ENCLOSURE 3: DEFENSE-IN-DEPTH OBSERVATIONS AND DETAILED HISTORY ML13277A421

DISCUSSION

Coming to an understanding of defense-in-depth, it is necessary to understand the importance of this "philosophy" or "process." That is, why defense-in-depth is essential to a regulatory structure that is designed to provide for adequate protection of the public health and safety. A major part of this understanding is also understanding the objective of defense-in-depth; that is, what is defense-in-depth attempting to accomplish. Additional aspects of understanding defense-in-depth involves defining an approach for accomplishing the objective, criteria for the approach, and criteria for ensuring adequate defense-in-depth has been achieved. These five "elements" of defense-in-depth, therefore, include:

- The need for defense-in-depth
- The objective of defense-in-depth (i.e., what is defense-in-depth attempting to accomplish)
- The approach or strategy used to achieve the goal of defense-in-depth
- The criteria used to implement the approach or strategy of defense-in-depth
- The criteria for determining whether there is adequate defense-in-depth

In reviewing the history on defense-in-depth (see Appendix A) and trying to understand the different perspectives, if indeed there are different perspectives, one can see that there are actually common themes. There are common themes regarding specific issues, for example, uncertainties, accident prevention, accident mitigation, multiple barriers, redundancy, and emergency preparedness. However, how these themes are classified differ. That is, while the actual views may be similar, whether the view is stating, for example, why is defense-in-depth needed or what is the objective of defense-in-depth, differs. Therefore, in reviewing the history, the views are summarized and grouped according to the above five elements, and discussed below.

The need for defense-in-depth

In reviewing the various sources regarding the first element of defense-in-depth, understanding why there is a need for defense-in-depth, the following statements are found:

- guard against unwanted events
- compensating for uncertainty in probabilistic analyses
- related to the issue of uncertainty
- the aggregate of provisions made to compensate for uncertainty and incompleteness in the knowledge of accident initiation and progression
- compensation for inadequacies, incompleteness, and omissions of risk analyses
- a strategy to ensure public safety given the unquantified uncertainty in risk assessments

- a strategy to ensure public safety given there exists both unquantified and unquantifiable uncertainty in engineering analyses (both deterministic and risk assessments)

- application of deterministic design and operational features for events that have a high degree of uncertainty

- ultimate purpose is to compensate for uncertainty (e.g., uncertainty due to lack of operational experience with new technologies and new design features, uncertainty in the type and magnitude of challenges to safety)

- 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 in knowledge of plant behavior, component reliability, or operator performance that might compromise safety

- to compensate for the recognized lack of knowledge of nuclear reactor operations and the consequences of potential accidents

The objective of defense-in-depth

In reviewing the various sources regarding the next element of defense-in-depth, understanding what is its objective; that is, what defense-in-depth is attempting to accomplish, the following statements are found:

- to protect the plant, the plant operators, and the health and safety of the public

- guarding against unwanted events

- ensure the protection of public health and safety

- reducing the potential for, and consequences of, severe accidents

- to increase the degree of confidence in the results of the probabilistic risk assessment (PRA) or other analyses supporting the conclusion that adequate safety has been achieved

- the probability of accidents must be acceptably low

- to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility

- if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large

- preventing the release of radioactive material to the environment

- averting damage to the plant

- the facility or system in question tends to be more tolerant of failures and external challenges

- to provide several levels or echelons of defense to challenges to plant safety, such that failures in equipment and human error will not result in an undue threat to public safety

- 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

The approach or strategy used to achieve the goal of defense-in-depth

In reviewing the various sources regarding the approach or strategy to achieve the goal of defense-in-depth, the following statements are found:

- three basic lines of defense: (1) superior quality in design, construction and operation, (2) accident prevention safety systems, and (3) consequences-limiting safety systems

- the greatest emphasis should be placed on the first line of defense, i.e., on designing, constructing, testing and operating a plant so that it will perform during normal and abnormal conditions in a reliable and predictable manner

- the principal defense is through the prevention of accidents

- three lines of defense: (1) prevention of accidents, (2) protective systems are provided to take corrective actions, and (3) engineered safety features to mitigate the consequences of postulated serious accidents

- multiple barrier approach

- three successive protective barriers: (1) preventing initiation of incidents (conservative design margins, etc.), (2) capability to detect and terminate incidents, and (3) protecting the public.

- the key elements are accident prevention, safety systems, containment, accident management, and siting and emergency plans.

- emphasize features such as containment, siting in less populated areas, and emergency planning as integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy

- maintaining multiple barriers against radiation release, and by reducing the potential for, and consequences of, severe accidents

- explains defense in depth by stating that "all safety activities, whether organizational, behavioral or equipment related, 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”

- depth ensures that successive measures are incorporated into the design and operating procedures for nuclear installations

- the strategy for defense-in-depth is twofold: first, to prevent accidents and, second, if prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions. Accident prevention is the first priority. . .

- five levels of defense are defined such that if one level fails, the subsequent level comes into play: (1) prevention of abnormal operation and system failures; (2) control of abnormal operation and detection of failures; (3) control of accident within the design basis; (4) control of severe conditions including prevention of accident progression and mitigation of the consequences of a severe accident; and (5) mitigation of the radiological consequences of significant external releases of radioactive materials

- the principle of defense-in-depth is implemented 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

- three layers of defense against the consequences of an event at a nuclear facility. The three layers are: (1) protection to prevent accidents from occurring, (2) mitigation of accidents if they occur, and (3) emergency preparedness to minimize the public health consequences of releases if they occur

The criteria used to implement the approach or strategy of defense-in-depth

In reviewing the various sources regarding the criteria to implement the approach or strategy to achieve the goal of defense-in-depth, the following statements are found:

- the keys to achievement of this objective are quality and quality assurance, independently and concurrently; the work must be done well and then checked well, in order for the chance for errors and flaws to be reduced to an acceptable level.

- 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

- provide multiple barriers to the escape of radioactive material, from whatever cause, and to withstand the occurrences of natural forces . . . without compromising these barriers

- selection of proper materials, quality controls in fabrication of components, rigorous systems of inspection and testing, appropriate techniques and controls in workmanship.

- the requirement of high standards of engineering practice in design for critical components and systems

- regularly scheduled equipment checks and maintenance programs; prompt and thorough investigation and correction of abnormal events, failures or malfunctions

- the requirements of sound and well defined principles of good management in operation; a competent and well-trained staff, clearly assigned duties, written procedures, checks and balances in the procedures for revisions, periodic internal audits of operations, etc.

- redundancy in controls and shutdown devices; emergency power from independent sources—sometimes in triplicate—and emergency cooling systems

- containment building itself, building spray and washdown system, building cooling system . . ., and an internal filter-collection system

- the structuralist model asserts that defense-in-depth is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations.

- provide for defense-in-depth through requirements and processes that include design, construction, regulatory oversight and operating activities; additional defense-in-depth shall be provided through the application of deterministic design and operational features for events that have a high degree of uncertainty with significant consequences to public health and safety

- programmatic activities as compensatory measures; system redundancy, independence, and diversity; potential for common-cause failure (CCF); reliance on plant operators; and intent of the plant's design criteria

- no key safety functions will depend on a single element (i.e., SSC or action) of design, construction, maintenance or operation; the key safety functions include (1) control of reactivity, (2) removal of decay heat, and the functionality of physical barriers to prevent the release of radioactive materials.

- appropriate safety margins are provided

- containment functional capability

The criteria for determining whether there is adequate defense-in-depth

In reviewing the various sources regarding the criteria to whether adequate defense-in-depth has been achieved, the following statements are found:

- risk insights can make the elements of defense-in-depth more clear by quantifying them to the extent practicable

- 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

- in order to assure a proper balance between accident prevention and accident mitigation, the mean frequency of containment failure in the event of a severe core damage accident should be less than 1 in 100 severe core damage accidents

- severe core-damage accident should not be expected, on average, to occur . . .; containment performance . . . such that severe accidents . . . are not expected to

occur . . .; the goal for offsite consequences should be expected to be met after conservative consideration of the uncertainties . . .”

- the rationalist is: (1) establish quantitative acceptance criteria, such as the quantitative health objectives, core damage frequency and large early release frequency, (2) analyze the system using PRA methods to establish that the acceptance criteria are met, and (3) evaluate the uncertainties in the analysis, especially those due to model incompleteness, and determine what steps should be taken to compensate for those uncertainties

- the various compensatory measures taken for the purposes of defense-in-depth can be graded according to the risk posed by the activity, the contribution of each compensatory measure to risk reduction, the uncertainties in the risk assessment, and the need to build stakeholders trust.

- the ultimate objective is that any credible accident sequence, even considering the failures of lines of protection for the different levels of defense-in-depth, remain under the overall frequency consequence curve.

- defense-in-depth is adequate if the overall redundancy and diversity among the plant’s systems and barriers is sufficient to ensure the risk acceptance guidelines discussed in . . . . are met

- assessing the 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

OBSERVATIONS

In reviewing the history of defense-in-depth, there appears to be a general consensus among the five elements.

Regarding why defense-in-depth is needed, there is a common recognition that there is a lack of knowledge (or uncertainty) with regard to the design, construction, maintenance and operation of the facility. In answering the first question of why there is a need for defense-in-depth, it is to address the uncertainties in the design, construction, maintenance and operation of the nuclear facility.

Regarding the objective of defense-in-depth, there is a common recognition that because there is a lack of knowledge (or uncertainty) with regard to the design, construction, maintenance and operation of the facility, the objective of defense-in-depth is to avert damage to the plant thereby ensuring the protection of public health and safety while maintaining an acceptably low probability of accidents.

Regarding the approaches or strategies that have been defined for defense-in-depth, there are similar concepts of basic protections which involve, at a high level, prevention of accidents and mitigation of accidents. Prevention of accident can be defined as preventing the occurrence of an event to preventing the progression of an accident sequence. Mitigation of an accident can be defined from ending the progression of a severe accident, containing the effects of a severe accident, to mitigating the consequences of a severe accident. This approach or strategy is similar to the concept of multiple barriers which are achieving the same goal.

Regarding the criteria for implementing the approaches or strategies that have been defined for defense-in-depth, there are very similar criteria that include, for example, quality assurance, redundancy, independence, oversight, containment, emergency planning.

APPENDIX A

HISTORICAL BACKGROUND SUMMARY ON DEFENSE-IN-DEPTH

A summary of the variety of positions regarding defense-in-depth is provided in this Appendix. The documents summarized include:

- WASH-740
- Joint Committee on Atomic Energy Hearings
- Internal Study Group
- ECCS Hearings
- WASH-1250
- 10 CFR Part 60
- Post TMI Definitions and Examples
- NUREG/CR-6042
- Commission Policy Statements
- NUREG-1537
- MIT Speech by Chairman Jackson
- Commission White Paper
- Some Thoughts on Defense-in-Depth by Tom Kress
- PSA '99 paper
- ACRS letters
- 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 §50.69, 73.54, 73.55, 70.64, 73 Appendix C, Part 100
- 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)
- NUREG-1860
- INL NGNP report
- RG 1.174 other RGs
- NRC glossary
- RMTF
- SECYs
- OECD NEA/CNRA/CSNI Workshop

WASH-740, 1957 [Ref 1]

The earliest definition of defense-in-depth appears to be in WASH-740, "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants," includes the following, which can be considered defense-in-depth since it talks about "multiple lines of defense:"

"Looking to the future, the principle on which we have based our criteria for licensing nuclear power reactors is that we will require multiple lines of defense against accidents which might release fission products from the facility."

"Should some unfortunate sequence of failures lead to destruction of the reactor core with attendant release of the fission product inventory within the reactor vessel, however expensive this would be to the owners, no hazard to the safety of the public would occur unless two additional lines of defense were also breached: (1) the integrity of the reactor vessel; and, (2) the integrity of the reactor container or vapor shell. Accidents of sufficient violence to breach these successive lines of defense occurring concurrently with progressively unfavorable combinations of dispersive weather conditions have decreasing probabilities of occurrence."

"Thus the vapor container surrounding a reactor may be considered another line of defense for the protection of the public. These structures are not impregnable, but they are designed to be capable of confining the accidents which can be regarded as credible."

Joint Committee on Atomic Energy Hearings, 1967 [Ref 2]

The next definition of defense-in-depth, a decade later, appears to be in an April 1967 paper submitted by Clifford Beck (Deputy Director of Regulation) to the Joint Committee on Atomic Energy. In summary, the paper states:

> "For safety, three basic lines of defense are built into the physical systems of nuclear power reactor facilities,
>
> 1. The first and most important line of safety protection is the achievement of superior quality in design, construction and operation of basic reactor systems important to safety, which insures a very low probability of accidents. . . . Emphasis on this objective is reflected in:
>
>   The stress placed on selection of proper materials, quality controls in fabrication of components, rigorous systems of inspection and testing, appropriate techniques and controls in workmanship.
>
>   The requirement of high standards of engineering practice in design for critical components and systems. For example, the principles of fail-safe design, redundancy and backup, defense-in-depth, and extra margins of safety at key points are employed. The principle of defense-in-depth is illustrated by the successive barriers provided against the escape of fission products: (1) the ceramic uranium oxide fuel matrix has a very high retention capacity. . .; (2) the fuel pins are sheathed in impervious claddings of stainless steel or zirconium; (3) the fuel core is enclosed in a high-integrity, pressure-tested primary coolant system. . .; (4) a high-integrity pressure and-leak-tested containment building entirely surrounds each reactor structure.
>
>   Regularly scheduled equipment checks and maintenance programs; prompt and thorough investigation and correction of abnormal events, failures or malfunctions.
>
>   The requirements of sound and well defined principles of good management in operation; a competent and well-trained staff, clearly assigned duties, written procedures, checks and balances in the procedures for revisions, periodic internal audits of operations, etc.
>
> 2. The second line of defense consists of the accident prevention safety systems which are designed into the facility. These systems are intended to prevent mishaps and perturbations from escalating into major accidents. Included are such devices as redundancy in controls and shutdown devices; emergency power from independent sources—sometimes in triplicate—and emergency cooling systems.
>
> 3. The third line of defense consists of consequences-limiting safety systems. These systems are designed to confine or minimize the escape of fission products to the environment in case accidents should occur with the release of fission products from the fuel and the primary system. These include the containment building itself, building spray and washdown system, building cooling system . . ., and an internal filter-collection system.

Three related elements in the system of protection consist of the means for ensuring the effectiveness of these three basic lines of defense in the physical facility.

1. A major element is systematic analysis and evaluation of the proposed reactor design . . . up to and including the so-called “maximum credible accident.”

2. The system of numerous independent reviews by experts in the safety analysis and evaluation of a proposed facility by licensee experts and consultants, by the regulatory staff, the ACRS, the Atomic Safety and Licensing Boards, and the Commission.

3. A system of surveillance and inspection is the final element mentioned here. During construction and after the reactor becomes operative, surveillance is maintained by means of periodic inspections, periodic reports from the company, examination of operating records, and investigation of facility irregularities.”

Internal Study Group, 1969 [Ref 3]

Another reference to defense-in-depth occurs in the “Report to the Atomic Energy Commission on the Reactor Licensing Program,” by the Internal Study Group, June 1969. This study was initiated by the Atomic Energy Commission (AEC) in June 1968 to help assure that procedures keep pace with the rapid expansion of the nuclear industry. The study group members were appointed from the AEC staff, the Advisory Committee on Reactor Safeguards (ACRS), and the Atomic Safety and Licensing Board Panel. The report states:

"The achievement of an adequate level of safety for nuclear power plants is generally recognized to require defense-in-depth in the design of the plant and its additional engineered safety features. The degree of emphasis on defense-in-depth in the nuclear field is new to the power industry.

In seeking reliability of safety systems, there has been much attention in the nuclear field to redundancy, diversity, and quality control. As a result of the evolution of designs, and the large number of new orders for nuclear plants, questions have been raised regarding the proper balance among back-up systems with respect to the requirements of basic plant design.

The Study Group endorses the defense-in-depth concept, but believes that the greatest emphasis should be placed on the first line of defense, i.e., on designing, constructing, testing and operating a plant so that it will perform during normal and abnormal conditions in a reliable and predictable manner."

ECCS Hearings, 1971 [Ref 4]

The next historical document of interest is the testimony of the AEC Regulatory Staff at the Public Rulemaking Hearings on Interim Acceptance Criteria for Emergency Core Cooling Systems (ECCS) for Light Water Power Reactors, issued December 28, 1971. The introduction to this document includes a subsection titled “Defense-in-depth.” The testimony states:

"The safety goal, therefore, is the prevention of exposure of people to this radioactivity. This goal can be achieved with a high degree of assurance, though not perfectly, by use of the concept of defense-in-depth. The principal defense is through the prevention of accidents. All structures, systems, and components important to safety must be designed, built, and operated so that the probability of an accident occurring is very small. The keys to achievement of this objective are quality and quality assurance, independently and

concurrently. The work must be done well and then checked well, in order for the chance for errors and flaws to be reduced to an acceptable level.

However, excellent the design and execution, and however comprehensive the quality assurance, they must be acknowledged to be imperfect. As a second line of defense, protective systems are provided to take corrective actions as required should deviations from expected behavior occur, despite all that is done to prevent them. The protective systems include redundant elements, provision for periodic in-service testing, and other features to enhance performance and reliability.

Yet another defense—the third line—is provided by installing engineered safety features to mitigate the consequences of postulated serious accidents, in spite of the fact that these accidents are highly unlikely because of the first two lines of defense. Analogously to protective systems, engineered safety features are furnished with redundant elements, separate sources of energy and fluids, protection against natural phenomena and manmade accidents, and other similar elements to ensure their correct functioning in the unlikely event they are called upon.

The three separate lines of the defense-in-depth provided for power reactors are considered appropriate to reduce to an acceptable value the probability and potential consequences of radioactive releases. 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."

The same introductory section includes a subsection titled "Probability and Margins." That subsection states,

". . . the ECCS is part of the third line of defense, in the defense-in-depth concept used to ensure reactor safety. The design basis for ECCS is the postulated spectrum of Loss of Coolant Accidents [sic] (LOCAs), for which the ECCS is required to provide protection for the public. This is consistent with defense-in-depth, and we believe the provision of such protection, with this design basis, to be proper."

In addition, in a subsection titled "Conclusions," it states:

"Quality in the design, manufacture, installation and operation of the primary system is a necessary part of the defense-in-depth."

WASH-1250, 1973 [Ref 5]

Another document that was in development at the same time the above testimony was prepared is WASH-1250, "The Safety of Nuclear Power Reactors (Light Water Cooled) and Related Facilities." This document was completed in 1973.

The first chapter, "Description of Light Water Reactor Power Plants and Related Facilities," states that

"While differences in detail exist among pressurized water reactors [sic] (PWR) plants and among boiling water reactors [sic] (BWR) plants, the basic features of each type are much the same. All are massive and complex structures, designed and built to provide multiple barriers to the escape of radioactive material, from whatever cause, and to withstand the occurrences of natural forces . . . without compromising these barriers." The term "defense-in-depth" is not introduced at that point.

Chapter 2, titled “Basic Philosophy and Practices for Assuring Safety," states that

> "the basic philosophy underlying the AEC Rules of Procedure and Regulatory Standards, and underlying industrial practices . . . is frequently called a 'defense-in-depth' philosophy.” The discussion goes on to note that "Previous mention has been made of the use of multiple barriers against the escape of radioactivity . . . Of equal importance, however, is the need to assure that these barriers will not be jeopardized by off-normal occurrences . . . In this regard, the industry strives to protect the plant, the plant operators, and the health and safety of the public by application of a “defense-in-depth” design philosophy, as required within the variation allowed by the regulatory envelope of rules, procedures, criteria and standards. A convenient method of describing this "defense-in-depth" is to discuss it in the broader concept of three levels of safety."

Post-TMI Definitions and Examples, 1981 [Ref 7]

R.J. Breen, Deputy Director of Electric Power Research Institute’s (EPRI's) Nuclear Safety Analysis Center, published a paper titled "Defense-in-depth Approach to Safety in Light of the Three Mile Island Accident.” Breen refers to defense-in-depth as a "concept," and states that ". . . the principle of guarding against unwanted events by providing successive protective barriers is frequently called "defense-in-depth." Breen acknowledges that there are various ways of describing the application of defense-in-depth, and then chooses a "fairly common three level description emphasizing functions," which he lists as:

1. Preventing initiation of incidents (conservative design margins, etc.)
2. Capability to detect and terminate incidents
3. Protecting the public.

Breen then goes on to pose the question, to what extent can defense-in-depth be quantified? He notes that one of the functions of PRA, when the technology is more fully developed, is to help quantify defense-in-depth. Until that time arrives, when confronted with a long list of possible safety enhancements, the problem is to determine which activities make the greatest contribution to safety. He mentions that NRC used a point system in NUREG-660, and then goes on to describe a ranking system developed by Nuclear Science Advisory Committee (NSAC) and the Atomic Industrial Forum. The system was based on (1) the number of important accident sequences affected, (2) the likelihood that the specified action can be implemented and will reduce risk, (3) a downside assessment (hazards or risks that may result from implementing a proposed action), and (4) the time required to implement the proposed action.

10 CFR Part 60, Statements of Consideration (1983) [Ref 6]

The term "defense-in-depth" does appear in the Statements of Consideration (SOC) for 10 CFR Part 60. In this case, defense-in-depth appears to be defined in terms of multiple barriers (as much systematic as physical), and the concept of balance is introduced. Specifically, the SOC for the final rule (48 FR 28194-28299), contain the statement:

> "The Commission suggested that a course that would be "reasonable and practical" would be to adopt a "defense-in-depth" approach that would prescribe minimum performance standards for each of the major elements of the geologic repository, in addition to prescribing the Environmental Protection Agency [sic] (EPA) standard as a single overall performance standard. There was general acceptance of the Commission's multiple barrier

approach, with its identification of two major engineered barriers (waste package and underground facility) in addition to the natural barrier provided by the geologic setting."

Later the SOC state "There is nothing inconsistent between the multiple barrier, defense-in-depth approach and a unitary EPA standard."

NUREG/CR-6042 , Perspectives on Reactor Safety, 1994 [Ref 8]

NUREG/CR-6042, "Perspectives on Reactor Safety," by F. E. Haskin (University of New Mexico) and A. L. Campbell (Sandia National Laboratory), 1994, which describes a one week course in reactor safety concepts offered by the NRC Technical Training Center introduces defense-in-depth by listing "the key elements of an overall safety strategy that began to emerge in the early 1950s and has become known as defense-in-depth." The key elements listed are accident prevention, safety systems, containment, accident management, and siting and emergency plans.

NRC Commission Policy Statements, 1986, 1994 (2008), 1995 [Ref 9]

The term defense-in-depth is mentioned prominently in three Commission Policy Statements: the Safety Goal Policy Statement, the Advanced Nuclear Power Plant Policy Statement (2008), and the PRA Policy Statement. None of these documents offer a definition of defense-in-depth, except by example or implication.

Commission policy statement on Safety Goals (1986) contains the following statements:

> "The Commission recognizes the importance of mitigating the consequences of a core-melt accident and continues to emphasize features such as containment, siting in less populated areas, and emergency planning as integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy."
>
> ". . . the probabilistic results should also be reasonably balanced and supported through use of deterministic arguments. In this way, judgements can be made by the decisionmaker about the degree of confidence to be given to these estimates and assumptions. This is a key part of the process of determining the degree of regulatory conservatism that may be warranted for particular decisions. This defense-in-depth approach is expected to continue to ensure the protection of public health and safety."
>
> "A defense-in-depth approach has been mandated in order to prevent accidents from happening and to mitigate their consequences. Siting in less populated areas is emphasized. Furthermore, emergency response capabilities are mandated to provide additional defense-in-depth protection to the surrounding population."

Additional views offered by two individual Commissioners (not the Policy of the Commission):

> ". . .the Commission should have developed a policy on the relative emphasis to be given to accident prevention and accident mitigation. Such guidance is necessary to ensure that the principle of defense-in-depth is maintained."
>
> "In order to assure a proper balance between accident prevention and accident mitigation, the mean frequency of containment failure in the event of a severe core damage accident should be less than 1 in 100 severe core damage accidents."

". . . a containment performance objective is an element of ensuring that the principle of defense-in-depth is maintained."

"Consistent with the Commission's long-standing defense-in-depth philosophy, both core-melt and containment performance criteria should therefore be clearly stated parts of the Commission's safety goals."

". . .this pudding lacks a theme. Meaningful assurance to the public; substantive guidance to the NRC staff; the regulatory path to the future of the industry—all these should be provided by plainly stating that, consistent with the Commission's "defense-in-depth" philosophy:

(1) Severe core-damage accident should not be expected, on average, to occur . . .
(2) Containment performance . . . such that severe accidents . . . are not expected to occur . . .
(3) The goal for offsite consequences should be expected to be met after conservative consideration of the uncertainties . . ."

Commission policy statement on Regulation of Advanced Reactors (1994/2008) contains the following statement:

"Designs that incorporate the defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for, and consequences of, severe accidents."

Commission policy statement on PRA (1995) contains the following statements:

In response to public comments regarding the role of PRA, the NRC response stated that "It is not the Commission's intent to replace traditional defense-in-depth concepts with PRA. . . "

In response to public comments on PRA methodology, the NRC response stated that "Deterministic-based regulations have been successful in protecting the public health and safety and PRA techniques are most valuable when the serve to focus the traditional, deterministic-based, regulations and support he defense-in-depth philosophy."

In the discussion on deterministic and probabilities approaches to regulation, regarding the defense-in-depth philosophy, the NRC states "In the defense-in-depth philosophy, the Commission recognizes that complete reliance for safety cannot be placed on any single element of the design, maintenance, or operation of a nuclear power plant. Thus, the expanded use of PRA technology will continue to support the NRC's defense-in-depth philosophy by allowing quantification of the levels of protection and by helping to identify and address weaknesses or overly conservative regulatory requirements applicable to the nuclear industry. Defense-in-depth is a philosophy used by NRC to provide redundancy for facilities with "active" safety systems, e.g., a commercial nuclear power, as well as the philosophy of a multiple-barrier approach against fission product releases. Such barrier principles are mandated by the Nuclear Water Policy Act of 1982, which provides redundancy for a geologic repository to contain and isolate nuclear waste from the human environment."

The policy statement itself states that "the use of PRA technology should . . . complement the NRC's deterministic approach and support the "NRC's traditional defense-in-depth philosophy."

NUREG-1537, Part 1, 1996 [Ref 10]

NUREG-1537 (Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors) very briefly references defense-in-depth. It states, regarding describing "the principal architectural and engineering design criteria for the structures, systems and components that are required to ensure reactor facility safety and protection of the public," that the "material presented should emphasize the safety and protective functions and related design features that help provide defense-in-depth against uncontrolled release of radioactive material."

Chairman Jackson MIT Speech, 1997 [Ref 11]

Chairman Jackson, in a talk at the Massachusetts's Institute of Technology (MIT) Nuclear Power Reactor Safety Course, notes that "the NRC safety philosophy . . . comprises several closely interrelated elements . . . The elements are: defense-in-depth, licensee responsibility, safety culture, regulatory effectiveness, and accountability to the public. Defense-in-Depth ensures that successive measures are incorporated into the design and operating procedures for nuclear installations to compensate for potential failures in protection or safety measures, wherever such failures could lead to serious public or national security consequences."

Some Thoughts on Defense-in-Depth by Tom Kress, 1997 [Ref 12]

At an ACRS subcommittee meeting on August 27, 1997, Dr. Kress presented a paper on defense-in-depth. In the paper, Dr. Kress notes that the techniques and tools for determining risk were not well developed and risk measures were unavailable to the regulator. The NRC developed a regulatory philosophy that it called defense-in-depth which can be viewed as providing balance among three "levels" of protection: preventing the initiation of accidents, stopping (or limiting) the progression of an accident, and providing for evacuation in the event of accidental release of fission products. Each of the three levels are to be implemented by providing multiple independent provisions to accomplish the desired function. He also notes that "balanced" does not mean "equal."

Regarding the three elements, he explains that the first (defense-in-depth prevention) is implemented through provisions that include such things as quality in construction, Quality Assurance (QA), inspections and maintenance, testing, redundant and diverse emergency power supplies. The second element includes such concepts as multiple physical barriers, redundant and diverse shutdown systems. The third element includes provisions for siting and the plans for evacuation and sheltering. This implementation of defense-in-depth results in about everything the NRC does is part of defense-in-depth and become difficult to separate out just those things that would be considered purely defense-in-depth requirements.

Dr. Kress believes that all aspects of defense-in-depth are reflected in the PRA. The first level is reflected in the initiating event frequencies of the various accident sequences, the second level in the core damage frequency (CDF), conditional core damage frequency (CCFP) and large early release frequency (LERF), and the third level in the final conditional risk measure on early and late fatalities as well as on land contamination. He concludes that the PRA results can be considered a measure of the effectiveness of the overall implementation of defense-in-depth. Moreover, use of defense-in-depth would be a means to reduce both the risk and the uncertainty defense-in-depth is a philosophy that guides the regulatory process and the defense-in-depth provision and requirements are implicit and scattered throughout the entirety of the regulatory activities and regulations. These already spell out the necessary and sufficiency conditions.

Dr. Kress agrees on the need for a policy statement, which would describe three levels. For the first and third level, there appears to be little need or basis for further clarification. The second level, which is most closely related to design and hardware issues, further clarification may be needed, particularly on what constitutes appropriate regulatory balance between CDF and CCFP.

He provides some additional thoughts regarding a rational approach for developing a policy statement which would be:

- Presume the current regulations and requirements for level 1 and level 3 elements are sufficient
- Establish "N+1" as a defense-in-depth principle
- Establish risk acceptance criteria on CDF and CCFP that takes into account the uncertainties
- Establish (via expert judgment) and appropriate regulatory balance between CDF and CCFP (or LERF)
- Mandate that certain Level 2 defense-in-depth features be required (e.g., redundant and diverse shutdown systems, ECCS and long-term cooling, containment)
- Mandate that the containment design must accommodate all severe accident loads and not fail by virtue of only its volume, strength, and natural heat transfer properties..

Commission White paper, 1999 [Ref 13]

Chairman Jackson has also recently provided her thoughts on defense-in-depth in a March 1999 White Paper. In it, she states that "The concept of defense-in-depth 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 more clear 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." She goes on to state that "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."

PSA Paper, 1999, [Ref 14]

For the 1999 Probabilistic Safety Analysis (PSA) Conference, a paper by J.N. Sorenson, et. al., was presented entitled "On the Role of Defense in Depth in Risk-Informed Regulation." The authors note that there are "two different schools of thought (models) on the scope and nature

of defense in depth. The models came to be labeled ‘structuralist’ and ‘rationalist.’" The paper provides a discussion of the two models:

> “The structuralist model asserts that defense in depth is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations. The requirements for defense in depth are derived by repeated application of the question, "What if this barrier or safety feature fails?" The results of that process are documented in the regulations themselves, specifically in Title 10, Code of Federal Regulations. In this model, the necessary and sufficient conditions are those that can be derived from Title 10: It is also a characteristic of this model that balance must be preserved among the high-level lines of defense, e.g., preventing accident initiators, terminating accident sequences quickly, and mitigating accidents that are not successfully terminated. One result is that certain provisions for safety, for example reactor containment and emergency planning, must be made regardless of our assessment of the probability that they may be required. Accident prevention alone is not relied upon to achieve an adequate level of protection.
>
> The rationalist model asserts that defense in depth is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression. This model is made practical by the development of the ability to quantify risk and estimate uncertainty using probabilistic risk assessment techniques. The process envisioned by the rationalist is: (1) establish quantitative acceptance criteria, such as the quantitative health objectives, core damage frequency and large early release frequency, (2) analyze the system using PRA methods to establish that the acceptance criteria are met, and (3) evaluate the uncertainties in the analysis, especially those due to model incompleteness, and determine what steps should be taken to compensate for those uncertainties. In this model, the purpose of defense in depth is to increase the degree of confidence in the results of the PRA or other analyses supporting the conclusion that adequate safety has been achieved.
>
> The underlying philosophy here is that the probability of accidents must be acceptably low. Provisions made to achieve sufficiently low accident probabilities are defense in depth. It should be noted that defense in depth may be manifested in safety goals and acceptance criteria which are input to the design process. In choosing goals for core damage frequency and conditional containment failure probability, for example, a judgment is made on the balance between prevention and mitigation.
>
> What distinguishes the rationalist model from the structural model is the degree to which it depends on establishing quantitative acceptance criteria, and then carrying formal analyses, including analysis of uncertainties, as far as the analytical methodology permits. The exercise of engineering judgment, to determine the kind and extent of defense in depth measures, occurs after the capabilities of the analyses have been exhausted.”

The authors propose two options:

1. defense in depth as a supplement to risk analysis (the rationalist view)
2. a high-level structural view and a low-level rationalist view.

> “Option (1) requires a significant change in the regulatory structure. The place of defense in depth in the regulatory hierarchy would have to change. The PRA policy statement could no longer relegate PRA to a position of supporting defense in depth. Defense in depth would become an element of the overall safety analysis.

Option (2) is to a large degree compatible with the current regulatory structure. The structuralist model of defense in depth would be retained as the high-level safety philosophy, but the rationalist model would be used at lower levels in the safety hierarchy."

The authors view "Option (2) as a pragmatic approach to reconciling defense in depth with risk-informed regulation. However, "the rationalist model, Option (1), will ultimately provide the strongest theoretical foundation for risk-informed regulation."

ACRS Letters, 1999, 2000 [Ref 15]

The ACRS has provided their insights on defense-in-depth over the years in numerous letters (see Table 1); however, there are two specific letters (in 1999 and 2000) regarding reactors and nuclear materials where defense-in-depth is discussed in detail.

In the first letter, the Committee's views on reactors are provided in a May 19, 1999, letter to Chairman Shirley Jackson entitled "The Role of Defense in Depth in a Risk-Informed Regulatory System." In this letter, the Committee discusses the appropriate relationship and balance between probabilistic risk assessment and defense in depth in the context of risk-informed regulation. The Committee states:

"Improved capability to analyze nuclear power plants as integrated systems is leading us to reconsider the role of defense in depth. Defense in depth can still provide needed safety assurance in areas not treated or poorly treated by modem analyses or when results of the analyses are quite uncertain. To avoid conflict between the useful elements of defense in depth and the benefits that can be derived from quantitative risk assessment methods, constraints of necessity and sufficiency must be imposed on the application of defense in depth and these must somehow be related to the uncertainties associated with our ability to assess the risk.

We believe that two different perceptions of defense in depth are prominent. In one view (the "structuralist" view. . .), defense in depth is considered to be the application of multiple and redundant measures to identify, prevent, or mitigate accidents to such a degree that the design meets the safety objectives. This is the general view taken by the plant designers. The other view (the "rationalist"), sees the proper role of defense in depth in a risk-informed regulatory scheme as compensation for inadequacies, incompleteness, and omissions of risk analyses. We choose here to refer to the inadequacies, incompleteness, and omissions collectively as uncertainties. Defense-in-depth measures are those that are applied to the design or operation of a plant in order to reduce the uncertainties in the determination of the overall regulatory objectives to acceptable levels. Ideally then, there would be an inverse correlation between the uncertainty in the results of risk assessments and the extent to which defense in depth is applied. For those uncertainties that can be directly evaluated, this inverse correlation between defense in depth and the uncertainty should be manifest in a sophisticated PRA uncertainty analysis.

When defense in depth is applied, a justification is needed that is as quantitative as possible of both the necessity and sufficiency of the defense-in-depth measures. Unless defense-in-depth measures are justified in terms of necessity and sufficiency, the full benefits of risk-informed regulation cannot be realized.

The use of quantitative risk-assessment methods and the proper imposition of defense-in-depth measures would be facilitated considerably by the availability of risk-acceptance criteria applicable at a greater level of detail than those we now have. Development of the

additional risk-acceptance criteria would have to take into consideration safety objectives embodied in the existing regulations. . . . Setting such acceptance values is a policy role, very much like setting safety goal values. The uncertainties that are intended to be compensated for by defense in depth include all uncertainties (epistemic and aleatory). Not all of these are directly assessed in a normal PRA uncertainty analysis. Therefore, when acceptance values are placed on uncertainty, these would have to appropriately incorporate consideration of the additional uncertainties not subject to direct quantification by the PRA. These considerations would have to be determined by judgment and expert opinion. As a practical matter, we suggest that the acceptance values be placed on only those epistemic uncertainties quantifiable by the PRA but that these be set sufficiently low to accommodate the unquantified aleatory uncertainties.

When acceptance values have been chosen as policy for the regulatory objectives and their associated uncertainties, it would be possible to develop objective limits on the amount of defense in depth required for those design and operational elements that are subject to evaluation by PRA. . . .

The balance between CDF and CCFP can serve as an example of this defense-in-depth concept. . . In our view, three acceptance criteria must be satisfied -one each on CDF, LERF, and the epistemic uncertainty associated with LERF. . . We believe this concept of defense in depth can provide a rational way to develop sufficiency limits wherever the defense-in-depth measures can be directly evaluated by PRA. We acknowledge however, that considerable judgment will have to be exercised to set limits on uncertainty, especially uncertainties not quantified by the PRA."

In the second letter, the Committee's views on nuclear materials are provided in a May 25, 2000, letter to Chairman Richard Meserve entitled "Use of Defense in Depth in Risk-Informing Nuclear Material Safety and Safeguards (NMSS) Activities." In this letter, the Committee provided their review of the use of defense in depth in risk informing the activities of NMSS. The Committee states:

1. The various compensatory measures taken for the purposes of defense in depth can be graded according to the risk posed by the activity, the contribution of each compensatory measure to risk reduction, the uncertainties in the risk assessment, and the need to build stakeholders trust.

2. The treatment of defense in depth for transportation, storage, processing and fabrication should be similar to its treatment for reactors. Defense in depth for industrial and medical applications can be minimal and addressed on the basis of actuarial information.

3. Defense in depth for protecting the public and the environment from high-level waste (HLW) repositories is both a technical and a policy issue. It is important that a reasonable balance be achieved in the contribution of the various compensatory measures to the reduction of risk. The staff should develop options on how to achieve the desired balance. The opinions of experts and other stakeholders should be sought regarding the appropriateness of each option.

4. Since the balancing of compensatory measures to achieve defense in depth depends on the acceptability of the risk posed by the facility or activity, risk-acceptance criteria should be developed for all NMSS-regulated activities.

The Committee further states:

> We agree that there is a need for a common understanding of defense in depth as it relates to a risk-informed regulatory system and that a good working definition is provided in the Commission's White Paper on Risk-Informed and Performance-Based Regulation (Reference 1): 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 primary need for improving the implementation of defense in depth in a risk-informed regulatory system is guidance to determine how many compensatory measures are appropriate and how good these should be. To address this need, we believe that the following guiding principles are important:
>
> - Defense in depth is invoked primarily as a strategy to ensure public safety given the unquantified uncertainty in risk assessments. The nature and extent of compensatory measures should be related, in part, to the degree of uncertainty.
>
> - The nature and extent of compensatory measures should depend on the degree of risk posed by the licensed activity.
>
> - How good each compensatory measure should be is, to a large extent, a value judgment and, thus, a matter of policy.

With regard to nuclear reactors, the Committee states:

> ". . . It is the CDF distribution that should determine if additional compensatory measures are needed due to inadequate models. In general, the more such measures are added, the more this distribution shifts to lower frequency values. What CDF distribution is acceptable is a matter of policy. As noted above, the current regulatory system for reactors has evolved without the benefit of these probability distributions. Consequently, the structuralist approach to defense in depth was employed that involves placing compensatory measures on important safety cornerstones to satisfy acceptance criteria for defined design-basis accidents that represent the range of important accident sequences."

With regard to nuclear materials, the Committee states:

> "The issue of defense in depth and the suggested guiding principles have to be considered somewhat differently when it comes to nuclear materials. For example, there is much less experience in the application of PRA methods to nuclear materials than for nuclear reactors. Although materials systems are not as complex as those for reactors in terms of the assessment of risk, there is greater diversity in materials licensed activities. Perhaps the biggest difference relates to the basic differences in the safety issues between reactors and nuclear waste disposal, especially with regard to HLW repositories. The principal concern in the safety of such repositories is not a catastrophic release of radiation resulting from an accident, but rather the loss through contamination of a valuable life-supporting resource such as ground water or land use. Both can be pathways for radiation exposure to humans. On the other hand, both lend themselves to simple interdiction and intervention measures for the protection of public health and safety. Therefore, the concept of defense in depth for repositories should be targeted more towards protecting resources where there are high uncertainties due to the very long time involved. Although the accident perspective is somewhat important during pre-closure operations, it is not the dominant safety issue in the

area of nuclear waste. Pre-closure operations do, however, lend themselves to using risk assessment methods similar to those applied to reactor facilities.

With respect to the issue of the diversity of nuclear materials, SECY-99-100 categorizes nuclear materials into four groups. The four groups are abbreviated here as nuclear material activities involving: (1) disposal, (2) transportation and storage, (3) processing and fabrication, and (4) industrial and medical applications.

For disposal (Group 1), the reactor example suggests an approach for considering the effectiveness of protective barriers. For waste disposal facilities, defense in depth is implemented through the use of multiple barriers. For transportation and processing facilities (Groups 2 and 3), PRA methods similar to those applied to reactors can be used and defense in depth can be treated as it is for reactors. For industrial and medical applications (Group 4), we believe that sufficient data exist for many of these nuclear materials activities so that the uncertainties in estimating risks are relatively small. For Group 4 materials, defense in depth can be minimal and can be addressed on the basis of actuarial information, an advantage not available to the same extent for Groups 1-3."

The Committee goes on to state:

"Implementation of regulations within a risk-informed framework, including the use of defense in depth, requires the establishment of risk-acceptance criteria for each regulated activity. In most cases, a facility (or a proposed design) already exists with compensatory measures in place. The questions then become (1) Are these measures sufficient for the facility or design to meet the risk-acceptance criteria? (2) Do the measures compensate sufficiently for uncertainties in their assessment? (3) Will the measures gain stakeholder acceptance? Answering these questions is the most difficult aspect of the appropriate utilization of defense in depth in a risk-informed regulatory framework and is the key to establishing limits of necessity and sufficiency.

. . . For nuclear materials applications, including HLW repositories, we recommend the following pragmatic approach for selecting compensatory measures:

1. The contribution that each individual safety system makes in achieving the risk acceptance criterion should be determined by risk assessment with quantified uncertainty distributions.

2. The adequacy of the risk-assessment models should be evaluated quantitatively where possible and qualitatively in all aspects.

3. Whether the appropriate balance has been achieved can be judged through the opinions of experts and of other stakeholders and is ultimately a policy issue.

4. Policy options should be formulated on how the appropriate balance can be achieved. The impact of each option on building stakeholder trust should be evaluated."

Joint ACNW/ACRS Subcommittee, January 13/14, 2000 [Ref 16]

A joint subcommittee was held with the focus on defense-in-depth. The following is a summary for the various presenters.

Defense-in-depth: Perspective for Risk-Informing 10 CFR 50, Tom King, Gary Holahan

The presenters noted that defense-in-depth philosophy is included in reactor regulations, in licensing and licensee amendment process, and in reactor oversight process. Defense-in-depth includes multilayer protection from fission products; for example, ceramic fuel pellets, metal cladding, reactor vessel and piping, containment, exclusion area, low population zone and evacuation plan, and population center distance. GDCs provide for defense-in-depth; for example, 1-5, 10-18, 20-29, 30-46, 50-57, and 60-64. Reactor oversight process cornerstones are a defense-in-depth concept.

They believed that a working definition of defense-in-depth should be developed that establishes an approach in risk-informing 10 CFR Part 50. It should provide for multiple lines of defense, balance between prevention and mitigation, and provide for a framework to address uncertainties in accident scenarios. It should consist of two parts: fundamental elements that should be provided in all cases, and implementation elements that may vary depending on uncertainty and reliability and risk goals. The fundamental elements should build upon the cornerstone concept, assure for prevention and mitigation, and assure balance between prevention and mitigation to achieve an overall level of safety consistent with CDF and LERF goals. The implementation elements would use redundancy, diversity, QA, Equipment Qualification (EQ), Inservice Testing (IST), safety margins, etc. in a variable manner, as necessary, to achieve reliability and risk goals and balance of prevention and mitigation.

Design Defense-in-Depth in a Risk-Based Regulatory System with Imperfect PRA, Tom Kress

Dr. Kress noted that defense-in-depth is a design and operational strategy for dealing with uncertainty in risk assessment. However, he further stated that there are two concerns: (1) defense-in-depth does not constitute a precise definition in terms of risk assessment, and (2)a definition or criteria does not exist that allows for placing limits on defense-in-depth.

Dr. Kress noted that the defense-in-depth philosophy consist of four principles: prevent accident from starting (initiation), stop accident at early stages before they progress to unacceptable consequences (intervention), provide for mitigating the release of the hazard vector (mitigation), and provide sufficient instrumentation to diagnose the type and progress of any accident (diagnosis). Base on these principles, he proposed a definition of defense-in-depth: “design defense-in-depth is a strategy of providing design features to achieve acceptable risk (in view of the uncertainties) by the appropriate allocation of the risk reduction to both prevention and mitigation.”

Dr. Kress concluded by proposing to put limits on defense-in-depth. He stated that, you must have risk acceptance criteria that you desire to allocate (preferably expressed in terms of confidence levels), and where quantifiable uncertainty should come out of the PRA, unquantifiable uncertainty should be estimated by expert opinion, and the acceptance criteria should include both uncertainties. Moreover, allocation is a value judgment where criteria are needed for how much to value prevention versus mitigation. He further noted that allocation could depend on several factors: on the level of inherent hazard (the more hazardous the activity the more to value prevention), on the extent of uncertainty in the risk assessment, depend on how much the uncertainty is unquantifiable. In deterministic space, he noted that you may want to minimize uncertainty, and may be based on the “loss function” of decision theory.

Defense-in-Depth, Robert Bernero

Dr. Bernero noted that defense-in-depth can be viewed by addressing six questions:

1. "What is defense-in-depth? Defense-in-depth is an element of NRC's Safety Philosophy that employs successive compensatory measure to prevent accident 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 questions tends to be more tolerating of failures and external challenges. Defense-in-depth is not a formula for adequate protection; it is part of the safety philosophy, a strategy for safety analysis."

2. "Is there an overarching philosophy of defense-in-depth? Yes, as a strategy of safety analysis. Defense-in-depth prevents undue reliance on single occurrence, design feature, barrier, or performance model. It is not a formula for acceptability, defense-in-depth may not be enough defense. It is risk-informed and should achieve a sufficient margin of safety, neither too close nor too far from the unacceptable."

3. "Are current safety goals and objectives clear for general use? No, it is not for general use. The span of protection includes public safety, worker safety, patient safety, environmental protection. The range of authorize practices include reactors, fuel cycle facilities, industrial and medical uses, exempt distribution, and transportation."

4. "What is the role of defense-in-depth in risk-informed regulation of nuclear reactors? Does not apply to routine releases. It is the basis for evaluating areas of heavy reliance in accident analysis; for example, seismic safety, reactor pressure vessel (RPV) rupture, steam generator tube rupture, human action. It is a graded defense with graded goals."

5. "What is the role of defense-in-depth in risk-informed regulation of radioactive material processes and uses? May sometimes apply to routine releases, for example, exempt products. It needs graded goals for graded defenses. It needs to be thought through considering potential consequences, potential barriers, potential actions, and balanced chose of defense. It has "knotty" problems, for example, patient safety and medical QA."

6. "What is the role of defense-in-depth in risk-informed regulation of radioactive disposal? It definitely applies to release barriers. One fundamental basis of acceptability is the Total System Performance Assessment [sic] (TSPA) with proper uncertainty analysis. There is apparent confusion since defense-in-depth analysis is a form of uncertainty analysis. Part 63 proposal is a sound approach to defense-in-depth, develop the body of information for the exercise of judgment. You need graded goals for graded uncertainties; for example, clearly acceptable, acceptable, clearly tolerable, tolerable, life-threatening, unacceptable."

On the Quantification of Defense-in-Depth, John Garrick

Dr. Garrick presentation proposed a conceptual framework for quantifying the defense-in-depth aspects of the various levels of protection, provided in nuclear plants and nuclear waste repositories, against the release of radiation to the public and the environment. The main feature of his proposed approach was how best to use PRA results to quantify and make visible the performance of the various defense-in-depth systems designed to provide multiple levels of protection against the release of radiation. He noted that the key to using PRA and probabilistic performance assessment (PPA) to determine whether we are getting our money's worth from multiple levels of defense and whether we need more or less is (1) understanding the role that the individual safety systems play in providing protection against the release of radiation to the environment, and (2) the effect of the individual systems acting in concert. His approach involves examining, in a top-down approach, the risk versus the performance of the function, system and finally to the component.

Defense-in-Depth for Risk-Informed Performance-Based Regulation: A Provisional NMSS Perspective, Norman Eisenberg

Dr. Eisenberg notes that NMSS framework requires reexamination of regulatory approaches including defense-in-depth and that defense-in-depth is addressed in various parts of the framework and in risk-informed activities (e.g., Part 63). He further notes that there are several factors affecting implementation of defense-in-depth in NMSS; for example, nature of licensees and activities regulated, NMSS regulators systems with less hazard than nuclear power reactors.

He proposed both a structuralist and rationalist approach to defense-in-depth. Regarding the structuralist, the need for and extent of defense-in-depth is related to the system structure. For the rationalist approach, the need for and extent of defense-in-depth is related to the residual uncertainties in the system.

Dr. Eisenberg points out that there are two type of residual uncertainty. Type 1 (Best available risk assessment) involves a system for which a fairly complete risk analysis or safety analysis has been performed, so residual uncertainty relates to the confidence or lack of confidence in the analysis; i.e., the analysis does not represent all uncertainty because the state of knowledge is incomplete. Type 2 (Limited risk assessment) involves a system for which the risk or safety analysis is somehow limited (e.g., by not being complete, or not quantifying certain types of uncertainty). Details are provided in his presentation describing the differences in the limitations of Type 1 versus Type 2.

In his presentation, he notes that the NMSS safety philosophy is three-fold: (1) goal is reasonable assurance of protecting public health and safety, etc. (2) design concept assist in achieving this goal; for example, safety margin, defense-in-depth, diversity, redundancy, etc. and (3) defense-in-depth is a risk management method.

He describes safety margins and discusses a concept of margin in a probabilistic context. He notes that there are differences between defense-in-depth and margin:

- Margin relates to the "cushion" between required performance and expected performance
- Defense-in-depth relates to the characteristic of the system to (1) not rely on any single element of the system and (2) be more robust to challenges

- Margin describes expected performance of a system versus the safety limit; defense-in-depth describe the ability of the system to compensate for unanticipated performance, which results from limitations on knowledge

- Margin and defense-in-depth are orthogonal, so defense-in-depth can be added without increasing margin

- Increasing margin in a system that relies on a single component, does not necessarily increase defense-in-depth

- Defense-in-depth assures that if any component fails, the rest of the system compensates, so consequences are not unacceptable

He points out that two different systems with the same reliability can have different defense-in-depth characteristics. Furthermore, he proposes a process for determining the amount of defense-in-depth that is needed by examining the potential consequences posed by a system against the uncertainty in the performance of the system.

Dr. Eisenberg concludes that:

- Defense-in-depth is related to, but different from, other design concepts such as safety margin, redundancy, and diversity

- Defense-in-depth is not necessarily equivalent to meeting a safety goal or the margin associated with meeting the goal

- Defense-in-depth can be implemented in a risk-informed, performance-based regulatory context as a system requirement, rather than as a set of subsystem requirements

- Defense-in-depth can be used to address residual uncertainties concerning the performance of a safety system

- The need for defense-in-depth depends on the degree of residual uncertainty and the degree of hazard (i.e., consequences)

Dr. Eisenberg also identifies several issues needing resolution:

- How to measure the degree of defense-in-depth?

- How to measure the degree of uncertainty in performance of the safety system, encompassing quantified and unquantified uncertainty?

- How to measure the degree of potential hazard (i.e., consequences) posed by a system?

- How to use current state of knowledge to make reasonable tests for a system to have sufficient defense-in-depth, which allows for incomplete knowledge?

- How to explain to stakeholders the flexibility inherent in a risk-informed, performance-based approach to defense-in-depth, which also provides reasonable assurance of safety?

International Atomic Energy Agency (IAEA) Documents, 1988, 1996, 1999, 2006, 2009, 2012 [Ref 17]

INSAG -3, 1988

The International Nuclear Safety Advisory Group in INSAG-3, "Basic Safety Principles for Nuclear Power Plants," IAEA, 1988, explains defense in depth by stating that "All safety activities, whether organizational, behavioral or equipment related, 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. This idea of multiple levels of protection is the central feature of defence in depth, and it is repeatedly used in the specific safety principles that follow."

The document then goes on to state the principle of defense-in-depth is "To compensate for potential human and mechanical failures, a defense in depth concept is implemented, centered on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barrier by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective."

INSAG-10, 1996

INSAG-10, "Defense in Depth in Nuclear Safety," IAEA, 1996, restates the explanation on defense in depth provided in INSAG-3. It further states that “Defense in depth consists in a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment, in normal operation, anticipated operational occurrence and, for some barriers, in accident in the plant.” The report states the objectives of defense in depth are to “compensate for potential human and component failures, maintain the effectiveness of barriers by averting damage to the plant and to the barrier themselves, and protect the public and environment from harm in the event that these barriers are not fully effective.” It goes on to state that “the strategy for defense in depth is twofold: first, to prevent accidents and, second, if prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions. Accident prevention is the first priority. . .“

Five levels of defense are defined such that if one level fails, the subsequent level comes into play. The objectives of the five levels are as follows:

1. Prevention of abnormal operation and system failures

2. Control of abnormal operation and detection of failures

3. Control of accident within the design basis

4. Control of severe conditions including prevention of accident progression and mitigation of the consequences of a severe accident

5. Mitigation of the radiological consequences of significant external releases of radioactive materials.

With respect to the above levels, the report states that “the general objective of defense in depth is to ensure that a single failure, whether equipment failure or human failure, at one level of

defense, and even combinations of failures at more than one level of defense, would not propagate to jeopardize defense in depth at subsequent levels." Moreover, for each of the levels, further explanation is provided along with examples of how to implement. The report also states that "For the effective implementation of defense in depth, some basic prerequisites apply to all measures at Levels 1 to 5. These prerequisites . . . are appropriate conservatism, quality assurance and safety culture." The goal for each prerequisite is provided in the report.

INSAG-12, 1999

INSAG-12, "Basic Safety Principles for Nuclear Power Plants," provides a logical framework for understanding the underlying objectives and principles of nuclear safety, and the way in which its aspects are interrelated. Defense in depth is discussed as a fundamental principle. These statements regarding defense in depth, while similar, are slightly different than in INSAG-3 or 10. In this report, defense in depth is a principle "to compensate for potential human and mechanical failures, a defense in depth concept is implemented, centered on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective." The report goes on to state the "the principle of defense in depth is implemented 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. These barriers are physical, providing for the confinement of radioactive material at successive locations. The barriers may serve operational and safety purposes, or may serve safety purposes only. Power operation is only allowed if this multi-barrier system is not jeopardized and is capable of functioning as designed." This report also states that the strategy for defense in depth is twofold: first, to prevent accident and second, if prevention fails, to limit the potential consequences of accidents and to prevent their evolution to more serious conditions." It provides a definition and criteria for accident prevention and accident mitigation. Moreover, it also uses the same five levels presented in INSAG-10. It is also consistent with INSAG-10 in stating "the existence of several levels of defense in depth is never justification for continued operation in the absence of one level." INSAG-12 goes further than INSAG-10 in that it relates the five levels of defense in depth to the five operational states of nuclear power plants and classifies them either as accident prevention or accident mitigation as follows:

Accident prevention –

- Level 1 (Prevention of abnormal operation and failure) – normal operation
- Level 2 (Control of abnormal operation and detection of failures) – anticipated operational occurrences
- Level 3 (Control of accidents below the severity level postulated in the design basis) – design basis and complex operating states

Accident mitigation –

- Level 4 (Control of severe plant conditions, including prevention of accident progression, and mitigation of the consequences of severe accidents, including confinement protection) – severe accidents beyond the design basis

- Level 5 (Mitigation of radiological consequences of significant releases of radioactive materials) – post-severe accident situation

IAEA SF-1, 2006

Safety Fundamentals, SF-1, IAEA Safety Standards, "Fundamental Safety Principles," establishes safety objective, safety principles and concepts that provide the bases for the IAEA's safety standards and its safety related programs. This standard provides ten safety principles. Principle 8, "Prevention of accidents," does not use the term defense-in-depth, its concept is used in its definition: "all practical efforts must be made to prevent and mitigate nuclear or radiation accidents."

The standard reads:

> "The most harmful consequences arising from facilities and activities have come from the loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or other source of radiation. Consequently, to ensure that the likelihood of an accident having harmful consequences is extremely low, measures have to be taken:
>
> - To prevent the occurrence of failures or abnormal conditions (including breaches of security) that could lead to such a loss of control
> - To prevent the escalation of any such failures or abnormal conditions that do occur
> - To prevent the loss of, or the loss of control over, a radioactive source or other source of radiation
>
> The primary means of preventing and mitigating the consequences of accidents is 'defence in depth'. Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. The independent effectiveness of the different levels of defence is a necessary element of defence in depth.
>
> Defence in depth is provided by an appropriate combination of:
>
> - An effective management system with a strong management commitment to safety and a strong safety culture
> - Adequate site selection and the incorporation of good design and engineering features providing safety margins, diversity and redundancy, mainly by the use of:
>   – Design, technology and materials of high quality and reliability
>   – Control, limiting and protection systems and surveillance features
>   – An appropriate combination of inherent and engineered safety features
> - Comprehensive operational procedures and practices as well as accident management procedures

> Accident management procedures must be developed in advance to provide the means for regaining control over a nuclear reactor core, nuclear chain reaction or other source of radiation in the event of a loss of control and for mitigating any harmful consequences."

IAEA TECDOC-1570, 2007

IAEA TECDOC-1570, "Proposal for a Technology-Neutral Safety Approach for New Reactor Designs," provides a technology-neutral safety approach to guide the design, safety assessment and licensing of innovative reactors. As part of the proposed approach, three "main pillars" are proposed, one of which defense in depth which includes probabilistic considerations. The document references INSAG-10 in terms of the five levels, however, it also provides safety goals that are to be factored into the implementation of defense in depth. Quantitative Safety Goals targets are correlated to each level of defense in depth via a frequency consequence curve (the consequences being various accidents against acceptable frequencies). For example, normal operational occurrences are accommodated only within the first level of defense in depth and result in no consequences, as the aim of this level is to prevent deviations from normal operation and to prevent system failures. The second level of defense in depth assures, by detecting and intercepting deviations from normal operational states, that the consequences of events above a frequency of 10-2/yr (i.e., anticipated operational occurrences) are within the success criteria of this second level of defense. Similar approach is followed for the remaining three levels. "The ultimate objective is that any credible accident sequence, even considering the failures of lines of protection for the different levels of defence in depth, shall remain under the overall frequency-consequence curve."

IAEA TECDOC-1570 also introduced the concept of a line of protection (LOP). A LOP is identified in the document for each safety function and for each level of defense in depth. "It is an effective defense against a given mechanism or event that has the potential to impair a fundamental safety function. It is used for any set of inherent characteristics, equipment, system (active or passive), etc., that is part of the plant safety architecture, the objective of which is to accomplish the mission needed to achieve a given safety function. For a given event, and against a given safety function, the LOPs provide the practical means of successfully achieving the objectives of the individual levels of defense."

IAEA, SSR-2/1, 2012

Specific Safety Requirements, SSR-2/1, IAEA Safety Standards, "Safety of Nuclear Power Plants: Design," establishes "design requirements for the structure, systems and components of a nuclear power plant, as well as for procedures and organizational processes important to safety, that are required to be met for safe operation and for preventing events that could compromise safety, or for mitigating the consequences of such events, were they to occur."

SSR-2/1 describes a concept of defense-in-depth. It states that

> "The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth [1, 5, 6]. This concept is applied to all safety related activities, whether organizational, behavioral or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth throughout design and operation provides protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human

induced events within the plant, and against consequences of events that originate outside the plant.

Application of the concept of defence in depth in the design of a nuclear power plant provides several levels of defence (inherent features, equipment and procedures) aimed at preventing harmful effects of radiation on people and the environment, and ensuring adequate protection from harmful effects and mitigation of the consequences in the event that prevention fails. The independent effectiveness of each of the different levels of defence is an essential element of defence in depth at the plant and this is achieved by incorporating measures to avoid the failure of one level of defence causing the failure of other levels. There are five levels of defence:

The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. . .

The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. . .

For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop. . .

The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. . .

The purpose of the fifth and final level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accident conditions. . .

A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations."

Requirement 7 of SSR-2/1, "Application of defence in depth," states that "The design of a nuclear power plant shall incorporate defence in depth. The level of defence in depth shall be independent as far as is practicable." It also gives details regarding the implementation of the requirement:

"The defence in depth concept shall be applied to provide several levels of defence that are aimed at preventing consequences of accidents that could lead to harmful effects on people and the environment, and ensuring that appropriate measures are taken for the protection of people and the environment and for the mitigation of consequences in the event that prevention fails.

The design shall take due account of the fact that the existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence in depth shall be kept available at all times and any relaxations shall be justified for specific modes of operation.

The design:

a) Shall provide for multiple physical barriers to the release of radioactive material to the environment

b) Shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect

c) Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible

d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized

e) Shall provide for systems, structures and components and procedures to control the course of and, as far as practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems

f) Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation

To ensure that the concept of defence in depth is maintained, the design shall prevent, as far as is practicable:

a) Challenges to the integrity of physical barriers;
b) Failure of one or more barriers;
c) Failure of a barrier as a consequence of the failure of another barrier;
d) The possibility of harmful consequences of errors in operation and maintenance.

The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant."

10 CFR Part 50, Appendix R, 2000 [Ref 18]

The term defense-in-depth only appears in the regulations in Title 10 of the Code of Federal Regulations Part 50, Appendix R ("Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979"), where it appears once. The specific statement occurs in Section II.A, General Requirements, Fire Protection Program, which states in part,

"The fire protection program shall extend the concept of defense-in-depth to fire protection in fire areas important to safety, with the following objectives:

- To prevent fires from starting;

- To detect rapidly, control, and extinguish promptly those fires that do occur;

- To provide protection for systems, structures and components important to safety so that a fire that is not promptly extinguished will not prevent the safe shutdown of the plant."

In June 2000, the NRC amended Appendix R to remove the requirement that fire barrier penetration seal materials be noncombustible, and to make other minor changes. As part of the rule change, a public comment was received which related to defense-in-depth:

> "By providing for the acceptance of combustible penetration seals, the NRC is reducing the level of defense-in-depth without fully analyzing the risks associated with accelerated burn-through of seals from the combination of these widely documented factors."

A Risk-Informed Defense-in-Depth Framework for Existing and Advanced Reactors, Karl Fleming, Fred Silady, July 2002, [Ref 19]

This paper provides a review of the current definitions (at that time), offers solutions to the technical issues identified from the review, and proposes a general definition that can be used for any reactor concept.

The paper notes that over time the definition of defense-in-depth has evolved from a simple set of strategies to apply multiple lines of defense to a more comprehensive set of cornerstones, strategies and tactics to protect the public health and safety. Based on the various definitions, the paper classifies the definitions as either design defense-in-depth, process defense-in-depth or scenario defense-in-depth. Design defense-in-depth focuses on strategies implemented during the design phase including the selection of inherent features, definition of reactor specific safety functions, and passive and active engineered safety features that together with the inherent features support the maintenance of radionuclide barriers. Process defense-in-depth sets requirements and criteria for decisions that are made in the life cycle of the plant that contribute to plant safety and is the focus of may regulatory decisions to support licensing and regulations of nuclear power. Scenario defense-in-depth provides a framework for the evaluation of safety using appropriate combinations of deterministic and probabilistic approaches and serves as the "referee" in determining how well the design and process defense-in-depth decisions are implemented.

The paper provides insights regarding the need to incorporate risk insights into the definitions of defense-in-depth. A summary of these insights include:

- Risk is dominated by events beyond design basis
- Events beyond the design basis are not always rare
- Radionuclide barriers are not independent
- Containments mitigate some events beyond design basis
- Containments are rarely an independent barrier
- Common cause failures are important for redundant active systems

10 CFR §50.69, 2004 [Ref 20]

In November, 2004, the final rule on "Risk-Informed Categorization and Treatment of Structures, Systems and Components for Nuclear Power Reactors," (10 CFR §50.69) was published. In the Federal Register Notice (FRN) announcing the final rule, defense-in-depth is discussed in several places.

As part of the background discussion, it states in the FRN that:

> "Defense-in-depth is an element of the NRC's safety philosophy that employs successive measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. Defense-in-depth is a philosophy used by the NRC to provide redundancy as well as the philosophy of a multiple barrier approach against fission product releases. 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."
>
> "The primary need for improving the implementation of defense-in-depth in a risk-informed regulatory system is guidance to determine how many measures are appropriate and how good these should be. Instead of merely relying on bottom-line risk estimates, defense-in-depth is invoked as a strategy to ensure public safety given there exists both unquantified and unquantifiable uncertainty in engineering analyses (both deterministic and risk assessments).
>
> 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 is appropriate from a regulatory perspective. 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."

As part of the final rule regarding the basis for reduction in scope with regard to Appendix J containment leakage testing:

> "Because it is likely that most containment isolation valves [sic] (CIVs) will be categorized as RISC–3, the licensee or applicant must evaluate the proposed change in the treatment of RISC–3 CIVs to ensure that defense-in-depth is maintained by ensuring with reasonable confidence that the RISC–3 CIVs are capable of performing their safety related functions under design basis conditions. Although the licensee or applicant is allowed flexibility in addressing this issue, the rule requires that the licensee or applicant ensure with reasonable confidence the capability of RISC–3 CIVs to perform their safety functions to maintain defense-in-depth as discussed in RG 1.174."

10 CFR §50.69(c)(1)(iii) requires that the categorization process maintain defense-in-depth. In the FRN, it states that to

> "satisfy this requirement, when categorizing structures, systems and components [sic] (SSCs) as low safety significant, the integrated decisionmaking process [sic] (IDP) must

demonstrate that defense-in-depth is maintained. Defense-in-depth is adequate if the overall redundancy and diversity among the plant's systems and barriers is sufficient to ensure the risk acceptance guidelines discussed in Section V.4.4 are met, and that:

- Reasonable balance is preserved among prevention of core damage, prevention of containment failure or bypass, and mitigation of consequences of an offsite release.

- System redundancy, independence, and diversity is preserved commensurate with the expected frequency of challenges, consequences of failure of the system, and associated uncertainties in determining these parameters.

- There is no over-reliance on programmatic activities and operator actions to compensate for weaknesses in the plant design.

- Potential for common cause failures is taken into account.

The Commission's position is that the containment and its systems are important in the preservation of defense-in-depth (in terms of both large early and large late releases). Therefore, as part of meeting the defense-in-depth principle, a licensee should demonstrate that the function of the containment as a barrier (including fission product retention and removal) is not significantly degraded when SSCs that support the functions are moved to RISC–3 (e.g., containment isolation or containment heat removal systems). The concepts used to address defense-in-depth for functions required to prevent core damage may also be useful in addressing issues related to those SSCs that are required to preserve long-term containment integrity. Where a licensee categorizes containment isolation valves or penetrations as RISC–3, the licensee should address the impact of the change in treatment to ensure that defense-in-depth continues to be satisfied."

10 CFR Part 73 [Ref 21]

There are requirements, although not specific to reactors, that provide for defense-in-depth with similar concepts.

10 CFR §73.54, 2009

73.54 requirement is "Protection of digital computer and communication systems and networks." Section (b)(2) states "apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks

10 CFR §73.55, 2009

73.55 requirement is "Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage." Section (b)(3) requires that "Provide defense-in-depth through the integration of systems, technologies, programs, equipment, supporting processes, and implementing procedures as needed to ensure the effectiveness of the physical protection program. Section (b)(9)(i) requires that implementation of "defense-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent significant core damage and spent fuel sabotage."

10 CFR §70.64, 2000

70.64, "Requirements for new facilities or new process at existing facilities," Section (b) requires that "Facility and system design and facility layout must be based on defense-in depth practices," and provides a definition of defense-in-depth:

> "Defense-in-depth practices means a design philosophy, applied form the outset and through completion of the design, that is based on providing successive levels of protection such that health and safety will not be wholly dependent upon any single element of the design, construction, maintenance, or operation of the facility. The net effect of incorporating defense-in-depth practices is a conservatively designed facility and system that will exhibit greater tolerance to failure and external challenges. The risk insight obtained through performance of the integrated safety analysis can be then used to supplement the final design by focusing attention on the prevention and mitigation of the higher-risk potential accidents."

10 CFR Part 73, Appendix C,

Appendix C to Part 73, "Nuclear Power Plant Safeguards Contingency Plans, there are two places where defense-in-depth is discussed:

- Section II(B)(3)(c)(i) states "Physical security systems and security systems hardware to be discussed include security systems and measures that provide defense in depth, such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems.

- Section II(B)(3)(c(v)(4) states that the protective strategy shall "Contain a description of the physical security systems and measure that provide defense in depth such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems."

10 CFR Part 100, 1996 [Ref 22]

Section 100.1(d) provides for defense-in-depth with regard to siting:

> "The Commission intends to carry out a traditional defense-in-depth approach with regard to reactor siting to ensure public safety. Siting away from densely populated centers has been and will continue to be an important factor in evaluating applications for site approval."

NEI 02-02. 2002 [Ref 23]

Nuclear Energy Institute (NEI) formed a "New Plant Regulatory Framework Task Force" which was charged with developing a new and optional risk-informed, performance-based regulatory framework for commercial nuclear reactors, focusing mainly on technical and operational requirements. The results of this task force is documented in a white paper, NEI 02-02, entitled "A Risk-Informed, Performance-Based Regulatory Framework for Power Reactors," date May 2002. The paper includes a discussion on "How to treat defense-in-depth in a risk-informed, performance-based regime."

The paper provides principles for a risk-informed, performance-based regulatory framework where one principle is "The framework shall provide for defense-in-depth through requirements and processes that include design, construction, regulatory oversight and operating activities. Additional defense-in-depth shall be provided through the application of deterministic design and operational features for events that have a high degree of uncertainty with significant consequences to public health and safety." The paper does provide the guidance for achieving its defined principle on defense-in-depth. The guidance involves a series of iterative steps:

1. The first step is to complete the initial design.

2. The second step is to perform a risk assessment of the design that includes a PRA. At this point, the design may be modified to meet risk acceptance criteria (which would need to be defined) and in internal industry and licensee guidelines. As a result of any modifications to the design, the PRA would be revised to reflect the changes.

The next series of steps involves addressing the uncertainties. The paper states that "the defense-in-depth opportunities are considered to compensate for unacceptable risk uncertainty." These steps are "based on the cornerstones established in the reactor oversight process that encompass design, construction, regulatory oversight and operational activities."

3. The third step involves identifying key uncertainties.

4. The forth step is to perform an assessment regarding the acceptability of the identified uncertainties. If it is determined that the uncertainties are acceptable, then the design may be considered final. However, if it is determined that the uncertainties are not considered acceptable, then "four discrete defense-in-depth options" are defined.

5. The fifth step defines the four options as:
   - Define risk management activity
   - Increase performance monitoring
   - Add safety margin
   - Add redundancy or diversity

6. The sixth step re-evaluates the acceptability of the uncertainties. If determined acceptable, then the design can be considered final; however, it determined unacceptable, then the design and PRA are revisited.

Petition on Davis-Besse, 2003 [Ref 24]

By letter dated February 3, 2003, Congressman Dennis Kucinich, Representative for the 10th Congressional District of the State of Ohio in the United States House of Representatives, filed a Petition requesting that the NRC "immediately revoke the First Energy Nuclear Operating Company's (FENOC's or the licensee's) license to operate the Davis-Besse Nuclear Power Station, Unit 1 (Davis-Besse)." In the Director's Decision, it is stated that

> "The NRC's approach to protecting public health and safety is based on the philosophy of "defense-in-depth." Briefly stated, this philosophy
>
> 1. requires the application of conservative codes and standards to establish substantial safety margins in the design of nuclear plants;

2. requires high quality in the design, construction, and operation of nuclear plants to reduce the likelihood of malfunctions, and promotes the use of automatic safety system actuation features;

3. recognizes that equipment can fail and operators can make mistakes and, therefore, requires redundancy in safety systems and components to reduce the chance that malfunctions or mistakes will lead to accidents that release fission products from the fuel;

4. recognizes that, in spite of these precautions, serious fuel-damage accidents may not be completely prevented and, therefore, requires containment structures and safety features to prevent the release of fission products; and

5. further requires that comprehensive emergency plans be prepared and periodically exercised to assure that actions can and will be taken to notify and protect citizens in the vicinity of a nuclear facility."

Remarks of Nils J. Diaz, Chairman, U.S. Nuclear Regulatory Commission, 2004 [Ref 25]

On June 3, 2004, at the 3rd Annual Homeland Security Summit Session on "The Best-Laid Plans: A Case Study in Preparedness Planning," Chairman Diaz gave a speech entitled "The Very Best-Laid Plans (the NRC's Defense-in Depth Philosophy)." In his remarks, he states that defense-in-depth "is really more than a philosophy: it is an action plan, an approach to ensuring protection. The concept of "defense-in-depth" is a centerpiece of our approach to ensuring public health and safety, and it goes beyond pieces of equipment. It calls for, among other things, high quality design, fabrication, construction, inspection, and testing; plus multiple barriers to fission product release; plus redundancy and diversity in safety equipment; plus procedures and strategies; and lastly, emergency preparedness, which includes coordination with local authorities, sheltering, evacuation, and/or administration of prophylactics (for example, potassium in defense-in-depth tablets). This approach addresses the expected as well as the unexpected; it actually accommodates the possibility of failures. . . . The events of 9/11 brought to this country a new recognition of the importance of physical security and emergency preparedness in the world of 21st century America. . . What the post-9/11 review of security issues highlighted is how tightly interconnected are reactor safety, security and emergency preparedness. Many of the same issues are involved in avoiding and mitigating reactor accidents as in preventing and mitigating acts of terrorism. . . The fact is that nuclear reactor design requirements for structures to withstand severe external events (hurricanes, tornadoes, and floods), and for safety systems to include redundant emergency core cooling, redundant and diverse heat removal, fire protection features, and station blackout capabilities, provide built-in means of dealing with attempted terrorist attacks. Existing emergency operating procedures and enhanced severe accident management guidelines are well suited for mitigating the effects of accidents or intentional attacks on nuclear power plants. . . . Further, the studies confirm that even in the unlikely event of a radiological release due to terrorist use of a large aircraft, NRC's emergency planning basis remains valid. Defense-in-depth provides the time needed to use the right protective strategies. . . . The analyses, conclusions, and insights that I just presented for nuclear power plants also apply to spent fuel pools, since they are also well engineered and protected structures, and are amenable to simple and effective mitigative actions, if needed. . . . Defense-in-depth works for nuclear facilities. It is definitely a case study in total preparedness planning."

Digital Instrumentation and Controls, 1994, 1996, 1997, 2007, 2009 [Ref 26]

There are several documents that discuss this issue. These include NUREG/CR-6303 (Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems) dated December 1994; Regulatory Guide 1.152 (criteria for Digital Computers in Safety Systems of Nuclear Power Plants), dated January 1996; NUREG-0800, Branch Technical Position (BTP) HICB-19 (Guidance for Evaluation of Defense-in-depth and Diversity in Digital Computer-Based Instrumentation and Control Systems), dated June 1997; NUREG-0800, Standard Review Plan (SRP), BTP 7-19 (Guidance for Evaluation of Defense-in-depth and Diversity in Digital Computer-Based Instrumentation and Control Systems), dated March 2007; and DI&C-ISG-02 (Digital Instrumentation and Controls), dated June 2009.

NUREG/CR-6303, 1994

In NUREG/CR-6303, entitled "Method for Performing Diversity and Defense-in-depth Analyses of Reactor Protection Systems," states that "Defense-in-depth is a principle of long standing for the design, construction and operation of nuclear reactors, and may be thought of as requiring a concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. The classic three physical barriers to radiation release in a reactor—cladding, reactor pressure vessel, and containment—are an example of defense-in-depth.

"Echelons of defense" are specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it. Specifically, the echelons are the control system, the reactor trip or scram system, the Engineered Safety Features actuation system (ESFAS), and the monitoring and indicator system. The echelons may be considered to be concentrically arranged in that when the control system fails, the reactor trip system shuts down reactivity; when both the control system and the reactor trip system fail, the ESFAS continues to support the physical barriers to radiological release by cooling the fuel, thus allowing time for other measures to be taken by reactor operators to reduce reactivity. All four echelons depend upon sensors to determine when to perform their functions, and a serious safety concern is to ensure that no more than one echelon is disabled by a common sensor failure or its direct consequences.

Regulatory Guide 1.152, 1996

This Regulatory Guide (RG) describes a method acceptable to the NRC staff for complying with the Commission's regulations for promoting high functional reliability and design quality for the use of digital computers in safety systems of nuclear power plants. In this RG, it notes the staff concern regarding the potential to propagate a common cause failure of redundant equipment and the software programming errors can defeat the redundancy achieved by the hardware architectural structure. Because of this concern, the RG states that "the NRC staff has placed significant emphasis on defense-in-depth against propagation of common cause failures within and between functions." In addition, it states that "the principle of defense-in-depth is to provide several levels or echelons of defense to challenges to plant safety, such that failures in equipment and human error will not result in an undue threat to public safety. A detailed defense-in-depth study and failure mode and effect analysis or an analysis of abnormal conditions or events should be made to address common cause failure."

NUREG-0800, BTP HICB-19, 1997

One of the main objectives of this branch technical position (BTP) is "verify that adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements." In the BTP, it provides the same four echelons of defense as listed in NUREG/CR-6303; however, associated acceptance guidelines are provided:

- "Control system – The control echelon consists of that non-safety equipment which routinely prevents reactor excursions toward unsafe regimes of operation, and is used for normal operation of the reactor.

- RTS – the reactor trip echelon consists of that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

- ESFAS – The ESFAS echelon consists of that safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment).

- Monitoring and indicators – The monitoring and indication echelon consists of sensors, displays, data communications systems, and manual controls required for operators to respond to reactor events."

NUREG-0800, BTP 7-19, 2007

In the BTP, one of the main objectives is the same as noted in BTP HICB-19. The same four defense echelons are also defined in this BTP. The BTP also provides a four-point position that requires a D3 (diversity and defense-in-depth) assessment:

"Point 1 The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.

Point 2 In performing the assessment, the vendor or applicant/licensee should analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events.

Point 3 If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

Point 4 A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3."

DI&C-ISG-02, 2009

This Interim Staff Guidance (ISG) provides acceptable methods for implementing diversity and defense-in-depth (D3) in digital I&C system designs. With regard to specifics, this ISG is consistent with the BTP 7-19 and NUREG/CR-6303.

NUREG-1860, 2007 [Ref 27]

The comprehensive examination of defense-in-depth can be found In NUREG-1860, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing" (also known as the technology-neutral framework, or framework). It addresses several questions: what should be the role of defense-in-depth, how should defense-in-depth be factored into the regulatory framework, what is the purpose of defense-in-depth, and how is defense-in-depth related to uncertainties? It states that "The ultimate purpose of defense-in-depth is to compensate for uncertainty (e.g., uncertainty due to lack of operational experience with new technologies and new design features, uncertainty in the in the type and magnitude of challenges to safety)." Defense-in-depth, in the NUREG, is defined as "defense-in-depth is an element of NRC's safety philosophy that is used to address uncertainty by employing successive measure including safety margins to prevent and mitigate damage if a malfunction, accident or naturally caused event occurs at a nuclear facility." The Framework defines four objectives for defense-in-depth:

- "compensate for uncertainties, including events and event sequences which are unexpected because their existence remained unknown during the design phase,
- compensate for potential adverse equipment performance, as well as human actions of commission (intentional adverse acts are part of this) as well as omission,
- maintain the effectiveness of barriers and protective systems by ensuring multiple, generally independent and separate, means of accomplishing their functions, and
- protect the public and environment if these barriers are not fully effective.

The first objective emphasizes the importance of providing some means to counterbalance unexpected challenges. The second objective addresses uncertainty in equipment and human actions. It encompasses equipment design and fabrication errors, as well as both deliberate acts meant to compromise safety, and errors or inadequacy in carrying out procedures meant to ensure safety. The third objective addresses the uncertainty in the performance of the systems, structures, and components (SSCs) that constitute the barriers to radionuclide release, as well as in the SSCs whose function is to protect those barriers. The final objective emphasizes the concept of layers of protection, in that it addresses the need for additional measures should the barriers to radionuclide release fail after all."

The Framework approach incorporates both deterministic and probabilistic elements.

"The two principal deterministic defense-in-depth elements of the approach are

1. Ensuring the implementation of all of the five protective strategies. . . The protective strategies were selected based on engineering judgment, as a minimal set to provide protection for lines of defense against accident and exposure of the public and environment to radioactive material.

2. Ensuring that the defense-in-depth principles . . . are followed to develop licensing potential requirements. . . the defense-in-depth principles are established by examining the different kinds of uncertainties to be treated, and incorporating successful past practices and lessons learned related to defense-in-depth.

The probabilistic elements of the approach consist of

1. Using the PRA, to the extent possible, to search for and identify unexpected scenarios, including their associated uncertainties.

2. To subsequently establish adequate defense-in-depth measures, including safety margins, to compensate for those scenarios and their uncertainties which are quantified in the PRA model. . ."

The process chosen in the Framework to initially identify and define the requirements and regulations is to define safety fundamentals using a defense-in-depth approach, in the form of protective strategies that, if met, will ensure the protection of the public health and safety with a high degree of confidence. The protective strategies provide defense-in-depth that offer multiple layers of protection of public health and safety. The five protective strategies and their objectives are:

1. "The **Physical Protection** objective is to protect workers and the public against intentional acts (e.g., attack, sabotage, and theft) that could compromise the safety of the plant or lead to radiological release.

2. The **Stable Operation** objective is to limit the frequency of events that can upset plant stability and challenge safety functions, during all plant operating states, i.e., full power, shutdown, and transitional states.

3. The **Protective Systems** objective is to ensure that the systems that mitigate initiating events are adequately designed, and perform adequately, in terms of reliability and capability, to satisfy the design assumptions on accident prevention and mitigation during all states of reactor operation. Human actions to assist these systems and protect the barriers are included here.

4. The **Barrier Integrity** objective is to ensure that there are adequate barriers to protect the public from accidental radionuclide releases from all sources. Adequate functional barriers need to be maintained to protect the public and workers from radiation associated with normal operation and shutdown modes and to limit the consequences of reactor accidents if they do occur. Barriers can include physical barriers as well as the physical and chemical form of the material that can inhibit its transport if physical barriers are breeched.

5. The **Protective Actions** objective is to ensure that adequate protection of the public health and safety in a radiological emergency can be achieved should radionuclides penetrate the barriers designed to contain them. Measures include emergency procedures, accident management, and emergency preparedness."

The Framework also defines a set of six defense-in-depth principles with associated criteria that are evaluated against the requirements for each protective strategy. The principles defined in the Framework include:

- "**Measures against intentional as well as inadvertent events are provided**. -- This principle ensures that defense-in-depth measures are applied not just against random failures of SSCs or human errors, but also against acts of sabotage, theft of nuclear materials, armed intrusion, and external attack. Such measures can be incorporated in the design of the plant, be part of operating practices, and include the capability to respond to intrusion or attack.

- **The design provides accident prevention and mitigation capability**. -- This principle ensures an apportionment in the plant's capabilities between limiting disturbances to the plant and mitigating them, should they occur. This apportionment is present in both the design and operation of the plant. It is not meant to imply an equal apportionment of capabilities. Some of the protective strategies (stable operation, protective systems) are more preventive, while others (protective actions, and to some extent barrier integrity) are more mitigative. Physical protection clearly falls into both areas. By requiring that all of the strategies have to be incorporated into plant design and operation, the presence and availability of both preventive and mitigative features is ensured.

- **Accomplishment of key safety functions is not dependent upon a single element of design, construction, maintenance or operation**. -- This principle ensures that redundancy, diversity, and independence in SSCs and actions are incorporated in the plant design and operation, so that no key safety functions will depend on a single element (i.e., SSC or action) of design, construction, maintenance or operation. The key safety functions include (1) control of reactivity, (2) removal of decay heat, and the functionality of physical barriers to prevent the release of radioactive materials.

- **Uncertainties in SSCs and human performance are accounted for in the safety analysis and appropriate safety margins are provided**. -- This principle ensures that when risk and reliability goals are set, at the high level and the supporting intermediate levels, the design and operational means of achieving these goals account for the quantifiable uncertainties, and provide some measure of protection against the ones that cannot be quantified as well.

- **The plant design has containment functional capability to prevent an unacceptable release of radioactive material to the public**. -- This principle ensures that regardless of the features incorporated in the plant to prevent an unacceptable release of radioactive material from the fuel and the reactor coolant system (RCS), there are additional means to prevent an unacceptable release to the public should such a release occur that has the potential to exceed the dose acceptance criteria. The purpose of this principle is to protect against unknown phenomena and threats, i.e., to compensate for completeness uncertainty affecting the magnitude of the source term.

- **Plants are sited at locations that facilitate the protection of public health and safety**. -- This principle ensures that the location of regulated facilities facilitates the protection of public health and safety by considering population densities and the proximity of natural and human-made hazards in the siting of plants. Physical protection aspects associated with security concerns are additional considerations in selecting the site. Siting factors and criteria are important in ensuring that radiological doses from normal operation and postulated accidents will be acceptably low, that natural phenomena and potential human made hazards will be accounted for in the design of the plant, that site characteristics are such that adequate security measures to protect the plant can be developed, and that

physical characteristics unique to the proposed site that could pose a significant impediment to developing emergency plans are identified."

INL NGNP, 2009 [Ref 28]

Idaho National Laboratory (INL) published INL/EXT-09-17139, "Next Generation Nuclear Plant Defense-in-Depth Approach," in December 2009. The report documents a definition of defense-in-depth and the approach to be used to assure that its principles are satisfied for the Next Generation Nuclear Plant (NGNP) project. It states the "defense-in-depth is a safety philosophy in which multiple lines of defense and conservative design and evaluation methods are applied to ensure the safety of the public. The philosophy is also intended to deliver a design that is tolerant to uncertainties in knowledge of plant behavior, component reliability, or operator performance that might compromise safety." For NGNP, a defense-in-depth framework is proposed that defines three major elements:

1. "Plant capability defense-in-depth that reflects the decision made by the designer in the selection of functions, structures, systems and components for the design that ensure defense-in-depth in the physical plant.

2. Programmatic defense-in-depth that reflects the decisions made regarding the processes of manufacturing, constructing, operating, maintaining, testing, and inspecting the plant and the processes undertaken that ensure plant safety throughout the lifetime of the plant.

3. Risk-informed evaluation of defense-in-depth that reflects the development and evaluation of strategies that manage the risks of accidents, including the strategies of accident prevention and mitigation. This aspect provides the framework for performing deterministic and probabilistic safety evaluations, which help determine how well the other two defense-in-depth elements have been implemented."

For each of the above elements, principles and criteria are defined for each. For example, for plant capability defense-in-depth, it includes "the use of multiple barriers, diverse and redundant means to perform safety functions to protect the barriers, conservative design principles and safety margins, site selection, and other physical and tangible elements of the design that use multiple lines of defense and conservative design approaches to protect the public."

As part of the risk-informed evaluation defense-in-depth element, a decision process with associated criteria is proposed. It evaluates whether the developed frequency-consequence curve has been met in conjunction with determining if there is adequate prevention and mitigation and adequate safety margins. It further evaluates whether the uncertainties have been adequately addressed and if the defense-in-depth principles have been met. If the above have each been adequately addressed, then it is determined that there is adequate treatment of defense-in-depth. If at any point in the decision process one of the decisions has not been adequately addressed, then plant defense-in-depth capabilities and the programmatic assurance are each enhanced and the entire decision criteria are re-evaluated.

RG 1.174, 2012 [Ref 29]

RG 1.174, Revision 2, dated May 2011, provides guidance on the use of PRA findings and risk insights to support licensee requests for changes to a plant's licensing basis (LB), as in requests for license amendments and technical specification. In the RG, it provides an approach for "implementing risk-informed decisionmaking, LB changes are expected to meet a set of key

principles. Some of these principles are written in terms typically used in traditional engineering decisions (e.g., defense-in-depth). While written in these terms, it should be understood that risk analysis techniques can be, and are encouraged to be, used to help ensure and show that these principles are met." One principle states "The proposed change is consistent with a defense-in-depth philosophy."

In response to a Commission SRM, RG 1.174 is being revised to better address defense-in-depth. Proposed Revision 3 (Draft Guide (DG) 1285) was issued in May 2012 and states:

> "The engineering evaluation should evaluate whether the impact of the proposed LB change (individual and cumulative) is consistent with the defense-in-depth philosophy. In this regard, the intent of this principle is to ensure that the philosophy of defense-in-depth is maintained, not to prevent changes in the way defense-in-depth is achieved. 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.
>
> At a high level, there are three layers of defense against the consequences of an event at a nuclear facility. The three layers are (1) protection to prevent accidents from occurring, (2) mitigation of accidents if they occur, and (3) emergency preparedness to minimize the public health consequences of releases if they occur. An important element of the three layers is that a reasonable balance should be preserved among them. Another major aspect of defense-in-depth is maintaining multiple barriers to the release of fission products. While it could be reasoned that multiple fission product barriers represent one approach to implementing the three high-level layers of defense-in-depth, the use of barriers is so fundamental to this philosophy that it warrants its own discussion."

DG 1285 provides a discussion on the three high-level layers of defense-in-depth, followed by a discussion of fission product barriers. A discussion is also provided of some factors that licensees should consider when assessing whether a proposed change to the plant is consistent with the three layers and the multiple-barrier philosophy.

> "<u>Preserving Balance Among the Three Layers of Defense-in-Depth</u>
>
> A reasonable balance of these layers (i.e., preventing accidents, mitigating accidents, and emergency preparedness) helps to ensure an apportionment of the plant's capabilities between limiting disturbances to the plant and mitigating their consequences. "Balance" is not meant to imply an equal apportionment of capabilities. A reasonable balance is preserved if the proposed plant change does not significantly reduce the effectiveness of a layer that exists in the plant design before the proposed change. The NRC recognizes that there may be aspects of a plant's design that may cause one of the three layers to be adversely affected. For these situations, the balance between the other two layers becomes especially important when evaluating the impact of a proposed change to the LB and its impact on defense-in-depth.

Preserving Multiple Fission Product Barriers

The plant's LB includes fission product barriers and engineered structures, systems, and components (SSCs) that support or maintain those barriers. These barriers, as exemplified by current reactors, are generally considered to be the fuel elements' cladding, the reactor coolant system pressure boundary, and the containment systems and structure. Adverse conditions created during reactor accidents (e.g., high temperature, high pressure) can challenge the integrity of barriers. Consequently, the concept of multiple barriers provides for separate means to contain and mitigate fission products. The intent of preserving multiple barriers may be adversely affected if the proposed plant change reduces the effectiveness of any of the barriers. The licensee should evaluate the impact of the proposed change on the fission product barriers and supporting systems and consider any cause and effect relationship between the barrier and the aspect of the plant proposed to be changed.

Factors To Consider When Evaluating the Impact of a Change on Defense-in-Depth

When evaluating the impact of a proposed plant change on the three high-level layers (Section 2.1.1.1 above) and the multiple fission product barriers (Section 2.1.1.2 above) of defense-in-depth, the licensee should consider the following factors:

- programmatic activities as compensatory measures,
- system redundancy, independence, and diversity,
- potential for CCF,
- reliance on plant operators, and
- intent of the plant's design criteria.

These factors are not meant to be a comprehensive list, but are intended to help the licensee assess how the proposed change could affect one of the three layers of defense or one of the multiple barriers."

DG 1285 provides a discussion explaining each of the above factors including examples for additional clarification.

There are other RGs where defense-in-depth is either mentioned or discuss, see Table 2.

NRC Glossary, 2012 [Ref 30]

The NRC Glossary describes 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. For further information, see Speech No. S-04-009, *The Very Best-Laid Plans (the NRC's Defense-in Depth Philosophy)*."

Proposed Risk Management Regulatory Framework, 2012 [Ref 31]

At the request of Chairman Gregory B. Jaczko, a task force headed by Commissioner George Apostolakis was assembled whose charter was to develop a strategic vision and options for adopting a more comprehensive, holistic, risk-informed, performance-based regulatory

approach for reactors, materials, waste, fuel cycle, and transportation that would continue to ensure the safe and secure use of nuclear material. In the report, defense-in-depth plays a key role in their recommendation regarding a proposed Risk Management Regulatory Framework. The task force reviewed across the various arenas and notes:

- "After decades of use, there is no clear definition or criteria on how to define adequate defense-in-depth protections.

- The concept of defense-in-depth has served the NRC and the regulated industries well and continues to be valuable today. However, it is not used consistently, and there is no guidance on how much defense-in-depth is sufficient**.**

- The term "defense-in-depth" has been used since the 1960s in the context of ensuring nuclear reactor safety. The concept was developed and applied to compensate for the recognized lack of knowledge of nuclear reactor operations and the consequences of potential accidents.

- The Risk Management Task Force (RMTF) has reviewed a number of documents[1] that historically have helped to shape the characterization of defense-in-depth. Since the characterizations provided in these documents are not completely consistent and are focused on operating power reactors, the RMTF concluded that clarifying what the U.S. Nuclear Regulatory Commission (NRC) means by defense-in-depth is a necessary part of the development of a holistic strategic vision."

The RMTF characterizes defense-in-depth as follows:

"Provide risk-informed and performance-based defense-in-depth protections to:

- Ensure appropriate barriers, controls, and personnel to prevent, contain, and mitigate exposure to radioactive material according to the hazard present, the relevant scenarios, and the associated uncertainties.
  - Each barrier is designed with sufficient safety margins to maintain its functionality for relevant scenarios and account for uncertainties.
  - Systems that are needed to ensure a barrier's functionality are designed to ensure appropriate reliability for relevant scenarios.
  - Barriers and systems are subject to performance monitoring.

  And

- Ensure that the risks resulting from the failure of some or all of the established barriers and controls, including human errors, are maintained acceptably low."

[1] The documents reviewed by the RMTF include (1) Safety," INSAG-10, A Report by the International Nuclear Safety Advisory Group, 1996; (2) Idaho National Laboratory, "Next Generation Nuclear Plant Defense-in-Depth Approach," INL/EXT-0917139, December 2009; (3) U.S. Nuclear Regulatory Commission, Staff Requirements Memorandum Regarding SECY-98-44, "White Paper on Risk-Informed and Performance-Based Regulation," March 1, 1999, Agencywide Documents Access and Management System (ADAMS) Accession No. ML003753601; (4) U.S. Nuclear Regulatory Commission, "Risk-Informed Categorization and Treatment of Structures, Systems, and Components for Nuclear Power Reactors," 10 CFR 50.69, Published in the Federal Register on November 22, 2004 (69 FR 68008); and U.S. Nuclear Regulatory Commission, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing," NUREG-1860, Volume 1, December 2007, ADAMS Accession No. ML080440170.

SECY's, 1977-2011

There have been numerous SECY's over the years that have discussed defense-in-depth, these are summarized in Table 3.

NEA/CNRA/CSNI Joint Workshop on Challenges and Enhancements to DiD in light of the Fukushima Dai-ichi Accident, 2013

On June 5th, 2013, OECD NEA/CNRA/CSNI (Organization for Economic Co-operation and Development/Nuclear Energy Agency/Committee on Nuclear Regulatory Activities/Committee on the Safety of Nuclear Installations) held an international workshop on defense-in-depth. Reference 32 provides the presentations by the various speakers at the workshop. In reviewing the presentations, several common key messages among the presenters are noted:

- Defense-in-depth has worked well
- Lower frequency but higher consequence events occur and can breach all layers of defense-in-depth
- Concept of defense-in-depth involves different, multiple barriers
- Independence among barriers is critical
- Prevention and mitigation are both essential
- Need to strengthen the role of defense-in-depth

Table 1 ACRS Discussions on Defense in Depth (see Notes 1 and 2)

Document	Subject	Defense in Depth Discussion
Letter from D. A. Powers, ACRS Chairman, to Honorable S. A. Jackson, NRC Chairman, dated February 18, 1999	NFPA 805, "Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plants"	There is an alignment of defense in depth for fire protection and risk analysis. Defense in depth for fire protection consists of steps to prevent fires from occurring, to detect and suppress fires, and to protect safety-related equipment from the effects of fires. Fire risk analyses attempt to quantify the effectiveness of these defense-in-depth steps.
Letter from D. A. Powers, ACRS Chairman, to Honorable S. A. Jackson, NRC Chairman, dated May 19, 1999	The Role of Defense In Depth In a Risk-Informed Regulatory System	ACRS outlines an approach for developing a systematic methodology for the evaluation of defense-in-depth; however, lacking such a methodology at the present time, decisions on defense-in-depth will have to be based on judgment.
Letter from D. A. Powers, ACRS Chairman, to Honorable R. A. Meserve, NRC Chairman, dated February 8, 2000	SECY-00-0011, "Evaluation of the Requirement for Licensee to Update Their Inservice Inspection and Inservice Testing Programs Every 120 Months"	ACRS continue to believe that 10 CFR 50.109 evaluation are not well suited to assess the appropriateness of defense-in-depth measures, such as the ASME Code updates.
Letter from D. A. Powers, ACRS Chairman, to Honorable R. A. Meserve, NRC Chairman, dated February 14, 2000	Impediments to the Increased Use of Risk-Informed Regulation	ACRS states that if defense-in-depth is viewed as measures taken to compensate for the PRA inadequacies and uncertainties, then there is a need for guidance to help quantify how many compensatory measures are necessary and how good these have to be.
Letter from D. A. Powers, ACRS Chairman, to Honorable R. A. Meserve, NRC Chairman, dated April 17, 2000	Reactor Safety Goal Policy Statement	ACRS states that NRC's defense-in-depth philosophy calls for a requirement that the uncertainties be quantified or estimated and entered into the decision on how much to rely strictly on the PRA results (rationalist approach) and how much to fall back on the traditional judgmental application of defense in depth (structuralist approach).
Letter from D. A. Powers, ACRS Chairman, to Honorable R. A. Meserve, NRC Chairman, dated May 25, 2000	Use of Defense In Depth in Risk-Informing NMSS Activities	ACRS and NRC staff discusses the NRC's defense-in-depth philosophy in the regulatory process emphasizing its role in NMSS activities, particularly in the licensing of a high-level radioactive waste repository.
Letter from D. A. Powers, ACRS Chairman, to Dr. W. D. Travers, NRC Executive Director for Operations, dated September 8, 2000	Proposed High-Level Guidelines for Performance-Based Activities	ACRS recommends that guidance should be given on the extent to which multiple performance parameters that proved redundant information should be use to satisfy the defense-in-depth philosophy.
Letter from D. A. Powers, ACRS Chairman, to Honorable R. A. Meserve, NRC Chairman, dated September 14, 2000	Pre-Application Review of the AP1000 Standard Plant Design – Phase I	ACRS states that if the staff is to properly assess the AP1000 design with respect to acceptance values of risk metrics and its compliance with the defense-in-depth philosophy, the PRA will need to include an uncertainty analysis. Without such a PRA, ACRS will be faced with insufficient information on which to base its judgment on the defense-in-depth acceptability of the AP1000 containment.

Table 1 ACRS Discussions on Defense in Depth (see Notes 1 and 2)

Document	Subject	Defense in Depth Discussion
Letter from G. E. Apostolakis, ACRS Chairman, to Honorable R. A. Meserve, NRC Chairman, dated February 14, 2002	Review and Evaluation of the Nuclear Regulatory Commission's Safety Research Program	Some of the new plant designs may also challenge current defense-in-depth precepts. For example, the traditional balance between prevention and mitigation may not be offered by new designs that rely heavily on fuel integrity during accidents rather than mitigating systems. Uncertainty criteria to allow setting appropriate limits on defense-in-depth requirements may need to be developed.
Letter from G. E. Apostolakis, ACRS Chairman, to Honorable R. A. Meserve, NRC Chairman, dated November 13, 2002	Recommendations Proposed by the Office of Nuclear Regulatory Research for Resolving Generic Safety Issue-189, "Susceptibility of Ice Condenser and Mark III Containments to Early Failure From Hydrogen Combustion During a Severe Accident"	ACRS agreed with the NRC staff that backup power for the hydrogen igniters as a safety enhancement was justified on a defense-in-depth basis, and the ACRS suggested that NRR investigate the viability of implementing backup power requirements through plant-specific severe accident management guidelines (SAMGs).
Letter from M. V. Bonaca, ACRS Chairman, to Dr. W. D. Travers, NRC Executive Director for Operations, dated April 29, 2003	NUREG-CR-6813, "Issues and Recommendation for Advancement of PRA Technology in Risk-Informed Decision Making"	The report states "Although it was obvious that the consequences of a severe core damage event would exceed those of a design basis event, a key insight here was that the frequency of severe core damage events was much higher than expected using traditional defense-in-depth thinking."
Letter from M. V. Bonaca, ACRS Chairman, to Honorable N. J. Diaz, NRC Chairman, dated April 22, 2004	Options and Recommendations for Policy Issues Related to Licensing Non-Light Water Reactor Designs	The intent of a core damage frequency (CDF) goal has always been twofold: (1) to limit the chances of having an accident anywhere in the country over the projected lifetime of the plants, and (2) to serve as a defense-in-depth measure that balances accident prevention and mitigation for any given design. ACRS states that the extension of this concept to a site CDF goal is going far beyond the original intent.
Letter from M. V. Bonaca, ACRS Chairman, to Honorable N. J. Diaz, NRC Chairman, dated April 27, 2004	SECY-04-0037, "Issues Related to Proposed Rulemaking to Risk-Inform Requirements Related to Large Break Loss-of-Coolant Accident (LOCA) Break Size and Plans for Rulemaking on LOCA with coincident Loss-of-Offsite Power"	ACRS recommends that the risk-informed revision to 10 CFR 50.46 should permit a wide range of applications of the new break size as long as it can be demonstrated that the resulting changes in risk are small and adequate defense-in-depth is maintained. ACRS recommends that explicit criteria to ensure mitigative capability for breaks beyond the new maximum break size and to limit the risk associated with late containment failure should be developed as part of the revised rule to ensure that sufficient defense-in-depth is maintained as plant changes are made.
Letter from M. V. Bonaca, ACRS Chairman, to Honorable N. J. Diaz, NRC Chairman, dated July 20, 2004	Report on the Safety Aspects of the Westinghouse Electric Company Application for Certification of the AP1000 Passive Plan Design	The AP1000 design has a defense-in-depth provision for external flooding of the reactor vessel which is intended to provide for in-vessel retention of any accident-induced core melt. The active nonsafety-related systems support normal operation and minimize challenges to the passive safety systems. Although these systems are not credited in the safety evaluation case, they provide additional defense-in-depth.

Table 1 ACRS Discussions on Defense in Depth (see Notes 1 and 2)

Document	Subject	Defense in Depth Discussion
Letter from M. V. Bonaca, ACRS Chairman, to Honorable N. J. Diaz, NRC Chairman, dated November 2, 2004	Report on "An Overview of Differences in Nuclear Safety Regulatory Approaches and Requirements Between United States and Other Countries"	The report states that the U.S. safety philosophy of defense in depth was adopted by the regulatory authorities in western Europe, Japan, and Korea, not only for the barriers to the release of radioactive substances, but also in the design, construction, quality assurance, inspection, and operational practices. However, there may be differences in the implementation of the defense-in-depth principle, e.g., in levels of diversity and redundancy required from the safety systems.
Letter from M. V. Bonaca, ACRS Chairman, to Honorable N. J. Diaz, NRC Chairman, dated November 19, 2004	Draft Proposed Rule on Post-Fire Operator Manual Actions	The staff contends that fire detection and automatic suppression systems are necessary to preserve the physical component of a plant's fire protection defense-in-depth.
Letter from M. V. Bonaca, ACRS Chairman, to Honorable N. J. Diaz, NRC Chairman, dated December 10, 2004	Estimating Loss-of-Coolant Accident Frequencies Through the Elicitation Process	The ACRS state that the decisionmakers will have to compensate for the uncertainties created by these limitations by evaluating their impact and resorting to structuralist defense-in-depth measures (e.g., by adding conservatism to the ultimate results of the study).
Letter from M. V. Bonaca, ACRS Chairman, to L. A. Reyes, NRC Executive Director for Operations, dated December 17, 2004	Risk-Informing 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors	ACRS states that a risk-informed 10 CFR 50.46 should maintain defense in depth by including requirements intended to provide reasonable assurance of a coolable core geometry for breaks up to the double-ended guillotine break (DEGB) of the largest pipe in the reactor coolant system. The ACRS also states that a better quantitative understanding of the possible risk benefits of a smaller transition break size is needed to arrive at a final choice of the transition break size. If the defense-in-depth capability to mitigate breaks greater than the transition break size is maintained, a smaller choice of transition break size may be supportable.
Letter from G. B. Wallis, ACRS Chairman, to Honorable N. J. Diaz, NRC Chairman, dated January 4, 2006	Vermont Yankee Extended Power Uprate	ACRS states that the probabilities associated with the governing physical phenomena may be regarded as more secure than some other inputs to the usual PRA assessment. Conclusions based on them may help to convince those who doubt if conventional risk-based arguments alone should allow the relaxation of defense-in-depth that is achieved by the independence of cladding and containment barriers to radioactivity release.
Letter from G. B. Wallis, ACRS Chairman, to L. A. Reyes, NRC Executive Director for Operations, dated August 2, 2006	Draft NUREG Report, "Integrating Risk and Safety Margins"	ACRS states that the draft report could have substantial regulatory benefits by providing an approach to quantify changes in safety margins and defense in depth and therefore recommends that it should be pursued in the context of the technology-neutral framework and for future revisions of Regulatory Guide (RG) 1.174.

Table 1 ACRS Discussions on Defense in Depth (see Notes 1 and 2)

Document	Subject	Defense in Depth Discussion
Letter from G. B. Wallis, ACRS Chairman, to Honorable D. E. Klein, NRC Chairman, dated November 16, 2006	Draft Final Rule to Risk-Inform 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors"	ACRS states that proposed Rule needed to be revised to strengthen the assurance of defense in depth for breaks beyond the transition break size (TBS), in particular, by requiring that licensees submit the codes used for the analyses of breaks beyond the TBS to the NRC for review and approval.
Letter from W. J. Shack, ACRS Chairman, to Honorable D. E. Klein, NRC Chairman, dated July 27, 2007	Draft NUREG/CR, Review of NUREG-0654, Supplement 3, "Criteria for Protective Action Recommendations for Severe Accidents"	ACRS states considering challenges that may arise both from conventional reactor safety concerns and security concerns, ACRS concurs with the NRC staff's position that emergency preparedness is a critical element of defense-in-depth that should include protective actions for any scenario involving a potential release from the containment, including those with rapidly evolving source terms.
Letter from W. J. Shack, ACRS Chairman, to Honorable D. E. Klein, NRC Chairman, dated September 26, 2007	Development of a Technology-Neutral Regulatory Framework *ACRS review of draft NUREG-1860, "Framework for Development of a Risk-Informed, Performance-Based Alternative to 10 CFR Part 50"*	In the staff's current approach to a framework, these requirements have been used to develop an F-C curve where the frequency is frequency of an individual PRA sequence and the consequence is the dose associated with that sequence, calculated at prescribed distances that vary with the frequency. ACRS states that such an approach can also be viewed as a defense-in-depth measure that sets high-level requirements for reliability and inspection. Limits on the frequencies of smaller releases on this F-C curve control the allowable degradation of "barriers" that prevent the inadvertent release of radioactive material to the environment.
Letter from W. J. Shack, ACRS Chairman, to R. W. Borchardt, NRC Executive Director for Operations, dated October 29, 2008	Interim Letter 5: Chapters 19 and 22 of the NRC Staff's Safety Evaluation Report with Open Items Related to the Certification of the ESBWR Design	ACRS states that specific issues need to be clarified to ensure the functionality of the Basemat-internal Melt Arrest and Coolability device as a 'defense-in-depth measure for severe accident conditions.
Letter from M. V. Bonaca, ACRS Chairman, to R. W. Borchardt, NRC Executive Director for Operations, dated March 18, 2009	Crediting Containment Overpressure In Meeting the Net Positive Suction Head Required to Demonstrate That the Safety Systems Can Mitigate the Accidents as Designed	ACRS states If hardware changes are not practical and the requested amount and the duration of COP credit are not "small" or operator actions are introduced, Regulatory Guide 1.82 should be revised to request that the licensee provide additional analyses and/or tests to help understand the impact on safety margins and defense in depth of granting COP credit.
Letter from S. Abdel-Khalik, ACRS Chairman, to R. W. Borchardt, NRC Executive Director for Operations, dated May 19, 2010	Draft Guidance on Crediting Containment Accident Pressure in Meeting the Net Positive Suction Head Required to Demonstrate that Safety Systems Can Mitigate Accidents as Designed	In regards to the containment accident pressure credit issue, ACRS states that licensee should submit upper bound and mean estimates as well as the 95/95 estimate to proved a more complete assessment of the available margins and impact on defense-in-depth.

Table 1 ACRS Discussions on Defense in Depth (see Notes 1 and 2)

Document	Subject	Defense in Depth Discussion
Letter from S. Abdel-Khalik, ACRS Chairman, to Honorable G. B. Jaczko, NRC Chairman, dated September 17, 2010	Comments on SECY-10-0113, "Closure Options for Generic Safety Issue – 191, Assessment of Debris Accumulation in Pressurized Water Reactor Sump Performance"	ACRS agrees with NRC staff that that expanding the scope of GDC-4 to allow leak-before-break credit for resolving ECCS performance issues is a policy matter. ACRS agreed with NRC staff that the option would be inconsistent with the basic defense-in-depth principles of the NRC. In particular, this option enables a LOCA to disable both the system that prevents core damage (ECCS) as well as the system that mitigates offsite releases (containment spray).
Letter from S. Abdel-Khalik, ACRS Chairman, to R. W. Borchardt, NRC Executive Director for Operations, dated January 24, 2011	Draft Final Revision 2 to Regulatory Guide 1.174 and Revision 1 to Regulatory Guide 1.177	ACRS recommends the NRC staff should reinstate guidance on the consideration of late containment failure in RG 1.174; i.e., as part of the assessment of impacts on defense-in-depth, licensees should include an assessment of the potential for an increase in the likelihood of late containment failure. This assessment can be qualitative.
Letter from S. Abdel-Khalik, ACRS Chairman, to Honorable G. B. Jaczko, NRC Chairman, dated February 17, 2011	SECY-11-0014, "Use of Containment Accident Pressure in Analyzing Emergency Core Cooling System and Containment Heat Removal System Pump Performance in Postulated Accidents"	ACRS disagrees with NRC staff and states that crediting containment accident pressure is a serious compromise of the independence of the prevention and mitigation functions, a basic element of the defense-in-depth philosophy.
Letter from S. Abdel-Khalik, ACRS Chairman, to R. W. Borchardt, NRC Executive Director for Operations, dated May 19, 2011	Response to the February 5, 2011, EDO Letter Regarding the Final Safety Evaluation Report Associated with the Amendment to the AP1000 Design Control Document	ACRS states in order to ensure that the defense-in-depth role is fulfilled; unavailability of manual Diverse Actuation System should be minimized, limited to on the order of no more than 72 hours.

Notes:

1. This list is not meant to imply that it is complete, but to indicate the many ACRS letters and history of defense-in-depth that has been the attention of the Committee over the years.
2. This list of ACRS letters was compiled by Donald Chung, Dylanne Duvigneaud, Brian Metzgar, and Jigar Patel of NRR.

Table 2 Defense-in-depth Defined in Regulatory Guidance Documents (see Notes 1 and 2)

RG No.	Definition of Defense in Depth	Accession Number	Date
1.152	The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense in depth (provided by the reactor protection, engineered safety features actuation, control, and monitoring instrumentation and control systems) can be applied as defense against common-cause failures. Manual operator actuations of safety and nonsafety systems are acceptable, provided that the necessary diverse controls and indications are available to perform the required function under the associated event conditions and can be completed within the acceptable time.	ML102870022	1/31/2011
1.174	Defense in depth consists of a number of elements, as summarized below. These elements can be used as guidelines for making that assessment. Other equivalent acceptance guidelines may also be used. Consistency with the defense-in-depth philosophy is maintained if: • A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation. • Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided. • System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties (e.g., no risk outliers). • Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed. • Independence of barriers is not degraded. • Defenses against human errors are preserved. • The intent of the General Design Criteria in Appendix A to 10 CFR Part 50 is maintained.	ML023240437	11/29/2002
1.175	Same as RG 1.174	ML003740149	8/31/1998
1.176	The engineering evaluation should assess whether the impact of the proposed change is consistent with the defense-in-depth philosophy. An acceptable set of guidelines for making that assessment is summarized below. Other equivalent decision guidelines are acceptable. • A reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved.	ML003740172	8/31/1998

Table 2 Defense-in-depth Defined in Regulatory Guidance Documents
(see Notes 1 and 2)

RG No.	Definition of Defense in Depth	Accession Number	Date
	• Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided. • System redundancy, independence, and diversity are preserved commensurate with the expected frequency and consequences of challenges to the system and uncertainties (e.g., no risk outliers). • Defenses against potential common cause failures are preserved and the potential for introduction of new common cause failure mechanisms is assessed. • Independence of barriers is not degraded. • Defenses against human errors are preserved. • The intent of the General Design Criteria in Appendix A to 10 CFR 50 is maintained.		
1.177	"The defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions and prevent the release of radioactive material. It has been and continues to be an effective way to account for uncertainties in equipment and human performance. When a comprehensive risk analysis can be performed, it can be used to help determine the appropriate extent of defense in depth (e.g., balance among core damage prevention, containment failures, and consequence mitigation) to ensure protection of public health and safety." Consistency with the defense-in-depth philosophy is maintained if: • A reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved, i.e., the proposed change in a TS has not significantly changed the balance among these principles of prevention and mitigation, to the extent that such balance is needed to meet the acceptance criteria of the specific design basis accidents and transients, consistent with 10 CFR 50.36. TS change requests should consider whether the anticipated operational changes associated with a TS change could introduce new accidents or transients or could increase the likelihood of an accident or transient (as is required by 10 CFR 50.92). • Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided, e.g., use of high reliability estimates that are primarily based on optimistic program assumptions. • System redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of		9/15/1998

Table 2 Defense-in-depth Defined in Regulatory Guidance Documents
(see Notes 1 and 2)

RG No.	Definition of Defense in Depth	Accession Number	Date
	challenges to the system, e.g., there are no risk outliers. The following items should be considered. - Whether there are appropriate restrictions in place to preclude simultaneous equipment outages that would erode the principles of redundancy and diversity, - Whether compensatory actions to be taken when entering the modified AOT for preplanned maintenance are identified, - Whether voluntary removal of equipment from service during plant operation should not be scheduled when adverse weather conditions are predicted or at times when the plant may be subjected to other abnormal conditions, and - Whether the impact of the TS change on the safety function should be taken into consideration. For example, what is the impact of a change in the AOT for the low-pressure safety injection system on the overall availability and reliability of the low-pressure injection function? • Defenses against potential common cause failures are maintained and the potential for introduction of new common cause failure mechanisms is assessed, e.g., TS change requests should consider whether the anticipated operational changes associated with a change in an AOT or STI could introduce any new common cause failure modes not previously considered. • Independence of physical barriers is not degraded, e.g., TS change requests should address a means of ensuring that the independence of barriers has not been degraded by the TS change (e.g., when changing TS for containment systems). • Defenses against human errors are maintained, e.g., TS change requests should consider whether the anticipated operation changes associated with a change in an AOT or STI could change the expected operator response or introduce any new human errors not previously considered, such as the change from performing maintenance during shutdown to performing maintenance at power when different personnel and different activities may be involved. • The intent of the General Design Criteria in Appendix A to 10 CFR Part 50 is maintained.		
1.178	"..The defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions and prevent the release of radioactive material. It has been and continues to be an effective way to account for uncertainties in equipment and human performance "	ML032510128	9/30/2003

Table 2 Defense-in-depth Defined in Regulatory Guidance Documents
(see Notes 1 and 2)

RG No.	Definition of Defense in Depth	Accession Number	Date
1.183	Consistency with the defense-in-depth philosophy is maintained if system redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties. In all cases, compliance with the General Design Criteria in Appendix A to 10 CFR Part 50 is essential. Modifications proposed for the facility generally should not create a need for compensatory programmatic activities, such as reliance on manual operator actions.	ML003716792	7/31/2000
1.186	The staff considers aspects of the designed defense-in-depth strategies such as redundancy, diversity, and independence to be important aspects of the plant's principal design criteria. These strategies and criteria are specifically required by several regulations, especially the General Design Criteria. These criteria require that such capabilities be implemented for individual structures, systems, and components through plant design features, such as multiple components, independent power supplies, and physical separation. These criteria provide part of the standard for judging the adequacy of the plant's design bases.	ML003754825	12/31/2000
1.189	Fire protection for nuclear power plants uses the concept of defense in depth to achieve the required degree of reactor safety. This concept entails the use of echelons of administrative controls, fire protection systems and features, and safe-shutdown capability to achieve the following objectives: • Prevent fires from starting. • Detect rapidly, control, and extinguish promptly those fires that do occur. • Protect SSCs important to safety, so that a fire that is not promptly extinguished by the fire suppression activities will not prevent the safe shutdown of the plant.	ML092580550	10/27/2009
1.191	The goal of the fire protection program during decommissioning of nuclear power plants is to provide an appropriate level of defense-in-depth protection against the threat of fires. Defense in depth, relative to fire protection, involves a comprehensive program of administrative controls, physical fire protection features, emergency response capabilities, and protection of SSCs necessary to prevent or mitigate the potential of an unacceptable release of radioactive materials. This combination of fire protection elements acts to reduce both the probability and consequences of fire events, and it provides assurance that the failure of any one element within the fire protection program is adequately compensated for by the others, thereby minimizing the risks to the public, environment, and plant personnel.	ML011500010	5/31/2001
1.195	Consistency with the defense-in-depth philosophy is maintained if: • A reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved, i.e., the proposed change in a TS has not significantly	ML031490640	5/31/2003

Table 2 Defense-in-depth Defined in Regulatory Guidance Documents
(see Notes 1 and 2)

RG No.	Definition of Defense in Depth	Accession Number	Date
	changed the balance among these principles of prevention and mitigation, to the extent that such balance is needed to meet the acceptance criteria of the specific design basis accidents and transients, consistent with 10 CFR 50.36. TS change requests should consider whether the anticipated operational changes associated with a TS change could introduce new accidents or transients or could increase the likelihood of an accident or transient (as is required by 10 CFR 50.92). • Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided, e.g., use of high reliability estimates that are primarily based on optimistic program assumptions. • System redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system, e.g., there are no risk outliers. The following items should be considered. – Whether there are appropriate restrictions in place to preclude simultaneous equipment outages that would erode the principles of redundancy and diversity, – Whether compensatory actions to be taken when entering the modified AOT for preplanned maintenance are identified, – Whether voluntary removal of equipment from service during plant operation should not be scheduled when adverse weather conditions are predicted or at times when the plant may be subjected to other abnormal conditions, and – Whether the impact of the TS change on the safety function should be taken into consideration. For example, what is the impact of a change in the AOT for the low-pressure safety injection system on the overall availability and reliability of the low-pressure injection function? • Defenses against potential common cause failures are maintained and the potential for introduction of new common cause failure mechanisms is assessed, e.g., TS change requests should consider whether the anticipated operational changes associated with a change in an AOT or STI could introduce any new common cause failure modes not previously considered. • Independence of physical barriers is not degraded, e.g., TS change requests should address a means of ensuring that the independence of barriers has not been degraded by the TS change (e.g., when changing TS for containment systems). • Defenses against human errors are maintained, e.g., TS change requests should consider whether the anticipated operation		

Table 2 Defense-in-depth Defined in Regulatory Guidance Documents
(see Notes 1 and 2)

RG No.	Definition of Defense in Depth	Accession Number	Date
	changes associated with a change in an AOT or STI could change the expected operator response or introduce any new human errors not previously considered, such as the change from performing maintenance during shutdown to performing maintenance at power when different personnel and different activities may be involved. • The intent of the General Design Criteria in Appendix A to 10 CFR Part 50 is maintained		
1.205	"…maintains fire protection defense in depth (fire prevention, fire detection, fire suppression, mitigation, and post-fire safe-shutdown capability)." The philosophy of nuclear safety defense in depth is maintained when a reasonable balance is preserved among prevention of core damage, prevention of containment failure, and mitigation of consequences. Regulatory Guide 1.174 provides guidance on maintaining the philosophy of nuclear safety defense in depth that is acceptable for NFPA 805 plant change evaluations.	ML091960258	10/30/2009
3.6	These various successive barriers to the release of radioactivity form a defense in depth on which overall safety depends. "Defense in depth" carries a broader connotation than just that related to successive protective features to prevent release of radioactivity. For example, the principle applies to control and alarm instrumentation (i.e., redundancy and backup); to people, equipment, and procedural interactions; and to review and audit by various groups at several levels of management.	ML003740163	4/8/1973
3.12	"…A tertiary confinement zone should be provided in areas outside the secondary confinement zone to provide defense in depth between potentially contaminated areas and the environment."	ML102730431	12/31/2010
4.2	The occurrences in Class 9 involve sequences of postulated successive failures more severe than those postulated for establishing the design basis for protective systems and engineered safety features. Their consequences could be severe. However, the probability of their occurrence is so small that their environmental risk is extremely low. Defense in depth (multiple physical barriers), quality assurance for design, manufacture, and operation, continued surveillance and testing, and conservative design are all applied to provide and maintain the required high degree of assurance that potential accidents in this class are, and will remain, sufficiently remote in probability that the environmental risk is extremely low.	ML003739519	7/31/1976
5.63	The requirement for a capability to detect attempted penetrations of the transport containing the SSNM was intended to provide SSNM shipments with defense in depth an added level of protection beyond that provided for by the controlled access area-which becomes especially important when many personnel must be allowed access into the controlled access area for servicing vehicles, handling other cargo, etc.	ML003739273	7/31/1982
5.71	Defense-in-depth strategies represent a documented collection of	ML092670517	10/9/2009

Table 2 Defense-in-depth Defined in Regulatory Guidance Documents
(see Notes 1 and 2)

RG No.	Definition of Defense in Depth	Accession Number	Date
	complementary and redundant security controls that establish multiple layers of protection to safeguard CSs. Under a defense-in-depth strategy, the failure of a single protective strategy or security control should not result in the compromise of a safety, important-to-safety, security, or emergency preparedness function. Defense-in-depth is achieved in multiple ways. From a security architecture perspective, it involves setting up multiple security boundaries to protect CSs and networks from cyber attack. In this way, multiple protection levels of mechanisms must fail for a cyber attack to progress and impact a critical system or network. Therefore, defense-in-depth is achieved not only by implementing multiple security boundaries, but also by instituting and maintaining a robust program of security controls that assess, protect, respond, prevent, detect, and mitigates an attack on a CDA and with recovery.		
8.24	Audible-alarm dosimeters are not generally substitutes for conventional survey meters. The dosimeters provide a complementary function. They provide some redundancy or "defense in depth" where (1) the operator fails to perform a survey. **(2)** the operator fails to make a fully adequate survey, or (3) the survey meter has malfunctioned, unknown to the operator.	ML003739382	8/31/1981

Notes:
1. This list is not meant to imply that it is complete, but to indicate the many RGs and history of defense-in-depth that has been the attention of the staff over the years.
2. This list of RGs was compiled by Donald Chung, Dylanne Duvigneaud, Brian Metzgar, and Jigar Patel of NRR.

Table 3 Discussion of Defense in Depth in SECY documents (see Notes 1 and 2)

SECY Num	Subject	Discussion
77-0439	Single Failure Criterion	The central conclusion to be drawn from this staff work is that the Single Failure Criterion has served well in its use as a licensing review tool to assure reliable systems as one element of the defense in depth approach to reactor safety. The Reactor Safety Study Indicates that its use had led to a generally acceptable level of hardware redundancy in most systems important to safety.
82-0288	10CFR Part 60 – Disposal of High-Level Radioactive Wastes in Geologic Repositories: Technical Criteria	The geologic setting and the engineered system differ both in their contributions to isolation and in the degree of confidence which can be placed on predictions of their long-term performance. Any mined geologic repository will contain some combination of these engineered and natural barriers which together must provide isolation. This is commonly called the multiple-barrier or the defense-in-depth approach.
83-269		The fixed suppression system is intended to prevent a fire in that area from becoming large enough to threaten adjacent areas containing safe shutdown equipment and to provide defense-in-depth to limit the adverse effects of a fire.
89-228	Draft safety Evaluation Report on Chapter 5 of The Advanced Light Water Reactor Requirements Document	In Section 2.1 of the draft SER, wherein the staff discusses the acceptability of the ALWR Public Safety Goal and the concept of defense in depth, the staff proposes to establish a containment performance criterion for evolutionary reactors.
90-016	Evolutionary Light Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements	Defense in depth, a long standing fundamental principle of reactor safety, results in the concept that multiple barriers should be provided to ensure against any significant release of radioactivity.
93-092	Issues Pertaining to Advanced Reactor (PRISM, MHTGR & PIUS) & CANDU 3 Designs & Their Relationship to Current Regulatory Requirements	Consistent with the current regulatory approach, the staff views the inclusion of emergency preparedness by advanced reactor licensees as an essential element in NRC's "defense in depth" philosophy. Briefly stated, this philosophy (1) requires high quality in the design, construction, and operation of nuclear plants to reduce the likelihood of malfunctions in the first instance; (2) recognizes that equipment can fail and operators can make mistakes, thus requiring safety systems to reduce the chances that malfunctions will lead to accidents that release fission products from the fuel; and (3) recognizes that, in spite of these precautions, serious fuel damage accidents can happen, thus requiring containment structures and other safety features to prevent the release of fission products off site. The added feature of emergency planning to the defense-in-depth philosophy provides that, even in the unlikely event of an offsite fission product release, there is reasonable assurance that emergency protective actions can be taken to protect the population around nuclear power plants.
93-087 Non-Publicly Available	Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs.	The recommendations on containment performance, as outlined in SECY 93-087, could be read to imply that the staff is no longer proposing to use the concept of conditional containment failure probabilities (CCFP). However, based on discussions held during the Commission meeting on this subject, the staff informed the Commission that it intends to continue to apply the 0.1 CCFP in implementing the Commission's defense in depth regulatory philosophy and the Commission's policy on Safety Goals.

Table 3 Discussion of Defense in Depth in SECY documents (see Notes 1 and 2)

SECY Num	Subject	Discussion
93-190	Policy Issue (Information), "Regulatory Approach to Shutdown and Low-Power Operations."	The improvements reflect the NRC safety philosophy of defense-in-depth in that they address: (a) prevention of credible challenges to safety functions through improvements in outage planning and fire protection; (b) mitigation of challenges to redundant protection systems, through improved procedures, training, improved technical specifications and contingency plans.
94-0239	Proposed Amendments to 10 CFR Part 60 on Disposal of High-level Radioactive Wastes in Geologic Repositories-Design basis Events for the Geologic Repository Operations Area	Defense-in-depth is provided for, during the pre-closure period, by conservatism, redundancy, and diversity in design; the application of a comprehensive quality assurance program, to facility design, construction, operation, and maintenance; the imposition of radiation protection standards, for both workers and members of the public, to limit the potential adverse consequences of licensed activities to levels that are well within the bounds of risks accepted in other productive activities in society; and requirements for radiation safety programs and procedures and emergency plans.
98-0225 Non-Publicly Available	Proposed Rule: 10 CFR Part63, "Disposal of High-level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada."	The defense-in-depth principle has served as a cornerstone of NRC's deterministic regulatory framework for nuclear reactors, and it provides an important tool for making regulatory decisions, with regard to complex facilities, in the face of significant uncertainties. NRC also has applied the concept of defense-in-depth elsewhere in its regulations to ensure safety of licensed facilities through requirements for multiple, independent barriers, and, where possible, redundant safety systems and barriers. Traditionally, the reliance on independence and redundancy of barriers has been used to provide assurance of safety when reliable, quantitative assessments of barrier reliability are unavailable. The Commission maintains, as it has in the past, that the application of the defense-in-depth concept to a geologic repository is appropriate and reasonable. The Commission now believes, however, that its implementation, in the context of a geologic repository, should be reexamined, in light of the advancement in methods to quantitatively assess the components of a geologic repository system and with due consideration of the Commission's goal of a regulatory program and associated requirements that are risk-informed and performance-based.
00-0007 Non-Publicly Available	Proposed Staff Plan for Low Power and Shutdown Risk Analysis Research to Support Risk-Informed Regulatory Decision	The defense-in-depth concept of NUMARC 91-06 is the qualitative approach widely used in the U.S. industry. The objectives of the qualitative defense-in-depth CRM approach are to (1) provide systems, structures, and components (SSCs) to ensure backup of key safety functions using redundant, alternate, or diverse methods; (2) plan and schedule outage activities in a manner that optimizes safety system availability; and (3) provide administrative controls that support and/or supplement the above elements.

Table 3 Discussion of Defense in Depth in SECY documents (see Notes 1 and 2)

SECY Num	Subject	Discussion
00-0022	Rulemaking Plan, "Decrease in the Scope of Random Fitness-for duty Testing Requirements for Nuclear Power reactor Licensees," for Amendments to 10 CFR 26	This process is consistent with the staff's strategy of defense in depth, which, in the case of security, requires passage through two barriers to reach vital equipment but only through one (the protected area barrier) to reach equipment of lesser significance to plant safety.
00-0048 Non-Publicly Available	Nuclear Byproduct Material Risk Review	Sometimes, however, it is advantageous to share the burden of prevention across multiple functional areas: in short, to adopt a kind of defense in depth approach.
00-0062	Risk-Informed Regulation Implementation Plan	In its February 14, 2000, letter to Chairman Meserve, the ACRS described a number of technical impediments to the increased use of risk information in agency regulatory activities. These included: • PRA inadequacies and incompleteness in some areas. • The need to revisit risk-acceptance criteria. • Lack of guidance on how to implement defense in depth and how to impose sufficiency limits.
00-0077	Modifications to the Reactor Safety Goal Policy Statement	In the existing Policy Statement, the Commission noted that current NRC regulations require conservatism in design, construction, testing, operation, and maintenance of nuclear power plants and indicated a defense-in-depth approach has been mandated in order to prevent accidents from happening and to mitigate their consequences. This importance of defense in depth is also clearly presented in the cornerstones of the reactor oversight process that relies on multiple lines of defense.
00-0080	Final Rule – Elimination of the Requirement for Noncombustible Fire Barrier Penetration Seal Materials and Other Minor Changes	Fire barrier penetration seals are one element of the defense-in-depth concept at nuclear power plants. The objectives of the defense-in-depth concept as applied to fire protection are to: (1) Prevent fires from starting; (2) Promptly detect, control, and extinguish those fires that do occur; and (3) Protect structures, systems, and components important to safety so that a fire that is not extinguished promptly will not prevent the safe shutdown of the plant.
00-0086	Status Report on Risk-Informing the Technical Requirements of 10 CFR Part 50 (Option 3)	• As a working definition, for use in the study, defense-in-depth is assessed by the application of the following strategies to protect the public: (1) limit the frequency of accident initiating events (2) limit the probability of core damage given accident initiation (3) limit radionuclide releases during core damage accidents (4) limit public health effects caused by core damage accidents • In implementing the defense-in-depth approach, both deterministic and probabilistic considerations are applied to preserve a reasonable balance among the four strategies, while maintaining the integrity of barriers. The deterministic considerations include addressing what role the single failure criterion should have, for both active and passive components.

Table 3 Discussion of Defense in Depth in SECY documents (see Notes 1 and 2)

SECY Num	Subject	Discussion
00-0212	Regulatory Guide Providing Guidance and Examples for Identifying 10 CFR 50.2 Design Bases	The staff's position is that aspects of the designed defense in depth strategies, such as redundancy, diversity, and independence, are important aspects of the plant's principal design criteria, as specifically required by several regulations, especially the General Design Criteria. These criteria require that such capabilities be implemented for individual structures, systems, and components through plant design features, such as multiple components, independent power supplies, and physical separation. These criteria provide part of the standard for judging the adequacy of the plant's design bases.
01-0009	Modified Reactor Safety Goal Policy Statement	A defense-in-depth approach has been mandated in order to prevent accidents from happening and to mitigate their consequences. Siting in less populated areas is emphasized. Furthermore, emergency response capabilities are mandated to provide additional defense-in-depth protection to the surrounding population. Risk insights can make the elements of defense-in-depth more clear 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.
01-0100	Policy Issues Related to Safeguards, Insurance, and Emergency Preparedness Regulations at Decommissioning Nuclear Power Plants Storing Fuel in Spent Fuel Pools	The Commission's defense-in-depth philosophy would be maintained based on the expectation that there would be reasonable assurance of implementing onsite mitigative actions and offsite protective actions given the slow developing nature of the spent fuel zirconium fire.
02-0030	Summary Report on NRC's Historical Efforts to Develop and use Performance Indicators	Plant safety PIs are based on the defense-in-depth principle and are organized into three areas: safety and quality of normal operations, operating events, and barrier integrity.
03-0047	Policy Issues Related to Licensing Non-Light-Water Reactor Designs	The staff recommends that the Commission take the following actions: Approve the development of a policy statement or description (e.g., white paper) on defense-in-depth for nuclear power plants to describe: • the objectives of defense-in-depth (philosophy) • the scope of defense-in-depth (design, operation, etc.) • the elements of defense-in-depth (high level principles and guidelines)

Table 3 Discussion of Defense in Depth in SECY documents (see Notes 1 and 2)

SECY Num	Subject	Discussion
04-0236	Southern Nuclear Operating Company's Proposal to Establish a Common Emergency Operating Facility at its Corporate Headquarters	Therefore, the staff concludes that the establishment of a common EOF will effectively and efficiently support the SNC emergency response capability. This is consistent with the defense in depth doctrine and provides reasonable assurance that protective measures can and will be implemented in the event of a radiological emergency at any of the SNC nuclear plants.
05-0006	Second Status Paper on the Staff's Proposed Regulatory Structure for New Plant Licensing and Update on Policy Issues Related to New Plant Licensing	The approach in the framework has the following elements: • The objectives of defense-in-depth compensate for potential adverse human actions and component failures and maintain the effectiveness of barriers by averting damage to the plant and the barriers themselves to protect the public and environment from harm. • The principles of defense-in-depth for achieving the objectives are (1) that there should be measures to protect against intentional as well as inadvertent events, (2) that designs should provide accident prevention and mitigation capability, (3) that accomplishing key safety functions should not depend upon a single element of design, construction, maintenance, or operation, (4) that uncertainties in structures, systems and components (SSCs) and human performance should be accounted for so that reliability and risk goals can be met, and (5) that plants should be sited in areas that meet the intent of Part 100 and are consistent with the siting principles established in Regulatory Guide 4.7 (General Site Suitability Criteria for Nuclear Power Plants). • The defense-in-depth model integrates deterministic and probabilistic elements. The model should impose certain deterministic defense-in-depth measures with complementary probabilistic guidelines. • The defense-in-depth implementation should be a decision process showing how to apply the defense-in-depth model. The model includes monitoring and feedback requirements to ensure that the defense-in-depth principles are properly integrated into the design, construction, maintenance, and operation.
05-0172	Duke Power Company's Request to Incorporate the Oconee Emergency Operations Facility into the EOF Shared by Catawba and McGuire Nuclear Station	Therefore, the staff concludes that the incorporation of the Oconee EOF into the Charlotte EOF will effectively and efficiently support the Duke Power emergency response capability. This is consistent with the defense in depth doctrine and provides reasonable assurance that protective measures can and will be implemented in the event of a radiological emergency at the Oconee nuclear plant.
06-0187	Semiannual Update of the Status of New Reactor Licensing Activities and Future Planning for New Reactor	The major focus areas of the most recent meetings involved the standards for defense in depth in the design, and the conduct of MGR safety analyses. The ANS 28 Subcommittee working group is now trying to complete the safety standard for review by the end of CY 2006.

Table 3 Discussion of Defense in Depth in SECY documents (see Notes 1 and 2)

SECY Num	Subject	Discussion
07-0205	Weekly Information Report – Week Ending November 16, 2007	On November 14 and 15, 2007, staff met with EPRI to discuss DI&C diversity and defense in depth, highly integrated control rooms, DI&C system risk assessment, human factors (including manual operator actions, computerized procedures, and a graded approach to HF reviews), human performance metrics and criteria, the assessment of graphical display techniques, instrumentation and control obsolescence management, and remote integrated work environments.
08-0019	Licensing and Regulatory Research related to Advanced Nuclear reactors	The current focus topics, documented in four PBMR (Pty)white papers, involve plans for probabilistic risk assessment (PRA) quality and completeness; how the PRA would be used to select licensing basis events (LBEs); the proposed approach for safety classification and special treatment of the PBMR structures, systems, and components (SSCs); and the proposed approach for providing adequate defense in depth.
09-0113	Update on the Development of Construction Assessment Process Policy Options and the Construction Inspection Program Information Management System	The screening process measures the safety significance of construction or operational events, because of design or construction errors, based on two main factors: (1) the degradation of barriers (i.e., reduction in defense in depth), and (2) the likelihood that the failure would not be detected before operation or the period of time it remained undetected during operation.
09-0140	Rulemaking Related to Decoupling an Assumed Loss of Offsite Power from a Loss-of-Coolant Accident, 10 CFR Part 50, Appendix A, General Design Criterion 35	The staff's March 24, 2008, letter details the conditions and limitations that the staff concluded were required for approval of NEDO-33148. Some of the outstanding technical issues include LOOP/LOCA frequency determinations, seismic contributions to break frequency, the maintenance of defense in depth, and the treatment of delayed LOOP and double sequencing issues. These issues would need to be adequately addressed in order to complete a regulatory basis that could support a LOOP/LOCA rulemaking.
10-0121	Modifying the Risk-Informed Regulatory Guidance for New Reactors	One of the staff's concerns is that the existing ROP may not provide for meaningful regulatory oversight for new reactors that can support the NRC's regulatory actions and inspection as performance declines. The current risk-informed baseline inspection program and risk-informed thresholds for performance indicators may not trigger a regulatory response before significant erosion occurs to the enhanced defense in depth and safety margins of the plant.
11-0014	Use of Containment Accident Pressure in Analyzing Emergency Core Cooling System and Containment Heat Removal System Pump Performance in Postulated Accidents.	Defense-in-depth is a basic element of the NRC's safety philosophy. Defense-in-depth has been applied in various forms. One application of defense-in-depth is to ensure that key safety functions do not depend on a single element of design, construction or operation. Another form of the defense-in-depth philosophy is a balance among accident prevention, accident mitigation and the limitation of the consequences of an accident. Redundant and diverse means may be used to accomplish key safety functions. One manifestation of defense-in-depth is the use of multiple independent fission product barriers.

Table 3 Discussion of Defense in Depth in SECY documents (see Notes 1 and 2)

SECY Num	Subject	Discussion
Notes: 1. This list is not meant to imply that it is complete, but to indicate the many SECY's and history of defense-in-depth that has been the attention of the staff over the years. 2. This list of SECYs was compiled by Donald Chung, Dylanne Duvigneaud, Brian Metzgar, and Jigar Patel of NRR.		

References

1. U.S. Atomic Energy Commission, “Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants,“ WASH-740, pages vii, 5, and 21, March 1957.

2. Beck, C., “Basic Goals of Regulatory Review: Major Considerations Affecting Reactor Licensing,” Statement submitted to the Joint Committee on Atomic Energy, Congress of the United States, hearings on Licensing and Regulation of Nuclear Reactor, April 4, 5, 6, 20 and May 3, 1967.

3. Internal Study Group, “Report to the Atomic Energy Commission on the Reactor Licensing Program,” submitted to the Joint Committee on Atomic Energy, Congress of the United States, Hearings on AEC Licensing Procedure and Related Legislation, June 1969.

4. Sorenson, J.N., “Historical Notes on Defense in Depth,” ML082740322, October 15, 1997.

5. WASH-1250, U.S. Atomic Energy Commission, “The Safety of Nuclear Power Reactors and Related Facilities,“ March 1973.

6. Federal Register Notice, “Disposal of High-level Radioactive Wastes in Geologic Repositories Technical Criteria,” Final Rule, Volume 48, Page 28194, June 21, 1983.

7. Breen, R.J., Deputy Director of EPRI's Nuclear Safety Analysis Center, published a paper titled "Defense-in-depth Approach to Safety in Light of the Three Mile Island Accident (Nuclear Safety, Vol. 22, No.5, Sept.-Oct. 1981).

8. NUREG/CR-6042, Revision 2, “Perspectives on Reactor Safety,” March 2002.

9. Policy statements:

   - U.S. Nuclear Regulatory Commission, ‘Safety Goals for the Operations of Nuclear Power Plants; Policy Statement’, Federal Register, Vol. 51, No. 149, pp.28044-28049, August 4, 1986 (republished with corrections, Vol. 51, No. 169, pg. 30028-30023, August 21, 1986).

   - U.S. Nuclear Regulatory Commission, “Policy Statement on the Regulation of Advanced Reactors; Final Policy Statement,” Federal Register, Vol. 73, No. 199, pg. 60612-60616, October 14, 2008.

   - U.S. Nuclear Regulatory Commission, “Policy Statement on Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement,” Federal Register, Vol. 60, No. 158, pg. 42622-42629, August 16, 1995.

10. NUREG-1537, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” February 1996.

11. “Current Regulatory Issues,” Speech by Dr. Shirley Ann Jackson, Chairman, U.S. Nuclear Regulatory Commission to Nuclear Power Reactor Safety Course,

Massachusetts Institute of Technology, Cambridge, Massachusetts, Commission Speeches, No. S-97-17, July 29, 1997.

12. Kress, T.S., "Some thoughts on Defense-in-Depth," Presented to Regulatory Policies and Practices ACRS Subcommittee, August 27, 1997.

13. Commission White Paper, "Risk-Informed and Performance-Based Regulation, " NRC Yellow Announcement No. 019, March 11, 1999.

14. Sorensen, J.N., Apostolakis, G.E., Kress, T.S., and Powers, D.A., "On the Role of Defense-in-Depth in Risk Informed Regulation," American Nuclear Society PSA '99, Washington DC, August 22-25, 1999.

15. ACRS letters

- Powers, D.A., ACRS letter to USNRC Chairman Jackson, "The Role of Defense in Depth in a Risk-Informed Regulatory System," May 19, 1999.

- Garrick, B.J, ACNW, Powers, D.A., ACRS letter to USNRC Chairman Meserve, "Use of Defense in Depth in Risk-Informing NMSS Activities," May 25, 2000.

16. Advisory Committee on Reactor Safeguards, Advisory Committee on Nuclear Waste Meeting of the Joint ACRS/ACNW Subcommittee, Room T-2b3, 11545 Rockville Pike, Rockville, MD, January 13-14, 2000.

17. IAEA Documents

- International Nuclear Safety Advisory Group (INSAG) INSAG- 3, International Atomic Energy Agency, Vienna, Austria, 1996.

- INSAG, "Defense in Depth in Nuclear Safety," INSAG- 10, International Atomic Energy Agency, Vienna, Austria, 1996.

- IAEA Safety Standards, "Fundamental Safety Principles, Safety Fundamentals," SF-1, November 2006.

- INSAG- 12, International Atomic Energy Agency, Vienna, Austria, 1996.

- IAEA TECDOC-1570, "Proposal for a Technology-Neutral Safety Approach for New Reactor Designs," September 2007.

- IAEA Safety Standards, "Safety of Nuclear Power Plants: Design, Specific Safety Requirements," SSR-2/1, January 2012.

18. "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979," Appendix R to 10 C.F.R. pt. 50 (2012).

19. Fleming, K.N., and Silady, F.A., "A Risk Informed Defense-in-Depth Framework For Existing and Advanced Reactors," Reliability Engineering & System Safety, Volume 78, issue 3, December 2002, Pg 205-225.

20. “Risk-informed Categorization and Treatment of Structures, Systems and Components for Nuclear Power Reactors,” 10 C.F.R. §50.69 (2012).

21. 10 CFR Part 73

- “Protection of Digital Computer and Communication Systems and Networks,” 10 CFR §73.54, 2009.
- “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage,” 10 CFR §73.55, 2009.
- “Requirements for New Facilities or New Processes at Existing Facilities,” 10 CFR §70.64, 2000.
- “Nuclear Power Plant Safeguards Contingency Plans,” Appendix C to 10 CFR Part 73, 2012.

22. “Reactor Site Criteria,” 10 CFR Part 100, 1996.

23. Nuclear Energy Institute, “A Risk-Informed Performance-Based Regulatory Framework for Power Reactors,” NEI 02-02, May 2002.

24. USNRC, Office of Nuclear Reactor Regulation, Director’s Decision, 2.206 Petition from Congressman Dennis Kucinich, Representative for the 10th Congressional District of the State of Ohio in the United States House of Representatives, “To revoke FirstEnergy Nuclear Operating Company license to operate Davis-Besse Nuclear Power Station, Unit 1,” ML032480751, September 12, 2003.

25. Speech-04-009: Chairman Nils J. Diaz, “The Best-Laid Plans (the NRC’s Defense-in-Depth Philosophy),” The Third Annual Homeland Security Summit, June 3, 2004.

26. Digital Instrumentation and Control (DI&C) documents:

- NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” December 1994.
- Regulatory Guide 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” January 1996.
- NUREG-0800, Branch Technical Position (BTP) HICB-19, “Guidance for Evaluation of Defense-in-depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,” June 1997.
- NUREG-0800, Standard Review Plan (SRP), BTP 7-19, “Guidance for Evaluation of Defense-in-depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,” March 2007.
- DI&C-ISG-02, “Digital Instrumentation and Controls,” June 2009.

27. NUREG-1860, “Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing,” U.S. Nuclear Regulatory Commission, December 2007.

28. Idaho National Laboratory (INL), “Next Generation Nuclear Plant Defense-in-Depth Approach,” INL/EXT-09-17139, December 2009.

29. NRC Regulatory Guide 1.174,”An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,“ November 2002.

    - USNRC Draft Guide 1285, Proposed Revision 3 to RG 1.174, ”An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,“ May 2012.

30. USNRC Public Website, Glossary, http://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth

31. NUREG-2150, “A Proposed Risk Management Regulatory Framework,” April 2012

32. OECD NEA/CNRA/CSNI (Organization for Economic Co-operation and Development/Nuclear Energy Agency/Committee on Nuclear Regulatory Activities/Committee on the Safety of Nuclear Installations) workshop. “Challenges and Enhancements to DiD in light of the Fukushima Dai-ichi Accident,” ADAMS Accession No. ML13337A461, June 5, 2013