Review and Evaluation of Defense-in-Depth

Presented by
Mary Drouin
Office of Nuclear Regulatory Research
1-15-15

Defense-in-Depth History

- Earliest discussion on reactor defense-in-depth (DID) dates back to 1957 and WASH-740, “Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants.”
- Since that time, numerous discussions on DID can be found in the literature.
  - Literature review includes reactor, materials, waste, security and international literature

DID Discussions

- A strategy to ensure public safety given there exists both unquantified and unquantifiable uncertainty in engineering analyses (both deterministic and risk assessments)
- To prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility
- Maintaining multiple barriers against radiation release, and by reducing the potential for, and consequences of, severe accidents
- Use of conservative codes and standards
- Programmatic activities as compensatory measures; system redundancy, independence, and diversity;
- No key safety functions will depend on a single element (i.e., SSC or action) of design, construction, maintenance or operation
- Appropriate safety margins are provided
- 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

Historical Review and Evaluation

- To better understand the history, review the history and group observations by the following:
  - Why is DID needed?
  - What is DID attempting to achieve?
  - What is the approach or structure used for DID?
  - What actions or strategy are used to achieve DID?
  - How DID adequacy determined?

Why is DID Needed?

- Ultimate purpose is to compensate for uncertainty
- An element of U.S. Nuclear Regulatory Commission's (NRC's) safety philosophy that is used to address uncertainty
- A safety philosophy intended to deliver a design that is tolerant to uncertainties
- To compensate for the recognized lack of knowledge of nuclear reactor operations and the consequences of potential accidents

⇒ Agreement in that defense-in-depth is needed to compensate for uncertainties; uncertainties regarding

- the basic design and operation of the "facility"
- knowledge in the performance of SSCs and operator actions under various facility conditions
- various phenomena, etc.
- the "unknown" (i.e., unknowns events and phenomena that are unanticipated because of lack of knowledge and therefore may not be addressed in the design or operation of the facility)

What is DID Attempting to Achieve?

- reducing the potential for, and consequences of, severe accidents
- prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility
- prevent the release of radioactive material to the environment
- to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials
- to prevent, contain, and mitigate exposure to radioactive material

⇒ General agreement in that defense-in-depth is to avert damage to protect the public from harm by preventing and mitigating accidents

Structure Used for DID?

- provide multiple barriers to the escape of radioactive material
- maintaining multiple barriers against radiation release
- all safety activities . . . are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large
- ensures that successive measures are incorporated . . . primarily by means of a series of barriers which would in principle never be jeopardized, and which must be violated in turn before harm can occur to people or the environment

⇒ Agreement in that DID is comprised of multiple layers of defense. This concept is described using different terminology; for example, layers of defense, lines of defense, echelons of defense, protective barriers, and successive measures.

Strategies to Achieve DID?

- redundant elements, provision for periodic in-service testing, and other features to enhance performance and reliability
- extensive and comprehensive quality assurance programs are required and used to assure the integrity of each line of defense and to maintain the different lines as nearly independent as practicable
- selection of proper materials, quality controls in fabrication of components, rigorous systems of inspection and testing, appropriate techniques and controls in workmanship

⇒ Agreement in that strategies involve specific principles (or measures involving design, operational or programmatic features) that are to be used in accomplishing the various layers of defense.

- The strategies are program area specific
- Many of the principles or measures are similar such as redundancy, independence, diversity, no reliance on a single element

How is DID Adequacy Determined?

- the adequacy . . . should reflect risk insights gained through identification of the individual performance of each defense system in relation to overall performance
- adequate if the overall redundancy and diversity among the plant's systems and barriers is sufficient to ensure the risk acceptance guidelines . . . are met
- adequacy via a process that uses a PRA to assess the acceptability of uncertainties and uses identified options (such as increasing performance monitoring) to determine the acceptability of the uncertainties or refine the design

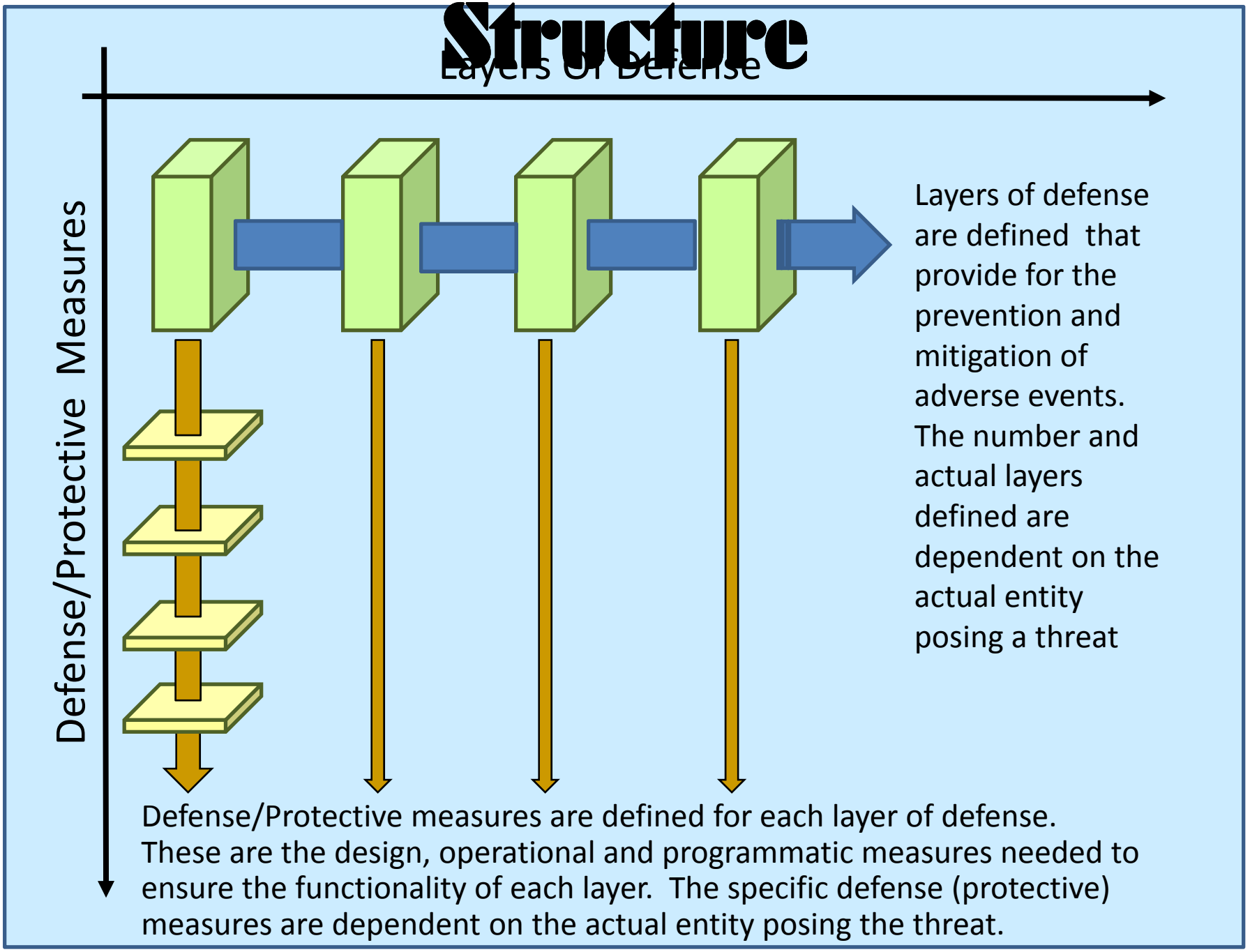
⇒ The various criteria defined for determining adequacy of defense-in-depth all use risk as the main criteria; for reactors, example criteria include

- propose that the elements (e.g., layer of defense) should be quantified,
- risk is used to access each defense system (e.g., safety measure)
- compensatory measures can be graded in order to reduce risk
- any sequence (given all defense layers have failed) remain under a frequency consequence curve
- redundancy and diversity is sufficient to ensure risk guidelines or met
- assessing the adequacy via a process that uses a PRA

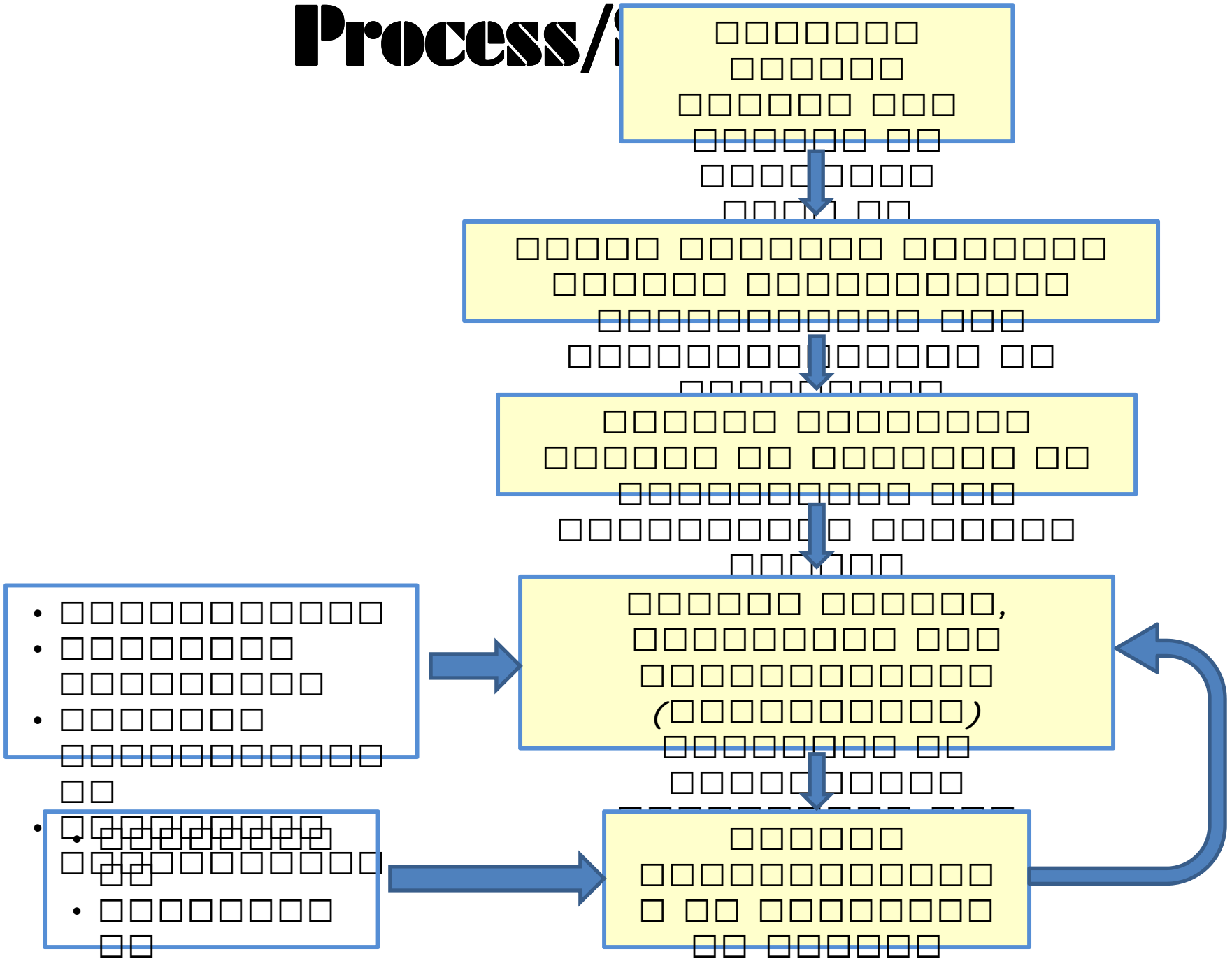
Generic/General Statement on DID

Defense-in-depth is an approach to developing and maintaining a regulatory structure that ensures necessary protective features are in place such that the operation of the entity (e.g., nuclear facility) poses no undue risk to the public. This structure is based on both preventing the occurrence of adverse events and mitigating the consequences if the events were to occur

Generic Defense-in-Depth Structure

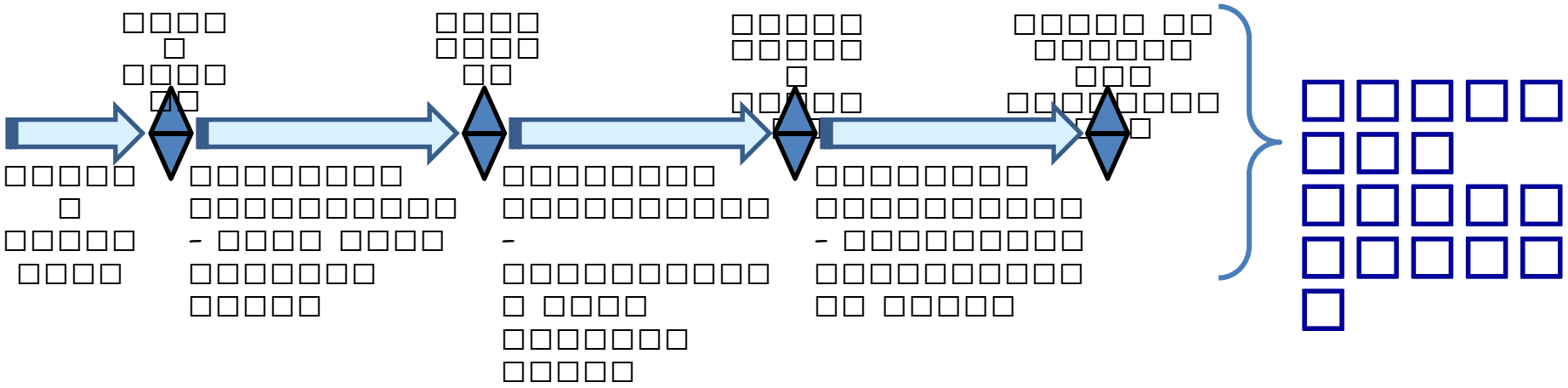


Defense-in-Depth Process/

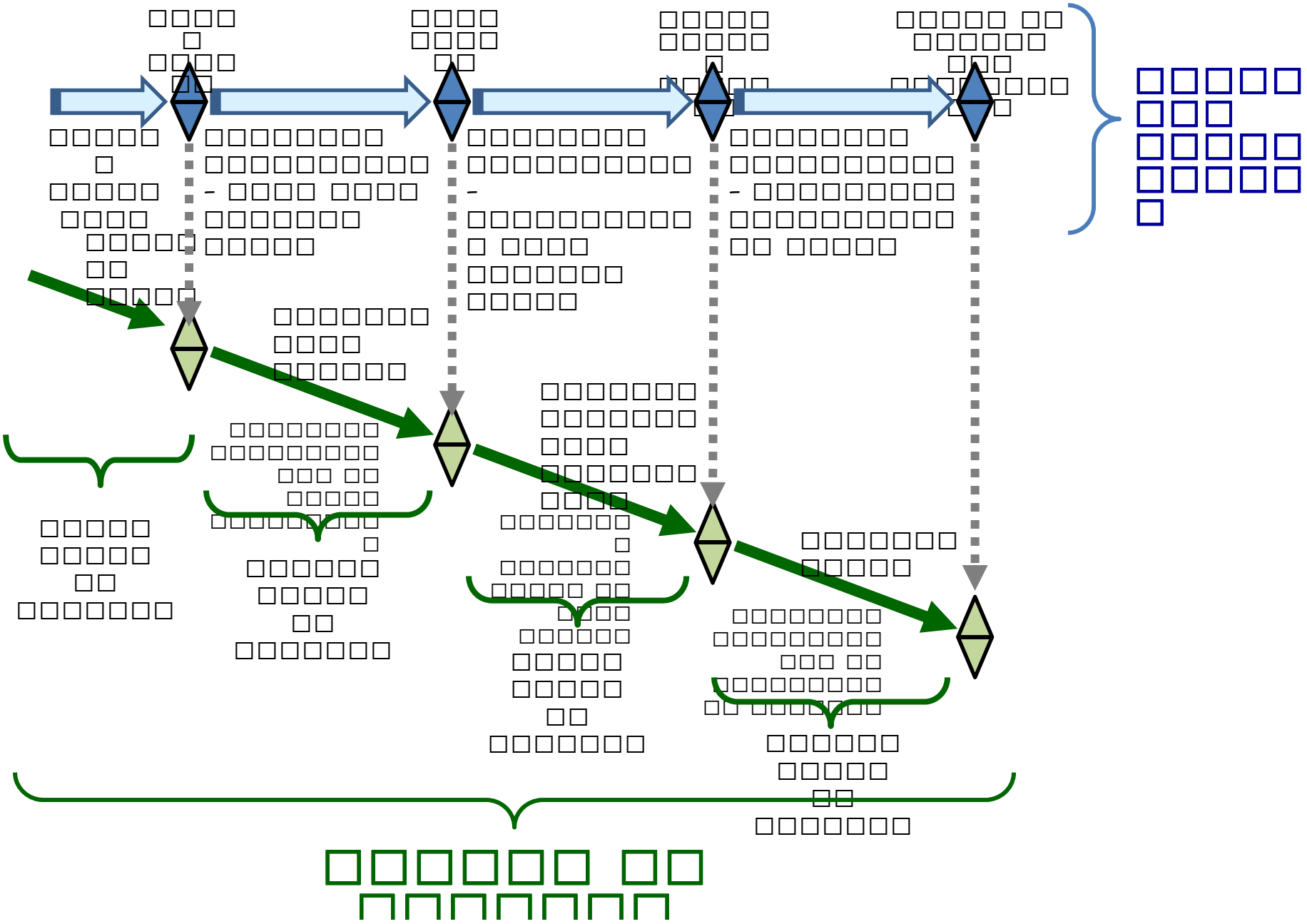


REACTOR EXAMPLE APPLICATION

Layers of Protection Applied with Accident Progression (1 of 4)



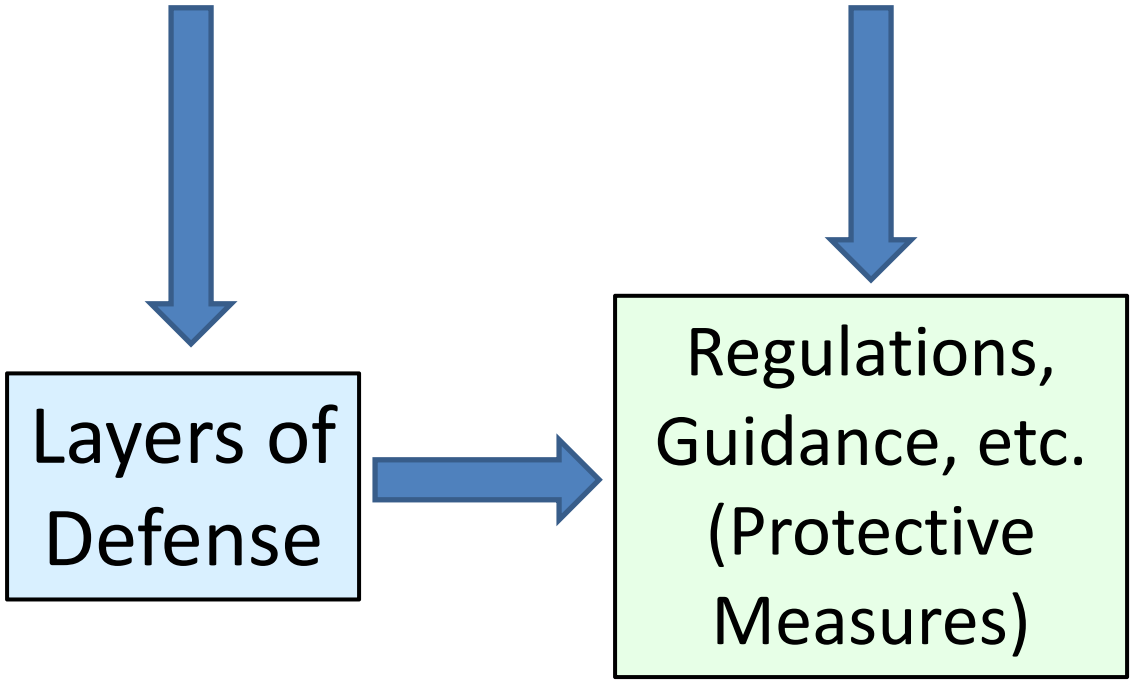
Layers of DID Aligned with Accident Progression (2 of 4)



Layers of DID Aligned with Accident Progression (3 of 4)

Defense-in-Depth Principles

- Measures against intentional as well as inadvertent events
- Appropriate barrier capability
- Key safety functions not dependent upon a single element of design or operation
  - Redundancy, diversity, independence
- Siting to facilitate protection of public health and safety
- Uncertainties accounted for in safety analyses
  - Safety margins



Layers of DID Aligned with Accident Progression (4 of 4)