Technical Session TH27 – Defense-in-Depth: A Historical Perspective within a Dynamic Regulatory Framework

"Historical Review and Evaluation of Defense-in-Depth"

Mary Drouin
Office of Nuclear Regulatory Research
March 12, 2015

Outline

- Background
- Defense-in-depth history
- Review and evaluation of DID history
- High level observations
- Reactor example DID application
- Path forward

Background

- SECY-13-0132, Enclosure 3 provided an historical review and evaluation of defense-in-depth (DID)
- Commission SRM: Enshrine Enclosure 3, "Defense-in-Depth Observations and Detailed History," as an agency knowledge management tool and republish in other formats to make it more widely available
- NUREG being developed
  - More complete historical review of reactors, materials, waste, security, international and other organizations being performed

Defense-in-Depth History

- Earliest discussion on reactor 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

4

Literature Review

- WASH-740
- Joint Committee on Atomic Energy Hearings
- Internal Study Group
- ECCS Hearings
- WASH-1250
- Post TMI Definitions and Examples
- NUREG/CR-6042
- Commission Policy Statements
- MIT Speech by Chairman Jackson
- Commission White Paper
- Some Thoughts on Defense-in-Depth by Tom Kress
- PSA '99 paper
- ACRS letters (2002 thru 2011)
- Joint ACNW/ACRS Subcommittee
- IAEA Documents (INSAG-3, 10, & 12, TECDOC-1570, SF-1, SSR-2/1)
- 10 CFR Part 50, Appendix R
- A Risk-Informed Defense-in-Depth Framework for Existing and Advanced Reactors, Karl Fleming, Fred Silady
- 10 CFR Part 30-39, 50, 60, 61, 63, 70-73
- NEI 02-02
- Petition on Davis Besse
- Remarks by Chairman Diaz
- Digital Instrumentation and Controls (NUREG/CR-6303, RG 1.152, NUREG-0800 BTP HICB-91, NUREG-0800 SRP BTP 7-19, DI&C-ISG-02)
- NUREGs (1520, 1536, 1537, 1556, 1567, 1804, 1860)
- INL NGNP report
- RG 1.174 and numerous other RGs
- NRC glossary
- RMTF
- SECYs (1977 thru 2011)
- OECD NEA/CNRA/CSNI Workshop

5

Small Sample of DID Statements

- 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

6

Historical Review and Evaluation

- To better understand the perspectives on DID, observations from historical review grouped 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 strategies are used to achieve DID?
  - How is DID adequacy determined?

7

Why is DID Needed?

- General agreement in that defense-in-depth is needed to compensate for uncertainties; uncertainties regarding, for example,
  - 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)

8

What is DID Attempting to Achieve?

- General agreement in that defense-in-depth is to avert damage to protect the public from harm by preventing and mitigating accidents
- For example,
  - Prevent release of radioactive material
  - Mitigate exposure to radioactive material

9

Structure Used for DID?

- General 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, multiple barriers, protective barriers, successive measures, etc.
- No agreement on process or criteria used to determine the actual layers (or multiple barriers)

10

Actions to Achieve DID?

- General agreement in that actions or strategies involve specific principles and protective 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, use of codes and standards, quality assurance, safety margins, monitoring

11

How is DID Adequacy Determined?

- No criteria or acceptance guidelines defined for determining whether adequate DID has been established or if DID has been violated
  - What is an acceptable set of layers of defense?
  - What is an acceptable set of principles?
  - What is an acceptable set of protective measures?
  - How to balance among the layers and protective measures?
- Literature does suggest that criteria should include risk as a factor in determining adequacy; for example,
  - 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

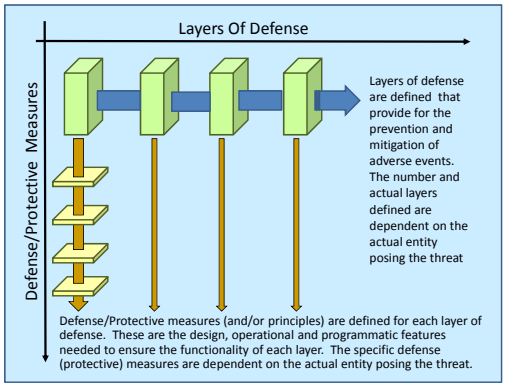
12

Example General Statement on DID

Defense-in-depth is an approach to developing and maintaining a regulatory structure comprised of multiple layers of defense that include the necessary protective features to ensure that the risk to the public is maintained acceptably low. This structure is based on layers of defense that both prevent the occurrence of adverse events and mitigate the consequences if the events were to occur.

13

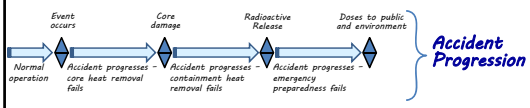
Generic Defense-in-Depth Framework



REACTOR EXAMPLE APPLICATION

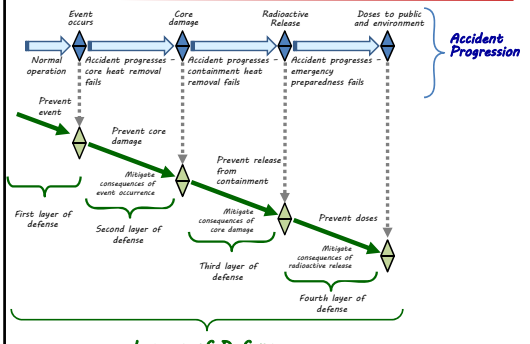
15

Reactor Example DID Framework (1 of 4)



16

Reactor Example DID Framework (2 of 4)



17

Reactor Example DID Framework (3 of 4)

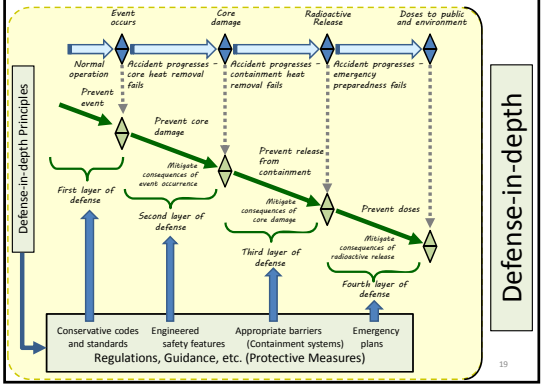
Defense-in-Depth Principles/Protective Measures

- Measures against intentional as well as inadvertent events
- 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
- Engineered safety features
- Emergency plans
- Equipment qualifications
- Appropriate barrier capability

Layers of Defense → Regulations, Guidance, etc.

18

Reactor Example DID Framework (4 of 4)



19

Path Forward

This calendar year:

- Complete draft NUREG
- Issue draft NUREG for public review and comment
- Publish final NUREG

20