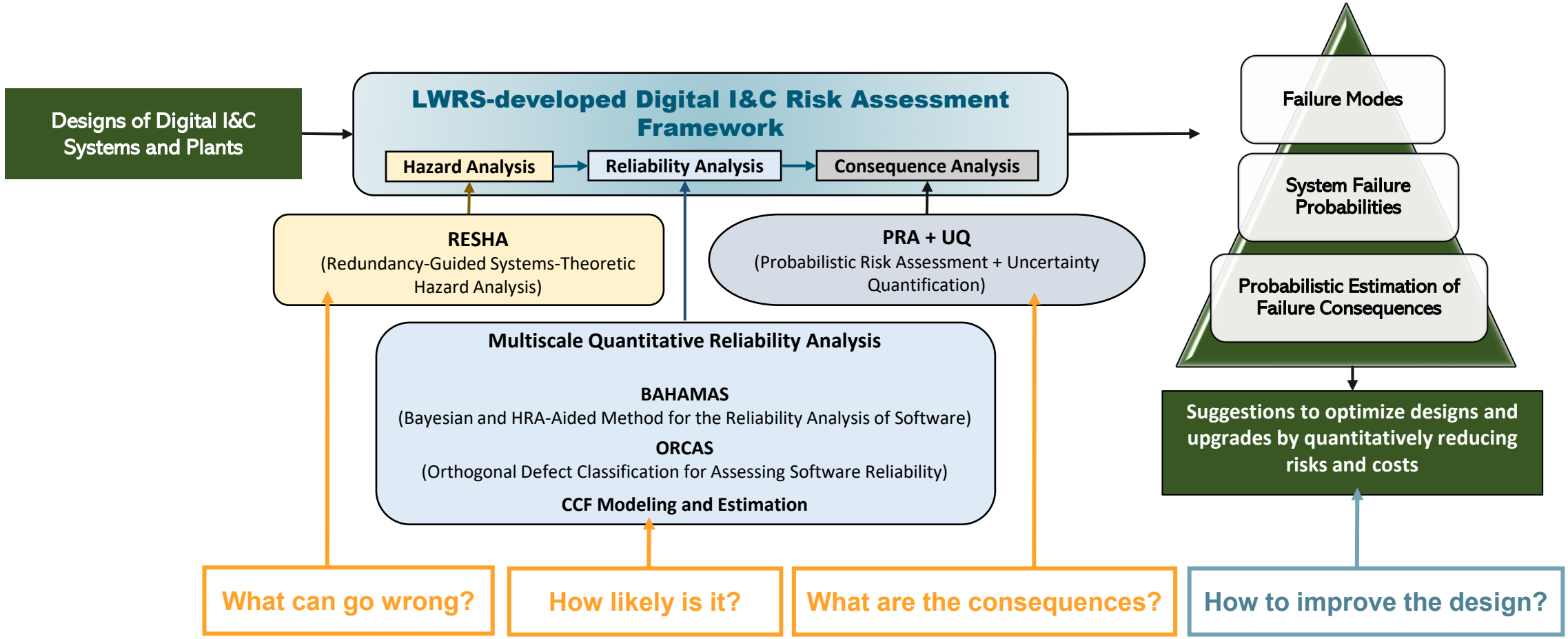
- **The framework** is envisioned and developed as **an integrated risk-informed tool** to support vendors and utilities with optimization of design solutions from economical perspectives GIVEN the constrain of meeting risk-informed safety requirements.

- **Quantitative Risk Analysis**
  - Software reliability metrics → DI&C system reliability → Plant safety analysis
- **Risk-informed Design**
  - Management strategy of CCFs
    - All elimination vs. selective elimination
  - Level of redundancy
    - 4 divisions vs. 2 divisions
    - 4 vs. 2 local logic processors per division
  - Level of diversity
    - Design: Analog? Digital? A combination of both?
    - Software: Design requirements, programming language, etc.
    - Hardware Equipment: Manufacturers, designs, architectures, etc.



A Four-Division Digital Reactor Trip System

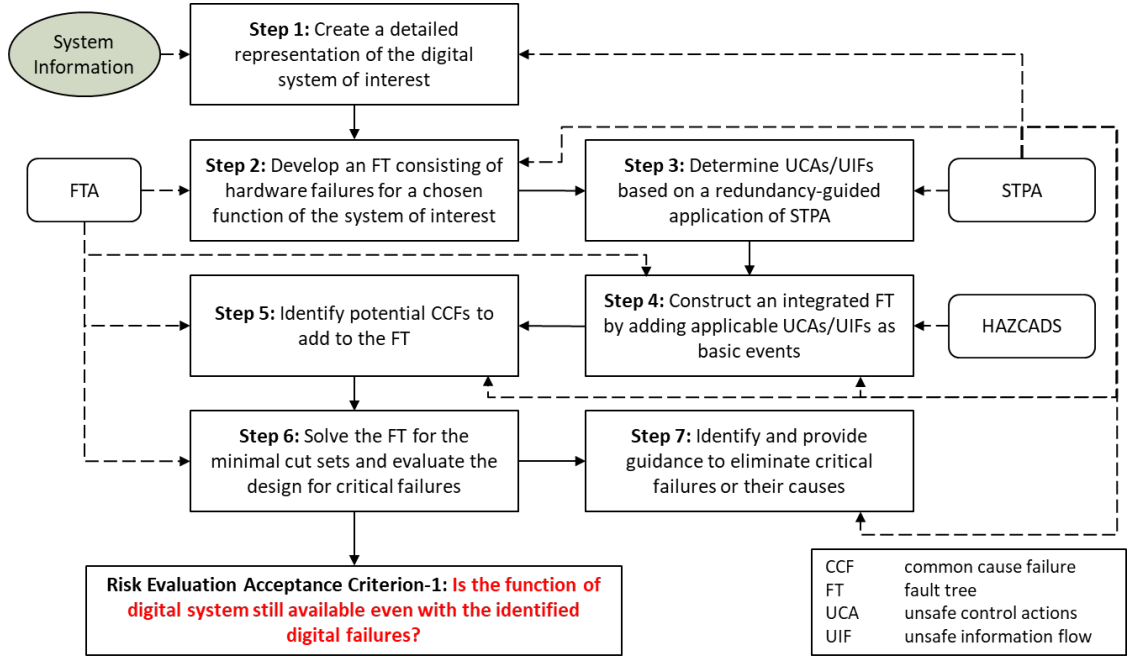
LWRS-developed DI&C Risk Assessment Framework

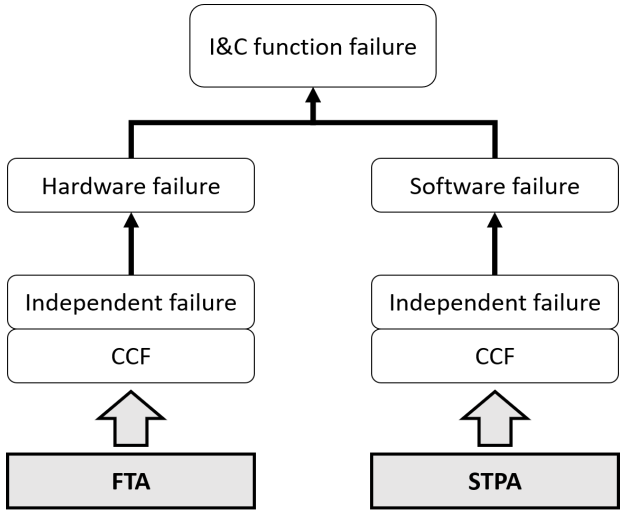


Redundancy-guided System-theoretic Hazard Analysis (RESHA)

Hazard analysis in the LWRS-developed framework:

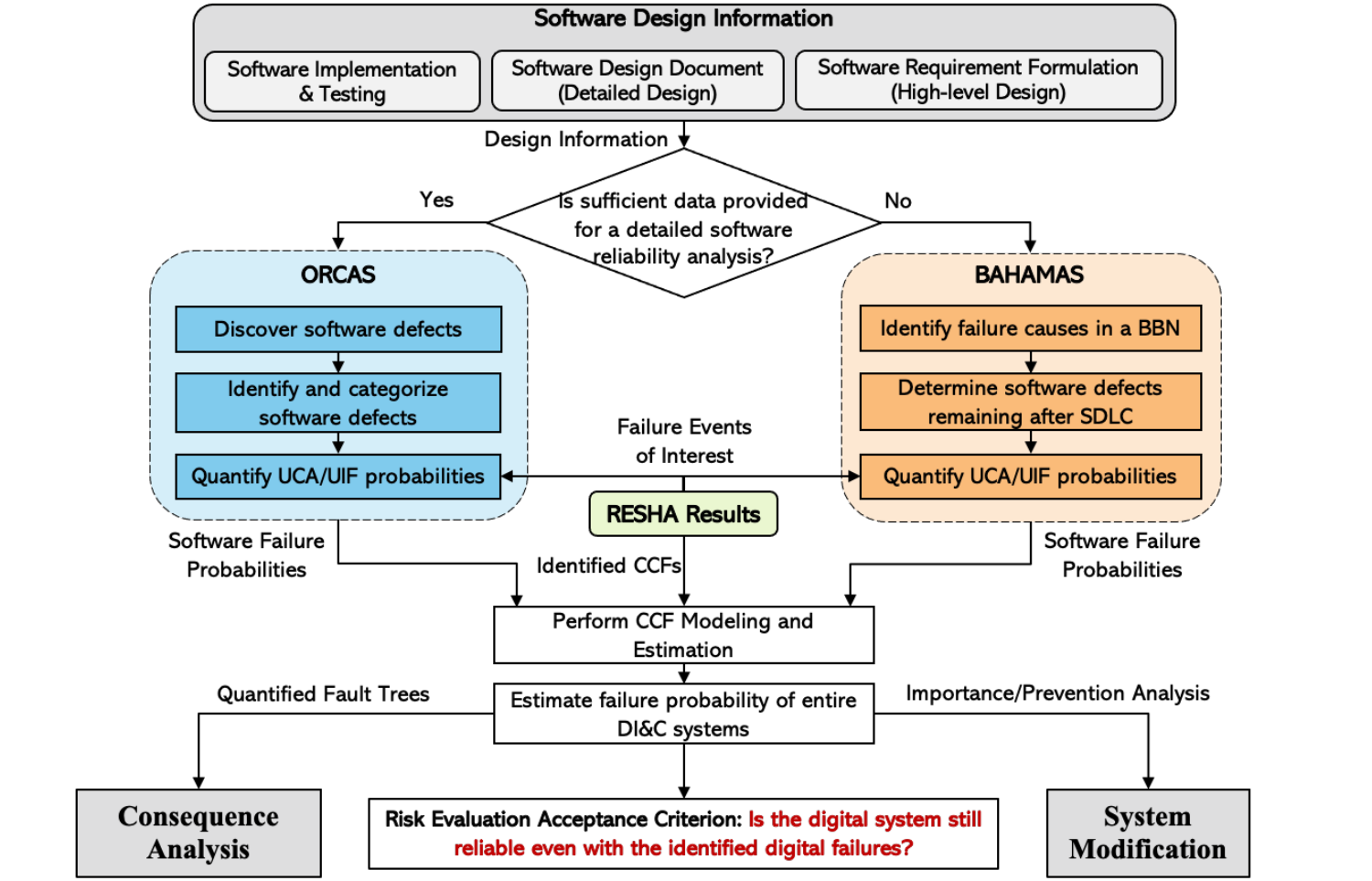
- Incorporates the concept of combining FTA and STPA from HAZCADS.
- Reframes STPA in a redundancy-guided way to identify various CCFs in highly redundant DI&C systems.
- Identifies and traces failures in both the actuation and information feedback pathway of DI&C systems due to unintended latent design or implementation defects or intended cyber attacks.





Workflow of the Redundant-guided System-theoretic Hazard Analysis (RESHA)

Multiscale Quantitative Reliability Analysis



BAHAMAS	Bayesian and human-reliability-analysis-aided method for the reliability analysis of software	CCF	common cause failure	RESHA	redundancy-guided systems-theoretic method for hazard analysis
		ORCAS	orthogonal-defect classification for assessing software reliability	SDLC	software development life cycle

Major Accomplishments in FY-23

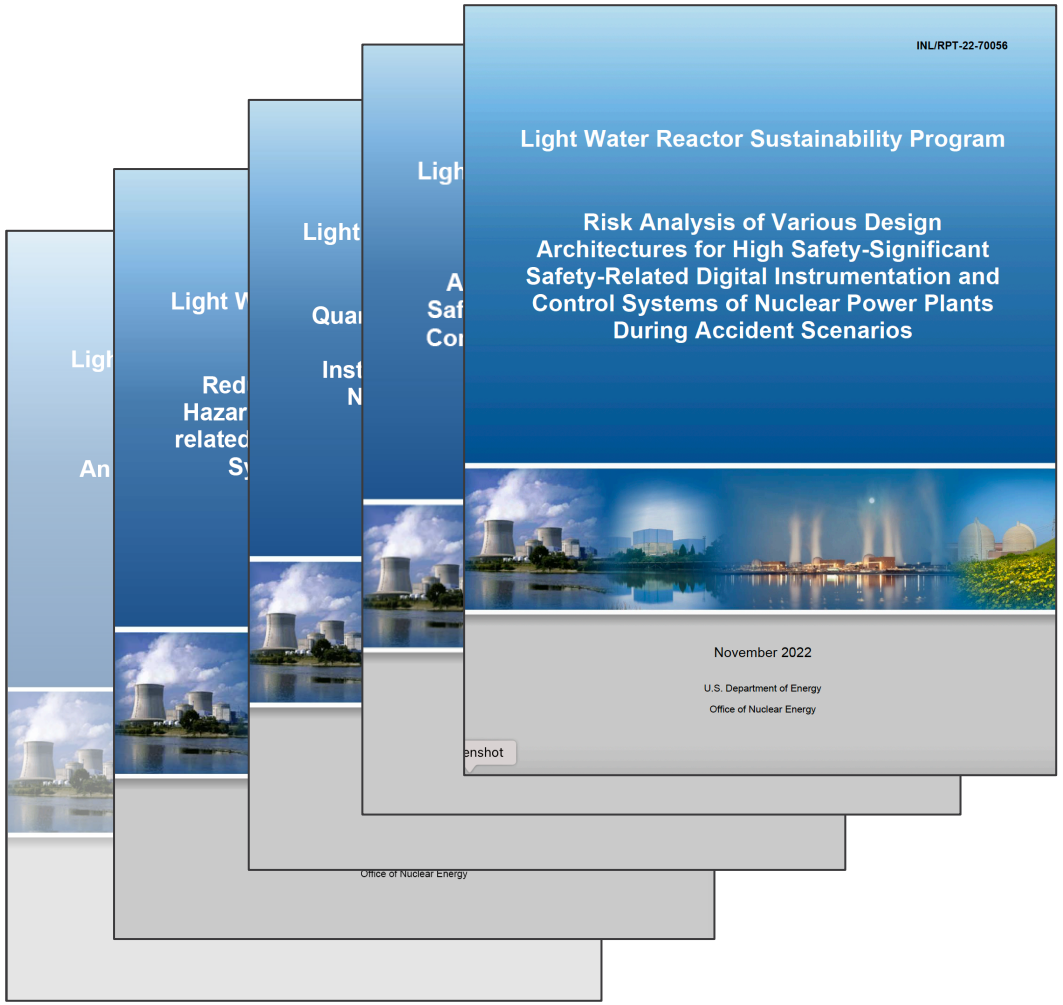
- Completed an industry peer review with reviewers from the *NRC, GEH, EPRI, and RPI*.
  - Feedbacks are positive pointing that framework addresses industry needs and closes gaps in the current state of practice.
  - Constructive suggestions are offered for methodology advancement and maturation, and integration with other toolsets (i.e., EPRI's framework) to gain the most benefits for the industry.
  - Delivered a peer review report in March 2023.

- Completed the reliability analysis of a safety-related DI&C system in collaboration with *PWROG*.
  - Feedback provided by the industrial collaborators for methodology refinement in FY-24.
  - Delivered a technical report in February 2023.

- Improved the current methods for identifying, quantifying, and evaluating potential software CCFs in highly redundant and diverse safety-related DI&C systems in collaboration with university partners.
  - Will deliver a technical report in September 2023.

Publications

- Published 6 journal articles, 7 milestone technical reports, 15 conference papers.



Research Activities in FY-24

- Improve and further develop the current framework and methods for risk assessment of multi-function DI&C systems in collaboration with the industry *(e.g., GE Hitachi)*.

- Refine the current methods to (1) keep supporting the need of DI&C reliability analysis from the industry *(e.g., PWROG);* (2) align better with international standards and existing risk-informed approaches and guides *(e.g., EPRI)*.

- Develop capabilities on risk-informed evidence generation and evaluation to support DI&C safety assurance and design optimization with the industry and other research institutions *(e.g., Halden and KAERI)*.

- Develop novel approaches to inform risk management and design optimization of advanced (semi-) autonomous DI&C systems designed for existing LWR fleets. *(with NCSU and KAERI)*

Collaborations

- **Industry:**
  - PWROG: DI&C reliability analysis and CCF evaluation
  - GE Hitachi: Risk assessment of multi-function DI&C platforms
  - Halden: DI&C hazard analysis and safety assurance

- **Universities (for new methodology exploration):**
  - University of Pittsburgh: Modeling and estimation of software CCF in safety-related DI&C systems.
  - North Carolina State University:
    - Development of a risk assessment framework for AI-aided control system designs
    - Software CCF modeling using model-based approaches.
  - Ohio State University: Software CCF modeling using dynamic methodologies.

Sustaining National Nuclear Assets

lwrs.inl.gov