



DID IN THE CONTEXT OF PRA REALISM

US NRC Improving PRA Realism Workshop



Fernando Ferrante
Program Manager

NRC Workshop on PRA Realism
October 2025



www.epri.com

© 2024 Electric Power Research Institute, Inc. All rights reserved.

First, Some Thoughts on “Realism” and Defense-in-Depth

- As discussed in the NRC/NEI 2023 Fall Risk Forum ([ML23254A388](#)):

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?”



First, Some Thoughts on “Realism” and Defense-in-Depth

- So, why discuss this again? Because it matters in both **fundamental**, and **nuanced ways** for critical decisions:
 - “Realistic” already depends on the context of the PRA:
 - An academic performing research on advanced PRA methods...
 - A vendor building a PRA model to inform the design for a new build...
 - A regulator checking the validity of assumptions of a licensing submittal...
 - A utility developing a PRA model submittal for a complex risk-informed application...

ALL VALID ACTIVITIES, ALL WITH DIFFERENT “REALISM” EXPECTATIONS, WITH DEGREES OF SUBJECTIVISM

- Now, let’s consider what PRA is mostly focused on; supporting risk-informed decision-making (RIDM):
 - What’s does “**PRA realism**” mean with respect to **RIDM** (and its RIDM principles)?
 - In fact, what does “**RIDM realism**” mean (or does it even mean anything)?
 - And how do the **RIDM principles** relate to “**realism**” (if at all)?

So, What does “Defense-in-Depth” really mean?

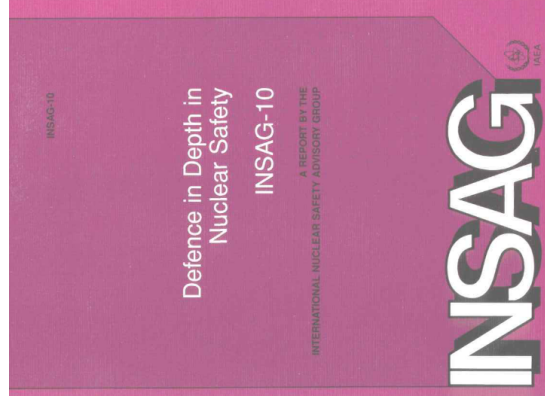
- Simple question, with a simple answer...right?

TERM AND DEFINITION	DISCUSSION
	The NRC Commission has referred to defense-in-depth as a concept that: Has always been and will continue to be a fundamental tenet of regulatory practice in the nuclear field, particularly regarding nuclear facilities. Risk insights can make the elements of defense-in-depth clearer by quantifying them to the extent practicable. Although the uncertainties associated with the importance of some elements of defense may be substantial, the fact that these elements and uncertainties have been quantified can aid in determining how much defense makes regulatory sense. Decisions on the adequacy of, or the necessity for, elements of defense should reflect risk insights gained through identification of the individual performance of each defense system in relation to overall performance. The Commission further states: Defense-in-depth is an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. The defense-in-depth philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility. The net effect of incorporating defense-in-depth into design, construction, maintenance, and operation is that the facility or system in question tends to be more tolerant of failures and external challenges.

[NUREG-2122, "Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking."](#)

So, What does “Defense-in-Depth” really mean?

- But also, view DID/SM has evolved through history of nuclear safety
- There are still aspects of DID/SM that can be challenging without a proper context and a structured approach to assess them, and
- There have been significant research and proposed approaches that could at a minimum inform, and help drive a more efficient/structured thinking



So, What does “Defense-in-Depth” really mean (wrt RIDM)?

- Simple question, with a simple answer...right?

Defense-in-Depth Formal definition requires Commission approval. (see <i>Safety Margin, Uncertainty, Rationalist, Structuralist</i>)	In a PRA, defense-in-depth is not an explicitly modeled element. Rather, the results of the PRA provide insights into defense-in-depth. Over time, various definitions have been used for defense-in-depth, including: • three barriers to contain radioactive material: fuel cladding, primary system boundary, and the containment • the use of successive measures to prevent an accident or to mitigate the consequences of an accident • the use of redundancy and diversity • implementation of the single failure criterion Regardless of its definition, defense-in-depth is an integral part of the NRC's safety philosophy. The NRC Web site Glossary (Ref. 36) defines defense-in-depth as: "An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures."
---	---

[NUREG-2122, "Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking."](#)

“Structuralist” Versus “Rationalist” View on DID

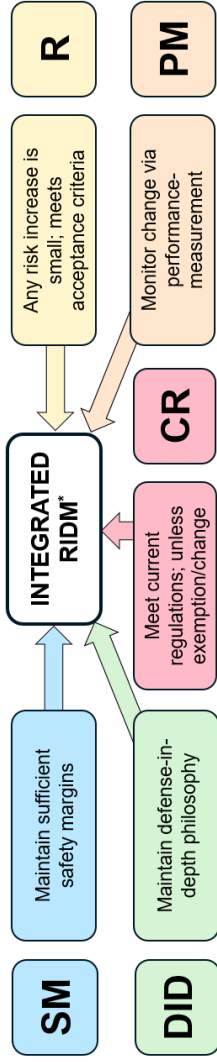
- “Structuralist” view sees DID defined in regulations and in the design of the facilities built to comply with those regulations
 - Often, DID is assumed to be defined if X, Y, Z requirements are met as prescribed by regulations, e.g., “have three layers of defense”, “have alternate shutdown means”
 - 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

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).

Nexus between DID/SM and RIDM aspects

- DID/SM are closely associated with RIDM but not one single, one size-fits-all concept:



- Internal events – more traditionally tied to the physical DID barriers



- Internal fire – e.g., early fire detection, manual suppression, fire brigade, fire barriers



- Internal flooding - consider detection of leaks, flooding, barriers



- Seismic Events – consider seismic-related reactor trip capabilities, structural integrity, treatment of seismic correlation



- External Flooding – forecasting, external flood barriers, internal flood barriers



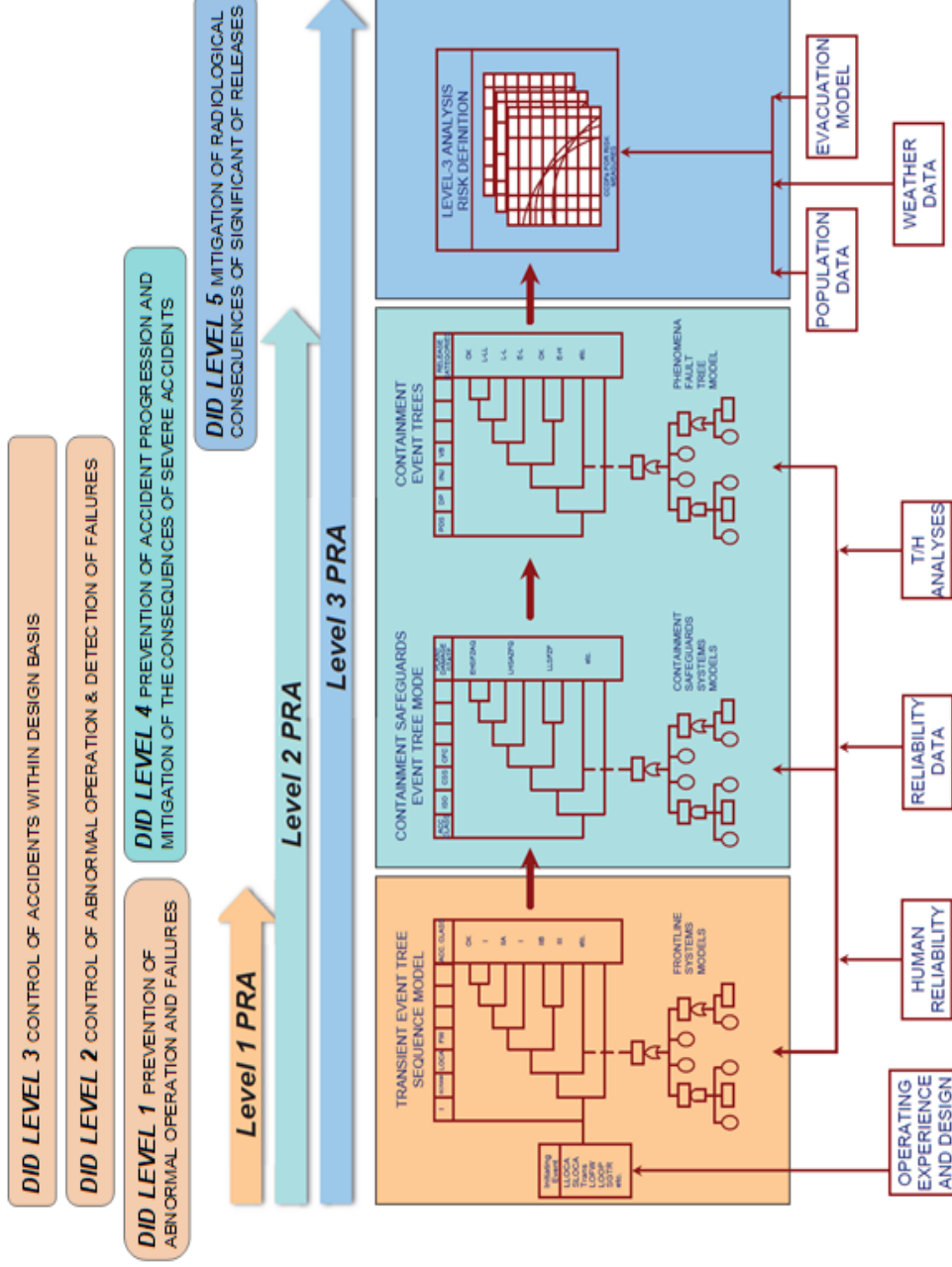
- Multi-unit accidents– consider aspects not covered by single unit considerations



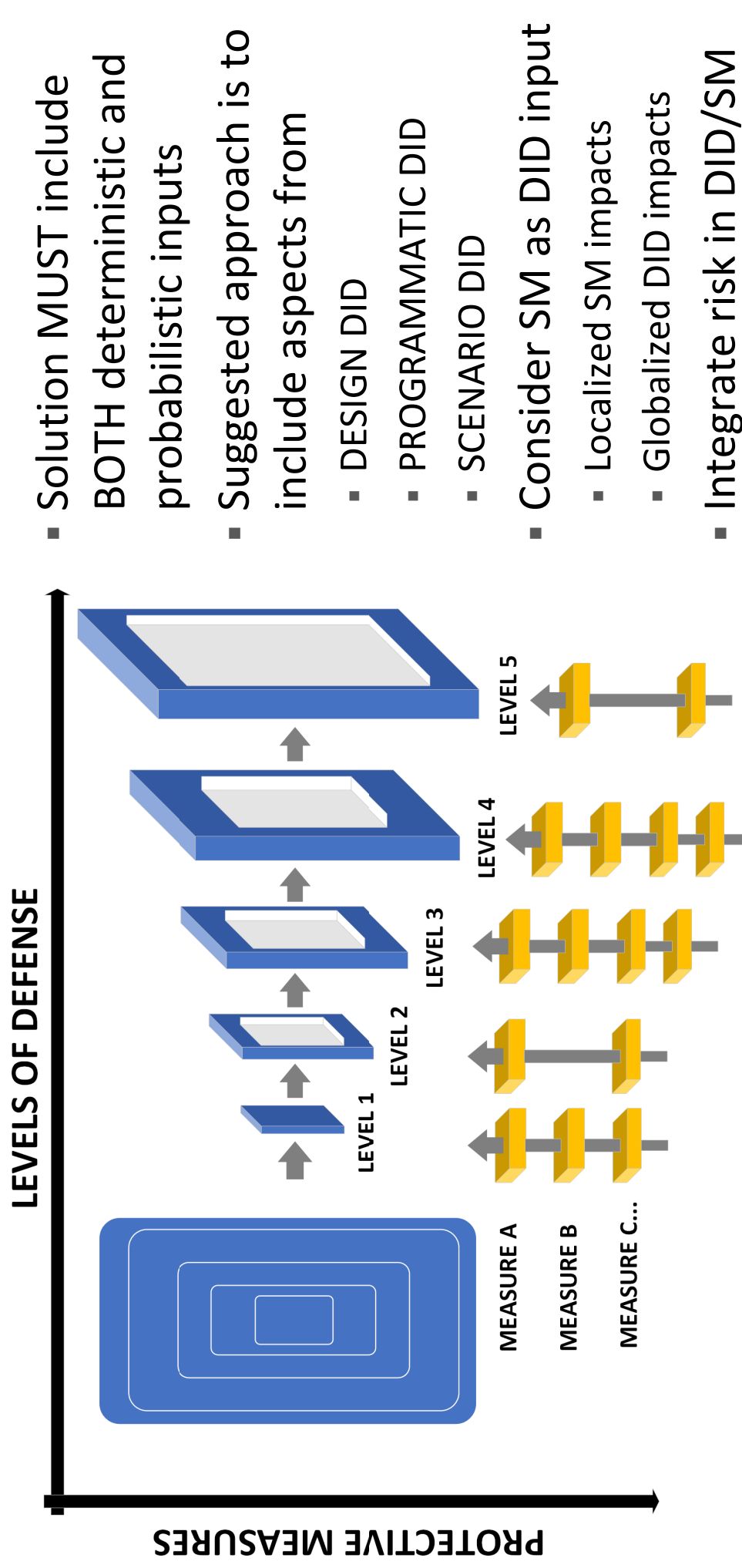
- Consider Spent Fuel Pool (SFP) and dry cask storage DID aspects

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

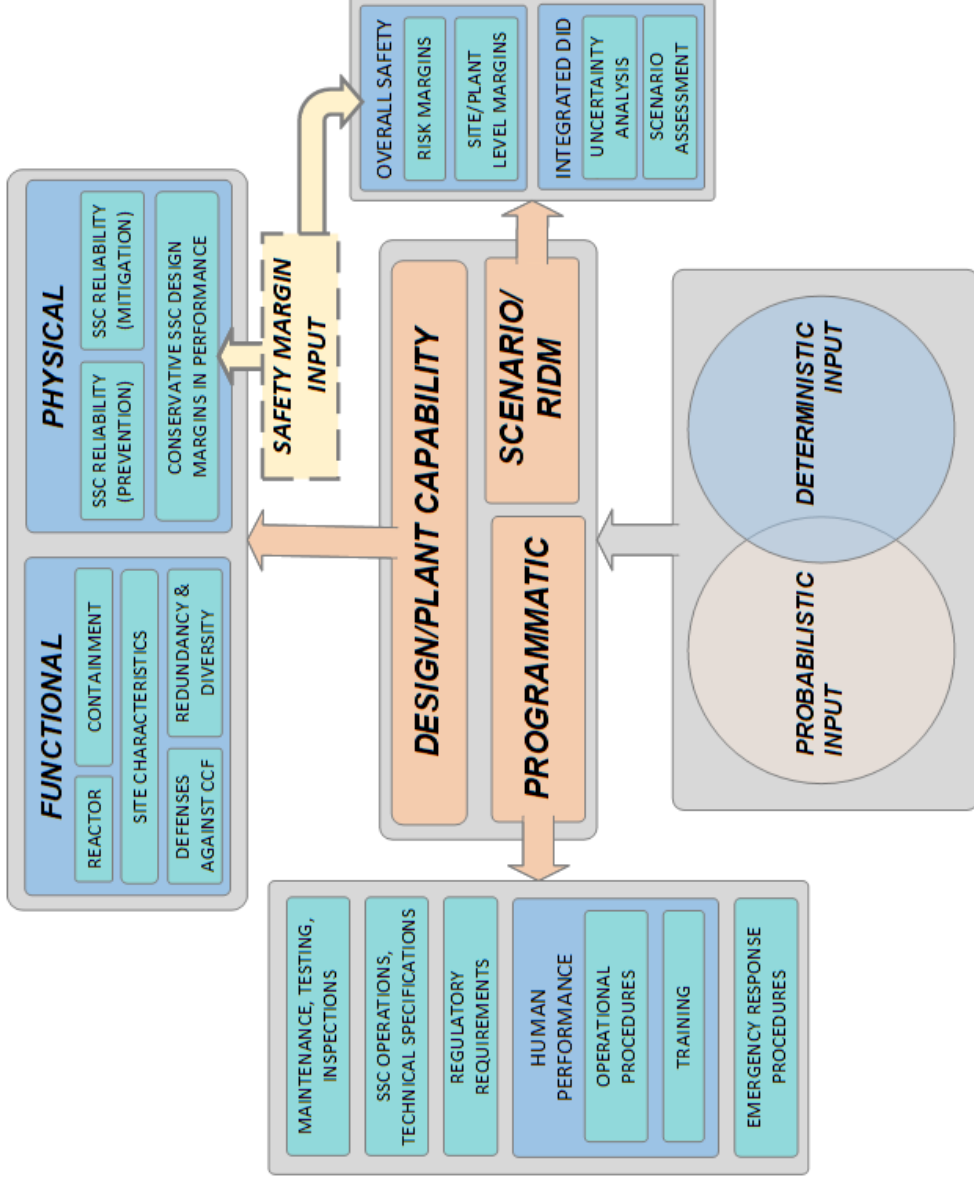
- Several deterministic inputs into DID are inputs for PRA
- Key scenarios considered for DID in licensing of NPPs are part of PRA
- Hence, PRA overlaps significantly with DID and SM
- PRA can explicitly consider what we know and don't know
- But role of PRA is not to “quantify” DID
 - Using PRA only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



Using a Structured “Thinking” to DID/SM and RIDM



Using a Structured “Thinking” to DID/SM and RIDM



- 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

Using a Structured “Thinking” to DID/SM and RIDM

- EPRI 3002020765 discusses DID/SM in RIDM for multiple areas:

	▪ Internal events		▪ Dry Cask Storage
	▪ Internal fire		▪ Digital Instrumentation & Control
	▪ Internal flooding		▪ Shutdown Risk
	▪ Seismic Events		▪ Periodic Safety Reviews
	▪ External Flooding		▪ Physical Security
	▪ Multi-unit accidents		▪ Portable Equipment
	▪ Spent Fuel Pool (SFP)		▪ 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)

Summary

- DID/SM continue to be a fundamental concept; intent of this discussion is **NOT** to suggest:
 - *“PRA results should be a measure of DID/SM”*
 - *DID/SM aspects are “less important” if the “risk is low”*
 - *Questions on DID/SM are not important in RIDM*
- What this discussion is intended to do is to suggest that:
 - If RIDM use and expansion is to **continue to progress forward**, then a structured understanding of DID/SM role can help both **PRA-intensive activities** AND **areas with RIDM elements but less PRA-intensive reliance** to be focused on “realistic” aspects
- A potential benefit, for example, can be to consider in more detail:
 - The role of DID/SM within RIDM with respect to, for example, **material-related** issues and/or **DI&C-related aspects**
 - To help clarify where **key questions** and **critical assumptions** need to be probed
 - To clear up in part the concern with the “*unknown unknowns*” or the potential perception that DID/SM in RIDM are a “*bring me a rock*” issue



TOGETHER...SHAPING THE FUTURE OF ENERGY®



www.epri.com

© 2024 Electric Power Research Institute, Inc. All rights reserved.