Enhancement of the Use of Defense-in-Depth and Safety Margin for Decision-Making Purposes

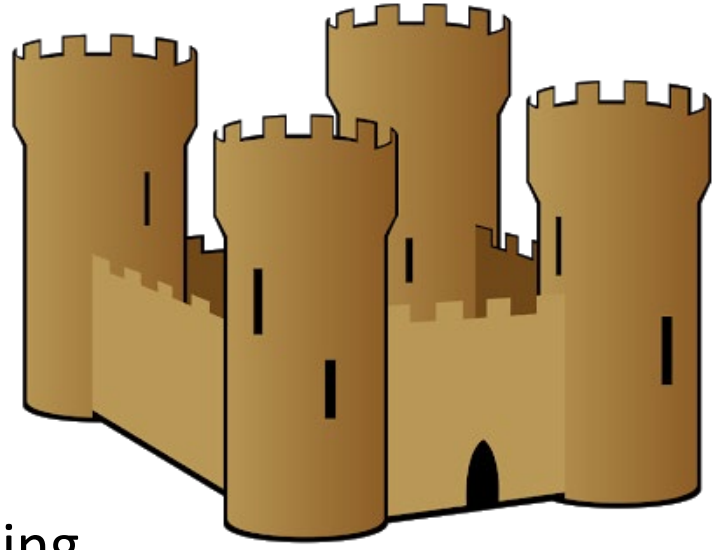
PSAM 16 Conference

Fernando Ferrante
Program Manager,
Risk & Safety Management

EPRI
June 27, 2022

Context of the Effort - Issues Challenging DID/SM in RIDM

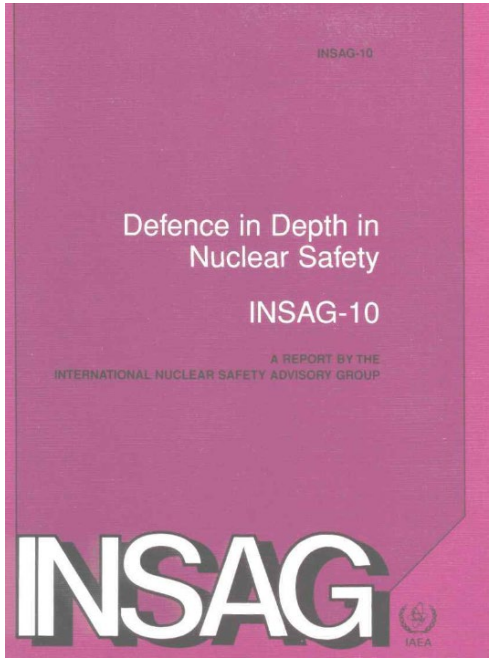
- Work in *EPRI 3002014783*, *"A Framework for Using Risk Insights in Integrated Risk Informed Decision Making (IRIDM)"* (2019) recognized DID and SM principles continued to be a challenge in RIDM applications
  - Often considered an afterthought in PRA-focused risk-informed applications
  - But can lead to challenges in applications with risk results near limits
  - Likely to be interpreted differently by deterministic/probabilistic viewpoints
  - Need to be firmly footed in plant experience, PRA modeling

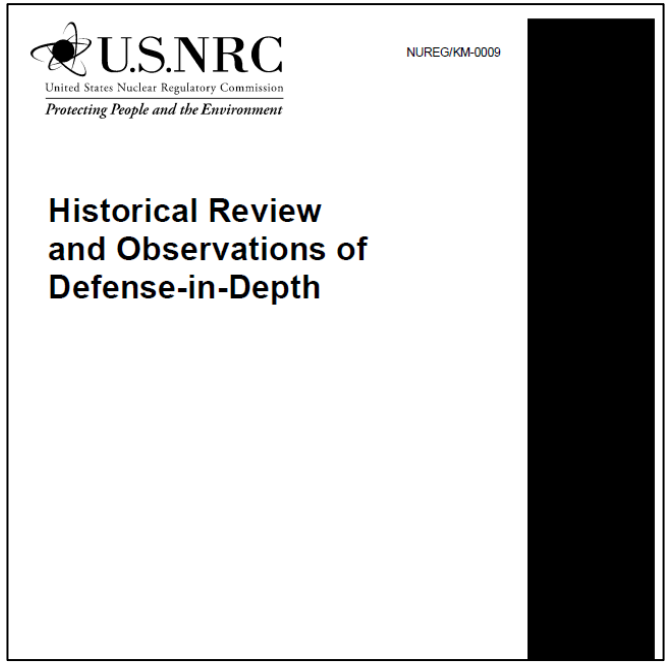


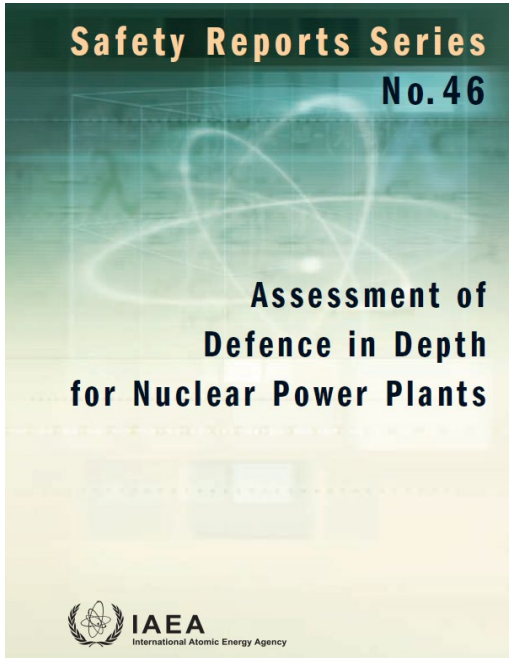
- Questions about DID and its context in RIDM continued to be raised
  - DID and SM are key principles in nuclear safety, hard to change the mindset
  - Efforts to quantify DID and SM are often not the best approach to address questions

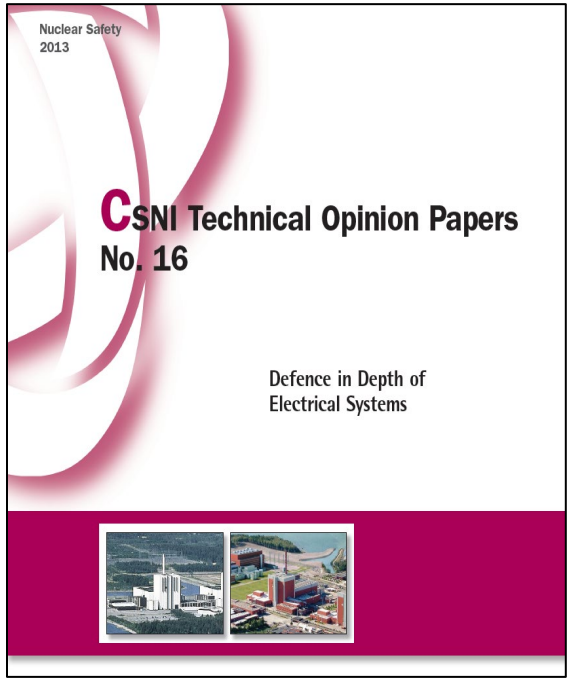
Issues Challenging DID/SM in RIDM

- View of DID/SM in RIDM has evolved through history of nuclear safety
- There are still aspects of DID/SM in RIDM that can be challenging without a proper context and a structured approach to assess them, and
- There has been significant research and proposed approaches that could drive a more efficient approach forward.







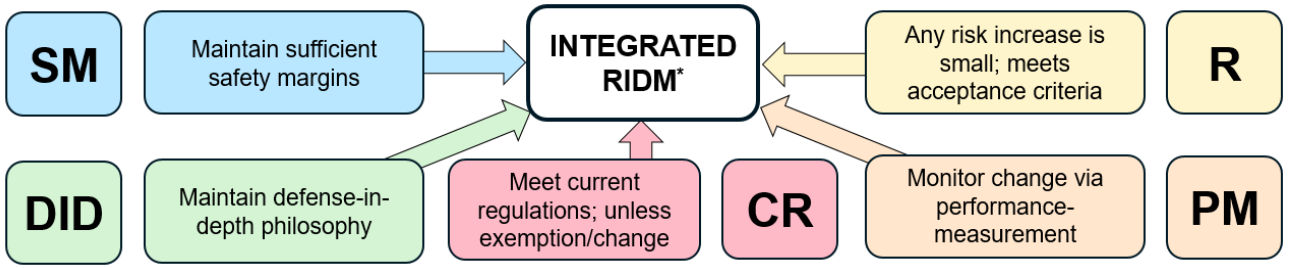


Defense in Depth in Regulatory Discussions

- IAEA-defined DID levels

DID Level	Objective	Essential Means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance feature
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedure
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

- NRC-defined DID levels according to Regulatory Guide 1.174 (for IRIDM)



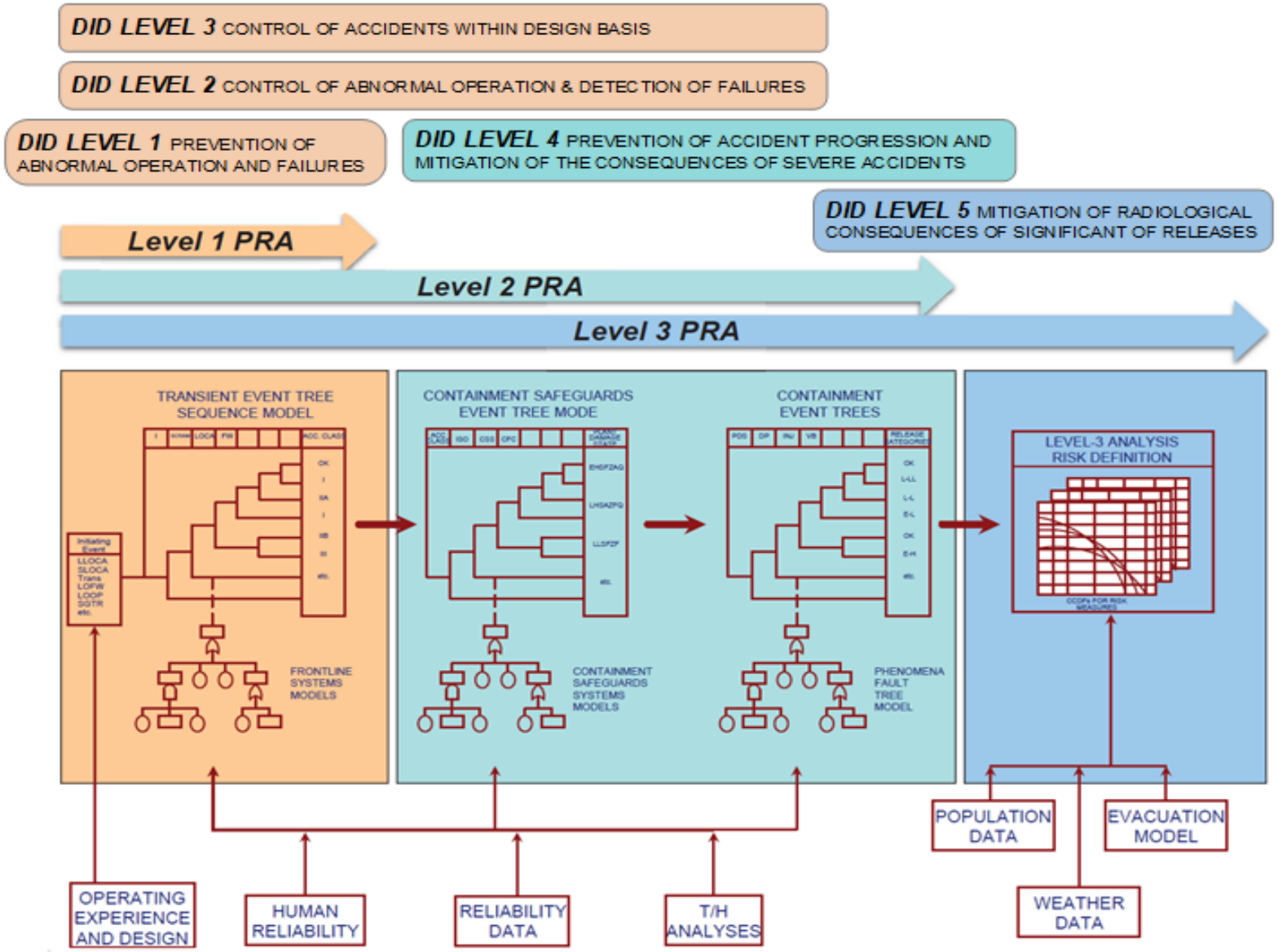
- Robust plant design to survive hazards and minimize challenges that could result in an event occurring,
- Prevention of a severe accident (core damage) if an event occurs,
- Containment of the source term if a severe accident occurs,
- Protection of the public from any releases of radioactive material (e.g., through siting in low-population areas and the ability to shelter or evacuate people, if necessary).

"Structuralist" Versus "Rationalist" View on DID

- "Structuralist" view sees DID defined in regulations and in the design of the facilities built to comply with those regulations
  - Often, DID is assumed to be defined if X, Y, Z requirements are met as prescribed by regulations, e.g., "have three layers of defense", "have alternate shutdown means"
  - PRA may be seen as not relevant ("regardless of low risk, meet requirements")

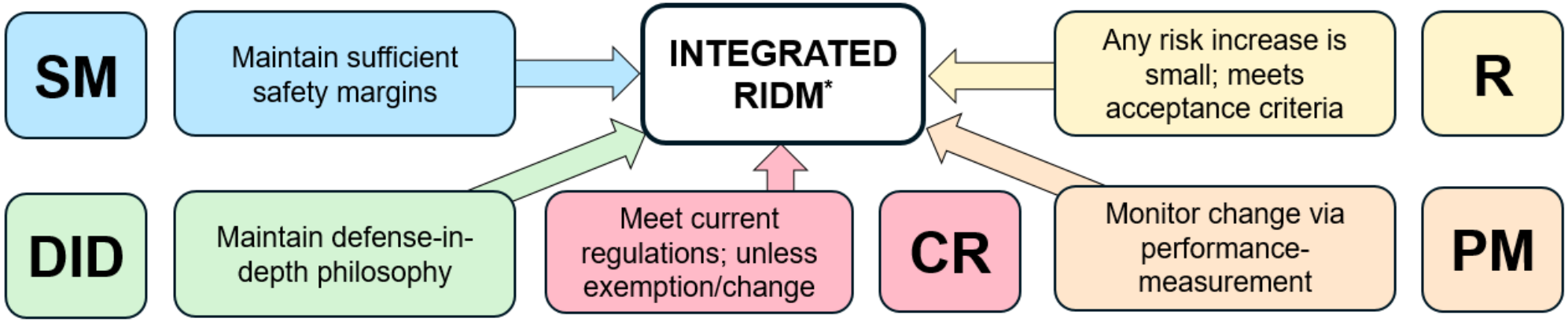
- "Rationalist" view sees DID as the aggregate of provisions made to compensate for uncertainty/incompleteness in the knowledge of accident initiation and progression in nuclear safety
  - This view recognizes that DID is met at a global level, in an aggregate sense
  - No single approach to meeting DID, different scenarios will have different DID
  - Due to uncertainty, incompleteness, there is always risk of DID failing

So, What is the Role of PRA in DID and SM?



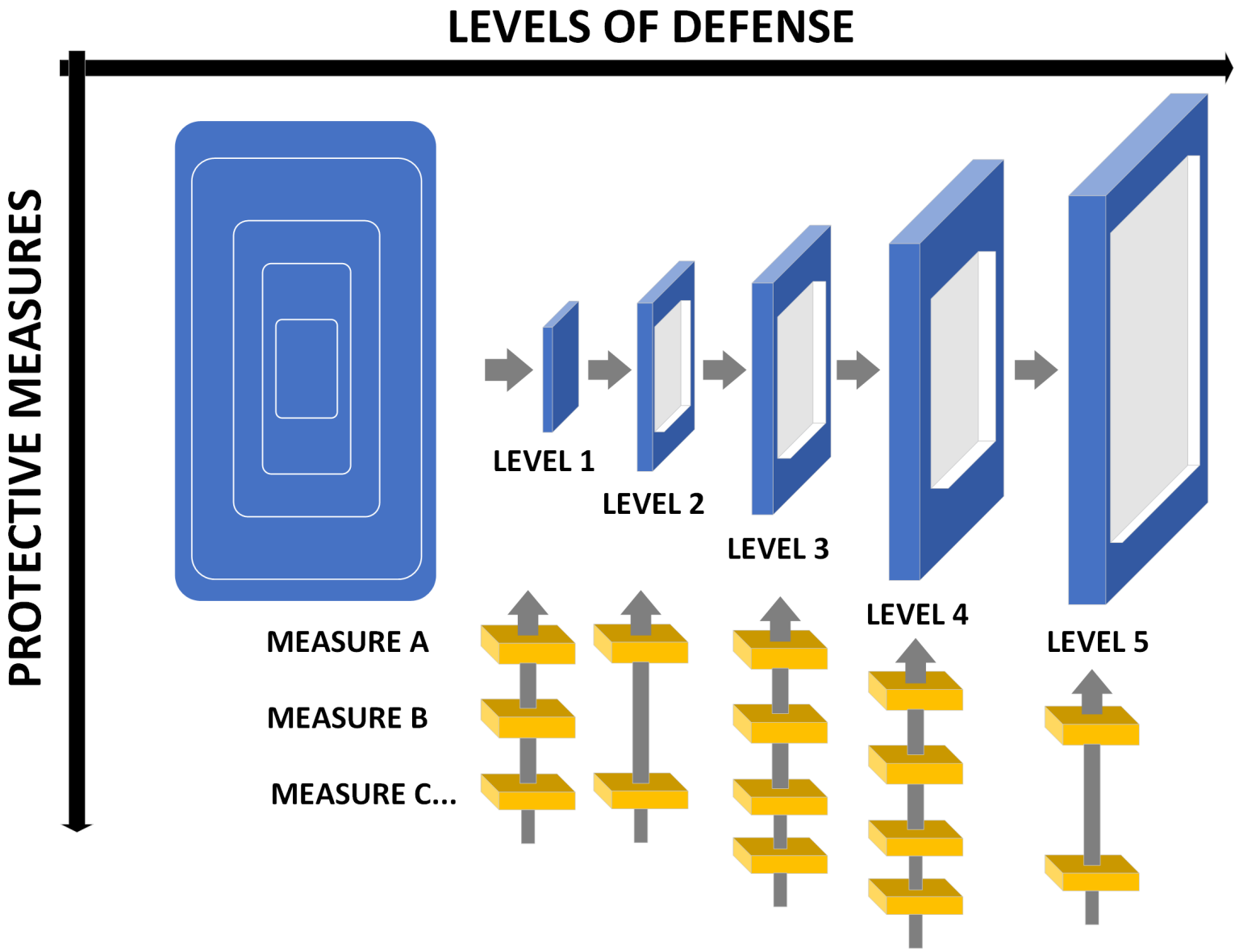
- Several deterministic inputs into DID are inputs for PRA
- Key scenarios considered for DID in licensing of NPPs are part of PRA
- Hence, PRA overlaps significantly with DID and SM
- PRA can explicitly consider what we know and don't know
- But role of PRA is not to "quantify" DID
  - Using PRA only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

So, What is the Role of SM in RIDM, DID and PRA?



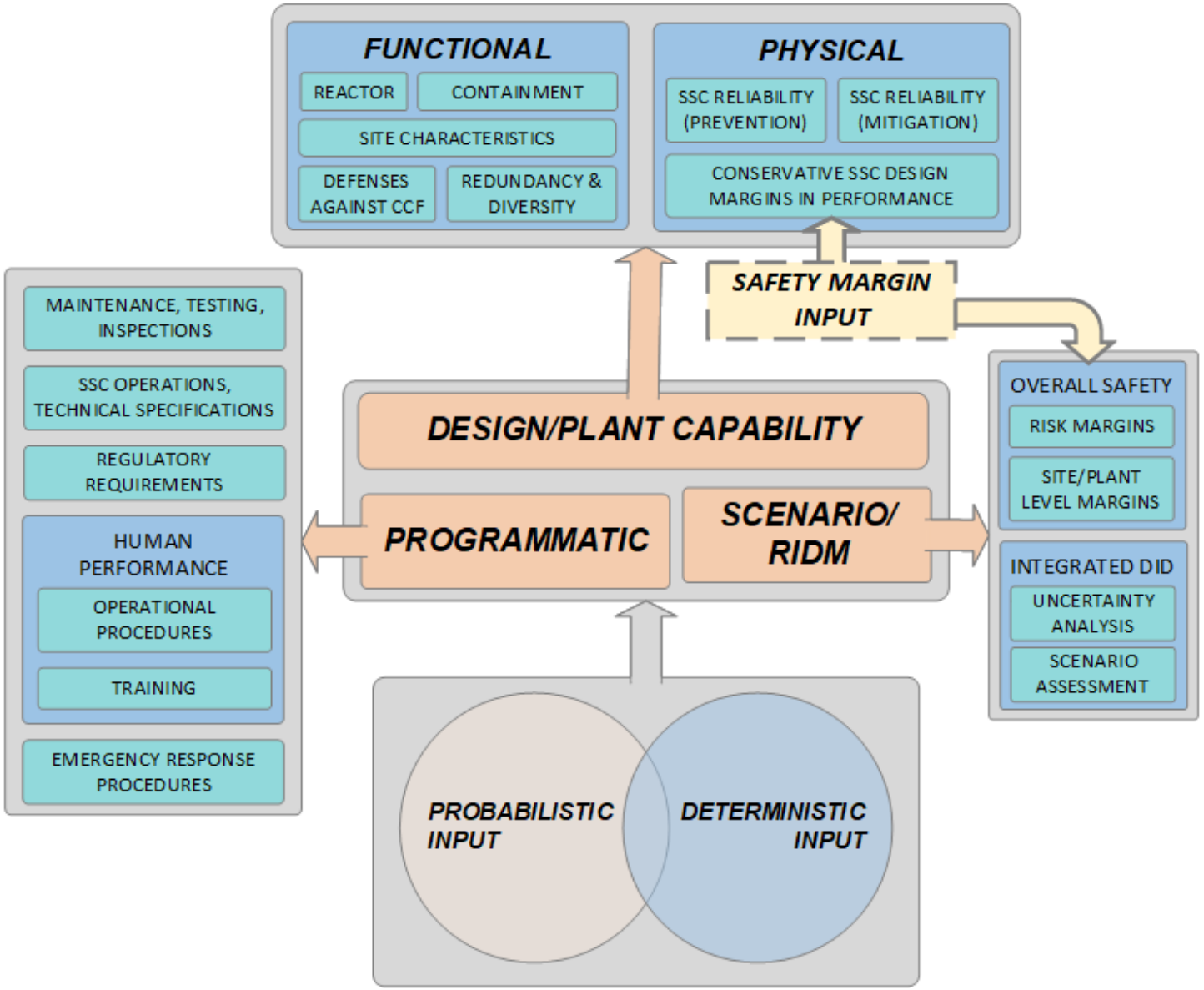
- Most of guidance in regulatory documents focuses on "meet codes/standards"
  - This is highly simplistic, incomplete, and ultimately lacking in clear guidance
- "Margin" can be deterministic or probabilistic, depending on the context
- There is no single SM that is considered in NPP applications; there are SMs met at a "localized" level, and those at a "global" level
- Fundamental insight: SM can be better leveraged as a support to DID (EPRI 3002020763 position is that is not logical to consider DID and SM separately)

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



- 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

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

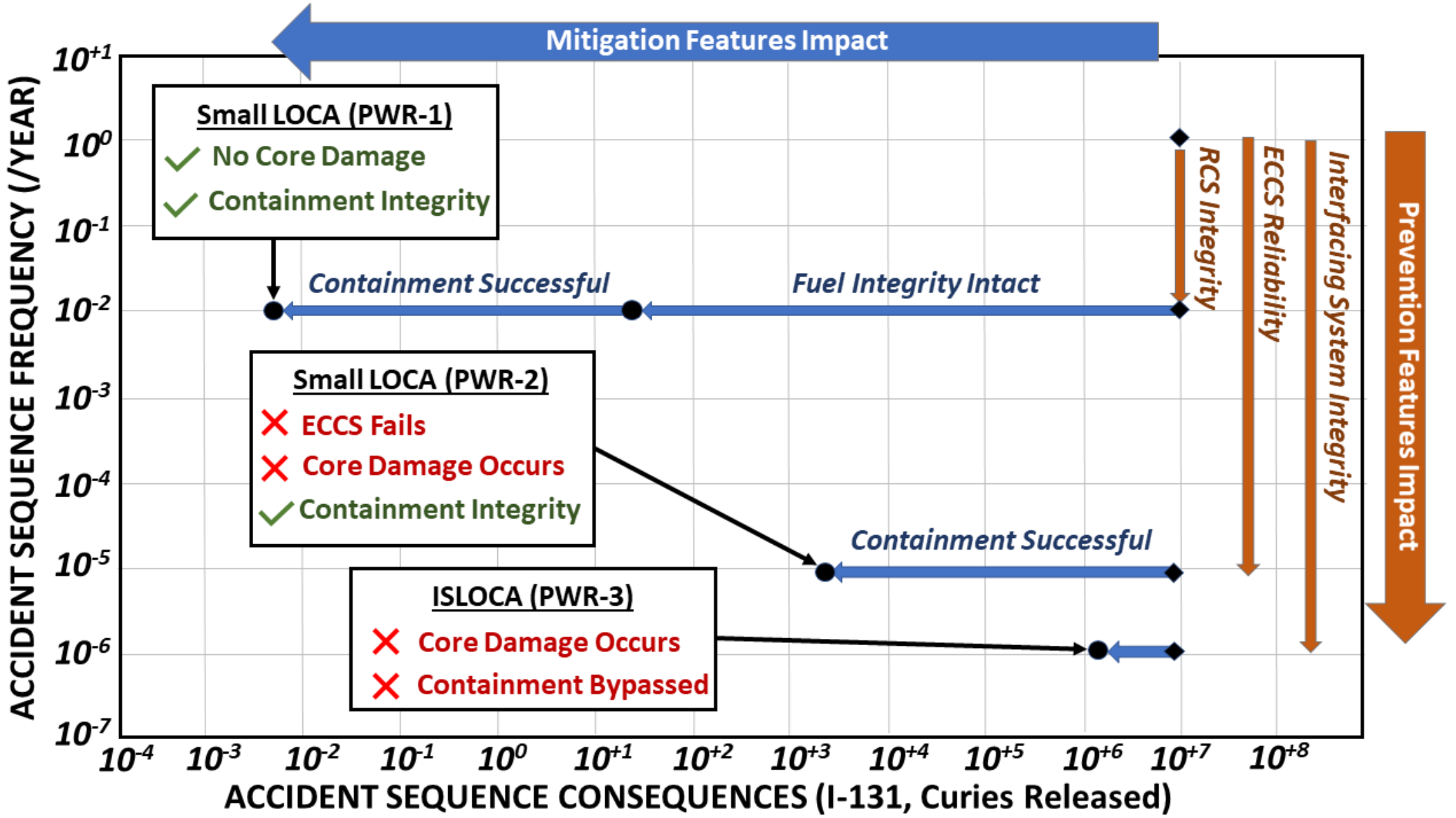

- Physical Security


- Portable Equipment

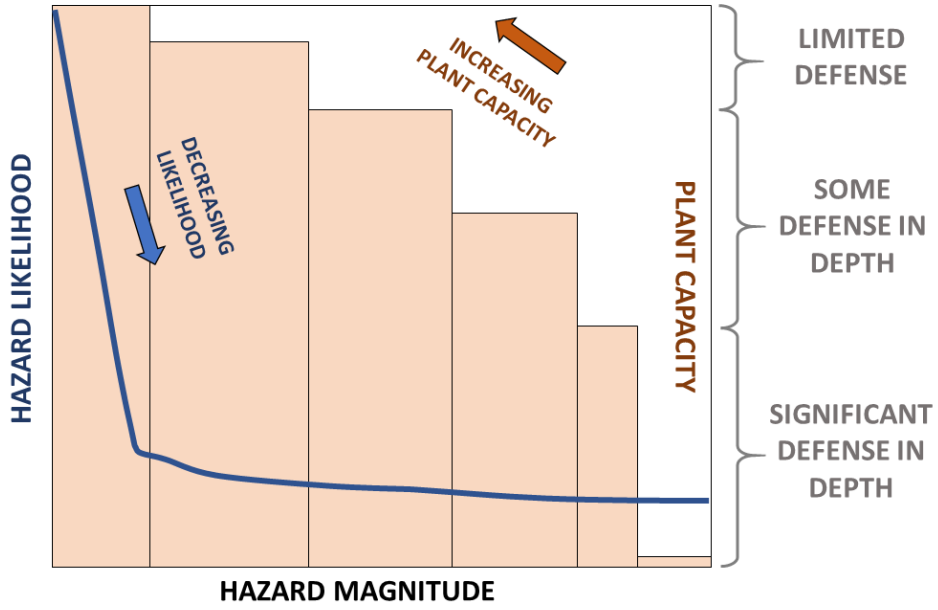

- Risk-Informed Applications

- **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)

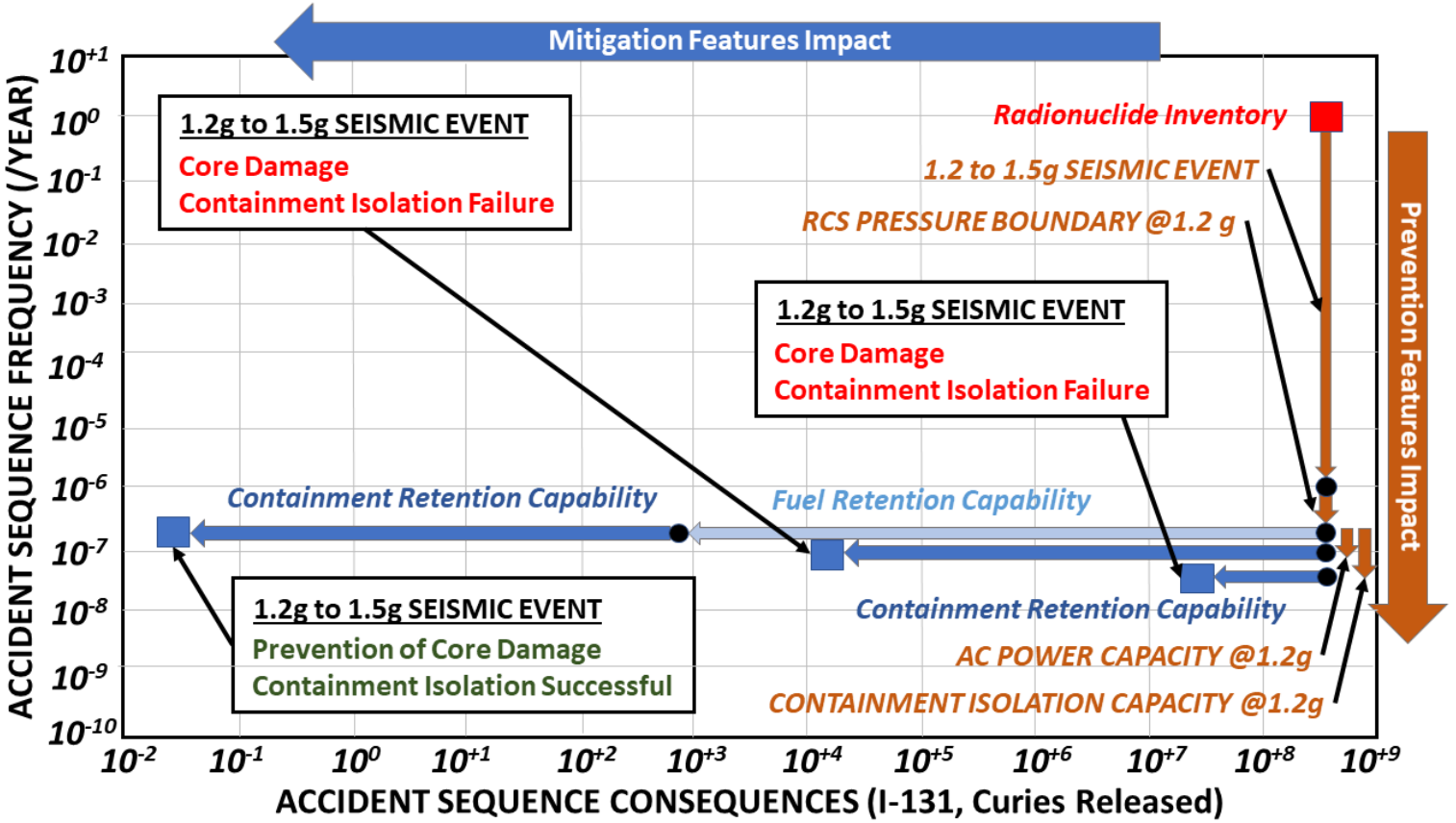
Role of Risk Insights in DID/SM for RIDM Purposes



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

Insights/Path Forward

- A more intelligent, efficient framework for consideration of DID/SM in RIDM is presented in *EPRI 3002020765*
- This is intended to support better understanding in PRA-intensive activities as well as activities where RIDM or risk assessment concepts are not yet used
- It is also intended to support countries implementing RIDM currently
- The framework presents DID/SM in a new, yet consistent manner; where the output of PRA is accounted for at the appropriate level
- Examples using an actual detailed PRA model show feasibility and value
- Future steps possible for this effort
  - Full evaluation of the framework for an NPP (with design, programmatic, scenario DID)
  - Development of an interface with visual tools in order to support activities related to Periodic Safety Review and other areas where DID/SM justifications are critical

Together…Shaping the Future of Electricity