U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/KM-0009

Historical Review and Observations of Defense-in-Depth

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Library at www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Mail Stop IDCC
   Washington, DC 20402-0001
   Internet: bookstore.gpo.gov
   Telephone: (202) 512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Rd., Alexandria, VA 22312-0002
   www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: **U.S. Nuclear Regulatory Commission**
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at NRC's Web site address www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
www.ansi.org
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractorprepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/KM-0009

Historical Review and Observations of Defense-in-Depth

Manuscript Completed: March 2016
Date Published: April 2016

Prepared by:
Mary Drouin, Brian Wagner; NRC
John Lehner, Vinod Mubayi, BNL

Brookhaven National Laboratory
PO Box 5000
Upton, NY 11973-5000

Office of Nuclear Regulatory Research

ABSTRACT

The concept of defense-in-depth is an important element of the U.S. Nuclear Regulatory Commission's (NRC) safety philosophy. Though the term has been in use for many years, it has not always been used or defined consistently. This Knowledge Management NUREG documents the historical use of the term (based on NRC literature – for example, technical reports, letters, regulations, regulatory guides, speeches, SECY papers, ACRS presentations and letters) for reactors, materials, and waste for both safety and security applications. Perspectives are included from other government agencies as well as the international community. This report includes general observations in the consistencies and inconsistencies in how defense-in-depth has been defined and used.

FOREWORD

This NUREG has been prepared in response to a Commission Staff Requirements Memorandum that directed the staff to “enshrine Enclosure 3, [from SECY-13-0132] as an agency knowledge management tool and republish in other formats to make it more widely available.” Enclosure 3 was not a thorough historical review and its purpose was only to illustrate the long history on defense-in-depth. This NUREG has a more complete historical review and observations of defense-in-depth for reactors, materials, waste, security, international and other agencies.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

This report documents the historical review and perspectives of defense-in-depth. This review involved looking at the various NRC documents, dating back to the 1950s, where defense-in-depth is discussed. The documents primarily included NUREG reports, letters, regulatory guides, SECY papers, Commission White papers, ACRS letters and proceedings, regulations, and conference proceedings. The authors of this Knowledge Management NUREG wish to acknowledge the contributions made by Donald Chung, Dylanne Duvigneaud, Brian Metzgar, and Jigar Patel. These individuals compiled the list of ACRS letters, Regulatory Guides and SECY papers documented in Tables 4-2 through 4-4.

1. INTRODUCTION

1.1 Background

The idea of defense-in-depth originated as a military strategy, early in history, as a concept to delay the advance of the opponent by relying on multiple, layered lines of defense instead of a single strong defensive line. The idea of defense-in-depth is now widely used for non-military applications to describe multi-layered, as well as diverse and redundant, protections, both tactical and strategic. In engineering, for example, defense-in-depth may mean redundancy or diversity in design; that is, designing a system to remain functional although a component in the system has failed, versus trying to design components that do not fail. For example, a ship with four reasonably reliable engines will be less likely to suffer total engine failure than a single-engine ship, no matter how much effort goes into making the single engine highly reliable. Diversity in the engine types (e.g., nuclear steam and diesel) would make total engine failure even less likely. This concept of defense-in-depth, protection against a single failure, is engrained in the nuclear industry. In nuclear safety, defense-in-depth denotes the practice of having multiple, redundant, and independent layers of safety systems or physical barriers to protect against the occurrence, as well as the consequences, of an accident. The aim is to reduce the risk to the public from a radiological accident. The concept of defense-in-depth is not limited to nuclear safety. For example, the defense-in-depth concept has been employed in nuclear security, both physical and cyber which both rely on layered defenses, including prevention, detection, and response. The layers are designed so that a breach of one layer only leads the attacker to the next layer of defense.

The concept of defense-in-depth appears frequently in nuclear history dating back to 1957 and WASH 740 (Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants") [WASH, 1957]. In that document, defense-in-depth is described as:

> "... criteria ... that ... will require multiple lines of defense against accidents which might release fission products from the facility" and "... no hazard to the safety of the public would occur unless two additional lines of defense were also breached."

Defense-in-depth has been described, discussed, and defined extensively over the years in various U.S. Nuclear Regulatory Commission's (NRC) documents including Title 10 of the *Code of Federal Regulations*, NUREG reports, SECY papers, regulatory guides, Commission policy statement, Advisory Committee on Reactor Safeguards (ACRS) letters, etc. It has been at the core of the NRC's safety philosophy, and remains fundamental to the safety and security expectations of NRC's regulatory structure. Over the years, however, defense-in-depth, in the various references, has not been described, discussed or defined consistently. This is not surprising, since different authors have invoked the defense-in-depth concept in ways that best suit the particular purpose of their document.

For example, in the NRC Strategic Plan [NRC, 2014], defense-in-depth is defined as:

> "... an element of the NRC's safety philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility. The NRC's safety philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility."

In the glossary on the NRC Website, defense-in-depth is defined 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."

These two definitions raise such questions as "is defense-in-depth successive compensatory measures, or is it creating multiple independent and redundant layers of defense?" The two definitions are conceptually similar, but can be interpreted differently. For example, can systems with multiple independent and redundant trains be considered layers of defenses, or are the layers meant to be multiple independent and redundant systems? Moreover, what is considered to be a compensatory measure (i.e., do multiple independent and redundant layers of defense serve as compensatory measures)? Is defense-in-depth a philosophy or is it an approach, and is there a difference between the two? In looking at the history, the various descriptions, discussions and definitions use different language and terminology and vary in length, from a few sentences to pages, to entire reports.

To further complicate the matter, the concept may not always be referred to as "defense-in-depth." For example, the ANSI/ANS-8.1 (American National Standards Institute/American Nuclear Society) standard [ANSI/ANS, 1998], whose purpose is to reduce the risk of inadvertent criticality, defines a "double-contingency principle." The double-contingency principle states that *"*process designs should, in general, incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible.*"* As can be seen, the idea of the double-contingency principle is similar to the concept of redundancy and diversity as expressed by defense-in-depth. Although similarities may exist in concept, sufficient differences may appear in the language and terminology to cause confusion and potential disagreement. The differences discussed above reflect a small set of references and the differences on defense-in-depth are greatly increased

when the history of defense-in-depth since 1957 is reviewed. Consequently, the ongoing discussions on defense-in-depth are understandable.

In SECY-13-0132, Enclosure 3 [NRC 2013a] provides a summary of the history of defense-in-depth and provides insights (i.e., observations) based on an historical review of defense-in-depth, mainly for nuclear power reactors. The Commission Staff Requirements Memorandum (SRM) to SECY-13-0132 [NRC 2013b] states that "Enclosure 3, 'Defense-in-depth Observations and Detailed History,' should be enshrined as an agency knowledge management tool and republished in other formats to make it more widely available." This NUREG is developed in response to the SRM and starts with, and builds on, the material found in Enclosure 3 of SECY-13-0132.

1.2 Objective

The objectives of this NUREG include the following:

- A summary of the history of defense-in-depth, specifically a summary of the various descriptions, discussions and definitions of defense-in-depth that have been used in the literature (see Section 1.3 for the scope of the literature reviewed).

- Overall historical observations on the concept of defense-in-depth.

1.3 Scope and Limitations

As noted above, this NUREG builds on the material in Enclosure 3 of SECY-13-0132. Enclosure 3 of SECY-13-0132 was not intended to serve as a historical reference on defense-in-depth. It was a limited review to illustrate the rich history and to demonstrate the various and similar perspectives and concepts. The history was primarily focused on reactors, although some history on nuclear materials, waste and security, and some international history on the treatment of defense-in-depth was included. To meet the needs as a "knowledge management tool," (i.e., to serve as a useful reference document) this document more fully addresses the history on reactors, materials, waste, and security and the perspectives of other domestic agencies as well as international agencies. This document is comprehensive but not necessarily exhaustive.

The historical summary in SECY-13-132 is based primarily on NRC documents and includes regulations, policy statements, NUREGs, regulatory guides, SECY papers, Commission speeches, ACRS presentations, and ACRS letters. Although in general, non-regulatory documents were not reviewed, the history of defense-in-depth included Internal Atomic Energy Agency (IAEA) documents, and some limited industry papers and national laboratory reports. The scope of this NUREG is expanded to include some material from other organizations (e.g., Department of Energy, National Aeronautics and Space Agency, Federal Aviation Administration, Department of Defense) and the international community beyond IAEA.

This document has been published as a KM NUREG because it "collects, compiles, and interprets historical information and references on technical topics to assist future, current, and former staff in understanding how the agency's regulatory system and technical knowledge have evolved" (per Management Directive 3.7). It does not represent a technical analysis; as such, it does not provide conclusions or recommendations.

1.4 Organization

This NUREG is organized as follows:

- Section 2 – list of acronyms
- Section 3 – a high-level summary of the history of defense-in-depth, specifically summarizing the various descriptions, discussions and definitions of defense-in-depth.
- Section 4 – summary of defense-in-depth from a reactor perspective
- Section 5 – summary of defense-in-depth from a non-reactor (i.e., materials, waste, uranium recovery, fuel cycle, interim spent fuel storage, and transportation) perspective
- Section 6 – summary of defense-in-depth from a security perspective
- Section 7 –summary of defense-in-depth from an international perspective
- Section 8– summary of defense-in-depth insights from other organizations
- Section 9 –overall historical observations on defense-in-depth
- Section 10 – list of references

2. LIST OF ACRONYMS

Acronym	Description
ACNW	Advisory Committee on Nuclear Waste
ACRS	Advisory Committee on Reactor Safeguards
AEC	Atomic Energy Commission
ALWR	Advanced Light Water Reactor
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOT	Allowed Outage Time
ASN	French Nuclear Safety Authority
BDBA	Beyond Design Basis Accident
BDC	Baseline Design Criteria
BOP	Balance of Plant
BTP	Branch Technical Position
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CCFP	Conditional Containment Failure Probability
CDA	Critical Digital Asset
CDF	Core Damage Frequency
CFR	Code of Federal Regulations
CIV	Containment Isolation Valve
COP	Containment Overpressure
CNRA	Committee on Nuclear Regulatory Activities
CNSC	Canada Nuclear Safety Committee
CRM	Configuration Risk Management
CS	Critical System
CSNI	Committee on the Safety of Nuclear Installations
D3	Diversity and Defense-in-Depth
DBA	Design Basis Accident
DEGB	Double Ended Guillotine Break
DG	Draft Guide
DHS	Department of Homeland Security
DI&C	Digital Instrumentation and Control
DiD	Defense-in-Depth
DOE	Department of Energy
DOI	Department of the Interior
DSS	Dry Cask Storage System
ECCS	Emergency Core Cooling System
EDO	Executive Director of Operations
EOF	Emergency Operations Facility
EP	Emergency Preparedness
EPA	Environmental Protection Agency

EPRI	Electric Power Research Institute
EQ	Equipment Qualification
ESF	Engineered Safety Features
ESFAS	Engineered Safety Systems Actuation System
FAA	Federal Aviation Administration
F-C	Frequency – Consequence
FPP	Fire Protection Plan
FRN	*Federal Register* Notice
FSME	Office of Federal and State Materials and Environmental Management Programs
GDC	General Design Criteria
HLW	High Level Waste
IAEA	International Atomic Energy Agency
IDP	Integrated Decisionmaking Process
INL	Idaho Engineering Laboratory
INSAG	International Nuclear Safety Advisory Group
IROFS	Items Relied on for Safety
IRSN	Institute of Radionuclide Protection and Nuclear Safety
ISG	Interim Staff Guidance
IST	In-Service Testing
LB	Licensing Basis
LBE	Licensing Basis Event
LERF	Large Early Release Frequency
LLW	Low-Level Waste
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LOP	Line of Protection
LWR	Light Water Reactor
MGR	Modular Gas Reactor
MIT	Massachusetts Institute of Technology
NASA	National Aeronautics Space Administration
NEA	Nuclear Energy Agency
NEI	Nuclear Energy Institute
NGNP	Next Generation Nuclear Plant
NMSS	Nuclear Materials Safety and Safeguards
NPP	Nuclear Power Plant
NRA	National Regulatory Authority
NRC	Nuclear Regulatory Commission
NRR	Office of Nuclear Reactor Regulation
NSAC	Nuclear Science Advisory Committee
NTTF	Near Term Task Force
NWPA	Nuclear Waste Policy Act
OECD	Organization for Economic Co-Operation and Development
QA	Quality Assurance

PPA	Probabilistic Performance Assessment
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
RCS	Reactor Coolant System
RES	Office of Nuclear Regulatory Research
RG	Regulatory Guide
RHWG	Reactor Harmonization Working Group
RIDM	Risk-Informed Decisionmaking
RISC	Risk-Informed Significance Classification
RMTF	Risk Management Task Force
ROP	Reactor Oversight Process
RPV	Reactor Pressure Vessel
SAMG	Severe Accident Management Guidelines
SAR	Safety Analysis Report
SER	Safety Evaluation Report
SIL	Safety Integrity Level
SMR	Small Modular Reactor
SNF	Spent Nuclear Fuel
SOC	Statements of Consideration
SRM	Staff Requirements Memorandum
SRP	Staff Review Plan
SSC	Structure, System and Component
SSNM	Strategic Special Nuclear Material
STI	Surveillance Test Interval
TBS	Transition Break Size
TMI	Three Mile Island
TS	Technical Specification
TSPA	Total System Performance Assessment
WANO	World Association of Nuclear Operators
WENRA	Western European Nuclear Regulator’s Association
YMRP	Yucca Mountain Review Plan

3. HIGH LEVEL HISTORICAL SUMMARY OF DEFENSE-IN-DEPTH

This section provides a high-level summary of defense-in-depth information gleaned from a review of the literature that addresses defense-in-depth.[1] Much of this literature, particularly in non-reactor areas, does not mention defense-in-depth by name but uses many of the same concepts. The summaries in this section are organized by:

- Reactor
- Non-reactor (materials waste, uranium recovery, fuel cycle, interim spent fuel storage, and transportation)
- Security
- International
- Other U.S. Agencies

More detailed summaries are provided in later sections.

3.1 High Level Historical Summary of Reactor Defense-In-Depth

There is a rich history on perspectives of defense-in-depth related to reactors covering a time period of roughly 60 years. The historical review of reactor defense-in-depth primarily includes an examination of Nuclear Regulatory Commission (NRC) literature. In reviewing this history it is evident that, for the first 30 years, defense-in-depth was viewed strictly from a deterministic or a structuralist perspective. As such, defense-in-depth was described as providing protections relying on multiple barriers, multiple layers of defense, etc. In the mid-1990s, as risk analyses matured and as the regulatory structure became more risk-informed, the use of risk results and insights became part of defense-in-depth. Risk results and insights were being used to identify where defense protections could be enhanced or relaxed, or used to determine the adequacy of such protections, and for addressing uncertainties and lack of knowledge. An additional observation from this earlier literature is that defense-in-depth, from the beginning, addresses both accident prevention and accident mitigation.

Table 3-1 provides the list of sources reviewed for the history of defense-in-depth for reactors in chronological order. Section 4 provides a detailed summary and a high-level summary is provided below.

Table 3-1 Sources for the History of Defense-in-Depth for Reactors

Sources (in Chronological Order)	
• AEC letters	• Commission White Paper
• WASH-740	• ACRS letters
• Joint Committee on Atomic Energy Hearings	• Joint ACNW/ACRS Subcommittee
• Internal Study Group	• 10 CFR Part 50, Appendix R

[1] The references for the various literature reviewed are provided in Sections 4, 5, 6, 7 and 8.

Sources (in Chronological Order)	
• AEC letter • ECCS Hearings • WASH-1250 • NRC Annual report • NRC Reactor fact sheet • NUREG-0050 • NUREG-0578 • NUREG-0585 • NUREG/CR-1250 • Post TMI Definitions and Examples • NUREG-0880 • Commission Policy Statements • NUREG/CR-6042 • NUREG-1537 • 10 CFR Part 100 • MIT Speech by Chairman Jackson • Some Thoughts on Defense-in-Depth by Tom Kress • PSA '99 paper	• A Risk-Informed Defense-in-Depth Framework for Existing and Advanced Reactors, Karl Fleming, Fred Silady • NEI 02-02 • Petition on Davis Besse • 10 CFR §50.69 • Remarks by Chairman Diaz • Digital Instrumentation and Controls (NUREG/CR-6303, RG 1.152, NUREG-0800 BTP HICB-19, NUREG-0800 SRP BTP 7-19, DI&C-ISG-02) • NUREG-1860 [• INL NGNP report • RG 1.174 other RGs • NTTF Review Report • NUREG-2150 RMTF • NRC glossary • SECYs, RGs, and ACRS letters

The earliest mention of a defense-in-depth like approach appears to be in a letter from W.F. Libby, Acting Chairman of the US Atomic Energy Commission (AEC) to the Honorable Bourke Hickenlooper of the Joint Committee on Atomic Energy Congress of the United States on March 14, 1956. Although the term "defense-in-depth" does not appear in the letter, it does describe "lines of defense" that can be considered as referring to defense-in-depth. This letter includes a discussion on three elements that could be interpreted as defense-in-depth:

> "1) Recognizing all possible accidents which could release unsafe amounts of radioactive materials; 2) Designing and operating the reactor in such a way that the probability of such accident is reduced to an acceptable minimum; 3) By appropriate combination of containment and isolation, protecting the public from the consequences of such an accident, should it occur."

The next description of defense-in-depth appears to be in WASH-740, "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants" in 1957. The discussion can be considered describing defense-in-depth since it talks about "multiple lines of defense." The multiple lines of defense are "(1) the integrity of the reactor vessel; and, (2) the integrity of the reactor container or vapor shell."

The next description of defense-in-depth, occurs a decade later, in a 1967 paper submitted by Clifford Beck (Deputy Director of Regulation) to the Joint Committee on Atomic Energy. In summary, the paper defines three basic lines of defense dealing with "superior quality in design,

construction and operation of basic reactor systems important to safety," accident prevention safety systems, and consequences-limiting safety systems. A subsequent reference to defense-in-depth occurs in the "Report to the Atomic Energy Commission on the Reactor Licensing Program," by the Internal Study Group in 1969. In their report, 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. The next historical document is a 1971 letter from Dr. Glen Seaborg, Chairman of the AEC, to Honorable John Pastore, Chairman to the US Senate Joint Committee on Atomic Energy Congress of the United States. The letter states that the probability of an accident occurring should be very small, and that engineered safety features to mitigate the consequences of such an accident should be provided. The next historical document is the testimony of the AEC Regulatory Staff at the Public Rulemaking Hearings on Interim Acceptance Criteria for Emergency Core Cooling Systems for Light Water Power Reactors, issued in 1971. This testimony also describes three lines of defense and states that the principal defense is through the prevention of accidents. The second line of defense includes protective systems and the third line is provided by installing engineered safety features to mitigate the consequences of postulated serious accidents. Another document that was in development at the same time as the above testimony was prepared is WASH-1250 in 1973. This document states:

> "... 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 ... A convenient method of describing this "defense-in-depth" is to discuss it in the broader concept of three levels of safety."

The NRC Annual Report of 1975 describes defense-in-depth as "three successive and mutually reinforcing echelons of defense…to prevent a serious accident affecting the public." The three echelons include preventing the accident through conservative design, the presence of safety systems to prevent or minimize damage from failures, and the incorporation of additional features to address design basis accidents. An NRC fact sheet that was under development in 1976 contains a discussion of defense-in-depth with similar definitions of the three levels of defense. In 1976, NUREG-0550, "Recommendations Related to Browns Ferry Fire", also provided similar definitions of the three levels. The NUREG went on to state that no one of these echelons of safety can be perfect, since humans are fallible and equipment is breakable, but that it is their multiplicity, and the depth thus afforded, that provide the required high degree of safety in spite of the lack of perfection in any given system.

In 1979, NUREG-0578, "TMI-2 Lessons-Learned Task-Force Status Report and Short-term Recommendations" states that:

> "The underlying philosophy of nuclear reactor safety has provided multiple levels of protection against the release of radioactivity, i.e., the concept of defense in depth. It includes diversity and redundancy of various safety

> functions and systems and multiple physical barriers (the fuel, the cladding, the primary coolant boundary, and the containment) … The functions and general characteristics of the systems required to provide defense-in-depth are specified in the General Design Criteria of the Commission regulations (Appendix A to Title 10 Code of Federal Regulations (10 CFR) Part 50)."

In 1979, NUREG-0585, "TMI-2 Lessons Learned Task Force Final Report" discusses defense-in-depth relative to recommended improvements based on lessons learned. It discusses the three levels of defense-in-depth and previous actions in response to the Three Mile Island (TMI) accident focused on the first two levels, preventing the accident. Moreover, it states:

> "The defense-in-depth concept is based on the premise that there is a limit to the effectiveness of any level of prevention. Unanticipated interactions and interrelationships among and between systems and the operators and the possibility of undetected common modes of failure are a bound on the assurance of any level of prevention. The TMI accident is illustrative of the point."

In 1980, NUREG/CR-1250 describes the three levels of defense and states that:

> "... application of the defense-in-depth concept also resulted in the provision of multiple physical barriers between the radioactivity contained in the reactor fuel and the environment outside the plant. The fuel is contained in a sealed metal cladding; the clad fuel is contained in a heavy steel primary coolant system, and the primary coolant system is enclosed in a sealable containment building."

In 1981, 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." In the paper, Breen states that "... the principle of guarding against unwanted events by providing successive protective barriers is frequently called defense-in-depth." Breen acknowledges the various ways of describing the application of defense-in-depth, and then chooses a "fairly common three level description emphasizing functions," that 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 discuss two systems used by the NRC and the Nuclear Science Advisory Committee to determine which activities make the greatest contribution to safety.

In 1983, the Glossary in Section XI of NUREG-0880 gives a definition of defense-in-depth:

> "Defense in depth in engineering practice as applied to nuclear power plants, involves careful quality assurance and control in plant design, construction, and operation to reduce the likelihood of accidents; installation of backup systems to nullify the consequence of malfunctions in important plants systems and to prevent individual malfunctions from escalating into major accidents; and installation of engineered safety features to confine the consequences of certain postulated major 'design basis accidents'; to minimize effects on the public health and safety. It also involves siting of nuclear plants in areas of low population density and in locations that are not near natural or manmade hazards, and calls for reasonable assurance that adequate protective measures can and will be taken by the licensee and the state and local authorities in the event of serious accidents."

NUREG/CR-6042 (1994), "Perspectives on Reactor Safety," describes a one-week course in reactor safety concepts. It describes key elements of defense-in-depth that are listed as accident prevention, safety systems, containment, accident management, and siting and emergency plans.

The term "defense-in-depth" occurs in three Commission Policy Statements: the Safety Goal Policy Statement, the Advanced Nuclear Power Plant Policy Statement, and the Probabilistic Risk Assessment (PRA) Policy Statement. None of these documents offer a definition of defense-in-depth except by example or implication. The Commission Safety Goal Policy Statement (1986) notes specific features (e.g., containment) as integral parts to defense-in-depth, and that understanding uncertainty is a key aspect of defense-in-depth. Additional views are provided by two Commissioners. The Commission Policy on Regulation of Advanced Reactors (1994/2008) notes that designs incorporate the defense-in-depth philosophy by maintaining multiple barriers against radiation release and by reducing the potential for, and consequences of, severe accidents. The Commission PRA Policy Statement (1995) stipulates that:

> "... complete reliance for safety cannot be placed on any single element of the design, maintenance, or operation of a nuclear power plant." The statement goes on to note that "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."

It also notes that defense-in-depth is used by the NRC to provide redundancy as well as a multiple-barrier approach.

In 1996, NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors" references defense-in-depth in several places. Part 1, Section 3,

"Design of Structures, Systems and Components" states that applications should discuss how structures, systems and components protect against uncontrolled release of radioactive material. Part 1, Section 6, "Engineered Safety Features," notes that:

> "... the concept of ESFs evolved from the defense-in-depth philosophy of multiple layers of design features to prevent or mitigate the release of radioactive materials to the environment during accident conditions."

Part 1 Section 7, "Instrumentation and Control Systems," discusses how defense-in-depth should protect against common cause failures. Part 2, Section 1.2, "Summary and Conclusions on Principal Safety Considerations," states:

> "The summary discussions and descriptions should include such safety considerations as a conservative restricted area to exclude and protect the public, confinement or containment to control radioactive releases, operation with thermal-hydraulic parameters that are conservative compared with the designed capabilities of the fuel and cladding, diversity and redundancy of instrumentation and control systems, and other defense-in-depth features."

In 1996, in Section 100.1(d), the regulation states on 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."

In 1997, in a talk at the Massachusetts Institute of Technology, Nuclear Power Reactor Safety Course, Chairman Jackson noted that one element of the NRC safety philosophy is defense-in-depth and that "defense-in-depth ensures that successive measures are incorporated into the design and operating procedures ... to compensate for potential failures ..." In 1999, Chairman Jackson further elaborated on defense-in-depth in a white paper. She stated that:

> "... defense-in-depth ... employs successive compensatory measures to prevent accidents or mitigate damage ... ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation ... the net effect ... of defense-in-depth ... is that the facility ... tends to be more tolerant of failures and external challenges."

At an August 27, 1997, Advisory Committee on Reactor Safeguards (ACRS) subcommittee meeting Dr. Kress presented a paper on defense-in-depth. In the paper, Dr. Kress noted that the techniques and tools for determining risk were not well developed and risk measures were unavailable to the regulator. He noted that the NRC developed a regulatory philosophy called defense-in-depth that can be viewed as providing balance among three "levels" of protection to be implemented by providing multiple independent provisions. The three levels include:

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. He also noted that PRA results can be considered a measure of the effectiveness of the overall implementation of defense-in- depth. In addition, Dr. Kress agreed on the need for a policy statement that would describe the three levels and what constitutes appropriate regulatory balance between core damage frequency and conditional containment failure probability.

In 1999, Chairman Jackson issued a White Paper that stated:

> "… Risk insights can make the elements of defense-in-depth more clear by quantifying them to the extent practicable." and 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."

For the 1999 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 noted two different schools of thought. One is the structuralist model that asserts 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 second one is the rationalist model that asserts defense-in-depth is the aggregate of provisions made to compensate for uncertainty and incompleteness in the knowledge of accident initiation and progression.

The ACRS has provided their insights on defense-in-depth over the years, and predominantly in one specific letter. In a May 1999, letter to Chairman Shirley Jackson, the Committee states that two different perceptions of defense-in-depth exist. 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. The other view (the rationalist view), sees the proper role of defense-in-depth in a risk-informed regulatory scheme as compensation for inadequacies, incompleteness, and omissions of risk analyses. The Committee stated that 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 the current ones.

In other letters, the ACRS has stated that defense-in-depth is intended to compensate for uncertainty, and should balance prevention and mitigation. The ACRS also has noted that emergency preparedness is a critical element of defense-in-depth, and that developing defense-in-depth acceptance criteria would be helpful.

For both reactors and nuclear materials, the Committee viewed defense-in-depth as a strategy to ensure public safety given the unquantified uncertainty in risk assessments, and agreed the extent of defense-in-depth should be related to the degree of uncertainty.

A joint Advisory Committee on Nuclear Waste (ACNW) and ACRS subcommittee meeting was held on January 13 and 14, 2000 with the focus on defense-in-depth. The following is a summary for the various presenters as related to reactors:

- Defense-in-Depth: Perspective for Risk-Informing 10 CFR 50, Tom King, Gary Holahan. The presenters noted where the defense-in-depth philosophy is used in the NRC's regulatory framework and provided examples of defense-in-depth. They believed a working definition of defense-in-depth should be developed that provides for multiple lines of defense, balance between prevention and mitigation, and a framework to address uncertainties in accident scenarios. Moreover, the definition 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.

- Design Defense-in-Depth in a Risk-Based Regulatory System with Imperfect PRA, Tom Kress. Dr. Kress stated two concerns with defense-in-depth: (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. He proposes 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 proposed putting limits on defense-in-depth by having risk acceptance criteria that includes uncertainties, with quantifiable uncertainty coming out of a PRA and unquantifiable uncertainty estimated by expert opinion.

- Defense-in-Depth, Robert Bernero. Dr. Bernero noted that defense-in-depth can be viewed by addressing six questions, which he answers.

    1. What is defense-in-depth?
    2. Is there an overarching philosophy of defense-in-depth?
    3. Are current safety goals and objectives clear for general use?
    4. What is the role of defense-in-depth in risk-informed regulation of nuclear reactors?
    5. What is the role of defense-in-depth in risk-informed regulation of radioactive material processes and uses?
    6. What is the role of defense-in-depth in risk-informed regulation of radioactive disposal?

- On the Quantification of Defense-in-Depth, John Garrick. Dr. Garrick's 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.

In 2002, Karl Fleming and Fred Silady published a paper, "A Risk-Informed Defense-in-Depth Framework for Existing and Advanced Reactors." The 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. It discusses design, process and scenario defense-in-depth.

The term defense-in-depth appears in several places in reactor regulations. Issued in 2000, *10 CFR Part 50, Appendix R Section II.A* states that the fire protection program shall extend the concept of defense-in-depth to fire protection in fire areas important to safety, with the objectives of dealing with prevention, detection and protection. Issued in 2004, *10 CFR §50.69* requires that the categorization process maintain defense-in-depth. In the *Federal Register* Notice (FRN) that published the rule (2004), defense-in-depth was discussed in several places. It provides criteria for when defense-in-depth is adequate (criteria that are similar to the principles stated in Revision 2 to RG 1.174). It is further stated in the FRN that the primary need for improving the implementation of defense-in-depth 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 that there exists both unquantified and unquantifiable uncertainty in engineering analyses (both deterministic and risk assessments).

In 2002, the Nuclear Energy Institute (NEI), in a white paper (NEI 02-02), describes a new and optional risk-informed, performance-based regulatory framework for commercial nuclear reactors that 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."

Guidance is provided for achieving its defined principle on defense-in-depth.

In 2003, a petition was filed requesting that the NRC "immediately revoke the First Energy Nuclear Operating Company's ... license to operate the Davis-Besse Nuclear Power Station, Unit 1 (Davis-Besse)." The Director's decision states that the NRC's approach to protecting public health and safety is based on the philosophy of defense-in-depth and defines six principles: (1) the application of conservative codes and standards; (2) the establishment of substantial safety margins; (3) high quality in the design, construction, and operation; (4) that equipment can fail and operators can make mistakes, thereby the need for redundancy; (5) requirement for a containment structure; and (6) requirement for comprehensive emergency plans that are periodically exercised.

In 2004, 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... 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 iodide tablets). This approach addresses the expected as well as the unexpected."

Over the years several documents (NUREG/CR-6303, 1994; Regulatory Guide (RG) 1.152, 1996; NUREG-0800, Branch Technical Position (BTP) HICB-19 1997; NUREG-0800, BTP 7-19, 2007; and DI&C [digital instrumentation and control]-ISG [Interim Staff Guidance]-02, 2009) were published where defense-in-depth has been a key factor. These documents note 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."

These documents also define "echelons of defense" which are the control system, the reactor trip or scram system, the Engineered Safety Features actuation system, and the monitoring and indicator system.

In NUREG-1860, 2007, a proposed Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing is described where defense-in-depth is a key component. 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 type and magnitude of challenges to safety)."

Defense-in-depth, in the NUREG, is defined as ". . . 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 NUREG defines

- four objectives for defense-in-depth;
- a combined structuralist and rationalist approach to defense-in-depth;
- a set of six defense-in-depth principles with associated criteria; and
- probabilistic criteria for evaluating defense-in-depth adequacy.

In 2009, Idaho National Laboratory (INL) published INL/EXT-09-17139 that provides a definition of defense-in-depth and an approach to be used to assure that its principles are satisfied for the Next Generation Nuclear Plant (NGNP) project. It states that "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 of 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, (2) programmatic defense-in-depth, and (3) risk-informed evaluation of defense-in-depth. For each of the above elements, principles and criteria are defined for each. As part of the risk-informed evaluation defense-in-depth element, a decision process with associated criteria is proposed. The criteria include probabilistic and deterministic criteria and also evaluates whether the uncertainties have been adequately addressed and if the defense-in-depth principles have been met.

In 2011, RG 1.174, Revision 2 was published. This regulatory guide provides an acceptable approach for assessing the nature and impact of proposed licensing basis changes by considering engineering issues and applying risk insights. The guidance includes an evaluation of the proposed change to ensure that the philosophy of defense-in-depth is maintained.

The guidance notes the defense-in-depth philosophy is maintained if the following occurs:

> "A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation."

> "Over-reliance on programmatic activities as compensatory measures associated with the change in the LB [licensing basis] 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 plant's design criteria is maintained."

Other regulatory guides exist where defense-in-depth is either mentioned or discussed. Many of these regulatory guides repeat the above seven elements found in RG 1.174. Others state that defense-in-depth is intended to compensate for uncertainties.

On July 12, 2011 the Near-Term Task Force completed its review of insights from the Fukushima Dai-ichi accident and published its finding in "Recommendations for Enhancing Reactor Safety in the 21st Century." A major theme in the report centers on defense-in-depth and its ability to provide for adequate protection. The report discusses defense-in-depth including how the multiple layers that defense-in-depth ensures are part of the design basis, and how the application of defense-in-depth could be improved by using risk insights and explicit requirements for beyond-design-basis events.

In 2012, NUREG 2150 was published and provided 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 that after decades of use, no clear definition or criteria exist on how to define adequate defense-in-depth protections; that the concept of defense-in-depth is not used consistently, and there is no guidance on how much defense-in-depth is sufficient**;** that 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 NUREG characterizes defense-in-depth as follows:

> "Provide risk-informed and performance-based defense-in-depth protections to: (1) 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 —(a) each barrier is designed with sufficient safety margins to maintain its functionality for relevant scenarios and account for uncertainties, (b) systems that are needed to ensure a barrier's functionality are designed to ensure appropriate reliability for relevant scenarios, and (c) barriers and systems are subject to performance monitoring— and (2) 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."

The glossary on the NRC Website defines defense-in-depth as:

> "... an approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense-in-depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures."

Over the years, numerous SECY papers to the Commission, RGs and ACRS letters have discussed defense-in-depth. These discussions (summarized in tables at the end of Section 4) have reiterated that defense-in-depth is a basic element of the NRC's safety philosophy to prevent accidents from happening and to mitigate their consequences. Definitions include defense-in-depth as having multiple barriers, balance among prevention and mitigation, and safety functions not be dependent on a single element of design. In addition, the papers mention several elements of defense-in-depth including: the single failure criterion, redundancy, diversity, independence, and emergency preparedness. Other papers discuss defense-in-depth principles, levels of defense-in-depth, and determining the adequacy of defense-in-depth. One paper noted that the lack of guidance is an impediment to increased use of risk information and another proposed developing a policy statement on defense-in-depth.

3.2 High Level Historical Summary of Non-reactor Defense-In-Depth

Unlike the reactor defense-in-depth history, the history on defense-in-depth with regard to non-reactors is primarily found in the regulations. Little discussion on defense-in-depth is contained in other documents (e.g., NUREGs, SECY papers, Regulatory Guides, other technical documents). The regulations are generally based on a defense-in-depth philosophy although the term itself is often not used; the following essentially equivalent terms have been employed: levels of defense, lines of defense, layers of defense (or layers of protection), factors of safety, and multiple barriers. The requirements generally do not describe or define defense-in-depth, they describe defensive measures.

A list of sources reviewed for the history of defense-in-depth for non-reactors include the following, shown in Table 3-2 below:

Table 3-2 Sources for the History of Defense-in-Depth for Non-Reactors

Sources (in Chronological Order)	
• ACRS letter 2000 • Joint ACNW/ACRS Subcommittee, January 2000 • Risk Informed Decisionmaking for Nuclear Material and Waste Applications, 2008 • 10 CFR Parts 30 to 39 • NUREG-1556 • NUREG-2150 • 10 CFR Parts 60, 61, 63 • SECY 97-300	• SECY 99-186 • *Federal Register* Notice 66, No. 213, Nov. 2, 2001 • 10 CFR Part 70 • NUREG-1520 • 10 CFR Part 71 • 10 CFR Part 72 • NUREG-1536 • NUREG-1567

Section 5 provides a detailed summary and a high-level summary is presented below for each of the following:

- 3.2.1 – Summary for All Non-Reactor Nuclear Arenas
- 3.2.2 – Summary for Byproduct Materials
- 3.2.3 – Summary for Uranium Recovery
- 3.2.4 – Summary for Disposal of High and Low-Level Wastes
- 3.2.5 – Summary for Domestic Licensing of Special Nuclear Material
- 3.2.6 – Summary for Transportation
- 3.2.7 – Summary for Storage of Spent Nuclear Fuel

3.2.1 Global Statements for All Non-Reactor Nuclear Areas

Only two sources were found that address the role of defense-in-depth in all non-reactor areas as a whole: In 2000 the ACRS provided its views on this matter in a letter to the NRC Chairman, and in the same year a joint ACNW/ACRS subcommittee meeting focused on this topic.

The ACRS' views on nuclear materials and activities are provided in a May 2000, letter to Chairman Richard Meserve. In this letter, the Committee states:

> "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 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."
>
> "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."
>
> "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 letter also discusses how defense-in-depth for materials differs from reactors because there is less experience in the application of PRA methods to nuclear materials than for nuclear reactors. Moreover, a greater diversity exists in materials licensed activities and accidents involving nuclear materials involve different consequences.

The Committee goes on to states that "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." These criteria can then be used to judge the adequacy of compensatory measures.

In January 2000, a joint ACNW/ACRS subcommittee was held with the focus on defense-in-depth. Dr. Eisenberg provided a presentation entitled "Defense-in-Depth for Risk-Informed Performance-Based Regulation: A Provisional NMSS Perspective." Dr. Eisenberg noted that defense-in-depth is addressed in several parts of the Nuclear Materials Safety and Safeguards (NMSS) framework and that NMSS regulates systems with fewer hazards than nuclear power plants (NPPs). He pointed out that there are two types of residual uncertainty. Type 1 involves the confidence or lack of confidence in analysis, and Type 2 involves a system for which the risk or safety analysis is somehow limited. Details are provided in his presentation describing the differences in the limitations of Type 1 versus Type 2. Dr. Eisenberg noted differences between defense-in-depth and safety margins. He proposed 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.

A document discussing Risk Informed Decisionmaking for Nuclear Material and Waste Applications was published in 2008. The purpose of this document is to provide a risk-informed framework for regulatory decision making to the staff of the NRC's Office of Nuclear Material Safety and Safeguards and Office of Federal and State Materials and Environmental

Management Programs. The document states that defense-in-depth and safety margin are attributes of risk-informed decision making and that the impact on defense-in-depth should be taken into account when analyzing a change or modification to an existing facility or activity. The document notes that:

> "Defense in depth is an element of NRC's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs." Moreover, the document states: "Defense in depth can be achieved by a variety of different measures such as passive containment systems (e.g., multiple barriers), active systems (e.g., ventilation systems), and administrative procedures. Redundancy and diversity can be used to manage uncertainties associated with system reliability. Hence, a minimal level of defense in depth may be necessary, despite very low quantitative risk estimates."

The document discusses the purpose and importance of defense-in-depth and safety margins. It states that defense-in-depth can vary with nature of the risk and/or uncertainty and it discusses the defense-in-depth measures needed for activities with varying levels of risk. The document provides guidance to the analyst in assessing the impact of a new issue or condition, e.g. a modification to an existing facility, new knowledge about potential challenges to facility operation, etc. on maintaining adequate defense-in-depth and safety margin. To assess the impact of the issue/condition on defense-in-depth, the document provides a set of questions for the analyst to evaluate in various areas including barrier integrity, layers of defense, and the effectiveness of various options in maintaining defense-in-depth.

3.2.2 Summary for Byproduct Materials

Discussions of defense-in-depth features regarding byproduct material can be found in the regulations of Title 10 of the *Code of Federal Regulations* (CFR) Parts 30 through 39, as well as two NUREGS.

A summary regarding how defense-in-depth is addressed in the regulations is provided below. 10 CFR §30.32 requires applicants to demonstrate:

> "The radioactive material is physically separated so that only a portion could be involved in an accident;"
>
> "All or part of the radioactive material is not subject to release during an accident because of the way it is stored or packaged;"
>
> "Means and equipment are available for mitigating the consequences of each accident, including those provided to protect workers onsite."

The rules in 10 CFR §32.22 through 10 CFR §32.32 indicate that the risk from device failure should be acceptably low, which is an important defense-in-depth principle.

10 CFR §34.20 which involves “performance requirements for industrial radiography equipment” has two preventive measures that may be considered as defense-in-depth: (1) “The guide tube exposure head connection must be able to withstand the tensile test for control units specified in ANSI N432-1980.” This requirement concerns the use of conservative codes and standards to ensure a large safety margin. (2) “Source changers must provide a system for ensuring that the source will not be accidentally withdrawn from the changer when connecting or disconnecting the drive cable to or from a source assembly.” This requirement relates to the design of equipment to reduce the likelihood of malfunctions.

10 CFR §36.21, “Performance criteria for sealed sources,” used in irradiators requires that such sources “must be doubly encapsulated.” 10 CFR §39.41, “Design and performance criteria,” for the sealed sources used in well logging, requires that “the sealed source is doubly encapsulated.”

There are a few NUREGs Concerning Byproduct Materials where defense-in-depth is addressed. These include the following:

NUREG-1556 V6 - Standard Review Plan for Irradiators (January 1999)

This document outlines a defense-in-depth feature in the design and operation of panoramic irradiators, as follows:

> “An independent backup access control system is required to provide a redundant means of preventing a person from being accidentally exposed to the source. In addition, instruction must be provided to at least one other individual who will be on site during operations on how to respond to the independent backup access control alarm and to promptly render or summon assistance.”

The independent backup access control embodies the principles of redundancy and diversity and hence is a defense-in-depth feature.

NUREG-2150 - A Proposed Risk Management Regulatory Framework (April, 2012)

This document comments on the use of defense-in-depth in the various non-reactor activities NRC regulates. Regarding materials NUREG 2150 states:

> “The terminology of defense-in-depth is not used consistently across the NRC’s materials regulatory programs. .....The concept of defense-in-depth, which is a central part of reactor regulation, is more of an implicit rather than explicit part of the materials program. ….Due to the wide variety of licensed materials uses, there is not a common understanding of the terms risk-informed, performance-based, and defense-in-depth within NRC or with these licensees.”

> "Defense-in-depth considerations are built into the design and manufacture of generally licensed devices so that an individual can possess and use such a device with no formal training or experience and only minimal requirements for accountability. For certain devices, which contain a sufficient amount of radioactive material that could pose a greater hazard, the NRC has required individuals to be registered (but not licensed)."

3.2.3 Summary for Uranium Recovery

Discussion of defense-in-depth features concerning uranium recovery can be found in NUREG-2150, "A Proposed Risk Management Regulatory Framework" (April, 2012). This document provides a brief summary of defense-in-depth in the NRC regulations governing uranium recovery, as follows:

> "The concept of defense-in-depth is not commonly used as an explicit consideration in the NRC's regulation of uranium recovery. In large measure, this reflects the fact that uranium recovery is a relatively low-risk activity. There are instances, including design features and regulatory review of mill tailings impoundments, as well as the arrangement of injection, recovery and monitoring wells at ISR facilities that reflect defense-in-depth considerations."

3.2.4 Summary for Disposal of High and Low-Level Wastes

Discussions of defense-in-depth features regarding the disposal of both high and low-level wastes can be found mainly in the regulations, but also in a few SECYs and other documents.

Defense-in-depth features of regulations in 10 CFR Part 60 - Disposal of High-level Radioactive Wastes in Geologic Repositories are the following:

10 CFR §60.21, "Content of application," states that the applications should discuss the effectiveness of barriers and the quality assurance program.

10 CFR §60.122, "Siting Criteria," discusses siting in a favorable area such that "the performance objectives relating to isolation of the waste will be met." The location of regulated activities at sites that facilitate the protection of public health and safety is a defense-in-depth principle.

10 CFR §60.131, "General Design Criteria for the repository operations area," requires:

> "(b) Criticality control. All systems for processing, transporting, handling, storage, retrieval, emplacement, and isolation of radioactive waste shall be designed to ensure that nuclear criticality is not possible unless at least two unlikely, independent, and concurrent or sequential changes have occurred in the conditions essential to nuclear criticality safety."

Defense-in-depth features of regulations in 10 CFR Part 61 - Licensing Requirements for Land Disposal of (Low-Level) Radioactive Waste are the following:

10 CFR §61.7, “Concepts,” establishes the need for a barrier (between the disposal trench and the boundary of the facility) by requiring a buffer zone, which:

> “... is a portion of the disposal site that is controlled by the licensee and that lies under the site and between the boundary of the disposal site and any disposal unit. It provides a controlled space to establish monitoring locations which are intended to provide an early warning of radionuclide movement, and to take mitigative measures if needed.”

The provision of a buffer zone combined with an intruder barrier is a defense-in-depth feature.

10 CFR §61.13, “Technical Analyses,” requires:

> “... analyses of the protection of individuals from inadvertent intrusion must include demonstration that there is reasonable assurance the waste classification and segregation requirements will be met and that adequate barriers to inadvertent intrusion will be provided.”

Defense-in-depth features of regulations in 10 CFR Part 63 - Disposal of High-Level Radioactive Wastes in a Geologic Repository at Yucca Mountain, Nevada are the following:

Under Subpart E--Technical Criteria, 10 CFR §63.113, “Performance objectives for the geologic repository after permanent closure,” requires:

> “(a) The geologic repository must include multiple barriers, consisting of both natural barriers and an engineered barrier system.”

> “(b) The engineered barrier system must be designed so that, working in combination with natural barriers, radiological exposures to the reasonably maximally exposed individual are within the limits specified at 10 CFR §63.311 of subpart L.”

10 CFR §63.112, “Requirements for preclosure safety analysis of the geologic repository operations area,” specifies that:

> “... the preclosure safety analysis of the geologic repository operations area must include… means to provide reliable and timely emergency power to instruments, utility service systems, and operating systems important to safety if there is a loss of primary electric power; and means to provide redundant

> systems necessary to maintain, with adequate capacity, the ability of utility services important to safety."

10 CFR §63.161, "Emergency Plan for the geologic repository operations area through permanent closure," requires:

> "DOE [Department of Energy] shall develop and be prepared to implement a plan to cope with radiological accidents that may occur at the geologic repository operations area, at any time before permanent closure and decontamination or decontamination and dismantlement of surface facilities."

All of the above rules can be regarded as defense-in-depth features found in the regulations for the repository.

Defense-in-depth features concerning waste can also be found in the following SECYs, *Federal Register* Notice and NUREG:

SECY-97-300 - Proposed Strategy for Development of Regulations Governing Disposal of High-Level Radioactive Wastes in a Proposed Repository at Yucca Mountain, Nevada

The development of NRC regulations for geologic disposal in 1983 represented a unique application of the defense-in-depth philosophy to a first-of-a-kind type of facility.

> "Application of defense-in-depth principles for regulation of repository performance, for long time periods following closure, must account for the difference between a geologic repository and an operating facility with active safety systems and the potential for active control and intervention. A closed repository is essentially a passive system, and assessment of its safety over long timeframes is best evaluated through consideration of the relative likelihood of threats to its integrity and performance. Although it is relatively easy to identify multiple, diverse barriers that comprise the engineered and geologic systems, the performance of any of these systems and their respective subsystems cannot be considered either truly independent or totally redundant."

SECY-99-186 Staff Plan for Clarifying How Defense-In-Depth Applies to the Regulation of a Possible Geologic Repository at Yucca Mountain, Nevada

This paper provides the staff's plan to address more clearly the NRC's defense-in-depth philosophy as it relates to disposal of high-level radioactive wastes.

Federal Register Notice 66, No. 213, Nov. 2, 2001

This notice also pertains to 10 CFR Part 63 the HLW geologic repository at Yucca Mountain, Nevada. This document explains features related to defense-in-depth that are contained in the final rule 10 CFR Part 63 concerning the HLW repository at Yucca Mountain, NV and responds to comments made by various stakeholders on the draft rule. Specifically, the document outlines the relationship between multiple barriers and defense-in-depth, stating that the Commission expects that if a repository system is made up of multiple barriers, then it will be more tolerant of unanticipated failures and external challenges.

NUREG-2150 – A Proposed Risk Management Regulatory Framework (April 2013)

This document addresses defense-in-depth in both low-level waste and high-level waste as follows:

Regarding Low-Level Waste:

> "There is not a common understanding and usage of the terms risk-informed, performance-based, and defense-in-depth within the NRC, as well as outside the NRC."
>
> "The concept of defense-in-depth is implicit in the requirements and structure of 10 CFR Part 61, although the term itself is not explicitly used. …The interlocking and reinforcing systems approach in 10 CFR Part 61 (site suitability, waste form and classification, intruder barrier, institutional controls, etc.) represents an implicit consideration of defense-in-depth features, based on the risk posed by various classes of waste."

Regarding High-Level Waste

> "Perhaps the most significant change to the NRC regulations was the approach to defense-in-depth during the post-closure period of a geologic repository (i.e., implementation of the multiple barrier requirements). A longstanding principle of geologic disposal has been a reliance on multiple barriers to limit the release and transport of radionuclides. Engineered barriers (such as waste packages and waste forms) should complement and work with the geological or natural barriers so that safety does not depend solely on a single barrier or phenomenon…."
>
> "The NRC's regulatory philosophy of defense-in-depth is reflected in the multiple-barrier requirement for post-closure in 10 CFR Part 63. Compliance with the multiple barrier requirements is demonstrated through the performance assessment."

3.2.5 Summary for Domestic Licensing of Special Nuclear Material

Discussion of defense-in-depth measures regarding domestic licensing of special nuclear material can be found in 10 CFR §70.64 and two NUREGs.

10 CFR §70.64, “Requirements for new facilities or new processes at existing facilities,” explicitly specifies that “facility and system design and facility layout must be based on defense-in-depth practices ...” As used in §70.64, Requirements for new facilities or new processes at existing facilities:

> “... defense-in-depth practices means a design philosophy, applied from 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 failures and external challenges. The risk insights 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 §70.64 also requires that the design must provide for criticality control including adherence to the double contingency principle.

Defense-in-depth features in NUREGs concerning special nuclear material in fuel cycle facilities can be found in the following NUREGs:

NUREG-1520) - Standard Review Plan for Fuel Cycle Facilities (June 2015)

Based on the information in the ISA Summary provided in accordance with 10 CFR §70.65, the NRC makes licensing decisions as required under 10 CFR §70.21, "Filing," 10 CFR §70.22, 10 CFR §70.23, and 10 CFR §70.60, "Applicability," through 10 CFR 70.66, "Additional Requirements for Approval of License Application." These decisions include compliance with the performance requirements, the baseline design criteria, defense-in-depth, and the adequacy of management measures.

NUREG-2150 - A Proposed Risk Management Regulatory Framework (April 2012)

> “The requirement for and definition of defense-in-depth in safety of fuel cycle facility processes is explicit in 10 CFR §70.64(b). That definition is identical to the one contained in SECY-98-144, “White Paper on Risk-Informed and Performance-Based Regulation,” which defined “risk-informed,” “defense-in-depth,” and related concepts... In addition, the double contingency principle

has been an industry standard in the nuclear criticality safety field for decades and is also mandated by 10 CFR §70.64(a)(9)."

3.2.6 Summary for Transportation

Discussion of defense-in-depth measures regarding transportation can be found in two regulations and one NUREG.

10 CFR §71.43, "General standards for all packages," states "Each package must include a containment system securely closed by a positive fastening device that cannot be opened unintentionally or by a pressure that may arise within the package."

10 CFR §71.55, "General requirements for fissile material packages," requires that a package used for the shipment of fissile material must be so designed and constructed and its contents so limited that it would be subcritical if water were to leak into the containment system, or liquid contents were to leak out of the containment system. The regulation states exemptions may be approved if no single packaging error would permit leakage.

NUREG-2150 - A Proposed Risk Management Regulatory Framework (April 2012)

> "While the term 'defense-in-depth' is not explicitly used, the current regulatory approach for approving and inspecting radioactive shipping packages follows the risk-informed and performance-based defense-in-depth approach in a general sense. For example, the safety requirements for different types of shipping packages become more stringent with the quantity (radioactivity), or hazard, contained. The threshold for an accident resistant package is based on an A1 (special form or encapsulated material) or A2 (normal form) quantity. In turn, the A1 and A2 quantities are based on accident models that keep the anticipated dose to first responders below the occupational exposure limit of 5 rem. If a package contains greater than an A1 or A2 quantity (i.e., has a potential to cause an exposure greater than 5 rem), it is required to meet Type B accident conditions. The current system also allows shipments of quantities that would normally require Type B packages to be made in less robust packages that take credit for the low, specific activity of the material being shipped."

3.2.7 Summary for Storage of Spent Nuclear Fuel

Discussion of defense-in-depth measures regarding storage of spent nuclear fuel can be found in two regulations and three NUREGs.

10 CFR §72.124, "Criteria for nuclear criticality safety," requires:

> "Design for criticality safety. Spent fuel handling, packaging, transfer, and storage systems must be designed to be maintained subcritical and to ensure

that, before a nuclear criticality accident is possible, at least two unlikely, independent, and concurrent or sequential changes have occurred in the conditions essential to nuclear criticality safety."

10 CFR §72.236, "Specific requirements for spent fuel storage cask approval and fabrication," require that the spent fuel storage cask must be designed to provide redundant sealing of confinement systems.

Defense-in-depth features in NUREGs concerning special nuclear material in fuel cycle facilities can be found in:

NUREG-1536: Standard Review Plan for Dry Cask Storage Systems (July 2010)

Table B-5, p. 321 and Attachment B-2 of this NUREG state:

"Defense-in-depth has long been a key element of the NRC's safety philosophy. It is intended to ensure that the accomplishment of key safety functions is not dependent upon a single element of design, construction, maintenance or operation. In effect, defense-in-depth is used to provide one or more additional measures to back up the front line safety measures, to provide additional assurance that key safety functions will be accomplished. Traditional defense-in-depth measures for reactors have included items such as confinement, containment, redundant and diverse means of decay heat removal and emergency evacuation plans. For dry cask storage systems, examples of measures associated with defense-in-depth are as follows:

- Confinement System (2nd barrier to fuel clad integrity);
- Operating Controls and Monitoring
- Non-mechanistic and bounding event analyses (to mitigate site-specific uncertainties)."

NUREG-1567: Standard Review Plan for Spent Fuel Dry Storage Facilities (March 2000)

This document indicates that in reviewing the fire protection plan (FPP) for spent fuel dry storage facilities, the reviewer should focus on defense-in-depth:

"The reviewer should verify that an FPP provides assurance that a fire will not significantly increase the risk of radioactive releases to the environment in accordance with the general design criteria of 72.122(c). A defense-in-depth approach should achieve balance among prevention, detection, containment, and suppression of fires."

NUREG-2150 - A Proposed Risk Management Regulatory Framework (April 2012)

> "The concept of defense-in-depth is not explicitly or consistently applied in the spent nuclear fuel storage regulatory program. … The concept is most notably incorporated in 10 CFR 72.124(a), the double contingency principle to prevent nuclear criticalities. In addition to the current licensing approach, defense-in-depth may also be inherent in the designs and operations of the various dry storage systems. However, these aspects are not explicitly identified or recognized as defense-in-depth considerations."

3.3 High Level Historical Summary of Security Defense-In-Depth

The term defense-in-depth is rarely used and when used is not used consistently in the security arena of nuclear facilities regulated by the NRC. However, as noted below, defense-in-depth features are found in various parts of Title 10 of the CFR, as well as in other source documents such as NUREGs, relating to security and physical protection.

A list of sources reviewed for the history of defense-in-depth for security includes the following in Table 3-3 below:

Table 3-3 Sources for the History of Security Defense-in-Depth

• 10 CFR Part 30 • 10 CFR Part 37 • NUREG-1556, Vol. 1	• 10 CFR Part 73 • NUREG-1804, Rev 2

Section 6 provides a detailed summary and a high-level summary is presented below for each of the following:

- 3.3.1 – Byproduct Materials
- 3.3.2 – Physical Protection of Plants and Materials

3.3.1 Byproduct Materials

The regulations governing security for byproduct material are found in 10 CFR Parts 30 and 37 and NUREG-1556. Below are examples of regulations which use defense-in-depth principles including multiple barriers, redundancy and diversity:

- 10 CFR §30.34 and 10 CFR §37.53 contain requirements for having *"two independent physical controls that form tangible barriers"* to prevent unauthorized removal of material.

- 10 CFR §37.49 requires maintaining monitoring and detection capability in the event of a loss of primary power.

- 10 CFR §37.79 requires redundant communications not subject to the same interference factors.

NUREG-1556 V1 – Standard Review Plan on Portable Gauge Licenses (May 2012)

The standard review plan for portable gauge licensees indicates the defense-in-depth measures, based on multiple physical barriers to unauthorized access that need to be taken to ensure security. The document states that "at all times, licensees are required to maintain control and constant surveillance of the portable gauge when it is in use and, at a minimum, use two independent physical controls to secure the portable gauge from unauthorized removal while it is in storage."

It continues:

> "As long as the licensee maintains constant control and surveillance while transporting the portable gauges, the licensee need only comply with the DOT [Department of Transportation] requirements for transportation (e.g., placarding, labeling, shipping papers, blocking and bracing). However, if the licensee leaves the vehicle and portable gauge unattended (e.g., while visiting a gas station, restaurant, store), the portable gauge must be secured by two independent controls as required by 10 CFR 30.34(i)."

3.3.2 Physical Protection of Plants and Materials

Discussions regarding defense-in-depth measures related to the physical protection of plants and materials can be found in in 10 CFR Part 73 and in NUREG-1804.

The regulations in 10 CFR Part 73 are primarily related to defense-in-depth by requiring redundancy and diversity in physical protection systems, guards, vehicles and communication. Examples are given below:

- 10 CFR §73.20 requires a physical protection system with "sufficient redundancy and diversity to ensure maintenance of the capabilities described in § 73.25 and §73.45"

- 10 CFR §73.25 requires that that physical protection system can survive a single adversary action.

- 10 CFR §73.26specifies the number of escort vehicles and armed escorts which must accompany cargo.

- 10 CFR §73.37 requires redundant communication.

- 10 CFR §73.45 and 10 CFR §73.50 require multiple physical barriers.

NUREG-1804, Rev 2, Yucca Mountain Standard Review Plan (July 2003)

This document reviews the requirements of the physical protection plan at the HLW repository at Yucca Mountain, NV and identifies those that may be considered defense-in-depth. The document states:

> "The U.S. Department of Energy has identified and adequately described those portions of the physical protection system for which redundant and diverse components and redundant and diverse subsystems and components are necessary to ensure adequate performance, as required by 10 CFR 73.51(b)(2). Access to material in the protected area shall require passage or penetration through two physical barriers—one barrier at the perimeter of the protected area, and one barrier offering substantial penetration resistance."

3.4 High-Level Historical Summary of International Defense-In-Depth

The list of sources reviewed for the history of defense-in-depth from the international community are mostly from the International Atomic Energy Agency (IAEA) as Table 3-4 below indicates. The IAEA has published several documents that address defense-in-depth with regards to reactors. Moreover, defense-in-depth has been a specific item of interest within the Organization for Economic Co-Operation and Development (OECD) Nuclear Energy Agency (NEA)/Committee on Nuclear Regulatory Activities (CNRA)/Committee on the Safety of Nuclear Installations (CSNI). This section provides a summary of international history.

Table 3-4 Sources for the History of International Defense-in-Depth

- IAEA Documents (INSAG-3, 10, & 12, SRS 46, TECDOC-1570, NP-T-2.2, SF-1, SSR-2/1, INFCIRC 225 Rev 5)
- OECD NEA/CNRA/CSNI Workshop
- Swedish Radiation Safety Authority (SSM 2015:04)
- NEA, OECD Booklet

The International Nuclear Safety Advisory Group (INSAG) of the IAEA has published several documents related to defense-in-depth (INSAG-3, 10, and 12 and NR-T-2.2):

- In 1988, INSAG-3 was published and 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." 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."

- In 1996, INSAG-10 was published which restates the explanation and principle 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 accidents at the plant." The report 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.

- In 1999, INSAG-12 was published which is consistent with INSAG-3 and 10 on defense-in-depth; however, it further states that the strategy for defense-in-depth is twofold: first, to prevent accidents 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. 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.

- In 2005, IAEA published a report in the Safety Report Series, SRS No. 46, dealing with the assessment of defense-in-depth for NPPs. This publication describes a method for assessing the defense-in-depth capabilities of an existing plant, including both its design features and the operational measures taken to ensure safety. A systematic identification of the required safety provisions for the siting, design, construction and operation of the plant provides the basis for assessing the comprehensiveness and quality of defense -in-depth at the plant. For easier and more user friendly applicability, the method is illustrated in the form of so called "objective trees."

- In 2006, IAEA published SF-1 which establishes safety objectives, safety principles and concepts that provide the bases for the IAEA's safety standards and its safety related programs. This standard provides 10 safety principles. Principle 8, "Prevention of accidents," is defined: "all practical efforts must be made to prevent and mitigate nuclear or radiation accidents." It points to "'defence-in-depth" as the primary means of preventing and mitigating accidents, through multiple levels of protection such that no single failure could lead to harmful effects.

- In 2007, IAEA published TECDOC-1570 which 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 is 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).

- In 2009, IAEA published NP-T-2.2, "Design features to achieve defence in depth in small and medium sized reactors." The overall objectives of this report are stated to be: "(1) To assist developers of innovative SMRs [small modular reactors] in defining consistent defence in depth approaches regarding the elimination of accident initiators/ prevention of accident consequences through design and the incorporation of inherent and passive safety features and passive systems in safety design concepts of such reactors; (2) To assist potential users of innovative SMRs in their evaluation of the overall technical potential of SMRs with inherent and passive safety design features, including their possible implications in areas other than safety."

- In 2012, IAEA published SSR-2/1, "Safety of Nuclear Power Plants: Design, Specific Safety Requirements," which 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." It describes defense-in-depth and states that it applies to all safety related activities. SSR-2/1 describes five levels of defense. Requirement 7 of SSR-2/1 states that "The design of a nuclear power plant shall incorporate defence in depth."

- The IAEA's Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities, INFCIRC 225, Rev 5, January, 2011, identifies defense-in-depth as one of the fundamental principles of risk-based physical protection systems and measures. The document states: "The State's requirements for physical protection should reflect a concept of several layers and methods of protection (structural, other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives. …(Fundamental Principle I: Defence in Depth)"

In 2013, OECD NEA/CNRS/CSNI held an international workshop on defense-in-depth. Presentations by various speakers led to several common key messages.

- 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

In 2015 the Swedish Radiation Safety Authority published a report entitled “Defense-in-Depth-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA,” (SSM 2015:04).

In SSM 2015:04, the author, Per Hellström, describes a project whose objective it is to investigate how, and to what extent, probabilistic safety assessment (PSA) (usually referred to as probabilistic risk assessment [PRA] in the United States) can be used to asses and improve the defense-in-depth of nuclear power plants. In the report (and the research project) defense-in-depth is based on the following concept from IAEA INSAG 12 which is based on IAEA INSAG 3: "All safety activities, whether organizational, behavioral or equipment related, are subject to layers of overlapping provisions, so that if a failure occurs 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."

The author wants to link quantities calculated in PSA to specific levels of defense-in-depth, as defined in INSAG 12 and other IAEA publications. A ranking of structures, systems, and components (SSCs) that have a role in the different defense-in-depth levels is sought in relation to their risk contribution.

The booklet provides insights into the implementation of defense-in-depth by regulators and emergency management authorities after the Fukushima Daiichi accident, “aiming to enhance global harmonization by providing guidance on:

> “... the background to the DiD concept;
>
> the need for independent effectiveness among the safety provisions for the various DiD levels, to the extent practicable;
>
> the need for greater attention to reinforce prevention and mitigation at the various levels;
>
> the vital importance of ensuring that common cause and common mode failures, especially external events acting in combination, do not lead to breaches of safety provisions at several DiD levels, taking note of the particular attention that human and organisational factors demand;
>
> the concept of “practical elimination” of sequences leading to significant radioactive releases;
>
> the implementation of DiD for new and existing reactors, multi-unit sites and other nuclear facilities;
>
> the implementation of DiD through regulatory activities …;
>
> the protection measures in the DiD concept of level 5 – off-site emergency arrangements.”

The booklet also identifies areas where further work may be beneficial, including:

> "... the impact of human and organisational factors on DiD;
>
> improvements on the use of the DiD concept for new reactor designs, multi-unit sites, fuel cycle facilities and research reactors;
>
> the implementation of countermeasures for level 5 of DiD;
>
> benchmarking and further harmonisation of regulatory use of DiD through training, workshops and other means;
> the impact of new technologies."

3.5 High Level Historical Summary of Other Agency's use of Defense-In-Depth

A review of literature from other agencies was not performed. However, a workshop on defense-in-depth was held with other agencies[2] to gain their perspectives. A more detailed write-up of this workshop is included in Section 8, but the key messages from this workshop include the following:

- Most agencies do not formally use the term "defense-in-depth" but many use similar concepts, or terms such as "resilience."
- The amount of risk that is acceptable is dependent on the agency mission.
- Defense-in-depth implementation varies and is dependent on the actual missions of each agency.
- Defense-in-depth is achieved through implementation of a combination of design, operational and programmatic requirements.
- Quantitative risk goals to measure defense-in-depth may be difficult to develop.
- Relative risk estimates for comparison purposes are more credible than absolute quantification of risk.
- Prevention and mitigation are key elements of defense-in-depth, however, because of the agency mission, restoration (i.e., resilience) may also be a significant aspect of defense-in-depth.

[2] Participants at the workshop included the Nuclear Regulatory Commission, National Aeronautics and Space Administration, Federal Aviation Administration, Department of Energy, Naval Nuclear Propulsion Program, Department of Homeland Security, Department of the Interior (Bureau of Safety and Environmental Evaluation), Army Corps of Engineers, and the Canadian Nuclear Safety Commission.

- Design, operational and/or programmatic requirements are dependent on the phase of the mission; for example, whether you are building from the ground up (a new design) or working with an existing design.

- The balance between prevention and mitigation depends on the application.

- From a security perspective, it is not always possible to eliminate the risk (e.g., activity will occur).

3.6 Overall Observations on Characterization of Defense-in-Depth

In performing a historical review of defense-in-depth and providing observations based on the review regarding the purpose, goal, strategy, structure, and definition, overall perspectives can be drawn regarding how defense-in-depth can be characterized.

- The purpose of defense-in-depth is meant to ensure that the risk of the regulated activity remains acceptably low regardless of lack of knowledge.

- The goal of defense-in-depth is meant to ensure that the public is protected from harm by preventing and mitigating accidents.

- The approach used for achieving defense-in-depth is to incorporate multiple layers of defense into the design and operation of the regulated activities and to ensure that these multiple layers address both prevention and mitigation.

- The actual layers are dependent on the posed threat.

- The strategies are the protective measures (i.e., design, operational or programmatic features) that are used to achieve each level of defense are dependent on both the level of defense and the actual threat (reactor core versus a medical device).

- There is almost no guidance on criteria for determining adequacy of defense-in-depth. The literature does suggest that the elements (e.g., layer of defense) should be quantified, that risk is used to access each defense system (e.g., safety measure), that compensatory measures can be graded to reduce risk, that any sequence (given all defense layers have failed) remain under a frequency consequence curve, that redundancy and diversity is sufficient to ensure risk guidelines are met, and that the adequacy could be assessed via a process using measures of risk.

- Principles are developed to help guide implementation of defense-in-depth. The principles define what defense-in-depth is to achieve for the subject regulated activity (i.e., goals). Overall, defense-in-depth should ensure that each regulated activity has appropriate defense-in-depth measures (i.e., design, operational and administrative features) for prevention and mitigation of adverse events and accidents.

4. HISTORICAL SUMMARY ON DEFENSE-IN-DEPTH FOR REACTORS

4.1 Introduction

This section provides a historical summary of defense-in-depth for reactor safety. The documents reviewed are summarized in Table 4-1 below.

Table 4-1 Sources for the History of Defense-in-Depth for Reactors

• AEC letters [AEC, 1956] • WASH-740 [AEC,1957] • Joint Committee on Atomic Energy Hearings [TCAE, 1967] • Internal Study Group [TCAE, 1969] • AEC letter [AEC, 1971a] • ECCS Hearings [AEC, 1971b] • WASH-1250 [AEC, 1973] • NRC Annual report [NRC, 1975] • NRC Reactor fact sheet [NRC, 1976a] • NUREG-0050 [NRC, 1976b] • NUREG-0578 [NRC, 1979a] • NUREG-0585 [NRC, 1979b] • NUREG/CR-1250 [NRC, 1980] • Post TMI Definitions and Examples [NRC, 1981] • NUREG-0880 [NRC, 1983] • Commission Policy Statements [NRC, 1986], [NRC, 1995], [NRC, 2008a] • NUREG/CR-6042 [NRC, 1994a] • NUREG-1537 ,[NRC, 1996b] • 10 CFR Part 100, 1996 [CFR] • MIT Speech by Chairman Jackson [NRC, 1997b] • Some Thoughts on Defense-in-Depth by Tom Kress [ACRS, 1997] • PSA '99 paper [Sorenson, 1997] • Commission White Paper [NRC, 1999a]	• ACRS letters [ACRS, 1999] • Joint ACNW/ACRS Subcommittee [ACRS, 2000a] • 10 CFR Part 50, Appendix R • A Risk-Informed Defense-in-Depth Framework for Existing and Advanced Reactors, Karl Fleming, Fred Silady [Fleming, 2002] • NEI 02-02 [NEI, 2002] • Petition on Davis Besse [NRC, 2003b] • 10 CFR §50.69, 2004 [CFR] • Remarks by Chairman Diaz [NRC, 2004] • Digital Instrumentation and Controls (NUREG/CR-6303, RG 1.152, NUREG-0800 BTP HICB-19, NUREG-0800 SRP BTP 7-19, DI&C-ISG-02), [NRC, 1994b], [NRC, 1996c], [NRC, 1997a], [NRC, 2007a], [NRC, 2009a] • NUREG-1860 [NRC, 2007b] • INL NGNP report [INL, 2009] • RG 1.174 other RGs [NRC, 2011a] • NTTF Review Report [NRC, 2011b] • NUREG-2150 RMTF [NRC, 2012a] • NRC glossary [NRC, 2014b] • SECYs, RGs, and ACRS letters [ACRS], [RG], [SECY]

The historical summary provided below is organized into four parts, (1) 1956-1976, (2) 1976-1986, (3) 1986-2002, and (4) 2002 to present.

4.2 Historical Review from 1956-1976

The term defense-in-depth appears early in Atomic Energy Commission (AEC) and NRC documents, but the discussion primarily involves physical barriers. Defense-in-depth is described as protecting against "unlikely" accidents; that is, design basis accidents (DBAs). There is no mention of severe accidents.

4.2.1 AEC Letter to US Senate, 1956

The earliest definition of defense-in-depth appears to be in a letter from W.F. Libby, Acting Chairman of the US Atomic Energy Commission to the Honorable Bourke Hickenlooper of the Joint Committee on Atomic Energy Congress of the United States on March 14, 1956. Although the term "defense-in-depth" does not appear in the letter, it does describe "lines of defense" that can be considered as representing defense-in-depth. These lines are described as:

> "A complete evaluation of all potential hazards of their particular reactor, and of the procedures to minimize the probability of occurrence of an accident which would result in the release of unsafe quantities of radioactive materials to the surroundings... to assure that the probability of an operating mishap has by adequate design and operating precautions been brought to an acceptably low level."
>
> "Evaluation ... shows what steps have been taken to protect the public in the event the highly improbable incident did occur and unsafe quantities of radioactive materials were released from the reactor itself... is essentially a vital second line of defense for the public that the relationship of the characteristics of the location of the reactor to the ability of the building to contain radioactive materials ... becomes an important factor."

The letter further includes a discussion on three factors that could be interpreted as defense-in-depth:

> "Recognizing all possible accidents which could release unsafe amounts of radioactive materials;"
>
> "Designing and operating the reactor in such a way that the probability of such accident is reduced to an acceptable minimum;"
>
> "By appropriate combination of containment and isolation, protecting the public from the consequences of such an accident, should it occur."

4.2.2 WASH-740, 1957

The next description of defense-in-depth appears to be in WASH-740, "Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants," and 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.”

4.2.3 Joint Committee on Atomic Energy Hearings, 1967

The next description 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."

4.2.4 Internal Study Group, 1969

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 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."

4.2.5 AEC Letter to US Senate, 1971

In a letter dated April 27, 1971, from Dr. Glen Seaborg, Chairman of the AEC to Honorable John Pastore, Chairman to the US Senate Joint Committee on Atomic Energy Congress of the United States, defense-in-depth is discussed along with lines of defense. Dr. Seaborg states that "our safety review is based on the important principle of defense-in-depth." His discussion on defense-in-depth includes the following:

> "All structures, systems, and components important to safety must be designed so that the probability of an accident occurring is very small... licensees to have and to apply effective quality assurance program to assure that nuclear power

plant are designed, built, and operated in a manner which is consistent with this objective."

"In accordance with the defense-in-depth concept, the conservative assumption is nevertheless made for design purposes that improbable accidents could occur. Engineered safety features are provided to mitigate the consequences of these postulated accidents... even though the probability of such accidents occurring is very small and even though there is a high degree of redundancy in engineered safety systems. Each line of defense must be reviewed carefully if the defense-in-depth concept is to be effectively implemented."

4.2.6 ECCS Hearings, 1971

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

4.2.7 WASH-1250, 1973

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."

4.2.8 NRC Annual Report, 1975

In the 1975 Annual Report, a defense-in-depth concept is discussed as one of the activities in ensuring safe design of nuclear power plants. The defense-in-depth concept is described as “three successive and mutually reinforcing echelons of defense ... to prevent a serious accident affecting the public.”

These three echelons are described as:

> “The first echelon of defense emphasizes accident prevention. It requires that the plant be soundly and conservatively designed, so that it can be built, tested, operated, and maintained in accordance with stringent quality standards and engineering practices with a high degree of freedom from faults and errors...”
>
> “The second echelon of defense is based on the assumption that failure or operating errors that potentially could lead to safety problems will occur ... Accordingly, safety systems are required to prevent or minimize damage from such failures... Conservative design practices, adequate safety margins, inspectability, and redundant detecting and actuating equipment must be incorporated into protection systems to assure both the effectiveness and the reliability of this second echelon of defense.”
>
> “The third echelon of defense supplements the first two through features that provide additional margins to protect the public against unlikely accidents. These margins are assessed primarily by evaluating the response of the plant to a number of arbitrarily assumed events ... From analyses of these postulated events, a number of accident sequences called “design basis accidents” are selected as a basis for the incorporation of additional features required for the extra margin of protection.”

4.2.9 NRC Fact Sheet on Reactor Safety, 1976

A Reactor Safety Fact Sheet was sent from John Harris, Director of Office of Public Affairs on April 6, 1976 to Bernard Rusche, Director of the Office of Nuclear Reactor Regulation (NRR), asking for comments and in which he noted in the letter that the fact sheet was developed to

summarize the “intensive review of a proposed nuclear power plant” and to be enclosed in “letters and ... with the news media.”

James Miller, Assistant to the Director of the Office of NRR, responded on April 20, 1976 and stated in his letter that “the descriptions used for the ‘defense in depth’ levels should agree with those used by Chairman Anders in his recent testimony before the Joint Committee.”

The revised fact sheet stated the following with regard to defense-in-depth:

> “The NRC’s review of a proposed plant is based on a concept that is referred to as ‘defense in depth.’ Under this concept, three successive and mutually reinforcing levels of defense against accidents and their consequences are considered.”
>
> ”The first level of defense is to provide a large margin of safety for possible human error, as well as for defects in materials and equipment and for acts of nature... “
>
> ”The second level is to provide backup systems that will compensate automatically for failure of essential equipment or human error that might occur in correcting any potentially unsafe condition. The aim ... is to prevent minor accidents from escalating into major accidents.”
>
> ”At the third level of defense, the design must provide equipment to limit the public consequences of even highly unlikely accidents. Engineered safety features, such as the containment building, the standby electrical power sources and emergency core cooling systems are provided to limit the consequences of accidents.”
>
> ”Of overriding importance in the design, construction, and operation of all three levels of safety protection is a vigorous program for quality assurance.”

4.3 Historical Review from 1976 to 1986

During this decade defense-in-depth is discussed mainly in relation to the occurrence of the Brown’s Ferry fire and the Three Mile Island (TMI) accident and its aftermath. With the Brown’s Ferry fire, the first mention of defense-in-depth as helping to mitigate severe potential accidents appears in the literature, and questions about the suitable balance among defense-in-depth echelons are raised. Post-TMI, the mention of defense-in-depth protection for “beyond design basis accidents” appears in the literature, along with the first mention of probabilistic risk assessment (PRA) as a possible means for quantifying defense-in-depth, and for thus reducing risk.

4.3.1 NUREG-0050, Recommendations Related to Browns Ferry Fire, 1976

In this NUREG, Section 2.5, Perspectives on Reactor Safety: Defense in Depth, states that:

> "... the principal goal of the NRC ... is the assurance of adequate protection of the health and safety of the public, and the maintenance at an acceptably low value of the risk due to nuclear power technology. This means, principally, the containment of the radioactive materials, and the prevention of their release in significant quantities. The provisions of multiple barriers for such containment, and the concept of defense-in-depth, are the means for providing the needed safety assurance."

The report describes three echelons of safety that are embodied in defense-in-depth as:

> "High quality in the plant, including design, materials, fabrication, installation, and operation throughout plant life, with a comprehensive quality assurance program."
>
> "Provision of protective systems to deal with off-normal operations and failures of equipment that may occur."
>
> "Provision, in addition, of safety systems to prevent or mitigate severe potential accidents that are assumed to occur in spite of the means employed to prevent them and the protective systems provided."

The report goes on to state that:

> "No one of these echelons of safety can be perfect, since humans are fallible and equipment is breakable. It is their multiplicity, and the depth thus afforded, that provide the required high degree of safety in spite of the lack of perfection in any given system. The goal is a suitable balance of the multiple echelons; increased strength, redundancy, performance, or reliability of one echelon can compensate in some measure for deficiencies in the others."

4.3.2 NUREG-0578, TMI-2 Lessons-Learned, 1979

Section 3, "Future Work by the Lessons-Learned Task Force," discusses defense-in-depth. The report states:

> "The underlying philosophy of nuclear reactor safety has provided multiple levels of protection against the release of radioactivity, i.e., the concept of defense in depth. It includes diversity and redundancy of various safety functions and systems and multiple physical barriers (the fuel, the cladding, the primary coolant boundary, and the containment). The Task Force concludes that the defense-in-depth concept is sound and is not fundamentally challenged

by the occurrence of the accident; however, there is a need to improve the implementation of the concept in determining safety requirements."

"The functions and general characteristics of the systems required to provide defense-in-depth are specified in the General Design Criteria of the Commission regulations (Appendix A to Title 10 Code of Federal Regulations (10 CFR) Part 50)."

"The specific design and performance requirements of these systems are determined, generally by analysis, so that the consequences of specified events, such as anticipated operational transients and design basis accidents, are within specific acceptance criteria. At Three Mile Island, some of the safety systems were challenged to a greater extent or in a different manner than was anticipated in their design basis. Many of the events that occurred were known to be possible, but were not previously judged to be sufficiently probable to require consideration in the design basis. Operator error, extensive core damage, and production of a large quantity of hydrogen from the reaction of zircalloy cladding and steam were foreseen as possible events, but were excluded from the design basis, since plant safety features are provided to prevent such occurrences. The Task Force will consider whether revisions or additions to the General Design Criteria or other requirements are necessary in light of these occurrences. A central issue that will be considered is whether to modify or extend the current design basis events or to depart from the concept. For example, analysis of design basis accidents could be modified to include multiple equipment failures and more explicit consideration of operator actions or inaction, rather than employing the conventional single-failure criterion. Alternatively, analyses of design basis accidents could be extended to include core uncovery or core melting scenarios. Risk assessment and explicit consideration of accident probabilities and consequences might also be used instead of the deterministic use of analysis of design basis accidents."

This report also discusses some specific defense-in-depth actions regarding hydrogen control and operator training.

4.3.3 NUREG-0585, TMI-2 Lessons Learned Task Force Final Report, 1979

In this NUREG, Section 3.3 discusses defense-in-depth relative to recommended improvements based on lessons learned. It states:

"In current practice, there are essentially three levels of protection of the public from releases of radioactivity in the defense-in-depth concept. Each of the first two levels of protection has a design objective in the form of a limit on the release of radioactivity of a characteristic frequency. For normal operation, the design objective is to keep the-levels of radioactive materials in effluents to unrestricted areas as low-as reasonably achievable during conditions that are

expected to occur one or more times during the life of the nuclear power unit. For accident conditions, the objective is to limit offsite radiation exposure to well within the guideline values contained in 10 CFR Part 100 following any of a set of design basis accidents that are representative of those events judged sufficiently likely to require consideration, as discussed in Section 3.2 [design requirements]. The functions and general characteristics of the equipment, systems, and structures required for these two levels of protection are specified in the General Design Criteria contained in Appendix A to 10 CFR Part 50 of the NRC regulations."

"The third and less completely defined level of protection has as a design objective the reduction of exposure of the public when an accident occurs, including accidents beyond the so-called design basis accidents used in specifying the second level of defense in depth. This protection is provided by the requirements for siting nuclear power plants (i.e., 10 CFR Part 100) and for emergency response plans (i.e., Paragraph 50.34 and Appendix E of 10 CFR Part 50)."

"Except for actions to upgrade emergency plans and a proposal to modify siting requirements, the recommendations resulting from evaluations of the accident at TMI-2 have, up to now, been generally directed toward improving the first two levels of protection. That is, the actions are generally directed toward the prevention of high-consequence accidents beyond the current design basis, rather than toward mitigation of the consequences of such accidents."

"The defense-in-depth concept is based on the premise that there is a limit to the effectiveness of any level of prevention. Unanticipated interactions and interrelationships among and between systems and the operators and the possibility of undetected common modes of failure are a bound on the assurance of any level of prevention. The TMI accident is illustrative of the point."

4.3.4 NUREG/CR-1250, 1980

In this NUREG, it states that:

"... licenses are issued for those nuclear power plants which ... are found to meet the safety criteria and standards required ... These safety standards include requirements for considerable margins between design and operating conditions and for redundancy in primary and backup equipment, in order to compensate for the fact that no body of knowledge can ever be complete enough to reduce uncertainties and risks to zero ... require plant builders and operators to take all those actions considered necessary to assure that the risk to public health and safety is, and continues to be acceptably low."

The report notes that this safety objective is achieved by the use of the defense-in-depth concept which calls for three levels of safety:

> “The first level requires that measures be taken to design, build and operate a nuclear power plant so it will, with a high degree of assurance, operate without failures that could lead to accidents. The plant is designed to conservative standards so that it will be safe in all phases of operation and have a substantial tolerance for errors, off-normal operation and component malfunction.”
>
> ”The second level of safety requires the provision of measure to cope with them [failures or errors must be expected to occur during the service life of a nuclear power plant]. Protection ... is provided by protection devices and systems designed so that expected occurrences and off-normal conditions will be detected and either arrested or accommodated safety.”
>
> ”The third level of safety supplements the first two by requiring design features and equipment to protect the public, even in the event of the occurrence of very unlikely accidents. The additional safety margins provided by these features are assessed primarily by evaluating the response of the plant to a number of assumed accidents ... From analyses of these postulated accidents, a number of sequences called ‘design basis accidents’ are selected as a basis for the design of the additional plant features and equipment that are provided to further protect public health and safety.”

In addition to describing three levels of safety, the NUREG goes on to state that:

> “... application of the defense-in-depth concept also resulted in the provision of multiple physical barriers between the radioactivity contained in the reactor fuel and the environment outside the plant. The fuel is contained in a sealed metal cladding; the clad fuel is contained in a heavy steel primary coolant system, and the primary coolant system is enclosed in a sealable containment building.”

4.3.5 Post-TMI Definitions and Examples, 1981

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 the 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.

4.3.6 NUREG-0880, 1983

In Section XI, Glossary, a definition of defense-in-depth is provided:

> "Defense in depth in engineering practice as applied to nuclear power plants, involves careful quality assurance and control in plant design, construction, and operation to reduce the likelihood of accidents; installation of backup systems to nullify the consequence of malfunctions in important plants systems and to prevent individual malfunctions from escalating into major accidents; and installation of engineered safety features to confine the consequences of certain postulated major 'design basis accidents'; to minimize effects on the public health and safety. It also involves siting of nuclear plants in areas of low population density and in locations that are not near natural or manmade hazards, and calls for responsible assurance that adequate protective measures can and will be taken by the licensee and the state and local authorities in the event of serious accidents."

4.4 Historical Review from 1986 to 2000

During this period, defense-in-depth is mentioned extensively in Commission Policy Statements, and ACRS members express views which deal extensively with defense-in-depth. It is in this era that the discussion becomes more focused on defense-in-depth as a means to deal with severe core damage accidents. The balance between prevention and mitigation with ideas on the desired frequency of core damage and containment failure is discussed, as is the use of risk as a measure of defense-in-depth effectiveness (e.g., quantification of defense-in-depth).

4.4.1 NRC Commission Policy Statements, 1986, 1994 (2008), 1995

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.

The 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, judgments 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 ... ”

The 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."

In a Commission policy statement on PRA (1995) 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 they serve to focus the traditional, deterministic-based, regulations and support the 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 plant, as well as the philosophy of a multiple-barrier approach against fission product releases.”

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

4.4.2 NUREG/CR-6042, Perspectives on Reactor Safety, 1994

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, siting and emergency plans.

4.4.3 NUREG-1537, Part 1, 1996

In Part 1, Section 3, “Design of Structures, Systems and Components,” the NUREG states:

> “In this chapter of the SAR [Safety Analysis Report], the applicant should identify and describe 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. 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.”

Part 1 Section 6, “Engineered Safety Features (ESF),” notes that:

> “The concept of ESFs evolved from the defense-in-depth philosophy of multiple layers of design features to prevent or mitigate the release of radioactive materials to the environment during accident conditions.”

Part 1 Section 7, “Instrumentation and Control Systems,” includes Regulatory Guide (RG) 1.152, Revision 1, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” January 1996, as Appendix 7.1. This RG states:

> “… the NRC staff has placed significant emphasis on defense-in-depth against propagation of common cause failures within and between functions. 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 errors 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 failures.”

In Part 2 in Section 1.2, “Summary and Conclusions on Principal Safety Considerations,” under *Review Procedures* the NUREG states:

> “The reviewer should consider the stated criteria to ensure safety and to evaluate their application to the reactor facility design. The summary discussions and descriptions should include such safety considerations as a conservative restricted area to exclude and protect the public, confinement or containment to control radioactive releases, operation with thermal-hydraulic parameters that are conservative compared with the designed capabilities of the fuel and cladding, diversity and redundancy of instrumentation and control systems, and other defense-in-depth features.”

In Section 6 of Part 2, the same statement appears on the evolution of ESFs from defense-in-depth philosophy that is noted above for Section 6 of Part 1.

Finally, Part 2 Section 9.3, “Fire Protection Systems and Programs,” under *Areas of Review* states “Areas of review should include the following: … discussion of fire protection plans and protective equipment used to limit the consequences of a fire, including defense in depth in the event of escalation of a fire.”

4.4.4 10 CFR Part 100, 1996

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.”

4.4.5 Chairman Jackson MIT Speech, 1997

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.”

4.4.6 Some Thoughts on Defense-in-Depth by Tom Kress, 1997

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 during a good part of regulatory history the techniques and tools for determining risk were not well developed and risk measures were unavailable to the regulator. He goes on to state that 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 is 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, and redundant and diverse emergency power supplies. The second element includes such concepts as multiple physical barriers, and 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 the idea that just about everything the NRC does is part of defense-in-depth and it becomes 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 containment failure probability (CCFP) and large early release frequency (LERF), and the third level in the final conditional risk measures 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. For 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) an 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.

4.4.7 PSA Paper, 1999

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.”

4.4.8 Commission White paper, 1999

Chairman Jackson provided her thoughts on defense-in-depth in a March 1999 White Paper. In it, she stated 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.”
>
> “... 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.”

4.4.9 ACRS Letters, 1999, 2000

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"...), 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."

"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: 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."

4.4.10 Joint ACNW/ACRS Subcommittee, January 13/14, 2000

A joint subcommittee was held with the focus on defense-in-depth. The following is a summary of those parts of the presentations that related to reactors.

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. General Design Criteria (GDC) provide for defense-in-depth; for example, GDC 1-5, 10-18, 20-29, 30-46, 50-57, and 60-64. Reactor oversight process cornerstones are also a defense-in-depth concept.

The presenters 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, quality assurance (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 accidents 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). Based 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 while 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 prevention is valued), on the extent of uncertainty in the risk assessment, and on how much the uncertainty is unquantifiable. In deterministic space, he noted that one may want to minimize uncertainty, and the choice of how much defense-in-depth 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 the following questions:

> "What is defense-in-depth? Defense-in-depth is an element of NRC's Safety Philosophy that employs successive compensatory measure 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 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."

"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."

"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 authorized practices include reactors, fuel cycle facilities, industrial and medical uses, exempt distribution, and transportation."

"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."

"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 choices of defense. It has "knotty" problems, for example, patient safety and medical QA."

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 the component.

4.4.11 10 CFR Part 50, Appendix R, 2000

The term “defense-in-depth,” when referring to reactor safety, 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.”

4.5 Historical Review from 2002 to Present

During this time period, there appears to be a focus on more top down approaches (frameworks) for implementing defense-in-depth and a renewed emphasis of NRC’s overall defense-in-depth philosophy.

4.5.1 A Risk-Informed Defense-in-Depth Framework, July 2002

A paper written by Karl Fleming and Fred Silady 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 many 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

4.5.2 NEI 02-02. 2002

The Nuclear Energy Institute (NEI) formed a "New Plant Regulatory Framework Task Force" that 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 fourth 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.

4.5.3 Petition on Davis-Besse, 2003

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."

4.5.4 10 CFR §50.69, 2004

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, it is stated:

> "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."

4.5.5 Remarks of Nils J. Diaz, Chairman, U.S. Nuclear Regulatory Commission, 2004

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 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."

4.5.6 Digital Instrumentation and Controls, 1994, 1996, 1997, 2007, 2009

Several documents discuss this issue. These include NUREG/CR-6303 (Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems) dated December 1994; RG 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 [DI&C]"), dated June 2009.

NUREG/CR-6303, 1994

INUREG/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 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, the RG 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 BTP is to "verify that adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements."

The BTP 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.

4.5.7 NUREG-1860, 2007

A 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 measures 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:

1. Compensate for uncertainties, including events and event sequences which are unexpected because their existence remained unknown during the design phase.

2. Compensate for potential adverse equipment performance, as well as human actions of commission (intentional adverse acts are part of this) as well as omission.

3. Maintain the effectiveness of barriers and protective systems by ensuring multiple, generally independent and separate, means of accomplishing their functions, and

4. 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 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 accidents 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:

"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."

"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."

"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."

"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."

"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.”

4.5.8 INL NGNP, 2009

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 an approach to be used to assure that its principles are satisfied for the Next Generation Nuclear Plant (NGNP) project. It states that:

> "... 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, plant capability defense-in-depth 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 a 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, it is then 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.

4.5.9 RG 1.174, 2011

This RG provides an acceptable approach for assessing the nature and impact of proposed licensing basis (LB) changes by considering engineering issues and applying risk insights. The guidance provided includes an evaluation of the proposed change to ensure that the philosophy of defense-in-depth is maintained. The guidance states that:

> "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 and, in particular, to account for the potential for unknown and unforeseen failure mechanisms or phenomena, which (because they are unknown or unforeseen) are not reflected in either the PRA or traditional engineering analyses. If a comprehensive risk analysis is done, it can provide insights into whether the extent of defense-in-depth (e.g., balance among core damage prevention, containment failure, and consequence mitigation) is appropriate to ensure protection of public health and safety. However, to address the unknown and unforeseen failure mechanisms or phenomena, traditional defense-in-depth considerations should be used or maintained."

The guidance notes the defense-in-depth philosophy is maintained if the following occurs:

> "A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation."
>
> "Over-reliance on programmatic activities as compensatory measures associated with the change in the LB 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 plant's design criteria is maintained."

4.5.10 NTTF Report, 2011

On July 12, 2011 the Near-Term Task Force (NTTF) completed its review of insights from the Fukushima Dai-ichi accident and published its finding in "Recommendations for Enhancing Reactor Safety in the 21st Century." A major theme in the report centers on defense-in-depth and its ability to provide for adequate protection. The following statements regarding defense-in-depth can be found in the report:

"A more balanced application of the Commission's defense-in-depth philosophy using risk insights would provide an enhanced regulatory framework that is logical, systematic, coherent, and better understood."

"The application of the defense-in-depth philosophy can be strengthened by including explicit requirements for beyond-design-basis events."

"This approach, if implemented, as a more comprehensive and systematic application of defense-in-depth to NRC requirements for providing "adequate protection" of public health and safety."

"The accident similarly provides new insights regarding low-likelihood, high-consequence events that warrant enhancements to defense-in-depth on the basis of redefining the level of protection that is regarded as adequate."

"The agency's historical commitment to a defense-in-depth philosophy that ensures that the design basis includes multiple layers of defense."

"In the Policy Statement on Safety Goals, the Commission emphasized the importance of features such as containment, siting, and emergency planning as 'integral parts of the defense-in-depth concept associated with its accident prevention and mitigation philosophy.'"

"The Task Force has found that the defense-in-depth philosophy is a useful and broadly applied concept. It is not, however, susceptible to a rigid definition because it is a philosophy. For the purposes of its review, the Task Force focused on the following application of the defense-in-depth concept:

- protection from external events that could lead to fuel damage

- mitigation of the consequences of such accidents should they occur, with a focus on preventing core and spent fuel damage and uncontrolled releases of radioactive material to the environment

- emergency preparedness (EP) to mitigate the effects of radiological releases to the public and the environment, should they occur"

"Defense-in-depth concept in which each level of defense-in-depth (namely protection, mitigation, and EP [emergency preparedness]) is critically evaluated for its completeness and effectiveness in performing its safety function."

"The key to a defense-in-depth approach is creating multiple independent and redundant layers of defense to compensate for potential failures and external hazards so that no single layer is exclusively relied on to protect the public and the environment."

"The first level of defense-in-depth is protection."

"The second level of defense-in-depth is mitigation."

"If mitigation is not successful in preventing a release of radioactive materials from the plant, EP ensures that adequate protective actions are in place to protect public health and safety. Protective actions are taken to avoid or reduce radiation dose."

4.5.11 Proposed Risk Management Regulatory Framework, 2012 (NUREG-2150)

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 the task force recommendation regarding a proposed Risk Management Regulatory Framework. The task force reviewed across the various regulatory areas 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 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."

4.5.12 NRC Glossary, Present

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."

4.6 Additional Historical Review of SECY's, 1977-2011

A more thorough review was performed regarding ACRS correspondence, NRC Regulatory Guides, and staff Commission SECY papers. The reviews of these documents are summarized in Tables 4-2 through 4-4, respectively.

Table 4-2 ACRS Discussions on Defense-in-Depth (see Note 1)

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 evaluations 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 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 provided redundant information should be used to satisfy the defense-in-depth philosophy.

Document	Subject	Defense-in-Depth Discussion
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.
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 the Office of Nuclear Reactor Regulation (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 CDF goal has always been two-fold: (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

Document	Subject	Defense-in-Depth Discussion
		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.
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.

Document	Subject	Defense-in-Depth Discussion
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 RG 1.174.
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 frequency-consequence (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.

Document	Subject	Defense-in-Depth Discussion
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 containment overpressure (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 provide a more complete assessment of the available margins and impact on defense-in-depth.
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 loss of coolant accident (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.

Document	Subject	Defense-in-Depth Discussion
Letter from S. Abdel-Khalik, ACRS Chairman, to R. W. Borchardt, NRC Executive Director for Operations (EDO), 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.		

Table 4-3 Defense-in-Depth Defined in Regulatory Guides (see Note 1)

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	ML003740172	8/31/1998

RG No.	Definition of Defense-in-Depth	Accession Number	Date
1.176 (cont.)	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. • 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 technical specification (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		9/15/1998

RG No.	Definition of Defense-in-Depth	Accession Number	Date
1.177 (cont.)	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 allowed outage time (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 surveillance test interval (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.		

RG No.	Definition of Defense-in-Depth	Accession Number	Date
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
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

RG No.	Definition of Defense-in-Depth	Accession Number	Date
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 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 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.	ML031490640	5/31/2003

RG No.	Definition of Defense-in-Depth	Accession Number	Date
1.195 (cont.)	• 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
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
5.71	Defense-in-depth strategies represent a documented collection of complementary and redundant security controls that establish multiple layers of protection to safeguard critical systems (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 critical digital asset (CDA) and with recovery.	ML092670517	10/9/2009

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.

Table 4-4 Discussions of Defense-in-Depth in SECY Documents (see Note 1)

SECY No.	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.

SECY No.	Subject	Discussion
83-269	Fire Protection Rule	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 Non-Publicly Available	Draft safety Evaluation Report on Chapter 5 of The Advanced Light Water Reactor Requirements Document	In Section 2.1 of the draft Safety Evaluation Report (SER), wherein the staff discusses the acceptability of the Advanced Light Water Reactor (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 Non-Publicly Available	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 Non-Publicly Available	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 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 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.
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.
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 configuration risk management (CRM) approach are to (1) provide 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.

SECY No.	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.
00-0062 Non-Publicly Available	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.

SECY No.	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)

SECY No.	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 (EOF) 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 modular gas reactor (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.

SECY No.	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.
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 (loss of offsite power)/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 tor Reactor Oversight Process (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.

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.

5. HISTORICAL SUMMARY ON DEFENSE-IN-DEPTH FOR NON-REACTOR AREAS

In reviewing the literature for defense-in-depth related to the non-reactor areas, there is very little history regarding defense-in-depth as compared to the commercial power reactor area. There are few documents, e.g., technical reports, regulatory guides or SECY papers that discuss defense-in-depth either explicitly or implicitly. Explicitly means actual use of the term in discussing defense-in-depth. Implicitly means that the text is related to the concept of defense-in-depth. It is assumed related to the concept, if, at a minimum, it refers to one of the following:

- Multiple barriers
- Levels (or e.g., layers) of defense
- Appropriate safety margins are provided
- Accident prevention and mitigation capability are provided
- Key safety functions are not dependent upon a single element of design, construction, maintenance or operation
- Appropriate barrier capability is provided
- Regulated activities are carried out at locations that facilitate the protection of public health and safety.

Moreover, the majority of the history of use of defense-in-depth is found in the regulations pertaining to the non-reactor areas more in an implicit rather than an explicit manner.

The historical review of defense-in-depth as it pertains to non-reactor areas addresses the following:

- All non-reactor nuclear areas.
- By product materials.
- Uranium recovery.
- Disposal of high and low-level waste.
- Domestic licensing of special nuclear material.
- Transportation.
- Storage of spent nuclear fuel.

5.1 All Non-Reactor Nuclear Areas

In reviewing the literature, there are discussions that apply to all non-reactor areas (e.g., by product materials, uranium recovery, waste, storage, transportation). These global statements are from the following sources and summarized below.

- Advisory Committee on Reactor Safeguards (ACRS) letter 2000 [ACRS, 2000b].
- Joint Advisory Committee on Nuclear Waste (ACNW)/ACRS Subcommittee, January 2000 [ACRS, 2000a].
- Risk Informed Decisionmaking for Nuclear Material and Waste Applications [NRC, 2008b].

5.1.1 ACRS Letter

The views of the Advisory Committee on Reactor Safeguards (referred to as the Committee) 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:

> "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 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."
>
> "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."

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 *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*. ...

There are ways to improve the implementation of the defense-in-depth philosophy ... 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."

The Committee goes on to state:

"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 [probabilistic risk assessment] 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 [high level waste] 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. 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.

3. 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."

5.1.2 Joint ACNW/ACRS Subcommittee

A joint subcommittee was held on January 13 and 14, 2000 with the focus on defense-in-depth. Dr. Eisenberg provided a presentation entitled "Defense-in-Depth for Risk-Informed Performance-Based Regulation: A Provisional NMSS Perspective." The following is a summary of his presentation.

Dr. Eisenberg notes that the 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 regulates systems with less hazard than nuclear power reactors.

He proposed both a structuralist and rationalist approach to defense-in-depth. Regarding the structuralist approach, 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 types 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 characteristics 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. Moreover, 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?

At the joint subcommittee meeting Dr. Robert Benero offered the following regarding non-reactor defense-in-depth:

> "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."

5.1.3 Risk-Informed Decisionmaking for Nuclear Material and Waste Applications Technical Report

The purpose of the Technical Report: Risk Informed Decisionmaking for Nuclear Material and Waste Applications, Rev. 1, February 2008, is to provide a risk-informed framework for regulatory decision making to the staff of the Office of Nuclear Material Safety and Safeguards and the Office of Federal and State Materials and Environmental Management Programs of the U.S. Nuclear Regulatory Commission. There are five places in this document where defense-in-depth is discussed:

- Section 4.1.3
- Section 4.2.3.1
- Appendix I
- Appendix N
- Appendix O

5.1.3.1 Section 4.1.3 – Attributes Considered in RIDM

In this section, the document focuses on defense-in-depth and safety margin as attributes of risk-informed decision making (RIDM). The document indicates that the impact on defense-in-

depth should be taken into account when analyzing a change or modification to an existing facility or activity. The document states:

> "Staff should consider the effect of the proposed change on the defense-in-depth philosophy. Defense-in-depth guards against over-reliance on any one safety feature. For example, defense-in-depth may be provided by additional barriers, operating procedures, and limits, or by redundant and diverse equipment design. Staff must evaluate any changes that result in the elimination of a layer of protection and fully understand the consequences."

> "Defense-in-depth is an element of NRC's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs. Diverse and redundant barriers and safety systems serve to reduce the failure probability and increase the chance of success. The ACNW&M and the ACRS have jointly recommended to the Commission that risk-acceptance criteria be developed for all NMSS/FSME-regulated activities, to achieve defense-in-depth by balancing compensatory measures. Defense-in-depth can be achieved by a variety of different measures such as passive containment systems (e.g., multiple barriers), active systems (e.g., ventilation systems), and administrative procedures. Redundancy and diversity can be used to manage uncertainties associated with system reliability. Hence, a minimal level of defense-in-depth may be necessary, despite very low quantitative risk estimates."

> "A safety margin is a measure of the conservatism that is employed in a design or process to assure a high degree of confidence that it will perform a needed function. It can be defined as the probability or level of confidence that a design or process will perform an intended function. Sufficient safety margins should be maintained under any proposed regulatory change that relies on a risk-informed decision framework. This is typically done by demonstrating that sufficient conservatism is preserved in the design parameters, such that reliability and effectiveness are reasonably ensured against the most demanding challenge. An alternative approach often used is to demonstrate adherence to the acceptable Codes and Standards. Similar considerations are applicable to NMSS/FSME facilities."

> "Defense-in-depth and safety margins are both concepts that are used to address the impact of uncertainty on safe design and performance. Effective use of defense-in-depth and safety margins increases the likelihood of success in response to challenges."

5.1.3.2 Section 4.2.3.1 Defense-in-Depth and Safety Margins

In this section, the document provides guidance on defense-in-depth and safety margin for various activities that are characterized by different levels of risk and consequence, ranging from low risk/consequence to high risk/consequence. The document states:

> "In the decision algorithms, risk information needs to be used in a fashion consistent with the Commission's overall defense-in-depth philosophy. This philosophy helps ensure that key safety functions do not depend on a single element of design or operation and that uncertainties are taken into account. The extent of defense-in-depth can vary depending on the nature of the risk and/or uncertainty. The application of the defense-in-depth philosophy is, in fact, aided by the use of a risk-informed decision process, in that the risk-informed process provided generally employs quantitative guidelines that can be used in deciding on the need for, extent, nature, and effectiveness of defense-in-depth measures. In general, the relation between defense-in-depth and a risk-informed process can be summarized as follows:
>
> - For low-risk/consequence activities, where uncertainties are also low, defense-in-depth measures can be reduced.
>
> - For medium-risk/consequence activities, defense-in-depth measures should be considered to ensure that the levels of safety can be met with a specified level of confidence. The defense-in-depth measures considered should include:
>
>   - Ensuring key safety functions do not depend on a single element of design or operation;
>
>   - Using redundancy, diversity, and independence to improve reliability and/or avoid common mode failure, when necessary, to ensure safety is maintained;
>
>   - Providing safety margins to address uncertainties in modeling or equipment performance;
>
>   - Conducting regulated activities at locations that facilitate protection of public and worker safety; and
>
>   - Providing time for recovery operations.
>
>   - For high-risk/consequence activities, defense-in-depth measures similar to the above should be considered, as well as: Ensuring the design and operation have both accident prevention and mitigation measures; and

- Ensuring the design includes at least two independent barriers to the uncontrolled release of radioactive material."

"Accordingly, in making risk-informed decisions, one needs to consider whether defense-in-depth measures are needed (or could be relaxed). If the defense-in-depth measures are needed, consider the degree to which they are needed, based on the application of this process. In all cases, staff should monitor regulated activities to ensure that key assumptions used in the risk analysis remain valid and adjustments are made to reflect operating experience where necessary. In general, low-risk/consequences mean doses are in the range of 10 CFR Part 20 limits. High-risk/consequences mean doses can be large enough to cause one or more early fatalities; medium-risk/consequences correspond to the range between low and high. Please note that risk information can only provide defense-in-depth insights on the known uncertainties. However, risk information cannot provide defense-in-depth insights on the unknowns."

5.1.3.3 Appendix I: Application of Defense-In-Depth in a Risk-Informed Decisionmaking Approach

This section of the document re-states the definition of defense-in-depth and its application to NMSS/FSME activities. The document states:

"As discussed in the agency's Strategic Plan, defense-in-depth is an element of NRC's safety philosophy that employs successive compensatory measures to prevent accidents or lessen their effects. Defense-in-depth ensures that key safety functions are not dependent upon a single element of design, construction, maintenance, or operation. For example, defense-in-depth can provide for multiple lines of defense, where necessary, to address uncertainties. Preliminary high-level guidance on the application of this philosophy to NMSS/FSME-regulated activities has been included in the draft guidelines and will be tested and further refined in the application period."

5.1.3.4 Appendix N: Assessing the Impact of the Issue on Defense-in-Depth

This part of the document provides guidance to the analyst in assessing the impact of a new issue or condition, e.g. a modification to an existing facility, new knowledge about potential challenges to facility operation, etc. on maintaining adequate defense-in-depth and safety margin. The document states:

"It is generally assumed that if the current regulations are met, there is adequate defense-in-depth at least before the condition/issue arose. However, the analysts should assess the effect of the condition/issue on defense-in-depth. The analyst should first consider which of the high-level aspects of defense-in-depth is affected by the issue (for example, barrier integrity,

emergency preparedness). The analyst should also assess the effectiveness of compensatory measures (for example, operator actions) to compensate for the degradation of defense-in-depth. It is important to note that for an event sequence whose outcome is a given level of consequences and a given level of uncertainty in the risk, there should be a minimum level associated with defense-in-depth or safety margins. Thus, a relaxation of a safety requirement that reduces below the minimum level for defense-in-depth or safety margins should be rejected."

In order to assess the impact of the issue/condition on defense-in-depth, the document provides a set of questions for the analyst to evaluate in various areas including barrier integrity, layers of defense, and the effectiveness of various options in maintaining defense-in-depth.

Questions provided in the report related to assess the impact on barrier integrity (i.e., degradation of the effectiveness of barriers) include:

"Does the issue significantly change the failure probability of any individual barrier?"

"Is the degradation mechanism understood and information (e.g., test or operational data) available regarding the degradation-time relationship for short-term and long-term solutions?"

"Can the impact of the degradation be quantified and evaluated through the risk model?"

"Is the independence of barriers degraded? If so, which barriers?"

"Does the issue introduce new or additional failure dependencies among barriers that significantly increase the likelihood of failure compared to the existing conditions?"

"Does the issue result in a significant increase in the existing challenges to the integrity of the barriers?"

The document indicates the analyst should assess the potential for impact of the issue on multiple layers of defense-in-depth, as follows:

"Are the remaining elements of defense-in-depth intact?"

"What are they and what is the reason for assuming they are intact?

The intent of this question is to ascertain that the independence of the different layers of defense-in-depth is not compromised." The document states that the analyst needs to consider the effectiveness of various options in maintaining defense-in-depth, as follows:

> "The analyst needs to consider how a given option changes the defense-in-depth assessment. The analyst should use the defense-in-depth guidance above when considering the various alternative actions:
>
> - Does the option propose actions that can compensate for the degradation of defense-in-depth?
>
> - Discuss the proposed actions. Explain how and to what degree the action(s) can be successful (what level of confidence can be associated with this compensatory measure).
>
> - Does the option identify a programmatic activity that is proposed as a compensatory measure for the identified issue? For example, reliance on operator actions as monitors of plant conditions.
>
> - Describe how the option addresses degradation in defense-in-depth.
>
> - Identify sources of uncertainty with respect to (1) the assessment of the impact of the degradation of defense-in-depth, and (2) either the compensatory measures or monitoring approach.
>
> - List assumptions made to address the uncertainties and how they support the option. Assess the confidence level in the option.
>
> - Document why the methods used in the analyses above are considered adequate to support the conclusions."

5.1.3.5 Appendix O: Assessing the Impact of the Issue and Alternative Actions on Safety Margins

This section of the report provides guidance on assessing the impact of the issue/condition on safety margins to ensure that a minimum level of defense-in-depth and safety margin is maintained. The analyst is asked to consider: (1) whether and to what extent safety margin could be lost or degraded due to the condition/issue and to document the significance of the loss, (2) to assess the impact of alternative actions on safety margin, and discuss compensatory measures that could address the issue of loss or degradation, and (3) to identify the sources of uncertainty with respect to the assessment of the impact of the degradation of safety margin.

5.2 Byproduct Materials

There are only three sources in the literature that were found that discuss defense-in-depth. These include:

- 10 CFR Parts 30 to 39 [CFR]
- NUREG-1556 [NRC, 2012f]
- NUREG-2150 [NRC, 2012a]

5.2.1 10 CFR Parts 30 to 39

Byproduct materials are regulated under 10 CFR Parts 30 to 39. A few specific rules involve measures considered to embody the concept of defense-in-depth, such as prevention and mitigation, redundancy and diversity, use of conservative codes and standards, and safety margin, summarized above. These regulations are identified below in Table 5-1, which shows the 10 CFR part number, its title and the requirement. The comment column discusses how that requirement is related to defense-in-depth.

Table 5-1 Places in 10 CFR Parts 30 to 39 Where Defense-in-Depth is Referenced

Number	Title	Requirement	Comment
30.32	Application for Specific Licenses	"The radioactive material is physically separated so that only a portion could be involved in an accident; All or part of the radioactive material is not subject to release during an accident because of the way it is stored or packaged; Means and equipment for mitigating the consequences of each type of accident, including those provided to protect workers onsite."	This regulation is considered to address defense-in-depth because physical separation and ways of storage or packaging to lower the amount released in an accident can be considered to involve the presence of multiple barriers to release, which is a defense-in-depth principle; provision of mitigation of consequences is a defense-in-depth principle.
32.22	Self-luminous products containing tritium, Kr-85 or Pr-147: Requirements for license to manufacture, process, produce, or initially transfer	"A determination that the probabilities with respect to the doses referred to in § 32.23(d) meet the criteria of that paragraph."	The rules in Parts 32.22 through 32.31 indicate that the risk from device failure should be acceptably low, which is an important defense-in-depth principle.
32.23	Same: Safety criteria	"In use and disposal …the probability is low …that a person would receive an external radiation dose or dose commitment in excess of the dose to the appropriate organ as specified in	

Number	Title	Requirement	Comment
32.23 (cont.)		Column III of the table in § 32.24, and the probability is negligible that a person would receive an external radiation dose or dose commitment in excess of the dose to the appropriate organ as specified in Column IV of the table in § 32.24. Low—not more than one such failure per year for each 10,000 …units distributed Negligible—not more than one such failure per year for each 1 million …units distributed."	The rules in Parts 32.22 through 32.31 indicate that the risk from device failure should be acceptably low, which is an important defense-in-depth principle.
32.26	Gas and aerosol detectors containing byproduct material		
32.27	Same: Safety criteria	In use and disposal …the probability is low …that a person would receive an external radiation dose or dose commitment in excess of the dose to the appropriate organ as specified in Column II of the table in § 32.28, and the probability is negligible that a person would receive an external radiation dose or dose commitment in excess of the dose to the appropriate organ as specified in Column III of the table in § 32.28. [Low and negligible definitions of probability same as above]	
32.31	Certain industrial devices containing byproduct material: Safety criteria	In use, handling, storage, and disposal…the probability is low that the containment, shielding, or other safety features of the device would fail under such circumstances that a person would receive an external radiation dose or committed dose in excess of 5 mSv (500 mrem), and the probability is negligible that a person would receive an external radiation dose or committed dose of 100 mSv (10 rem) or greater.	

Number	Title	Requirement	Comment
32.31 (cont.)		[Low and negligible definitions of probability same as above]	
34.20	Performance requirements for industrial radiography equipment	"The guide tube exposure head connection must be able to withstand the tensile test for control units specified in ANSI N432-1980." "Source changers must provide a system for ensuring that the source will not be accidentally withdrawn from the chamber when connecting or disconnecting the drive cable to or from a source assembly."	This regulation addresses the use of conservative codes and standards (i.e., ANSI N432-1980) in the design to ensure an adequate safety margin which is a defense-in-depth principle. This requirement is related to the design of the equipment to provide additional accident prevention capability which is a defense-in-depth principle.
36.21	Performance criteria for sealed sources	"Must be doubly encapsulated."	Involves redundancy which is a defense-in-depth principle.
39.41	Design and performance criteria for sources	"The sealed source is doubly encapsulated."	Involves redundancy which is a defense-in-depth principle.

5.2.2 NUREG-1556 V6 - Standard Review Plan for Irradiators

This document outlines a defense-in-depth feature in the design and operation of panoramic irradiators, as follows:

> "An independent backup access control system is required to provide a redundant means of preventing a person from being accidentally exposed to the source. In addition, instruction must be provided to at least one other individual who will be on site during operations on how to respond to the independent backup access control alarm and to promptly render or summon assistance."

The independent backup access control embodies the principles of redundancy and diversity and is hence a defense-in-depth feature.

5.2.3 NUREG-2150 – By product Materials

This document provides a review of the defense-in-depth features of the NRC's regulations for byproduct materials, as follows:

> "The terminology of defense-in-depth is not used consistently across the NRC's materials regulatory programs. The concept of defense-in-depth, which is a central part of reactor regulation, is more of an implicit rather than explicit part of the materials program. Due to the wide variety of licensed materials uses, there is not a common understanding of the terms risk-informed, performance-

based, and defense-in-depth within NRC or with these licensees. The NRC should apply common risk approaches to safety and security based on the proposed risk management and defense-in-depth regulatory framework. The proposed risk management regulatory framework described in Chapters 2 and 3 is very broad and represents an evolutionary, not revolutionary, approach to the agency's mission of protecting public health, safety, and the environment. While the framework is predicated on a defense-in-depth philosophy, that term is not commonly used within the materials program."

"However, the defense-in-depth concepts of hazards and barriers described above are implicit in the materials program. Considering the three primary components of materials licensing—specific licenses, general licenses, and exemptions—NRC and Agreement State regulations, licenses, and guidance provide for barriers to the hazard presented by radioactive material commensurate with the risk presented by the type and form of that material."

"For example, licensing requirements for panoramic irradiators in 10 CFR Part 36, 'Licenses and Radiation Safety Requirements for Irradiators,' are arguably the most detailed requirements in the materials programs. The rule includes a system of defense-in-depth considerations that include physical barriers, engineered safeguards, access controls, and administrative and procedural controls designed to protect workers and members of the public from potentially significant exposure."

"The licensing requirements for less hazardous uses, types, and amounts of radioactive materials can be and are correspondingly less prescriptive and reflect a less robust consideration of defense-in-depth. For example, portable and fixed gauges use small radioactive sources that are double encapsulated and contained within a relatively robust housing. The gauges can be used by individuals with a modicum of training that can be taken online."

"Within 10 CFR Part 35 there are also defense-in-depth considerations to greater or lesser degrees based on the hazard or risk posed by the material or modality. For example, the requirements for therapeutic applications of byproduct material, particularly those involving high activity sources, such as high-dose rate after-loaders or gamma stereotactic radiosurgery units, are more robust than those for diagnostic nuclear medicine and may include multiple physical barriers and administrative controls to protect workers, patients, and members of the public."

"Defense-in-depth considerations are built into the design and manufacture of generally licensed devices so that an individual can possess and use such a device with no formal training or experience and only minimal requirements for accountability."

> "So while there are numerous implicit applications of defense-in-depth consideration in the materials program, what is missing is explicit consideration of that philosophy as part of program development, implementation, and oversight. As part of the implementation of the proposed risk management regulatory framework, the RMTF recommends that the materials program should more explicitly consider the defense-in-depth philosophy in rulemaking, guidance, and program implementation, and modify appropriate parts of staff training to make these concepts a central part of such training."

5.3 Uranium Recovery, NUREG-2150

This document [NRC, 2012a] provides a brief summary of defense-in-depth in the NRC regulations governing uranium recovery, as follows:

> "The concept of defense-in-depth is not commonly used as an explicit consideration in the NRC's regulation of uranium recovery. In large measure, this reflects the fact that uranium recovery is a relatively low-risk activity. There are instances, including design features and regulatory review of mill tailings impoundments, as well as the arrangement of injection, recovery and monitoring wells at ISR (in-situ recovery) facilities that reflect defense-in-depth considerations."

5.4 Disposal of High and Low-Level Wastes

There are only five sources in the literature that were found that discuss defense-in-depth with regard to disposal of high and low-level waste. These include:

- 10 CFR Parts 60 and 63 [CFR]
- SECY-97-300 [NRC, 1997c]
- SECY-99-186 [NRC, 1999b]
- *Federal Register* Notice 66 [FRN, 2000]
- NUREG-2150 [NRC, 2012a]

5.4.1 10 CFR Parts 60 and 63

High level wastes are regulated under 10 CFR Part 60 and 10 CFR Part 63, while low-level wastes are regulated under 10 CFR Part 61. The specific regulations that embody the principles of defense-in-depth are shown below in Table 5-2.

Table 5-2 Places in 10 CFR Parts 60, 61, and 63 Where Defense-in-Depth is Referenced

Number	Title	Requirement	Comment
60.21 Note 1	Content of application	"The effectiveness of engineered and natural barriers, including barriers that may not be themselves a part of the geologic repository operations area, against the release of radioactive material to the environment." "A description of the quality assurance program to be applied to the structures, systems, and components important to safety and to the engineered and natural barriers important to waste isolation."	The provision of barriers against release is a defense-in-depth principle. Assurance of high quality in design, construction, and operation is a defense-in-depth principle.
60.122	Siting Criteria	"A geologic setting shall exhibit an appropriate combination of the conditions specified in paragraph (b) of this section so that, together with the engineered barriers system, the favorable conditions present are sufficient to provide reasonable assurance that the performance objectives relating to isolation of the waste will be met."	The location of regulated activities at sites that facilitate the protection of public health and safety is a defense-in-depth principle.
60.131	General Design Criteria for the Geologic Repository Operations Area	*"Criticality control*. All systems for processing, transporting, handling, storage, retrieval, emplacement, and isolation of radioactive waste shall be designed to ensure that nuclear criticality is not possible unless at least two unlikely, independent, and concurrent or sequential changes have occurred in the conditions essential to nuclear criticality safety."	This regulation embodies redundancy and diversity, which is a defense-in-depth principle.
61.7	Concepts	"A buffer zone is a portion of the disposal site that is controlled by the licensee and that lies under the site and between the boundary of the disposal site and any disposal unit. It provides controlled space to establish monitoring locations which are intended to provide an early warning of radionuclide movement, and to take mitigative measures if needed."	Provision of mitigation capability is a defense-in-depth principle.
61.13	Technical Analyses	"Analyses of the protection of individuals from inadvertent intrusion must include demonstration that there is reasonable assurance the waste classification and segregation requirements will be met and that adequate barriers to inadvertent intrusion will be provided."	The provision of adequate barriers is a defense-in-depth principle.

Number	Title	Requirement	Comment
63.112	Requirements for preclosure safety analysis of the geologic repository operations area	"The preclosure safety analysis of the geologic repository operations area must include… Means to provide redundant systems necessary to maintain, with adequate capacity, the ability of utility services important to safety."	The provision of redundancy is a defense-in-depth principle.
63.113	Performance objectives for the geologic repository after permanent closure	"The geologic repository must include multiple barriers, consisting of both natural barriers and an engineered barrier system."	The provision of barriers is a defense-in-depth principle.
63.161	Emergency Plan for the Geologic Repository Area through permanent closure	"DOE [Department of Energy] shall develop and be prepared to implement a plan to cope with radiological accidents that may occur at the geologic repository operations area, at any time before permanent closure and decontamination or decontamination and dismantlement of surface facilities.	An emergency plan to cope with accidents is an element of mitigation capability, which is a defense-in-depth principle.

Notes:

1. 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."

5.4.2 SECY-97-300 A Proposed Repository at Yucca Mountain, Nevada

This SECY paper proposes a strategy for development of regulations governing disposal of high-level radioactive wastes at the proposed repository at Yucca Mountain, Nevada. The document provides a discussion of how defense-in-depth concepts were proposed to be applied in the development of regulations for the HLW repository at Yucca Mountain. The document states:

> "The Nuclear Regulatory Commission has applied the concept of defense-in-depth broadly throughout its regulations to ensure safety of its licensed facilities through requirements for multiple, independent barriers, and, where possible, redundant safety systems and barriers. 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 large uncertainties. 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. Because defense-in-depth is applied, generally speaking, without direct consideration of the relative likelihood of specific threats to barrier integrity, the approach is inherently conservative."

The document recognizes the unique features of defense-in-depth to this application that represents a first of a kind facility, which has no operating systems, only passive ones in the post-closure period. The document indicates:

"The development of NRC regulations for geologic disposal in 1983 represented a unique application of the defense-in-depth philosophy to a first-of-a-kind type of facility. While waste is being emplaced, and before a geologic repository is closed, its operation is readily amenable to regulation in much the same manner as any other NRC-licensed facility. Regulatory criteria for pre-closure operations contained in 10 CFR Part 60, in fact, reflect the defense-in-depth approach commonly used in other parts of NRC regulations, in that safety is ensured for the operating repository by the use of conservatism and diversity of design, application of comprehensive quality assurance and radiation safety programs and procedures, and the maintenance of appropriate emergency plans."

"Application of defense-in-depth principles for regulation of repository performance, for long time periods following closure, must account for the difference between a geologic repository and an operating facility with active safety systems and the potential for active control and intervention. A closed repository is essentially a passive system, and assessment of its safety over long timeframes is best evaluated through consideration of the relative likelihood of threats to its integrity and performance."

The document assesses the need to address how multiple barrier performance is related to defense-in-depth:

"The Nuclear Waste Policy Act of 1982 (NWPA), (hereafter the Act), as amended, directed the Commission to develop technical requirements and criteria for high-level waste (HLW) repositories that provide for a system of multiple barriers and which are not inconsistent with generally applicable U.S. Environmental Protection Agency (EPA) standards for HLW disposal. The Act also mandated that the technical criteria developed by the Commission "...shall provide for the use of a system of multiple barriers in the design of the repository." Although the law demands that NRC require a system of multiple barriers, the Issue of how the performance of those barriers should be

assessed, consistent with the Commission's policy of defense-in-depth, has been a major issue throughout the development, promulgation, and implementation of the Part 60 regulations."

5.4.3 SECY-99-186 Staff Plan for Clarifying Defense-In-Depth at Yucca Mountain

The objective of this document was to inform the Commission of the staff's plan to address defense-in-depth in the 10 CFR Part 63 regulations governing HLW disposal at Yucca Mountain. The document indicates:

> "The Staff Requirements Memorandum, issued on April 12, 1999, directed the staff to evaluate how the NRC could more clearly address repository defense-in-depth to foster a common understanding of this concept, and to inform the Commission of its findings. This paper responds to that direction and provides the staff's plan to clarify its expectations for a demonstration of defense-in-depth for a geologic repository… In completing Part 63 and the YMRP, the staff will incorporate the Commission's defense-in-depth philosophy as elaborated in the White Paper on Risk-Informed and Performance-Based Regulation, issued on March 1, 1999, and has identified specific activities to involve stakeholders.

A comprehensive review of the Commission's consideration of multiple barriers and "defense-in-depth" for Part 63 was provided as Attachment 3 to SECY-97-300, "Proposed Strategy for Development of Regulations Governing Disposal of High-Level Radioactive Wastes in a Proposed Repository at Yucca Mountain, Nevada." It is expected that defense-in-depth for pre-closure operations would be achieved in a manner similar to that for other operating nuclear facilities.

The document describes the differences relating to multiple barrier performance between 10 CFR Part 60, which prescribes numerical performance objectives, and (the then-proposed) Part 63, which proposed revisions to these objectives, in maintaining defense-in-depth post-closure. The document specifies:

> "To maintain the Commission's defense-in-depth philosophy, but avoid incorporation of numerical subsystem performance objectives in its site-specific regulation, the staff recommended (SECY-97-300), and the Commission accepted a proposed regulatory approach that includes assessment of repository barrier performance, without specifying numerical goals for subsystem performance…"
>
> "Such an approach will require the U.S. Department of Energy (DOE) to provide greater transparency of how multiple barriers contribute to overall performance, and associated uncertainty. The approach does not require compliance with separate performance objectives for individual barriers that are unrelated to the U.S. Environmental Protection Agency standards… As proposed at Part 63.114, DOE must:

1) Identify the design features of the engineered barrier system…

2) Describe the capability of barriers, identified as important to waste isolation, to isolate wastes, taking into account uncertainties in characterizing and modeling the barriers… and

3) Provide the technical basis for the description of the capability of barriers, identified as important to waste isolation, to isolate waste…"

"The staff believes that these requirements for multiple barriers, when combined with requirements for active and passive institutional control, are sufficient to provide for defense-in-depth for post-closure repository performance."

An attachment to the document repeats the Commission's definition of defense-in-depth in its "White Paper on Risk-Informed and Performance-Based Regulation," (issued on March 11, 1999):

"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."

The attachment then briefly clarifies how the multiple barrier system, consisting of both natural and engineered barriers, will "work in combination to enhance overall performance of the repository" and maintain defense-in-depth."

5.4.4 *Federal Register* Notice 66

This document, in the Section "Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, NV" explains features related to defense-in-depth that are contained in the final rule 10 CFR 63 concerning the HLW repository at Yucca Mountain, NV and responds to comments made by various stakeholders on the draft rule. Specifically, the document outlines the relationship between multiple barriers and defense-in-depth as follows:

Multiple Barriers and Defense-in-Depth

"The Commission believes that it presented a sound basis for the proposed approach to multiple barriers and defense-in-depth in the Supplementary

> Information accompanying the proposed part 63. In general, the Commission believes that a repository system should reflect the philosophy of defense-in-depth. The Commission expects that if a repository system is made up of multiple barriers, then it will be more tolerant of unanticipated failures and external challenges. The final regulations specify criteria for quantitatively evaluating postclosure performance (*e.g.,* individual protection, ground-water protection, and evaluation of human intrusion). These criteria help ensure defense-in-depth by requiring calculations that provide risk insights into the impact on performance of specific system attributes and external conditions. DOE must evaluate the performance of the repository system, as it performs as a result of compliance with general design criteria (*e.g.,* required use of multiple barriers and identification of the repository by markers). DOE must also evaluate the system's response to various external challenges (*e.g.,* disruptive events treated in the performance assessment, as well as a specified human intrusion scenario)… Although not necessarily required as a separate demonstration, this required information on the capability of barriers, integral to the performance assessment, illustrates the resilience or lack of resilience of the repository to unanticipated failures or external challenges. Also, quantitative insights about the defense-in-depth of the proposed repository emerge directly from the quantitative evaluations in the performance assessment… Thus, a complete performance assessment (i.e., one that complies with §63.114) will illustrate the effectiveness of the multiple barriers, and the implementation of the philosophy of defense-in-depth, such that the individual protection standard is shown to be met even when barriers are challenged."

The document goes on to outline how the natural (i.e. geologic) barrier provides defense-in-depth, as follows:

> "…The Commission is confident that evidence for the resilience, or lack of resilience, of a multiple-barrier system will be found by examining a comprehensive and properly documented performance assessment of the behavior of the overall repository system… This capability of geologic systems to ''retard'' or slow the improvement of contaminants exists whether or not the waste package is breached. Thus a geologic barrier can provide defense-in-depth irrespective of releases from the waste package."

5.4.5 NUREG-2150, Disposal of Low and High-Level Waste

This document summarizes the features of defense-in-depth in the NRC regulations governing low-level waste (LLW) and high-level waste, as follows.

Low-Level Waste

"There is not a common understanding and usage of the terms risk-informed, performance-based, and defense-in-depth within the NRC, as well as outside the NRC."

"The concept of defense-in-depth is implicit in the requirements and structure of 10 CFR Part 61, although the term itself is not explicitly used. The rule provides for a series of barriers or controls to assure that the performance objectives are met and that the public and the environment are adequately protected. For example, 10 CFR Part 61 requires that an applicant for a LLW disposal facility license to design disposal unit covers to minimize water intrusion into the disposal units. If water intrudes into the disposal units, other requirements in the rule on waste form, packaging, and placement serve as additional barriers or controls to minimize water coming into contact with the waste and serving as a transport mechanism for radionuclides. If somehow those radionuclides leach out of the waste, the rule requires additional barriers or controls in the form of a buffer zone between the disposal units and the disposal site boundary, which must be of sufficient size to allow mitigation measures to be taken."

"The interlocking and reinforcing systems approach in 10 CFR Part 61 (site suitability, waste form and classification, intruder barrier, institutional controls, etc.) represents an implicit consideration of defense-in-depth features, based on the risk posed by various classes of waste."

"The NRC should develop an explicit characterization of how defense-in-depth within the proposed risk management framework applies to the LLW program and build this into current and future staff guidance documents and into training and development activities for the staff."

High-Level Waste

"Perhaps the most significant change to the NRC regulations was the approach to defense-in-depth during the post-closure period of a geologic repository (i.e., implementation of the multiple barrier requirements). A longstanding principle of geologic disposal has been a reliance on multiple barriers to limit the release and transport of radionuclides. Engineered barriers (such as waste packages and waste forms) should complement and work with the geological or natural barriers so that safety does not depend solely on a single barrier or phenomenon."

"The NRC's regulatory philosophy of defense-in-depth is reflected in the multiple-barrier requirement for post-closure in 10 CFR Part 63. Compliance with the multiple barrier requirements is demonstrated through the performance assessment."

5.5 Domestic Licensing Of Special Nuclear Material

There are only three sources in the literature that were found that discuss defense-in-depth with regard to domestic licensing of special nuclear materials. These include:

- 10 CFR Part 70 [CFR]
- NUREG-1520 [NRC, 2015]
- NUREG-2150 [NRC, 2012a]

5.5.1 10 CFR Part 70

Facilities using special nuclear material, such as fuel cycle facilities, are regulated under 10 CFR 70. This regulation is unique among all non-reactor regulations in that defense-in-depth is explicitly specified in the regulation itself. The specific regulations that mention defense-in-depth or embody defense-in-depth principles are shown in Table 5-3.

Table 5-3 Places in 10 CFR Part 70 Where Defense-in-Depth is Referenced

Number	Title	Requirement	Comment
70.64	Requirements for new facilities or new processes at existing facilities	See below	See below
70.64(a)(9)	Criticality Control.	The design must provide for criticality control including adherence to the double contingency principle	The double contingency principle incorporates redundancy and diversity which is a defense-in-depth principle.
70.64(b)	No title	Facility and system design and facility layout must be based on defense-in-depth practices.[1] [1] As used in § 70.64, Requirements for new facilities or new processes at existing facilities, defense-in-depth practices means a design philosophy, applied from 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 failures and external challenges. The risk insights 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.	Defines defense-in-depth for fuel cycle facilities.

5.5.2 NUREG-1520: Standard Review Plan for Fuel Cycle Facilities

This document indicates that licensing decisions made by the NRC under various regulations of Part 70 for fuel cycle facilities include "compliance with the performance requirements, the baseline design criteria (BDC), defense-in-depth, and the adequacy of management measures." The document specifically identifies the need to consider defense-in-depth as follows:

> "The regulation in 10 CFR 70.64 states that the design process must be founded on defense-in-depth principles and must incorporate, to the extent practicable, preference for engineered controls over administrative controls and reduction of challenges to items relied on for safety (IROFS). Because of this regulation, new facilities with system safety designs lacking defense-in-depth practices, consisting of purely administrative controls, or relying on IROFS that are frequently or continuously challenged, are not acceptable, unless the application provides a justification showing that alternatives to achieve the design criteria are not feasible."
>
> "Other reliability qualities relate to characteristics of the IROFS or system of IROFS that protect against the following accident sequences as a whole, among others:
>
> - defense-in-depth
> - degree of redundancy
> - degree of independence
> - diversity
> - vulnerability to common-cause failure"

The document presents a description of defense-in-depth for fuel cycle facilities that incorporate features of safety systems specific to these facilities:

> **"**Defense-in-Depth: Defense-in-depth is the degree to which multiple IROFS or systems of IROFS must fail before the undesired consequences (e.g., criticality, chemical release) can result. IROFS that provide for defense-in-depth may be either independent or dependent, although IROFS should be independent whenever practical because of the possibility that the reliability of any single IROFS may not be as great as anticipated. This will make the results of the risk evaluation more tolerant of error. In addition, IROFS must be independent if the method for likelihood determination assumes independence (such as methods relying on summation of indices). IROFS are independent if there is no credible single event (common-mode failure) that can cause the safety function of each IROFS to fail. Multiple independent IROFS generally provide the highest level of risk reduction. The degrees of redundancy, independence, and diversity are important factors in determining the amount of risk reduction afforded by the system of IROFS."

> "Degree of Redundancy: Defense-in-depth is provided by specifying redundant IROFS that perform the same essential safety function. Redundant IROFS may be either diverse or nondiverse; it is not necessary for them to consist of identical equipment or operator actions. However, when identical equipment or operator actions provide redundancy, it is important to ensure that all credible common-mode failures have been identified."
>
> "Diversity: Diversity is the degree to which IROFS that perform different safety functions provide defense-in-depth. This means that different types of failures must occur before an accident is possible. Diverse controls may consist of controls on different parameters or different means of controlling the same parameter. In choosing redundant controls, preference should be given to diverse means of control, because they are generally less susceptible to common-mode failure than are nondiverse means. However, it is still necessary to consider all credible failure modes of the system when evaluating the overall likelihood of failure."
>
> "New processes at existing facilities also must meet the requirements of 10 CFR 70.64(b), which requires defense-in-depth and a preference for engineered controls over administrative controls."

The document identifies the elements of the review that focus on defense-in-depth and outlines the steps that should be taken in reviewing the applicant's integrated safety assessment (ISA):

> "The applicant describes how it performed the ISA for the new process and how the ISA satisfies the principles of the BDC and the performance requirements in 10 CFR 70.61. Defense-in-depth practices should be applied early through the completion of design by providing successive levels of protection such that health and safety will not wholly depend on any single element of the design, construction, maintenance, or operation of the facility. The applicant also explains how it applies defense-in-depth to higher risk accident sequences. Acceptable defense-in-depth principles for the criticality safety design are those that support a hierarchy of controls: prevention, mitigation, and operator intervention, in order of preference…"
>
> "…10 CFR 70.64(a)(9) requires that the design "provide for criticality control including adherence to the double contingency principle." Section 70.64(b) further specifies that new facilities or processes must incorporate defense-in-depth practices, which is defined as a "design philosophy, applied from 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."

"Acceptable defense-in-depth principles for the chemical process safety design are those that support a hierarchy of controls: prevention, mitigation, and operator intervention, in order of preference."

5.5.3 NUREG-2150, Domestic Licensing of Special Nuclear Materials

This document summarizes the features of defense-in-depth in fuel cycle facilities:

"The requirement for and definition of defense-in-depth in safety of fuel cycle facility processes is explicit in 10 CFR 70.64(b). That definition is identical to the one contained in SECY-98-144, "White Paper on Risk-Informed and Performance-Based Regulation," which defined "risk-informed," "defense-in-depth," and related concepts (NRC, 1998). In addition, the double contingency principle has been an industry standard in the nuclear criticality safety field for decades and is also mandated by 10 CFR 70.64(a)(9). Thus, defense-in-depth is applied in regulation of fuel cycle facilities consistent with Commission guidance. However, unlike power reactors, where more permanent barriers and controls, such as a containment, are built into the design and operation, defense-in-depth for each fuel cycle unit process is different. As new processes are added or existing ones are changed, the design and maintenance of defense-in-depth at these facilities are based on the characteristics of the most current operations. Therefore, defense-in-depth is a continuing process at fuel cycle facilities, not one permanently established by the initial design."

5.6 Transportation

The transportation of radioactive material is regulated under 10 CFR Part 71 [CFR]. Additional defense-in-depth discussion related to transportation is found in NUREG-2150.

The regulations that involve defense-in-depth are shown in Table 5-4.

Table 5-4 Places in 10 CFR Part 71 Where Defense-in-Depth is Referenced

Number	Title	Requirement	Comment
71.43	General Standards for All Packages	Each package must include a containment system securely closed by a positive fastening device that cannot be opened unintentionally or by a pressure that may arise within the package.	The containment system can be considered as a barrier against release, which is a defense-in-depth principle.
71.55	General requirements for fissile material packages	A package used for the shipment of fissile material must be so designed and constructed and its contents so limited that it would be subcritical if water were to leak into the containment system, or liquid contents were to leak out of the containment system so that,	To ensure subcriticality, under maximum credible accident conditions, the design is required to incorporate redundancy and diversity, which is a defense-in-depth principle.

Number	Title	Requirement	Comment
71.55 (cont.)		under [specified] conditions, maximum reactivity of the fissile material would be attained. The Commission may approve exceptions…if the package incorporates special design features that ensure that ***no single*** packaging error would permit leakage…	

NUREG-2150 [NRC, 2012a] points out that defense-in-depth is only used implicitly in the regulatory approach to transportation safety:

> "While the term "defense-in-depth" is not explicitly used, the current regulatory approach for approving and inspecting radioactive shipping packages follows the risk-informed and performance-based defense-in-depth approach in a general sense. For example, the safety requirements for different types of shipping packages become more stringent with the quantity (radioactivity), or hazard, contained. The threshold for an accident resistant package is based on an A1 (special form or encapsulated material) or A2 (normal form) quantity. In turn, the A1 and A2 quantities are based on accident models that keep the anticipated dose to first responders below the occupational exposure limit of 5rem. If a package contains greater than an A1 or A2 quantity (i.e., has a potential to cause an exposure greater than 5 rem), it is required to meet Type B accident conditions. The current system also allows shipments of quantities that would normally require Type B packages to be made in less robust packages that take credit for the low, specific activity of the material being shipped."

5.7 Storage of Spent Nuclear Fuel

There are only four sources in the literature that were found that discuss defense-in-depth with regard to storage of spent nuclear fuel. These include:

- 10 CFR Part 72 [CFR]
- NUREG-1536 [NRC, 2010b]
- NUREG-1567 [NRC, 2000c]
- NUREG-2150 [NRC, 2012a]

5.7.1 Regulations in 10 CFR 72

The regulations included in 10 CFR 72 involving defense-in-depth are shown in Table 5-5.

Table 5-5 Places in 10 CFR Part 72 Where Defense-in-Depth is Referenced

Number	Title	Requirement	Comment
72.124	Criteria for nuclear criticality safety.	*Design for criticality safety*. Spent fuel handling, packaging, transfer, and storage systems must be designed to be maintained subcritical and to ensure	To ensure criticality safety, the design is required to involve

Number	Title	Requirement	Comment
72.124 (cont.)		that, before a nuclear criticality accident is possible, at least two unlikely, independent, and concurrent or sequential changes have occurred in the conditions essential to nuclear criticality safety.	redundancy and diversity, which is a defense-in-depth principle.
72.236	Specific requirements for spent fuel storage cask approval and fabrication	The spent fuel storage cask must be designed to provide redundant sealing of confinement systems.	This requirement involves redundancy, which is a defense-in-depth principle.

5.7.2 NUREG-1536, Standard Review Plan for Dry Cask Storage Systems

This document outlines the concept of defense-in-depth and identifies elements of defense-in-depth for dry cask storage systems:

> "Defense-in-depth has long been a key element of the NRC's safety philosophy. It is intended to ensure that the accomplishment of key safety functions is not dependent upon a single element of design, construction, maintenance or operation. In effect, defense-in-depth is used to provide one or more additional measures to back up the front line safety measures, to provide additional assurance that key safety functions will be accomplished. Traditional defense-in-depth measures for reactors have included items such as confinement, containment, redundant and diverse means of decay heat removal and emergency evacuation plans. For dry cask storage systems (DSS), examples of measures associated with defense-in-depth are as follows:
>
> - Confinement System (2nd barrier to fuel clad integrity);
> - Operating Controls and Monitoring
> - Non-mechanistic and bounding event analyses (to mitigate site-specific uncertainties)."
>
> "Defense-in-depth measures are generally decided upon using deterministic considerations (i.e., engineering judgment) regarding the importance of the safety function and the potential uncertainties that could affect its performance."

The document outlines and prioritizes review procedures, in particular those that focus on defense-in-depth, as follows:

> "With respect to prioritizing the review procedures in this SRP [Standard Review Plan], a review procedure can be considered associated with defense-in-depth if it is related to providing a backup to the front line of defense (e.g.,

confinement is generally considered a defense-in-depth measure since it provides a backup to cladding integrity). Defense-in-depth measures are not intended to detract from the importance of front line safety measures. Defense-in-depth measures are intended to provide additional assurance so the safety function can be accomplished. It is not the intent of defense-in-depth to reduce the importance of the front line safety measures since, if their importance were reduced, the importance of the NRC staff review associated with those measures could also be reduced, which could affect the reliability or performance of the front line safety measures. This could leave the defense-in-depth measures as the primary means of performing the safety functions, instead of being the backup."

The document provides guidance on what measures could be considered defense-in-depth:

"In the dry cask SRP prioritization, each paragraph (or group of paragraphs) to be prioritized, would be examined individually from a defense-in-depth perspective to determine if that paragraph (or group of paragraphs) is related to defense-in-depth. If so, and if the paragraph is not met, a determination would then be made as to whether or not a defense-in-depth measure could be compromised and the risk significance. To determine if a defense-in-depth measure could be compromised, it is first necessary to decide what are defense-in-depth measures? To help make this decision, the following guidance was used."

"A defense-in-depth measure is any design feature or action that is required by the SRP as a backup measure to the front line safety measures. This ensures that, if the front line safety measure is lost, the backup measure is present to perform that safety function."

"SRP review procedures that relate to items that can be considered defense-in-depth should receive a defense-in-depth ranking."

"It should be noted that defense-in-depth measures are not intended to detract from the importance of front line safety measures. Defense-in-depth measures are intended to provide additional assurance so the safety function can be accomplished."

5.7.3 NUREG-1567, Standard Review Plan for Spent Fuel Dry Storage Facilities

This document indicates that in reviewing the fire protection plan for spent fuel dry storage facilities, the reviewer should focus on defense-in-depth:

"The reviewer should verify that a FPP provides assurance that a fire will not significantly increase the risk of radioactive releases to the environment in accordance with the general design criteria of 72.122(c). A defense-in-depth

approach should achieve balance among prevention, detection, containment, and suppression of fires."

5.7.4 NUREG-2150, Storage of Spent Nuclear Fuel

This document indicates that defense-in-depth is mostly used in an implicit manner in the spent fuel storage regulatory program, with one notable exception, and urges the NRC to make its use more explicit. The document states:

> "As noted in earlier portions of this report, defense-in-depth is an important part of the NRC's regulatory program. The concept of defense-in-depth is not explicitly or consistently applied in the spent nuclear fuel (SNF) storage regulatory program. The concept is most notably incorporated in 10 CFR 72.124(a), the double contingency principle to prevent nuclear criticalities. In addition to the current licensing approach, defense-in-depth may also be inherent in the designs and operations of the various dry storage systems. However, these aspects are not explicitly identified or recognized as defense-in-depth considerations. Therefore, while there are implicit applications of defense-in-depth consideration in the SNF storage regulatory program, more explicit consideration and application of that philosophy is warranted."
>
> "While elements of the proposed risk management approach have been used in the SNF storage regulatory approach to evaluate the acceptable level of risk and the sufficiency of defense-in-depth (physical barriers, controls or margins) more consistently, the NRC should develop the necessary risk information, the corresponding decision metrics, and numerical guidelines."
>
> "This is important in guiding further changes to the existing SNF storage regulatory approach and the evaluation of strategies for extended SNF storage activities. As part of the implementation of the proposed risk management regulatory framework, the NRC should more consistently consider the concept of defense-in-depth explicitly and evaluate its proper use in the SNF storage regulatory program. The NRC should also improve appropriate parts of staff training to make this concept a central part of such training."

6. DEFENSE-IN-DEPTH IN SECURITY

6.1 Introduction

The term defense-in-depth is rarely used, and when used is not used consistently in the security area of nuclear facilities regulated by NRC. However, as noted below, defense-in-depth features are found in various parts of Title 10 of the *Code of Federal Regulations*, as well as in other source documents such as NUREGs, Regulatory Guides and documents issued by the International Atomic Energy Agency relating to security and physical protection.

The material below is divided into two groups. The first group, in Section 6.2, consists of the security related defense-in-depth references found for byproduct materials in 10 CFR Parts 30 and 37 and an associated NUREG. The second group consists of the security-related defense-in-depth references found for the physical protection of plants and materials on 10 CFR Part 73 and associated guidance documents.

6.2 Byproduct materials

Two sources in the literature that discuss defense-in-depth with respect to security of byproduct materials are:

- 10 CFR Parts 30 and 37 [CFR]
- NUREG-1556, Vol. 1 [NUREG, 2012g]

6.2.1 10 CFR Parts 30 and 37

The regulations that deal with defense-in-depth issues for byproduct materials are listed in Table 6-1 below.

Table 6-1 Defense-in-Depth Related Statements in 10 CFR Parts 30 and 37

Number	Title	Requirement	Comment
30.34	Terms and Conditions of Licenses	Security requirements for portable gauges: Each portable gauge licensee shall use a minimum of two independent physical controls that form tangible barriers to secure portable gauges from unauthorized removal, whenever portable gauges are not under the control and constant surveillance of the licensee.	This regulation is considered as addressing defense-in-depth since it involves redundancy and diversity
37.47	Security Zones	(a) Licensees shall ensure that all aggregated category 1 and category 2 quantities of radioactive material are used or stored within licensee established security zones (c) Security zones must, at a minimum, allow unescorted access only to approved individuals through:..(1) Isolation of category 1 and category 2 quantities of radioactive materials by the use of continuous physical barriers that allow access to the security zone only through established access control points.	The requirement for continuous physical barriers is considered to be a defense-in-depth measure.

Number	Title	Requirement	Comment
37.49	Physical Protection of Category 1 and Category 2 Types of Radioactive Material: Requirements During Use	Security zones: "Licensees shall provide the means to maintain continuous monitoring and detection capability in the event of a loss of the primary power source, or provide for an alarm and response in the event of a loss of this capability to continuously monitor and detect unauthorized entries."	Provision of backup power or an alarm and response to maintain continuous monitoring is considered a defense-in-depth feature since it involves redundancy and diversity in maintaining security.
37.53	Requirements for mobile devices	Each licensee that possesses mobile devices containing category 1 or category 2 quantities of radioactive material must: (a) Have two independent physical controls that form tangible barriers to secure the material from unauthorized removal when the device is not under direct control and constant surveillance by the licensee…	The requirement for two independent controls is considered a defense-in-depth measure since it involves redundancy and diversity.
37.79	Requirements for physical protection of category 1 and category 2 quantities of radioactive material during shipment	(a) *Shipments by road.* (1) Each licensee who transports, or delivers to a carrier for transport, in a single shipment, a category 1 quantity of radioactive material shall:. (ii) Ensure that redundant communications are established that allow the transport to contact the escort vehicle (when used) and movement control center at all times. Redundant communications may not be subject to the same interference factors as the primary communication.	The requirement for redundant communications is a defense-in-depth measure.

6.2.2 NUREG-1556 V1 - Standard Review Plan on Portable Gauge Licenses

The standard review plan for portable gauge licensees indicates the defense-in-depth measures, based on multiple physical barriers to unauthorized access that need to be taken to ensure security. The document states:

> "At all times, licensees are required to maintain control and constant surveillance of the portable gauge when it is in use and, at a minimum, use two independent physical controls to secure the portable gauge from unauthorized removal while it is in storage. The physical controls used should be designed and constructed of materials suitable for securing the portable gauge from unauthorized removal, and both physical controls must be defeated in order for the portable gauge to be removed. The construction and design of the physical controls should be such that they will deter theft by requiring a more determined effort to remove the portable gauge. The security procedures

should ensure that the two physical barriers chosen increase the deterrence value over that of a single barrier and that the two physical barriers would make unauthorized removal of the portable gauge more difficult."

"As long as the licensee maintains constant control and surveillance while transporting the portable gauges, the licensee need only comply with the DOT requirements for transportation (e.g., placarding, labeling, shipping papers, blocking and bracing). However, if the licensee leaves the vehicle and portable gauge unattended (e.g., while visiting a gas station, restaurant, store), the portable gauge must be secured by two independent controls as required by 10 CFR 30.34(i)."

6.3 Physical Protection of Plants and Materials

Sources in the literature that discuss defense-in-depth with respect to physical protection of plants and materials are:

- 10 CFR Part 73 [CFR]
- Regulatory Guide 5.63 [NRC, 1982]
- Regulatory Guide 5.71 [NRC, 2010a]
- NUREG-1804, Rev 2 [NRC, 2003a]

6.3.1 10 CFR Part 73

There are several requirements that implicitly involve defense-in-depth or explicitly refer to defense-in-depth in 10 CFR Part 73, which pertains to the physical security of plants and materials regulated by the NRC. These are listed in Table 6-2 below:

Table 6-2 Defense-in-Depth Related Statements in 10 CFR Part 73

Number	Title	Requirement	Comment
73.20	General performance Objective and Requirement	(b)…a licensee shall establish and maintain, or arrange for, a physical protection system that: (2) Is designed with sufficient redundancy and diversity to ensure maintenance of the capabilities described in §§ 73.25 and 73.45	The requirement for redundancy and diversity is a defense-in-depth feature.
73.25	Performance capabilities for physical protection of strategic special nuclear material in transit	*(d)…the physical protection system shall: …* (4) Assure that a single adversary action cannot destroy the capability of armed escorts to notify the local law enforcement forces of the need for assistance.	Preventing single failure is a defense-in-depth measure.

Number	Title	Requirement	Comment
73.26	Transportation physical protection systems, subsystems, components, and procedures.	*Shipment by road:* A specially designed cargo vehicle truck or trailer that reduces the vulnerability to theft…. Two separate escort vehicles shall accompany the cargo vehicle. There shall be a total of seven armed escorts with at least two in the cargo vehicle. An armored car cargo vehicle: Three separate escort vehicles shall accompany such a cargo vehicle. There shall be a total of seven armed escorts, with at least two in the cargo vehicle.	The requirement to have multiple escort vehicles and seven armed escorts is a defense-in-depth feature since it involves redundancy.
73.37	Requirements for physical protection of irradiated reactor fuel in transit.	(c) *Shipments by road*… the physical protection system for any portion of a spent nuclear fuel shipment by road shall provide that:.. (3) The transport vehicle and each escort vehicle are equipped with redundant communication abilities.. (d) *Shipments by rail*… the physical protection system for any portion of a spent nuclear fuel shipment by rail shall provide that:.. (3) The train operator(s) and each escort are equipped with redundant communication abilities.. (e) *Shipments by U.S. waters*… the physical protection system for any portion of a spent nuclear fuel shipment traveling on U.S. waters shall provide that:.. (4) Each armed escort is equipped with redundant communication abilities..	The requirement for a redundant communication capability is a defense-in-depth feature.
73.45	Performance capabilities for fixed site physical protection systems	Physical barrier subsystems: …vital areas and material access areas must be located within a protected area so that access to vital equipment and to strategic special nuclear material requires passage through at least three physical barriers. The perimeter of the protected area must be provided with two separated physical barriers with an intrusion detection system placed between the two.	The requirement for physical barriers, including multiple barriers, to access is a defense-in-depth feature.
73.46	Fixed site physical protection systems, subsystems, components and procedures	(c) Physical barrier subsystems. (1)… vital areas and material access areas must be located within a protected area so that access to vital equipment and to strategic special nuclear material requires passage through at least three physical barriers. The perimeter of the protected area must be provided with two separated physical barriers with an intrusion detection system placed between the two. e) *Detection, surveillance and alarm subsystems and procedures*… (5) All alarms required pursuant to this section shall annunciate in a continuously manned central alarm station located within the protected area	The requirement for multiple barriers to impede access to vital and material access areas is identical to the one in 73.45 and is a defense-in-depth feature. The requirement to protect against a single act aimed to disable the alarm

Number	Title	Requirement	Comment
73.46 (cont.)		and in at least one other independent continuously manned onsite station not necessarily within the protected area, so that a single act cannot remove the capability of calling for assistance or responding to an alarm.	system is a defense-in-depth feature since it involves redundancy.
73.50	Requirements for physical protection of licensed activities.	*Physical barriers:* The licensee shall locate vital equipment only within a vital area, which, in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers… The licensee shall locate material access areas only within protected areas such that access to the material access area requires passage through at least two physical barriers. *Detection aids:* All alarms required pursuant to this part shall annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station, not necessarily within the protected area, such that a single act cannot remove the capability for calling for assistance or otherwise responding to an alarm.	The requirement for multiple physical barriers is a defense-in-depth measure. The requirement for multiple alarm sites to aid in detection is a defense-in-depth measure since it involves redundancy.
73.51	Requirements for the physical protection of stored spent nuclear fuel and high-level radioactive waste.	Spent nuclear fuel and high-level radioactive waste must be stored only within a protected area so that access to this material requires passage through or penetration of two physical barriers, one barrier at the perimeter of the protected area and one barrier offering substantial penetration resistance.	The requirement for two physical barriers is a defense-in-depth measure.
73.54	Protection of digital computer and communication systems and networks	Section (c)(2): The cyber security program must be designed to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks.	The regulation explicitly calls for defense-in-depth against cyber attack.
73.55	Physical protection for reactors.	Section (b)(3) (ii): “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.	The regulations explicitly require defense-in-depth strategies or methodologies to ensure reactor protection.

Number	Title	Requirement	Comment
73.55 (cont.)		Section (b)(9)(i): The insider mitigation program must monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorization to a protected or vital area, and implement 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 73 Appendix C	Licensee Safeguards Contingency Plans…II. Nuclear Power Plant Safeguards Contingency Plans	3. Licensee Planning Base. This category of information shall include factors affecting safeguards contingency planning that are specific for each facility...c. Safeguards Systems. The safeguards contingency plan must include a description of the physical security systems that support and influence how the licensee will respond to an event in accordance with the design basis threat described in § 73.1(a)… (i) 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…. (v) Licensees shall develop, implement, and maintain a written protective strategy to be documented in procedures… The protective strategy shall:… (4) Contain a description of the physical security systems and measures that provide defense-in-depth, such as physical barriers, alarm systems, locks, area access, armaments, surveillance, and communications systems.	The requirements explicitly identify defense-in-depth as part of the contingency plan for both physical security systems and protective strategies.

6.3.2 Regulatory Guide 5.63, Physical Protections for Transient Shipments

This 1982 Regulatory Guide (RG) describes measures acceptable to the NRC staff that can be taken by the licensee to provide the physical protection for scheduled and unscheduled transient shipments required by 10 CFR Part 70. Reference to defense-in-depth is made in the following statement:

> "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."

6.3.3 Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities

This RG provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by 10 CFR §73.1. Licensees may use methods other than those described within this guide to meet the Commission's regulations if the chosen measures satisfy the stated regulatory requirements. Regarding defense-in-depth the following statements are found:

> "Defense-in-depth strategies represent a documented collection of 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."

6.3.4 NUREG-1804, Rev 2, Yucca Mountain Standard Review Plan

This document reviews the requirements of the physical protection plan at the high-level waste repository at Yucca Mountain, NV and identifies those that may be considered defense-in-depth. The document states:

> "The U.S. Department of Energy has identified and adequately described those portions of the physical protection system for which *redundant and diverse components and redundant and diverse subsystems and components* are necessary to ensure adequate performance, as required by 10 CFR 73.51(b)(2). Access to material in the protected area shall require passage or penetration through *two physical barriers*—one barrier at the perimeter of the protected area, and one barrier offering substantial penetration resistance."

7. PERSPECTIVES ON DEFENSE-IN-DEPTH FROM THE INTERNATIONAL COMMUNITY

7.1 Introduction

Within the international community, the sources summarized include:

- Several International Atomic Energy Agency (IAEA) Documents

- The Nuclear Energy Agency/Committee on Nuclear Regulatory Activities/Committee on the Safety of Nuclear Installations (NEA/CNRA/CSNI) Joint Workshop on Challenges and Enhancements to DID in light of the Fukushima Dai-ichi Accident [NEA, 2014]

- DID-PAS: development of a Framework for Evaluation of the Defence-in-Depth with PSA, Swedish Radiation Safety Authority [SSM, 2015]

- Implementation of Defence in Depth at Nuclear Power Plants: Lessons Learnt from the Fukushima Daiichi Accident, Nuclear Energy Agency [NEA, 2016]

7.2 IAEA Documents

There are several reports that have been issued by IAEA that address defense-in-depth. These include the following documents and are summarized below:

- INSAG-3 [IAEA, 1996a]
- INSAG-10 [IAEA, 1996b]
- INSAG-12[IAEA, 1996c]
- IAEA SRS No. 46 [IAEA, 2005]
- IAEA SF-1 [IAEA, 2006]
- IAEA TECDOC-1570 [IAEA, 2007]
- IAEA, NP-T-2.2 [IAEA, 2009]
- IAEA, SSR-2/1 [IAEA, 2012]
- IAEA, INFCIRC 225 [IAEA, 2011]

The first seven publications deal with defense-in-depth measures in response to inadvertent events that can lead to accidents, while the last is concerned with defense-in-depth for security related issues.

7.2.1 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."

7.2.2 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 accidents at 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 in the report 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.

7.2.3 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 INSAG-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 there is a strategy for defense-in-depth which is twofold, “first, to prevent accidents 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.

This report 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

7.2.4 IAEA SRS No. 46, 2005

In 2005, IAEA published a report in the Safety Report Series dealing with the assessment of defense-in-depth for nuclear power plants (NPPs). This publication describes a method for assessing the defense-in-depth capabilities of an existing plant, including both its design features and the operational measures taken to ensure safety. A systematic identification of the required safety provisions for the siting, design, construction and operation of the plant provides the basis for assessing the comprehensiveness and quality of defense-in-depth at the plant.

For given objectives at each of the five levels of level of defense, a set of challenges is identified, and several root mechanisms leading to the challenges are specified. Finally, to the extent possible, a comprehensive list of safety provisions, which contribute to preventing these mechanisms from occurring, is provided. A broad spectrum of provisions, which encompass the inherent safety features, equipment, procedures, staff availability, staff training and safety culture aspects, is considered. For easier and more user friendly applicability, the method is illustrated in the form of so called "objective trees."

7.2.5 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, the concept of defense-in-depth is used in the definition of the principle: “all practical efforts must be made to prevent and mitigate nuclear or radiation accidents.”

The standard states:

> “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:
>
> - features providing safety margins, 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

- 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."

7.2.6 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 is defense-in-depth which includes probabilistic considerations. The TECDOC states:

"The proposed new pillars (discussed in detail later in this TECDOC), include quantitative safety goals, fundamental safety functions and quantitative targets to be achieved at each level of defence in depth (taking into account probabilistic considerations)."

The document references INSAG-10 in terms of the five levels of defense-in-depth, 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. A 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."

7.2.7 IAEA, NP-T-2.2, 2009

The objective section of this report states that it is intended for different categories of stakeholders, including designers and potential users of innovative small modular reactors (SMRs), as well as officers in ministries of atomic energy commissions in Member States responsible for implementing nuclear power development programs or evaluating nuclear power deployment options in the near, medium, and longer term. The overall objectives of this report are stated to be:

> "(1) To assist developers of innovative SMRs in defining consistent defence in depth approaches regarding the elimination of accident initiators/ prevention of accident consequences through design and the incorporation of inherent and passive safety features and passive systems in safety design concepts of such reactors; (2) To assist potential users of innovative SMRs in their evaluation of the overall technical potential of SMRs with inherent and passive safety design features, including their possible implications in areas other than safety."

The specific objectives of this report are stated to be:

> "To present the state of the art in design approaches used to achieve defence in depth in pressurized water reactors, pressurized light water cooled heavy water moderated reactors, high temperature gas cooled reactors, sodium cooled and lead cooled fast reactors, and non-conventional designs within the SMR range;"
>
> "To highlight benefits and negative impacts in areas other than safety arising from the implementation of inherent and passive safety design features;"
>
> "To identify issues of performance reliability assessment for passive safety systems in advanced reactors, and to highlight further research and development needs arising therefrom."

7.2.8 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…. 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 defense discussed:

> “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:
>
> - Shall provide for multiple physical barriers to the release of radioactive material to the environment
>
> - 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

- 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

- 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

- 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

- 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."

7.2.9 INFCIRC 225, Rev 5 of the International Atomic Energy Agency (Security)

The International Atomic Energy Agency's Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities, INFCIRC 225, Rev 5, January2011, identifies defense-in-depth as one of the fundamental principle of risk-based physical protection systems and measures. The document states:

"The State's requirements for physical protection should reflect a concept of several layers and methods of protection (structural, other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives."

"(FUNDAMENTAL PRINCIPLE I: Defence in Depth)

3.45. State requirements for physical protection should be based on the concept of defence in depth. The concept of physical protection is one which requires a designed mixture of hardware (security devices), procedures (including the organization of guards and the performance of their duties) and facility design (including layout).

3.46. The three physical protection functions of detection, delay, and response should each use defence in depth and apply a graded approach to provide appropriate effective protection.

3.47. Defence in depth should take into account the capability of the physical protection system and the system for nuclear material accountancy and control to protect against insiders and external threats."

In this document defense-in-depth is defined as "The combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised."

7.3 NEA/CNRA/CSNI Joint Workshop, June 2013

7.3.1 Workshop Summary

On June 5th 2013, Organization for Economic Co-operation and Development (OECD) NEA/CNRA/CSNI held an international workshop on defense-in-depth. Attendance at the workshop included top-level representatives from nuclear regulatory agencies and technical support organizations of the NEA member countries and associated members, senior representatives from industry and senior executives of the NEA and IAEA.

One of the main conclusions from the discussions was that the concept of defense-in-depth remains sound, and that its application is the primary means of preventing and mitigating accidents. The philosophy of defense-in-depth was seen as important in dealing with unknowns, imperfections, and failures.

One of the key discussion points was around the use of probabilistic safety assessment (PSA) for external events. The workshop considered that there was a need to balance the importance of using probabilistic methods for ensuring that more probable events have been appropriately addressed in the safety case against the scarcity of data to support external event frequencies and how low-frequency events can start to lose their meaning. The overall conclusion was that

further work is required on the application of PSA to external events. A related area of discussion was on the appropriate level of hazard for external events, and what types of events should be considered.

The main conclusions from the workshop were the following:

- The defense-in-depth concept remains valid, but strengthening may be needed.
- Implementation of defense-in-depth needs further work, in particular regarding external hazards.
- Additional guidance would be appropriate to help harmonize implementation.
- Improvements should focus not just on preventing accidents but also on mitigating the consequences of potential accidents should they occur.

The workshop encouraged the NEA to meet the needs of its members, and the broader international community, by preparing concise publications describing the state-of-the-art in defense-in-depth and commendable practices for implementation of defense-in-depth. The closing section of the workshop also suggested future areas for the NEA's program of work to consider in enhancing the understanding and implementation of defense-in-depth.

7.3.2 Summary of Individual Workshop Presentations

Mr. Luis Echávarri, NEA Director General made opening remarks for the workshop in which he commented on the impact of lessons learned from the Fukushima accident, NEA activities to enhance safety after the accident, the NEA summary report on the accident, and other key messages.

Highlights from the Work of CNRA on the Activities, Priorities and Challenges Related to Defense-in-Depth

Dr. Jean-Christophe Niel, the CNRA Chair, discussed the activities, priorities and challenges related to defense-in-depth, the concept and implementation of defense-in-depth, the responsibilities for defense-in-depth of the licensee and the regulator, prevention and mitigation aspects of defense-in-depth, defense-in-depth's design and site specific aspects, and the way forward as CNRA sees it.

The presentations by the various speakers at the workshop are briefly summarized below.

NEA/CNRA/CSNI Joint Workshop Remarks

Dr. Brian Sheron, CSNI Chair, talked briefly on the topic of defense-in-depth and external events. He noted that defense-in-depth has been defined as an element in NRC's safety

philosophy that is used to address uncertainty by employing successive measures, including safety margins, to prevent or mitigate damage if a malfunction, an accident, or a naturally or intentionally caused event occurs. He further observed that the key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures. This will ensure that no single layer—no matter how robust—is exclusively relied upon. He then stated how he thought of defense-in-depth: First, you must have a high-quality, highly reliable design. Second, you have to recognize that failure may still occur despite attempts to prevent it through a highly reliable design. For this reason, systems are designed to cope with and mitigate failures. Finally, it's prudent to acknowledge that since it is impossible to identify everything that can go wrong, we must design in margin to accommodate the unforeseen through areas such as structural design margins and emergency preparedness, to name only a few.

He observed that one of the difficulties in implementing a defense-in-depth design approach is that the appropriate balance between prevention and mitigation is not clearly defined. A licensee could demonstrate that the U.S. surrogate safety goals have been met by providing only preventative measures. Similarly, one could also envision the ability to meet the surrogate safety goals with only mitigative measures. One of the biggest difficulties is deciding what is the right balance between prevention and mitigation when it comes to defense-in-depth. He felt another aspect of defense-in-depth that is difficult to deal with is economic consequences. So a second questions is "If measures such as timely evacuation demonstrate that (public health) safety goals are met, how should any economic consequences be dealt with?"

He stated that these are two important questions that he believes are still subject to debate. Moreover, he noted that worldwide, nuclear plant improvements have reduced the risk from internal events to risk levels comparable to or below those from external events. With this in mind, the United States is looking at whether defense-in-depth goes far enough for external events. He felt that as a result of the Fukushima Daiichi accident no indication exists thus far that the concept of defense-in-depth is flawed, but the nuclear industry and the regulators need to take a harder look at whether there is enough defense-in-depth for external events. This, in turn, means we also need to take a harder look at how well we understand the magnitude and likelihood of external events, as well as their related uncertainties.

Dr. Sheron concluded his talk with brief remarks about activities the CSNI has undertaken related to external events, some of which are a direct result of the accident at Fukushima Daiichi.

Emergency and Recovery Planning and Management: The Last Defence in Depth Barriers

Dr. Thierry Schneider, Committee on Radiation Protection and Public Health Bureau, talked about defense-in-depth Emergency Management Issues such as:

- Communications was seen as important but posed problems. Improvements are warranted.

- Strategies for monitoring incoming products existed, but there was no common approach.

- Technical assessments of early, uncertain accident situations are important for decisions.

He noted the following defense-in-depth recovery management issues:

- Nationally, there has been much less focus on recovery planning than on emergency planning.

- Return to evacuated areas was seen as needing pre-determined criteria as a starting point.

- There is a need to clarify the relationship and to bridge the gap between self-help actions initiated by stakeholders, and support activities supplied by government authorities and radiation protection experts.

- Survey responses viewed stakeholder involvement in recovery as decision-aiding with regard to national or regional decisions.

- Much of the provisional aid seems to be focused on providing information to the affected populations, but communication and dialogue remain as issues for governments.

NEA/CNRA/CSNI Joint Workshop Remarks

Mr. Bill Borchardt, former NRC Executive Director for Operations, remarked that while it's proper to acknowledge defense-in-depth's positive contribution to safety, we must also acknowledge that the way it has been implemented has not prevented all serious events from occurring. He noted that we need defense-in-depth because we have imperfect knowledge, the consequences for serious events are potentially very high, failures do occur, and all human activities are inherently imperfect. He believes that defense-in-depth requires, among other things, a questioning attitude, a resistance to complacency, and a commitment to continuous learning - - in short, a strong safety culture.

Mr. Borchardt reflected briefly on the history of defense-in-depth and noted that over the past decades, the scope, range and prominence of defense-in-depth has grown so that today it reaches into every aspect of the technology. He echoed some of the characteristics of defense-in-depth mentioned by previous speakers. He noted that lessons learned from major events have tended to add detailed design and operational requirements based upon the specific event, however, these improvements have not reduced the importance of the defense-in-depth philosophy. Defense-in-depth remains vitally important in being prepared for the unknown, the unexpected, and the imperfection of any human activity. He believed that, as operating experience demonstrates, the need for defense-in-depth remains paramount. He noted that

Fukushima reinforces the realization that we must be prepared to protect against low probability/high consequence events that even decades of experience cannot prepare us for.

He remarked that the philosophy of defense-in-depth has held up well over the decades. In the U.S. the events of TMI and 9/11 showed that the concept is still sound. However, as a result of these and other events, the US has had to give the implementation of defense-in-depth additional thought and selected expansion to maintain its robustness and ability to account for challenges previously not considered and fully addressed. He expressed his belief that the philosophy of defense-in-depth continues to be sound, that the events at Fukushima represent the most recent major "test" for defense-in-depth, and an opportunity to further refine the approach to defense-in-depth implementation.

He commented that Fukushima was an extreme, beyond-design-basis event – exactly the kind of uncertainty that defense-in-depth exists to address. This accident highlighted not only the importance of multiple layers of defense, but also presented a number of new technical challenges to consider in implementing defense-in-depth: extreme natural events, maintaining spent fuel pool cooling capability, and loss of offsite power, among others.

In closing he offered a few ideas for further discussion:

- First, do we need to adjust the balance between prevention and mitigation features within our defense-in-depth approach?

- Second, this is an opportunity to reflect on the critical importance of a strong safety culture and a questioning attitude among regulators and the nuclear workforce that are essential to ensuring defense-in-depth.

- Third, and related to safety culture, as at TMI, we need to look closely at the role of the facility site operators. Do they have the independent authority, experience, training, and other resources necessary to fulfill their important role in defense-in-depth to prevent accidents and mitigate their onsite and offsite effects?

Defense-in-Depth for New Nuclear Power Plant Designs

Dr. Hans Wanner, Western European Nuclear Regulators' Association (WENRA) Chair, first presented basic information about WENRA, including members and observers, policy statements, working groups, and Reactor Harmonization Working Group (RHWG) tasks. He then presented detailed information on WENRA's strengthened defense-in-depth and safety objectives ideas for new nuclear power plants, which call for core melt accidents to be considered in the design and are summarized in Table 7-1 below.

Table 7-1 Defense-in-Depth for New NPP Designs

Levels of Defense in Depth	Associated Plant Condition Categories	Objective	Essential Means	Radiological Consequences
Level 1	Normal operation	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	Regulatory operating limits for discharge
Level 2	Anticipated operational occurrences	Control of abnormal operations and failures	Control and limiting systems and other surveillance features	
Level 3	Defense-in-Depth Level 3.a Postulated single initiating events	Control of accidents to limit radiological releases and prevent escalation to core melt conditions	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact
	Defense-in-Depth Level 3.b Postulated multiple failure events		Additional safety features, accident procedures	
Level 4	Postulated core melt accidents (short and long term)	Control of accidents with core melt to limit off-site releases	Complementary safety features to mitigate core melt, management of accidents with core melt (severe accidents)	Limited protective measures in area and time
Level 5		Mitigation of radiological consequences of significant releases of radioactive material	Offsite emergency response Intervention levels	Off-site radiological impacts necessitating protective measures

Recent Regulatory Challenges in Korea a Defense-in-Depth Perspective

Dr. Youn Won Park, Korea institute of Nuclear Safety President, gave an overview of safety issues identified in 2011 and 2012, how the issues are addressed from the defense-in-depth perspective, and what the regulatory challenges are from the defense-in-depth perspective. He raised the questions of how we make sure there are no unnecessary layers of defense? How to prioritize defense-in-depth layers? And how do we know how effective defense-in-depth is?

Defense-in-Depth Prevention, Mitigation, and Emergency Preparedness,

Mr. Glenn Tracy, Deputy Executive Director for Operations, talked about defense-in-depth prevention, mitigation, and emergency preparedness. He pointed out how the elements of defense-in-depth are addressed:

- Event Frequency is addressed through quality of design, manufacture, construction, operation and maintenance

- Prevention is addressed through high quality redundant safety systems and well-trained operators

- Consequence Mitigation is addressed through siting, containment reinforcement, and severe accident features in reactor designs

- Emergency Preparedness is addressed through emergency plans, siting, and emergency response

Mr. Tracy talked about the need for balance in defense-in-depth approaches. While early defense-in-depth approaches relied more heavily on the prevention of core damage, post Fukushima approaches emphasize a balanced approach. He noted that the USNRC Near Term Task Force Recommendations focused on defense-in-depth:

- Strengthen the roles of defense-in-depth and risk assessment, emphasizing beyond-design-basis and severe accident mitigation.

- A risk-informed defense-In-depth framework that includes extended design-basis requirements.

- A rationale for decision-making built around the defense-in-depth concept in which each level of defense-in-depth (namely prevention, mitigation, and EP) is critically evaluated for its completeness and effectiveness in performing its safety function.

He also discussed the contemporary defense-in-depth challenge with respect to digital instrumentation and controls, and answered the question of where do we go from here: for U.S. operating reactors: post-Fukushima requirements will enhance the ability to respond to seismic events, flooding and station blackout; for New and Advanced Reactors there is an opportunity to design-in enhanced defense-in-depth for post-Fukushima topics and other issues.

WANO Actions after Fukushima. How WANO Improves Defense-in-Depth?

Mr. Jacques Regaldo, World Association of Nuclear Operators (WANO) Chair, discussed the WANO organization and mission, the increase in defense-in-depth post Fukushima, some of the

cultural barriers to nuclear safety, and noted that WANO is strongly committed to reinforce defense-in-depth and in doing so to restore public trust.

Implementation of Defense-in-Depth Concept to External Events

Dr. Toyoshi Fuketa, NRA Commissioner, talked about the weaknesses found from the Fukushima accident: the insufficient design provisions against a tsunami, the lack of practical accident management, and insufficient provision for accidents that far-exceeded the postulated design conditions.

In his talk he emphasized (1) the importance of defense-in-depth Level 1 against external events (prevention of abnormal operation and failures), (2) Japan's general approach to cope with external events, (3) how to decide on margins for design basis hazards considering site specific characteristics, (4) design requirements and safety classification for specific SSCs, and (5) consideration of the effects of external events in the later (mitigative) stages of defense-in-depth.

Enhancement of Defense-in-Depth against External Events in French Nuclear Power Plants

Dr. Jacques Repussard, IRSN Director General, noted that after TMI accident, in France 2 levels have been added to the DID (4^{th} and 5^{th} levels) and design provisions have been implemented for existing plants to limit the consequences of core melt accidents. He discussed the differences in the implementation of defense-in-depth and consideration of external events used before and after Fukushima, resulting in the improvement of defense-in-depth after Fukushima.

Russia's Efforts to Improve Safety after Chernobyl and Fukushima Accidents

Dr. Leonid Bolshov, the Nuclear Safety Institute of the Russian Academy of Science Director General, spoke about the Chernobyl accident and the post Chernobyl efforts resulting in a changed attitude in Russia regarding severe accidents. Regarding defense-in-depth he mentioned the tests for defense-in-depth efficiency that have been done in Russia for each power unit in operation, taking into account all credible extreme impacts on the NPP that are specific to the site, and taking into account various combinations of these extreme impacts.

Issues on Defense-in-Depth perspective from French Nuclear Safety Authority (ASN)

Mr. Pierre Frank Chevet, ASN President, presented France's expectations for new reactors in some detail: Clear expectation to address in the original design what was often "beyond design" for the previous generation of reactors (multiple failure events, core melt accidents). He emphasized provisions to ensure independence of defense-in-depth levels and the post Fukushima accident defense-in-depth evolution.

7.4 DiD-PSA: Development of a Framework for Evaluation of the Defense-in-Depth with PSA

In SSM 2015:04 the author, Per Hellström, describes a project whose objective it is to investigate how, and to what extent, probabilistic safety assessment (PSA) (usually referred to as probabilistic risk assessment (PRA) in the United States) can be used to asses and improve the defense-in-depth of nuclear power plants. In the report (and the research project) defense-in-depth is based on the following concept from IAEA INSAG 12 which is based on IAEA INSAG 3:

> "All safety activities, whether organizational, behavioral or equipment related, are subject to layers of overlapping provisions, so that if a failure occurs 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."

Hellström wants to link quantities calculated in PSA to specific levels of defense-in-depth, as defined in INSAG 12 and other IAEA publications. A ranking of structures, systems, and components (SSCs) that have a role in the different defense-in-depth levels is sought in relation to their risk contribution. The IAEA defense-in-depth levels referred to are shown in Table 7-2:

Table 7-2 Levels of Defense-in-Depth

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

The project to link defense-in-depth levels with PSA results was carried out in several steps. It starts with a survey of qualitative parameters of each level of defense-in-depth that should be considered in the method. This includes identification and structuring of the SSCs that belong to each defense-in-depth level and that should thus be considered for potential PSA evaluation. The report shows the link of the IAEA defense-in-depth levels to SSCs as indicated in Table 7-3:

Table 7-3 Definitions of the Levels in the Concept of Defense-in-Depth

Level	Purpose	Main measures	SSCs that are the main measures
I	Prevention of abnormal operations and failures	Robust design and high quality requirements on design, operation and maintenance	No technical plant safety systems are part of this level of defense which consists of adequate design, requirements, manufacturing, maintenance, conditioning and testing etc. that minimizes the number of potential failures and cases with abnormal operation. Also choice of site is part of this level.
2	Control of abnormal operation and detection of failures	Control and protection systems as well as surveillance and in-service inspection	Design features of the process control and monitoring systems for allowing continued operation even in the case of abnormal operation and for detection of failures. Examples: Reserve capacity and standby redundancy in Balance of Plant (BoP) systems. All kind of monitoring of plant conditions and protective measures that minimizes the risk for a failure to escalate into accident conditions and needed for scram of the plant and that minimizes the probability for equipment being unavailable when called upon.
3	Control of accidents within the design basis	Technical safety functions as well as emergency operating procedures	Safety functions: Examples are reactivity control, primary water inventory control, and residual heat removal represented by technical safety systems including their monitoring and activation and related procedures and operator actions.
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Prepared engineered measures and effective accident management at the facility	Safety functions: Examples are containment integrity control, containment atmosphere control and containment release and filtering control represented by technical safety systems including their monitoring and activation and related procedures and operator actions.
5	Mitigation of consequences of significant releases of radioactive substances	Effective co-operation with the competent authorities for protection of the public and the environment	Plant systems for monitoring the scenario give input to decisions, e.g. alarming and evacuation. Choice of site is important for this defense-in-depth level.

In the next step, a review is made of PSA properties (both input data used and results that are, or can be, calculated by a PSA), and attempts are made to link them to the different defense-in-depth levels.

Hellström concludes that, as defined above, at least the first two IAEA defense-in-depth levels do not lend themselves to assessment via results commonly calculated in current PSAs.

After offering several interpretations of the defense-in-depth levels, the author proposes an elaborated model of defense-in-depth Levels 1 and 2 resulting in extended defense-in-depth level definitions as indicated in Table 7-4 below. In particular, the author splits defense-in-depth levels 1 and 2 into levels 1.1 and 1.2, and levels 2.1 and 2.2 to separate prevention of failures from detection of failures. With this scheme, Hellström proposes a sequential defense-in-depth schematic as shown below in Figure 7-1.

Table 7-4 Extended Defense-in-Depth Level Definitions

DiD Level	Description	Examples
1:1	Quality in design, manufacturing, installation, use of redundancy, fail safe principles, etc. to ensure high system reliability and availability.	Use of a specific Safety Integrity Level (SIL) in design, proven design, etc.
2:1	The monitoring and surveillance of the condition of SSCs in order to detect degradation and failures before they become critical, i.e. before they affect the performance of the sequential DID levels.	Systems for continuous monitoring or regular testing of vibrations, temperature, crack growth, etc. that can identify any signs of (precursors) to equipment failures.
1:2	BoP system, other operating systems. A failure means that DID 2.2 is needed to avoid shutdown.	Loss of offsite power, Failure of a feed water pump.
2:2	Systems for detection and control of disturbances resulting from failures in the BoP and other operating systems so 1hat the plant can continue operation. This also includes built in robustness in terms of thermal hydraulic design.	Monitoring of feed water flow, back-up feed water pump, abnormal operation relief valves, equipment for house turbine operation. Power reduction capability, e.g. partial scram, the built in thermal hydraulic and nuclear physics behavior.
3	Safety functions for prevention of fuel (core) damage; reactivity control, water level control, pressure control and residual heat removal. Control of an accident within the design basis.	Core Spray, auxiliary feedwater, low pressure injection, high pressure injection, safety relief valves, scram system, etc.
4	Safety functions for mitigation of a potential release resulting from damaged fuel. Releases above a certain level are Beyond Design Basis Accidents (BDBA).	Technical systems, mainly related to the containment - spray system, filters, containment design.

DiD Level	Description	Examples
5	Emergency measures for limiting public exposure to any release resulting from a BDBA	Site location, emergency planning and preparedness, alarm systems, iodine tablets, evacuation routes etc.

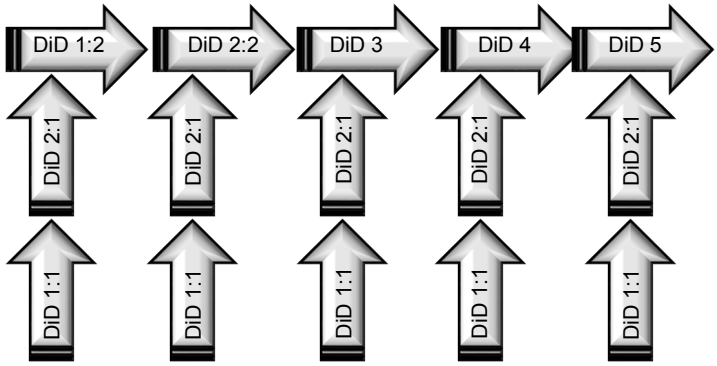

Figure 7-1 Hellström Defense-in-Depth Scheme

With these extended defense-in-depth level definitions, Mr. Hellström proposes that it is possible to extend PSA modeling to provide links to all the defense-in-depth levels. He notes that defense-in-depth level 3 and 4 already have strong links to PSA models and results. He goes on to state that to differentiate defense-in-depth Levels I:2 and 2:2 and to address defense-in-depth Level 5, extended PSA modelling is required which, in tum, calls for new definitions in the PSA framework. Further data analysis of root causes (defense-in-depth level 1.1 and 2.1) that are related to deficiencies in defense-in-depth Levels I:2 and 2:2 makes it possible to achieve a better understanding of the weaknesses and strengths of these defense-in-depth levels with regard to protection against disturbances and failures. Additional modelling of the actual control and protection systems that are part of defense-in-depth Level 2.2 also provides better means of evaluating this defense-in-depth level. The major systems of interest here are the Balance of Plant system and the power control and supply system.

He states other needed additional modelling activities are related to quantification of new "top" events and to calculation of importance measures for SSCs being part of the different defense-in-depth levels.

Hellström also notes that essential to an investigation of the strength of the existing plant is to agree that it is not possible to formulate an aggregated value of the strength of a certain defense-in-depth level. Instead the strength of a defense-in-depth level is always to be formulated in relation to a specific event. The event can in turn propagate to new measurable end states hopefully proven to have a lower frequency.

7.5 Lessons Learned from the Fukushima Daiichi Accident, 2016

The booklet, "Implementation of Defence in Depth at Nuclear Power Plants: Lessons Learnt from the Fukushima Daiichi Accident," provides insights into the implementation of defense-in-depth by regulators and emergency management authorities after the Fukushima Daiichi accident, aiming to enhance global harmonization by providing guidance on:

> "the background to the DiD concept; • the need for independent effectiveness among the safety provisions for the various DiD levels, to the extent practicable;"
>
> "the need for greater attention to reinforce prevention and mitigation at the various levels;"
>
> "the vital importance of ensuring that common cause and common mode failures, especially external events acting in combination, do not lead to breaches of safety provisions at several DiD levels"
>
> "the concept of "practical elimination" of sequences leading to significant radioactive releases;"
>
> "the implementation of DiD for new and existing reactors, multi-unit sites and other nuclear facilities;"
>
> "the implementation of DiD through regulatory activities (based on a survey among CNRA members);"
>
> "the protection measures in the DiD concept of level 5 – off-site emergency arrangements."

This booklet:

> "… describes the basis of the DiD concept and how it has been further developed in response to lessons derived from the accident …"
>
> "… addresses the main generic issues identified by the NEA workshop and CNRA as being of prime interest for further study and clarification in a regulatory context, for example:
>
> - The structure of the levels of DiD …;
> - DiD implementation … including:
>   - independence;
>   - impact of common cause and common mode threats (including external events);

    - human and organisational factors;
    - practical elimination of significant releases;
    - new and operating reactor considerations;
    - multi-plant sites;
    - DiD for other nuclear facilities;
    - regulatory implementation of DiD including survey results.
  - Emergency arrangements off-site …"

"… provides an overall discussion of the use of DiD post-accident for regulators, and concludes that further studies by the NEA would be beneficial to enhance implementation"

Chapter 2 of the booklet discusses the concept of defense-in-depth. It uses the principles from INSAG-10 as its basis. In discussing the concept, the booklet provides observations on:

- Regulatory considerations for defense-in-depth: lessons learnt from the Fukushima Daiichi accident

- Integrated defense-in-depth

With regard to regulatory considerations, the more significant observations are:

"There is therefore a clear message for regulators, reinforcing the need for close attention to the basis for the design and operation of a plant or site, and the need to review this basis – especially for external hazards and events – to ensure that safety functions at the various DiD levels have adequate, independent effectiveness."

"…the Fukushima Daiichi accident emphasised for regulators the need to gain assurance that the design basis accident and design extension requirements used by designers and safety assessors covers those needed to ensure the independent effectiveness of the safety provisions for INSAG levels 3 and 4."

"For INSAG level 4, regulators can expect that analysis methods and boundary conditions, or design and safety assessment rules, are developed according to a graded approach, based on probabilistic insights, and using best estimate methodology. Less stringent analysis rules and equipment performance requirements than those for INSAG level 3 may be applied if appropriately justified."

"… for the implementation of INSAG level 5 … it illustrated that no matter how much other levels are strengthened, and very rare severe event scenarios are practically eliminated, effective emergency arrangements and other responses

are essential parts of the DiD concept. To be effective, they have to be functional in the particular circumstances of the accident."

With regard to integrated defense-in-depth, the more significant observations are:

> "DiD as a concept is not just related to reactor design and its assessment but also covers all other aspects that may affect the safety of the NPP. In particular, human and organisational elements must be seen as part of the safety provisions at all levels in an integrated approach to DiD."

Chapter 3 of the booklet addresses areas of interest for regulators; specifically:

- General elements of implementation
- Independence of the levels of defense-in-depth
- Common cause and common mode failures
- Practical elimination of significant radiological releases

With regard to general elements of implementation, the booklet states:

> "DiD is implemented primarily through the combination of a number of consecutive levels of protection with independent effectiveness that would have to fail before harmful effects could be caused to people or to the environment. Design principles available to promote DiD include: redundancy, diversity, segregation, physical separation, train/channel independence, single-point failure protection and, as far as practical, independence between levels. It should be implemented in a manner that ensures that each level is effective in meeting its specific objective."

> "To maximise the effectiveness of the use of DiD, it must be part of the early design process and addressed in a consistent and effective way. … An illustration of the importance of this early use is that it is essential in developing the safety classification of systems and components. If classification and categorisation have developed without reference to DiD, rather than DiD being one of the drivers for classification and categorisation, later analysis can reveal that the independence of the safety provisions at the various layers of DiD has been undermined, with the possible introduction of a common cause failure into the design."

With regard to independence of the levels of defense-in-depth, the booklet states:

> "The concept of the independence of the levels of DiD applies to all five levels. As indicated above, the independent effectiveness of each of the safety provisions at the various levels is an essential basis for the safety of the plant.

The regulator would wish to be ensured that failure at one level (or barrier) of defence does not, as far as practical, cause the failure of others."

"Independent effectiveness is based on the adequate application of functional isolation, the diversity principle and physical separation of the SSCs depending on the threats."

"Complete independence of systems and components at the different levels may not be possible; however, the aim should be to ensure as far as is practicable that the SSCs provided at different levels are independent of one another for the event they are intended to prevent or mitigate."

"In addition to assurance about the provision of hardware SSCs, the regulator should also be interested in the human factor and performance aspects provided at each level of DiD, including the ability of NPP operation staff (and contractors where relevant) to implement effective emergency actions, especially for multi-unit sites."

With regard to common cause and common mode failures, the booklet states:

"… it is vital to consider the impact of common cause and common mode failures when implementing the concept of DiD, particularly from external hazards, as they can lead to a loss of several levels of DiD safety provisions or significantly reduce independent effectiveness."

"Applying the concept of DiD and the need for independence of the various levels is an effective way of identifying and addressing common cause and common mode failures."

"… a detailed analysis of the various hazards, initiating events and faults against the concept of independent effectiveness of safety provisions at the various levels of DiD. This can provide a very valuable assessment of the plant's robustness. Such analyses can lead to an enhancement of the diversity, separation and redundancy of safety provisions, and to increased attention to the qualification of safety equipment, particularly instrumentation and control (I&C). Of special importance is the need to ensure adequate robustness, under all conditions, of safety services and controls (including control centres)."

With regard to the practical elimination of significant radiological releases, the booklet states:

"Practical elimination of significant radioactive releases should be addressed in the design of new plants and can be applied to both prevention and mitigation safety measures."

"Practical elimination however, does not mean complete elimination or that events of significant releases are physically impossible, but rather that, with a high degree of confidence, such events have been demonstrated to be extremely unlikely. To date, there does not seem to be a common understanding of what that implies for reactor safety systems."

"The practical elimination concept is an approach that sets improved safety goals (or expectations) for nuclear installations by incorporating additional design features or, more rarely, operating provisions"

"… the practical elimination concept should specifically address challenges to containment performance; the last barrier to radioactive releases…"

"… accident conditions with significant radioactive releases are considered to have been practically eliminated:

- if it is physically impossible for the condition to occur; or
- if the condition can be considered with a high degree of confidence to be extremely unlikely to arise."

"… in the current implementation of DiD in some plants primarily by exposing the sensitivity of different levels of defence to the same hazard (the lack of independence, the inadequate design basis and the insufficient safety margins, which can result in a common mode failure. It is therefore important that features to deal with DECs, including severe accidents, are not depenedento n design elements which could have failed in the first three levels of DiD."

Observations are made in Chapter 3 with regard to the implementation of defense-in-depth in new and operating reactors:

"For new reactors, it is expected that DiD will be fully implemented as described in the IAEA's design requirements document SSR 2/1 or in the equivalent national standard.

For operating reactors, DiD is enhanced through ongoing regulatory oversight and through mechanisms such as periodic safety reviews (PSRs), plant-specific backfitting and feedback from operating experience."

Observations are also made in Chapter 3 with regard to consideration of defense-in-depth at multi-unit sites, and other nuclear facilities:

> "… concerns regarding multi-unit sites that are related to independence of the units. As such, DiD assessments should be carried out to determine the ability of each unit to function on its own…"
>
> "There are some key questions to be addressed as well regarding DiD implementation for multi-unit sites:
>
> - To what extent should each unit be autonomous?
> - What degree of sharing of SSCs, if any, should be permitted at multi-unit sites?"
>
> "The DiD concept can be useful for the nuclear fuel cycle facilities, research reactors and other nuclear facilities. … some of these sites may have been designed without the advantage of such a formal application of DiD. The practice varies from country to country, but some elements of DiD may have already been addressed (e.g. physical barriers and technical measures)."

Chapter 4 of the booklet addresses emergency arrangements and post-accident management off-site; specifically:

- Basis for emergency planning
- Decision making
- Countermeasures
- Communication
- Interactions with the recovery phase
- Interactions of authorities, response teams and other stakeholders

Key messages include:

> "Emergency preparedness should be based on a well trained system of response with timely and robust technical support, adequate procedures for radiation protection and countermeasures, and a smooth communication system for national and international use."
>
> "The roles and responsibilities of various decision makers should be clearly identified, and the structural aspects must be efficient and delegated appropriately down so as to enable rapid decisions … emergency arrangements should include clear guidance and initial criteria developed in advance for the establishment and cessation of countermeasures, ensuring processes to take full account of stakeholder concerns."

"… pre-accident planning and post-accident decision making for off-site responses may be more complicated than previously considered in emergency arrangements. More consideration of the risks from implementing protective countermeasures, particular to vulnerable groups, may thus be warranted."

"… communications must be understandable, clear, as up to date as possible, open and honest, and communicated using different channels understanding the possibilities and challenges of social media."

"… emergency arrangements have to take into account the information needs of foreign governments, overseas nuclear regulators and international organisations."

"… emergency arrangements normally have to include the ability to provide information:

- in English language;
- in real time;
- covering a wide range of topics concerning governmental decisions, including rationale and judgements."

"Recovery approaches need to be established as part of the pre-planning phase and must comprise considerable stakeholder input and involvement based on trusted relationships."

"… effective communication to promote common and appropriate understanding and balance among the various levels, noting that in some cases terms are used differently."

Chapter 5 of the booklet provides conclusions, some key ones include:

"Consideration of the accident has led to further work on DiD implementation, in particular on:

- reinforcing the need for independent effectiveness among the safety provisions for the various DiD levels, to the extent practical;
- emphasising the vital importance of ensuring that common cause and common mode failures, especially external events acting in combination, do not lead to breaches of safety provisions at several DiD levels;
- illustrating that greater attention is needed to reinforce prevention and mitigation at the various levels, particularly level 4;
- using the concept of practical elimination of sequences leading to significant radioactive releases;

- reinforcing the importance of assessments on the impact of human and organisational factors on DiD;
- providing useful insights into the issues associated with level 5 provisions (emergency arrangements) especially for long-term and multi-unit nuclear accidents, noting that the authorities and players involved are generally different."

"… areas where further work may be beneficial, such as on:

- the impact of human and organisational factors on DiD;
- improvements in the use of the DiD concept for new reactor designs, multi-unit sites, fuel cycle facilities and research reactors;
- the implementation of arrangements for level 5 of DiD;
- benchmarking and further harmonisation of the regulatory use of DiD through training, workshops and other means;
- the impact of new technologies."

8. OTHER AGENCY PERSPECTIVES ON DEFENSE-IN-DEPTH

On August 26 and 27, 2015, the Office on Nuclear Regulatory Research (RES) hosted an inter-agency workshop on defense-in-depth. The purpose of the workshop was to gain insights from other U.S. agencies on how defense-in-depth is used with regard to safety and security for the activities the other agencies are responsible for. The goal was to exchange information with the various agencies regarding how defense-in-depth is viewed and gain insights regarding the need for and the objective of defense-in-depth, the definition and scope of defense-in-depth; implementation approaches and challenges to defense-in-depth; the sufficiency or adequacy guidelines for defense-in-depth; and the relationship of risk analysis to defense-in-depth.

Agencies that participated in the workshop included the Nuclear Regulatory Commission, National Aeronautics and Space Administration (NASA), Federal Aviation Administration (FAA), Department of Energy (DOE), Naval Nuclear Propulsion Program, Department of Homeland Security (DHS), Department of the Interior (DOI) (Bureau of Safety and Environmental Evaluation), Army Corps of Engineers, and the Canadian Nuclear Safety Commission (CNSC).

8.1 Key Insights from Workshop

Key insights from the workshop include:

- Most agencies do not formally use the term “defense-in-depth” but many use similar concepts, or terms such as “resilience.”
- Defense-in-depth is an approach used to ensure the mission of each agency; e.g., public safety.
- Defense-in-depth is not the goal, but a tool that is used to achieve the mission.
- The amount of risk that is acceptable is dependent on the agency mission.
- Defense-in-depth implementation varies and is dependent on the actual missions of each agency.
- Defense-in-depth is achieved through implementation of a combination of design, operational and programmatic requirements.
- Quantitative risk goals to measure defense-in-depth may be difficult to develop.
- Relative risk estimates for comparison purposes are more credible than absolute quantification of risk.

- Prevention and mitigation are key principles of defense-in-depth, however, because of the agency mission, restoration (i.e., resilience) may also be a significant aspect of defense-in-depth.

- Design, operational and/or programmatic requirements are dependent on the phase of the mission; for example, whether you are building from the ground up (a new design) or working with an existing design.

- The balance between prevention and mitigation depends on the application.

- From a security perspective, it is not always possible to eliminate the risk (e.g., activity will occur).

8.2 Workshop Opening Remarks

Dr. Brian Sheron, former Director of the Office of Reactor Regulatory Research provided the following opening remarks.

> "Good morning, I welcome you to this workshop and thank you for taking the time to attend. I can tell from the diverse agencies attending that you each agree on the importance of this topic, defense-in-depth.
>
> Defense-in-depth is an essential element of all of our work to assure safe and secure functioning of the industries we regulate or the programs we conduct, whether associated with a nuclear power plant, medical devices, nuclear waste, a space craft, a nuclear submarine, a dam, or an oil rig. We are each challenged with ensuring safety and security and defense-in-depth plays a key role in the decisions we make.
>
> The Commission has asked the staff to provide insights regarding what constitutes defense-in-depth. And although this question can be answered at a conceptual level, not everyone agrees with how defense-in-depth is defined or should be implemented. For example, should defense-in-depth involve both prevention and mitigation, and if so, is there a way to determine what is the appropriate balance between the two? How do we determine whether we have adequate defense-in-depth; that is, how safe is safe enough? In responding to our Commission directive, the NRC is currently developing a report on how the NRC has addressed defense-in-depth over the years. This report will provide insights regarding, for example, the need for and the objective, definition and scope of defense-in-depth; implementation approaches and challenges to defense-in-depth; sufficiency or adequacy guidelines for defense-in-depth; and relationship of risk analysis to defense-in-depth. The goal of this effort is to identify whether further work needs to be done in answering the question of

whether we fully understand what defense-in-depth is, and we know how to implement it in a predictable and understandable manner.

We have invited you to participate in this workshop to gather your insights. I believe we each have similar concerns and questions that apply to our respective fields of interest, and that we can learn from each other. Through our discussions at this workshop we expect that we will mutually enhance our understanding of defense-in-depth and how we can better apply this philosophy in our decision-making.

Conceptually, we have a good understanding of defense-in-depth at the NRC. It is defined as an element in NRC's safety philosophy that is used to address uncertainty by employing successive measures, including safety margins, to prevent a malfunction or accident from occurring, or mitigate damage if a malfunction, an accident, or a naturally or intentionally caused event occurs. Consequently, over the past decades, the scope, range and prominence of defense-in-depth has grown. We have applied defense-in-depth principles to first preclude, to the extent practical through requiring highly reliable and redundant and diverse systems, events that challenge safety; secondly, even if an event occurs, we use defense-in-depth principles to provide for diverse and redundant systems that will mitigate the event and prevent it from leading to a more serious accident, in particular damage to the reactor core. Thirdly, even if core damage were to occur, ensure that there is a way to contain the radioactive material. And fourth, and finally, even if radioactivity cannot be contained, that emergency plans exist to protect the public (by this I mean evacuation plans).

However, historical experience has shown us that even with the good understanding, there is always the possibility, while hopefully very low, that there are initiators that we have not thought of that could lead to a serious accident. We recognize that, even with a mature nuclear power industry, potential safety and security issues will continue to emerge which we have to evaluate to ensure that we continue to have adequate protection and defense-in-depth. At the same time, risk analysis insights have become an increasingly important element of our decision-making. Risk insights enhance our efforts to more systematically and thoroughly identify potential vulnerabilities that we can protect against. But we have a fundamental challenge in determining whether we have adequate defense-in-depth. Our Commission has issue a Safety Goal Policy Statement, which basically defines how safe is safe enough by establishing acceptable levels of risk to the public from commercial nuclear power compared to the risk to the public from all other sources. In one sense, this approach answers the question “how safe is safe enough”? However, it does rely on an ability to quantify risk, and risk analysis is not an exact science. Moreover, the NRC also has a regulation, 10 CFR §50.109, often referred to as

the “Backfit Rule,” which requires that any new requirement that the NRC staff proposes to impose on an operating plant must result in a substantial improvement in safety and also be cost-beneficial. Implementing the Safety Goal Policy and the Backfit rule poses challenges to determining when there is sufficient defense-in-depth because both rely on an ability to quantitatively measure risk. And by definition, you cannot measure the risk of something that is not known. This is the challenge of assuring sufficient defense-in-depth versus quantitative safety goals.

So far, I have talked about defense-in-depth with regard to reactor power plant safety. Another aspect of NRC’s mission is the protection of the public health and safety from exposure to nuclear material and waste and from security-related events. In considering defense-in-depth with regard to materials and waste or security, as with reactor safety, we are faced with the same challenges. Defense-in-depth is needed to help ensure that the risk associated with materials and waste and the risk from malevolent behavior is maintained at an acceptably low level. However, we should acknowledge that we apply defense-in-depth in a graded approach depending on the complexity of the “facility” that uses nuclear material and the possible consequences of accidents. Consequently, for example, the amount of defense layers and associated protective measures varies.

There are a number of issues and challenges we face in determining whether we have adequate defense-in-depth:

- Do we need to adjust the balance between prevention and mitigation features within our defense-in-depth approach? Prevention has been emphasized historically to the extent that some claimed that serious accidents are so unlikely to occur that we do not need to do more in the mitigation area. Recent experience teaches us that we need to better account for low probability but high consequence accidents. So we ask ourselves, to what extent does defense-in-depth adequately address low probability and high consequence accidents? What are our respective roles in prevention versus our role with regard to mitigation? What does balance between prevention and mitigation mean? Can we quantify their impact in making determinations? What are the downsides to quantifying defense-in-depth?

- Can we ever determine that we have adequate defense-in-depth or is it a continuous quest? What role does risk analysis play in both identifying needed defense-in-depth and determining its adequacy?

- How is defense-in-depth for safety and security related? Should they be addressed separately or should they be addressed holistically? For

example, what about potential security measures that could have an adverse impact on safety and vice versa?

- Should defense-in-depth vary for different hazards and different facilities? Should the specific requirements for implementing defense-in-depth be general or be more application specific in addressing the different hazards?

- How are safety and security features (i.e., design and operational) determined for each layer of defense-in-depth? Should the principles be implemented across the layers of defense (e.g., can they be implemented separately for each layer)? For example: is diversity applied to a layer or should there be diversity among the layers? Is a "no single failure" criterion applied separately for each layer or across the layers?

These are just a few questions that merit discussion in looking at what constitutes defense-in-depth and how do we determine that we have adequate defense-in-depth. I think in sharing our ideas and experience, we can develop insights in resolving many of these significant issues.

I hope that by the end of the workshop we have learned from each other and have even agreed upon specific findings that can help guide us in the future in implementing effective and efficient defense-in-depth principles in our respective areas of interest. I greatly look forward to the proceedings of this workshop.

Thank you."

8.3 Workshop Presentations

The following presentations were made at the workshop:

- US NRC –Gary Holahan, Office of New Reactors
- US NRC – Mary Drouin, Office of Nuclear Regulatory Research
- US NRC – Joseph Rivers, Office of Nuclear Security and Incident Response
- US NRC – Dennis Damon, Office of Nuclear Material Safety and Safeguards
- CNSC – Doug Miller, Director of Regulatory Improvement and Major Projects Management
- NASA – Stephen Cash, Office of Safety and Mission Assurance
- NASA – Jesse Leitner Office of Safety and Mission Assurance
- NASA – Homayoon Dezfuli, Office of Safety and Mission Assurance

- US Naval Reactors – Thomas Roberts, Nuclear Propulsion Program
- FAA – Roberto Ortiz, National Airspace System
- DOI – Michael Else, Bureau of Safety Evaluation and Enforcement
- DHS – Michael Norman, Infrastructure Information Collection Division, National Protection and Programs Directorate
- DOE – Richard Donovan, Office of Enterprise Assessments
- DOE – James O'Brien, Office of Nuclear Safety
- Army Corp of Engineers – Susan Durden

9. OBSERVATIONS FROM A HISTORICAL REVIEW OF DEFENSE-IN-DEPTH

This section provides observations on defense-in-depth derived from a historical review of the literature where defense-in-depth is addressed, whether explicitly or implicitly. In providing observations (i.e., insights) based on a historical review of the literature that references defense-in-depth, either explicitly or implicitly, it is important to understand what this term is trying to express. In simple, plain English, defense-in-depth is meant to convey that there are in-depth (i.e., comprehensive, thorough) defenses (e.g., guards, barriers) that are incorporated into the design and operation of a facility to address the danger or threat associated with the handling of nuclear material. Consequently, the review of the literature focused on how the design and operation of activities associated with the use of nuclear materials provided comprehensive or thorough protections that were either denoted as defense-in-depth explicitly or expressed the concept of defense-in-depth implicitly. The concept was considered to be expressed implicitly if the discussion referred, at a minimum, to one of the following:

- Existence of multiple barriers
- Existence of levels or layers of defense
- Provisions for appropriate safety margins
- Provisions for accident prevention and mitigation capability
- Assurance that key safety functions are not dependent upon a single element of design, construction, maintenance or operation
- Provisions for appropriate barrier capability
- Assurance that regulated activities are carried out at locations that facilitate the protection of public health and safety.

In reviewing the literature, another challenge in providing insights was the different use in terminology, particularly in understanding the similarities and differences in perspectives on defense-in-depth. The terminology in the literature can significantly vary, and therefore, it can be difficult to determine whether apparent differences in perspectives are real differences, or are actually similar perspectives using different terminology. Therefore, to better understand statements about defense-in-depth, discussions and declarations (i.e., views) were summarized and grouped based on which of several questions about defense-in-depth they appeared to answer. This approach allows providing observations about similarities versus differences in perspectives.

The questions posed to help group the observations included the following:

- What is the definition of defense-in-depth?
- Why is defense-in-depth needed? That is, what is the purpose of defense-in-depth?
- What is defense-in-depth attempting to achieve? What is the objective or goal of defense-in-depth?
- What is the approach or framework used to achieve the objective of defense-in-depth?
- What are the strategies or protective measures used to implement or execute the defense-in-depth approach?
- How is it determined if there is adequate defense-in-depth?
- What are the principles, or the basic ideas behind the measures that implement the approach used to accomplish the goal of defense-in-depth?

After initial observations are first provided regarding the definition of defense-in-depth, the observations presented below are organized as follows:

- defense-in-depth for US reactors
- defense-in-depth for US non-reactor applications
- defense-in-depth aspects of US security
- international perspectives on defense-in-depth
- other US agency perspectives on defense-in-depth

Overall observations, regardless whether from reactor safety, international community, security, other agencies, are provided at the end of this section.

9.1 Definition of Defense-in-Depth

In the literature, despite the long history and the numerous places where defense-in-depth is discussed at length; there are only a few places where defense-in-depth is actually defined; that is, a definition is provided rather than a discussion or description. These include:

- NRC Glossary [NRC, 2014b]
- NRC Strategic Plan [NRC, 2012d]

- NUREG-1860 [NRC, 2007b]
- *Federal Register* Notice (FRN) on Final Rule for 10 CFR §50.69 [NRC, 2012c]
- Commission White Paper [NRC, 1999a]
- 10 CFR §70.64

The definitions include the following:

NRC Glossary (current): "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."

NRC Strategic Plan (2008-2013): "An element of the NRC's safety philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility. The NRC's safety philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well conceived and will work. Moreover, the philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility."

NUREG-1860 (2007): "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."

Commission White Paper (1999): "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."

FRN on Final Rule for 10 CFR §50.69: "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."

10 CFR §70.64: "Defense-in-depth practices means a design philosophy, applied from 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."

In reviewing these definitions, the following observations can be made:

- Almost all the definitions agree that defense-in-depth employs "successive measures;" however, some are specific in defining successive compensatory measures. Compensatory' is used to denote that each successive measure is designed to compensate for the failure of the previous measure. This concept does appear in another definition, but instead of using "successive compensatory measures," it defines defense-in-depth as "multiple lines of defense." Moreover, two of the definitions include safety margins as part of the successive measures.

- All the definitions agree that defense-in-depth involves both prevention and mitigation. Some of the definitions are more high level in that they just specify prevention and mitigation of "accidents" while others specify prevention and mitigation of malfunction of equipment, accidents and naturally caused events.

- All of the definitions, but one, indicate that defense-in-depth is a philosophy.

- A little over half of the definitions indicate that safety will not be wholly dependent on any single element and that defense-in-depth will ensure the facility (or system) will be more tolerant of failures.

- One definition includes redundancy as part of its definition.

To better understand how defense-in-depth has been characterized and integrated into the NRC regulatory structure, it is best to separate insights from defense-in-depth and reactor safety, from non-reactor safety and from security, and to decompose the observations into purpose, objective, approach, strategy, etc.

9.2 Observations Regarding US Reactor Defense-in-Depth

This section focuses on providing observations derived reviewing the rich history of defense-in-depth as related to reactor safety.

9.2.1 Purpose of Defense-in-Depth

In reviewing the various sources regarding the purpose of defense-in-depth, or why there is a need for defense-in-depth, the following statements, as related to reactor safety, are found:

- Means to reduce both the risk and the uncertainty.
- The aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression.
- Safety assurance in areas not treated or poorly treated.
- Proper role of defense-in-depth as compensation for ... uncertainties.
- Defense-in-depth measures are those that are applied ... to reduce uncertainties.
- Provide for a framework to address uncertainties.
- A design and operational strategy for dealing with uncertainty.
- Defense-in-depth is a form of uncertainty analysis.
- A strategy to ensure public safety given there exists ... uncertainty.
- Defense-in-depth shall be provided ... for events that have a high degree of uncertainty.
- Defense-in-depth opportunities are considered to compensate for unacceptable risk uncertainty.
- Addresses the expected as well as the unexpected.
- 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 type and magnitude of challenges to safety).
- Deliver a design that is tolerant to uncertainties in knowledge.
- To compensate for the recognized lack of knowledge of nuclear reactor operations and the consequences of potential accidents.

The above are statements in the literature that explicitly relate defense-in-depth to uncertainties. However, there are numerous places where defense-in-depth is implicitly related to uncertainties. Example statements include:

- However excellent the design and execution, and however comprehensive the quality assurance, they must be acknowledged to be imperfect.

- The principle of guarding against unwanted events.

This theme of defense-in-depth compensating for uncertainty is found throughout the literature, in recognition that our knowledge regarding the design or quality of the plant's SSCs is imperfect, that is, uncertain. Therefore, there is a need for defense-in-depth, e.g., multiple layers of defense, no reliance on a single element of the design, etc. (as discussed in the following sections).

There is general agreement that defense-in-depth is needed to compensate for uncertainties. These uncertainties can be uncertainties regarding the basic design and operation of the facility, uncertainties regarding knowledge in the performance of structures, systems and components (SSCs) and operator actions under various facility conditions, uncertainties regarding various phenomena, uncertainties how an adverse event may impact the plant (e.g., accident progression), etc.

To ensure the risk is acceptably low, there must be a recognition that our understanding of events (e.g., performance of SSCs, occurrences and impact of hazards) is not complete, and our knowledge of events that could occur may be lacking.

The uncertainties to be dealt with by defense-in-depth involve both the expected and unexpected. The expected includes the uncertainty for events[3] that are known or anticipated to potentially occur, but whose characteristics and impacts are to some extent uncertain. For example, accident scenarios including a fire may be anticipated, however, there is uncertainty regarding the magnitude of the fire, and there is also uncertainty regarding the impact of the fire on equipment. These uncertainties can be compensated by defense-in-depth provisions like diversity and conservative design based on conservative assumptions about the scenarios.

The unexpected includes those events that are unanticipated because of lack of knowledge, and therefore, may not be addressed directly in any form in the design or operation of the facility. These uncertainties are more challenging to compensate for because they are not expected, and yet they have occurred. For example, in the 1979 Three Mile Island accident the combined series of events leading to the accident was completely unexpected: a stuck open relief valve, but with instruments showing the valve was closed, led to (inadvertent) detrimental operator actions and resulted in a core melt accident. However, the defense-in-depth measure

[3] Events may include the performance (e.g., reliability) of a SSC under normal or adverse conditions (e.g., high temperature); the occurrence of a phenomena and its impact on SSCs.

of multiple barriers, which included a conservatively designed containment, prevented a significant radioactive release from occurring.

9.2.2 Objectives of Defense-in-Depth

As noted above, there is general agreement that defense-in-depth is needed to ensure the risk of reactor operation is acceptably low in spite of uncertainties. The next question is whether there is agreement regarding the objective of defense-in-depth; that is, agreement on what defense-in-depth is attempting to accomplish. In reviewing the various literature sources regarding the objective of defense-in-depth, the following statements are found:

- To achieve an adequate level of safety for nuclear power plants is generally recognized to require defense-in-depth.

- The prevention of exposure of people to this radioactivity ... can be achieved ... by the use of the concept of defense-in-depth.

- [To ensure that] The probability of an accident occurring is very small.

- To protect the plant, the plant operators, and the health and safety of the public by application of a ‘defense-in-depth” design philosophy.

- Defense-in-depth concept associated with its accident prevention and mitigation philosophy.

- Defense-in-depth approach ... to ensure the protection of public health and safety.

- A defense-in-depth approach ... to prevent accident ... and to mitigate their consequences.

- To prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs.

- Incorporating defense-in-depth ... is that the facility ... tends to be more tolerant of failures and external challenges.

- 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 identify, prevent or mitigate accidents.

- Providing design feature to achieve acceptable risk.

- Be developed that establishes an approach ... [that provides for] ... balance between prevention and mitigation.

- Defense-in-depth principles that the design provides accident prevention and mitigation capability.

- An approach ... that prevents and mitigates accidents.

With respect to the objective of defense-in-depth as characterized in the literature, there appears to be general agreement that the aim of defense-in-depth is to avert or minimize damage to the plant and thus protect the public from harm. More importantly, there is general agreement that averting or minimizing damage is realized by preventing and mitigating accidents. Consequently, the objective of defense-in-depth is meant to ensure that the public is protected from harm by employing protections instrumental for both preventing and mitigating accidents.

9.2.3 Approach for Achieving Defense-in-Depth

In reviewing the various sources regarding the approach to achieve the purpose and objective of defense-in-depth, the following statements are found:

- 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.

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

- 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 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 barriers to the escape of nuclear radioactive material.

- 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.

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

- Defense-in-depth … 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.

- 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.

- 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.

- Defense-in-depth 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 core damage frequency (CDF) and large early release frequency (LERF) goals.

- 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).

- 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.

- 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.

- Defense-in-depth … 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).

- Defense-in-depth … 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…"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.

Regarding the approach for achieving defense-in-depth, there is agreement in the literature that defense-in-depth is comprised of multiple layers of defense. This concept is described using different terminology; for example, layers of defense, lines of defense, echelons of defense, protective barriers, and successive measures. Moreover, there is also agreement that the layers are generally meant to provide accident protection (first by prevention, and failing that by mitigation) in a successive or consecutive manner such that if one layer fails, the next layer is meant to alleviate the failure of the previous layer, and so on, so that all the layers must fail before significant consequences will occur. Accordingly, the approach used for achieving defense-in-depth is one of multiple layers of defense incorporated into the design and operation of the facility and these multiple layers address both prevention and mitigation.

However, there are differences in the literature on the makeup of these layers, and the number of layers. Two broadly differing views regarding the layers of defense are the following: One view is that the multiple layers are actual physical barriers; this view is an early characterization of defense-in-depth. These physical barriers were generally viewed to be the fuel element cladding, the reactor vessel, and the containment. This view of barriers is more focused on mitigation and rather than prevention. In later views, the layers came to be more functional in nature, and not limited to physical barriers. The layers address both prevention and mitigation and generally involve measures to prevent an adverse event from occurring, and mitigating the consequences if the event were to occur.

As noted above, there is not agreement in the number of layers of defense. They vary from two layers, prevention and mitigation, to five layers:

There is one proposal in the literature for a two layer structure which includes:

1. prevent accidents and
2. limit the consequences and prevent evolution to more serious conditions.

These two layers appear to be more like principles rather than specific layers of defense.

There are four different proposals in the literature for a three layer structure:

1. (a) prevention of accidents,
   (b) protective systems to take corrective actions, and
   (c) engineered safety features to mitigate the consequences.

2. (a) prevent initiation of incidents,
   (b) capability to detect and terminate incidents, and
   (c) protecting the public.

3. (a) protections to prevent accidents from occurring,
   (b) mitigation of accidents if they occur, and
   (c) emergency preparedness to minimize the public health consequences of releases if they occur.

4. (a) superior quality in design, construction and operation,
   (b) accident prevention safety systems, and
   (c) consequences-limiting safety systems.

These four different descriptions of the layers of defense are similar in concept, some are just more specific in identifying how to accomplish the layer while others are more functional in what needs to be accomplished by the layer. For example,

- The first three proposals all specify the first layer as prevention, while the last proposal is specifying more how to accomplish prevention.

- For the second layer, the first proposal is prescribing the capability to detect and terminate incidents as in the second layer for the second proposal. In this regard, the second layer in the first two proposals is similar. For the last two proposals, their descriptions for the second layers are simply stating what the first two proposals are trying to accomplish.

- For the third layer, a resemblance can be seen in the four different descriptions of the layers of defense by each proposal. Engineered safety features to mitigate the consequences and

consequences-limiting safety systems are mechanisms for protecting the public, which is similar in concept to having emergency preparedness to minimize the public health consequences of release, if they occur.

- These different layer descriptions provide a good illustration of similar concepts, which nevertheless have distinct differences. In the last proposal, superior quality in design, construction and operation describes an approach or means to achieve prevention, while in the other references the definition of the layer is a functional description and does not prescribe the means for accomplishing the function. For some of these layers, the reference does include discussions on how to achieve each layer, while other documents just define, as above, the layers.

There are two proposals in the literature that define five layer structures:

1. (a) accident prevention,
   (b) safety systems,
   (c) containment,
   (d) accident management, and
   (e) siting and emergency plans.

2. (a) physical protection against intentional acts,
   (b) stable operations to limit the frequency of events,
   (c) protective systems to mitigate initiating events and are both reliable and capable to prevent and mitigate,
   (d) barrier integrity to ensure adequate barriers to protect from accidental radionuclide release, and
   (e) protective actions to protect public should radionuclides penetrate the barriers.

Similar observations can be made for the five layers of defense structures as were made for the three layer structures. However, for the five layer structures the layers all tend to be described functionally and the structures do not provide descriptive means for accomplishing the layers. As with the three layers, the different proposal may or may not include discussions on how to achieve each layer. Whether three or five layers are proposed, they include both prevention and mitigation.

9.2.4 Strategies for Implementing Defense-in-Depth

In reviewing the various sources regarding the strategies used to implement the approach to achieve the purpose and objective of defense-in-depth, the following statements are found:

- 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 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.

- 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.

- 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 various strategies found in the literature can be classified as either principles or protective measures (design, operational or programmatic features). The principles and protective measures are used to implement the various layers of defense. The difference between the principles and protective measure is that the principles generally define "what" is needed to ensure there is defense-in-depth, while the protective measures generally identify the actual design or operational feature that is used to accomplish the principle.

An example can include:

- The principle may be highly reliable structures, systems and components, and the associated protective measures may include quality controls in fabrication, inspection and testing, and prompt and thorough investigation and correction of failures or malfunctions.

Two other observations can be made in reviewing the literature with regard to principles and protective measures:

- Many of the principles and protective measures discussed in the literature are similar, such as redundancy, independence, diversity, no reliance on a single element.

- Many of the principles and protective measures are applicable to more than a single layer of defense.

9.2.5 Criteria Determining Defense-in-Depth Adequacy

Most of the literature does not include any discussion regarding criteria or guidance for determining the adequacy of defense-in-depth. However, there are a few statements that, while not specific, do relate to defense-in-depth adequacy.

Regarding the criteria used to determine 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 (approach to defense-in-depth) 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.

- 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.

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

9.3 Observations Regarding Non-Reactor Areas Defense-in-Depth

The literature on defense-in-depth for non-reactor nuclear areas (facilities and activities) is not as extensive as for reactors. While there are some sources that provide a discussion on the purpose, objectives approach and strategies of defense-in-depth, the majority of information is found in regulations that relate to defense-in-depth. In the write up below, observations are derived from looking both at the regulations and specific sources as noted with regard to defense-in-depth.

9.3.1 Purpose and Objectives of Defense-in-Depth

As already noted, the literature on defense-in-depth for non-reactor applications is considerably more limited than that for reactors. As a result it is more difficult to parse the available sources finely enough to distinguish between statements related to purpose and those related to objective. The statements below refer to one or the other or both.

- 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.

- Defense-in-depth for protecting the public and the environment from high-level waste (HLW) repositories is both a technical and a policy issue.

- Invoked primarily as a strategy to ensure public safety given the unquantified uncertainty in risk assessments.

- Concept for repositories should be targeted more towards protecting resources where there are high uncertainties…

- Relates to the characteristics of the system to (1) not rely on any single element of the system and (2) be more robust to challenges.

- Assures that if any component fails, the rest of the system compensates, so consequences are not unacceptable.

- 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).

- Guards against over-reliance on any one safety feature.

- An element of NRC's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs.

- Defense-in-depth and safety margins are both concepts that are used to address the impact of uncertainty on safe design and performance.

- Provide for multiple lines of defense, where necessary, to address uncertainties.

- The regulations assure that the risk from device failure is acceptably low.

- Due to the wide variety of licensed materials uses, there is not a common understanding of the terms risk-informed, performance-based, and defense-in-depth within NRC or with these licensees.

- The location of regulated activities at sites that facilitate the protection of public health and safety.

- Regulation embodies redundancy and diversity.

- The defense-in-depth ... provides an important tool for making regulatory decisions with regard to complex facilities, in the face of large uncertainties.

- The Commission believes that a repository system should reflect the philosophy of defense-in-depth.

- Facility and system design and facility layout must be based on defense-in-depth practices.

- Defense-in-depth practices ... 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.

- Defense-in-depth is applied in regulation of fuel cycle facilities consistent with Commission guidance.

- Defense-in-depth principles for the chemical process safety design are those that support a hierarchy of controls: prevention, mitigation, and operator intervention, in order of preference.

- Defense-in-depth measures are generally decided upon using deterministic considerations (i.e., engineering judgment) regarding the importance of the safety function and the potential uncertainties that could affect its performance.

The various statements stress that the purpose and objective of defense-in-depth, just as in the reactor area, is to assure safety. Further, most of the statements acknowledge the importance of prevention and mitigation in protecting public health and safety, and the environment. As can be inferred from the Commission White Paper on Risk-Informed and Performance-Based Regulation, some of the same defense-in-depth concepts used in the reactor area are applied to specific non-reactor areas like the waste repository. Many of the regulations cited incorporate various defense-in-depth principles in framing requirements for performance of specific facilities or devices.

9.3.2 Approach and Strategies of Defense-in-Depth

Again, because the literature on defense-in-depth for non-reactor applications is considerably more limited than that for reactors it is difficult to distinguish between statements related to defense-in-depth approach and defense-in-depth strategies in the available sources. The statements below refer to one or the other or both.

- For waste disposal facilities, defense-in-depth is implemented through … multiple barriers. For transportation and processing facilities, PRA methods similar to those applied to reactors can be used … For industrial and medical applications, … defense-in-depth can be minimal…

- 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.

- Structuralist and rationalist approach to defense-in-depth. Regarding the structuralist approach, 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.

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

- Defense-in-depth may be provided by additional barriers, operating procedures, and limits, or by redundant and diverse equipment design.

- Defense-in-depth can be achieved by a variety of different measures such as passive containment systems (e.g., multiple barriers), active systems (e.g., ventilation systems), and administrative procedures.

- The extent of defense-in-depth can vary depending on the nature of the risk and/or uncertainty.

- Risk information can only provide defense-in-depth insights on the known uncertainties. However, risk information cannot provide defense-in-depth insights on the unknowns.

- It is generally assumed that if the current regulations are met, there is adequate defense-in-depth.

- A system of defense-in-depth considerations that include physical barriers, engineered safeguards, access controls, and administrative and procedural controls designed to protect workers and members of the public from potentially significant exposure.

- Ensure safety of its licensed facilities through requirements for multiple, independent barriers, and, where possible, redundant safety systems...

- The degree to which multiple IROFS [items relied on for safety] or systems of IROFS must fail before the undesired consequences (e.g., criticality, chemical release) can result.

- Provided by specifying redundant IROFS that perform the same essential safety function.

- Diversity is the degree to which IROFS that perform different safety functions provide defense-in-depth.

- Used to provide one or more additional measures to back up the front line safety measures, to provide additional assurance that key safety functions will be accomplished.

- Multiple barriers to release of radioactive materials.

- Use of conservative codes and standards in the design to ensure an adequate safety margin.

- Requirements involve redundancy.

- Provision of barriers against release and assurance of high quality in design, construction, and operation.

Based on the statements found in different sources, the approach of defense-in-depth in the non-reactor areas is generally based on the provision of multiple barriers and the adoption of redundancy and diversity, which are themselves defense-in-depth principles. Compared to the reactor literature, there is no discussion about the existence or distinction between various levels of defense, with the exception of the mention of the need for both prevention and mitigation. With some allowances where references to similarities with reactor defense-in-depth are made, the emphasis of defense-in-depth for non-reactor areas is on the use of multiple barriers rather than more general means found for reactors, such as operational aspects, emergency planning, etc.

9.4 Observations Regarding Security Defense-in-Depth

There are very limited references to security in the literature. Security references related to defense-in-depth statements are contained mainly in the regulations and consists of requirements for physical barriers and redundancy and diversity of controls and communication systems to maintain effective monitoring. The statements below are typical.

- Requirements for portable gauges involve redundancy and diversity.

- Security zones for byproduct materials require continuous physical barriers to prevent unauthorized access.

- Have backup power... to maintain continuous monitoring and detection capability.

- Have two independent physical controls that form tangible barriers to prevent unauthorized removal.

- Physical protection during shipment requires redundant communications between the carrier and the escort vehicle.

- Physical protection of special strategic nuclear material in transit requires multiple escorts and escort vehicles.

- Physical protection at fixed sites requires that access to vital equipment and materials requires passage through at least three physical barriers and the outer perimeter is provided with two separated physical barriers with an intrusion detection system between them.

- Physical protection of licensed activity requires multiple physical barriers.

- Protection of digital computer and communication systems requires defense-in-depth strategies against cyber attacks.

- Physical protection for reactors requires defense-in-depth strategies to ensure effectiveness.

- Requirements for nuclear power plant safeguards and contingency plans explicitly identify defense-in-depth for both physical protective systems and protective strategies.

Although not explicit, the concepts of defense-in-depth for security are in places similar to those seen for reactor safety and materials and waste, but use very different terminology. For example, their objective is to advert and minimize damage, they rely on a multiple barrier approach, and use protective "strategies" (or measures) as part of their physical protection. Similar principles such as redundancy and independence can also be found in the defense-in-depth implementation.

9.5 Observations Regarding International Defense-in-Depth

The international literature surveyed for statements on defense-in-depth was almost exclusively focused on power reactor defense-in-depth. The observations made above for US reactors generally apply to the international literature as well. The international literature is mostly focused on the approach and strategies of defense-in-depth, with rather fewer high-level statements about purpose and objective.

9.5.1 Purpose of Defense-in-Depth

In reviewing the international literature, only one statement that is related to the purpose of defense-in-depth could be found.

- To compensate for potential human and mechanical failures, a defense-in-depth concept is implemented…

Although not explicit, it can be inferred from realizing the need to compensate for failures, is the recognition that the design and operation cannot prevent failures because of a lack of knowledge.

9.5.2 Objective of Defense-in-Depth

In reviewing the international literature, similar objectives to those described in the NRC literature are seen. There is general agreement that the aim of defense-in-depth is to avert or minimize risk by preventing or mitigating accidents. The following statements are found:

- 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.

- 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.

- The defense-in-depth concept shall be applied to ... prevent consequences of accidents that could lead to harmful effects on people and the environment, and ensure 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.

- 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...

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

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

There is general agreement in the international perspectives that the objective of defense-in-depth is to prevent and mitigate accidents.

9.5.3 Approach for Achieving Defense-in-Depth

In reviewing the international sources, the approach described for defense-in-depth is similar to that described in the NRC literature. The approach is to employ multiple layers of defense as shown below.

- 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 defense-in-depth and it is repeatedly used in the specific safety principles that follow.

- The primary means of preventing and mitigating the consequences of accidents is 'defense-in-depth'. Defense-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.

- 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.

- 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:

  - Prevention of abnormal operation and system failures,

  - Control of abnormal operation and detection of failures,

  - Control of accident within the design basis,

  - Control of severe conditions including prevention of accident progression and mitigation of the consequences of a severe accident, and

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

- 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.

- There are five levels of defense:

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

  - The purpose of the second level of defense 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 defense, 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 defense is to mitigate the consequences of accidents that result from failure of the third level of defense-in-depth...

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

- Concept of defense-in-depth involves different, multiple barriers.

- Prevention and mitigation are both essential.

In the international perspectives, a similar approach of defining layers of defense is used. However, they define the layers more to design concepts rather than to how the accident may progress if it was to occur.

9.5.4 Strategies for Implementing Defense-in-Depth

In reviewing the international sources, strategies (protective measures or principles) are identified for implementing the various layers of defense. The strategies suggested include the following:

- 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.

- Defense-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, and
    - An appropriate combination of inherent and engineered safety features.
  - Comprehensive operational procedures and practices as well as accident management procedures.
- A line of protection (LOP) is an effective defense against a given mechanism or event that has the potential to impair a fundamental safety function. This term 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." (Lines of protection are the procedural, qualitative, and physical means by which each level of defense is maintained. These are sometimes referred to as provisions, which may be fundamental design characteristics of the plant.)
- 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 defense-in-depth. 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 defense-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.
- The design:
  - Shall provide for multiple physical barriers to the release of radioactive material to the environment.

- 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.

- Shall provide for the control of plant behavior 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.

- 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.

- 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.

- 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.

Similar strategies can be found such as quality assurance (high quality), safety margins, diversity, redundancy, and conservatism.

9.5.5 Criteria Determining Defense-in-Depth Adequacy

In reviewing the international literature, there are statement with regards to determining adequacy of defense-in-depth. However, like the NRC sources, there are only general statements with no specific criteria for determining the adequacy of defense-in-depth.

- The existence of several levels of defense-in-depth is never justification for continued operation in the absence of one level.

- 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.

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

- When properly implemented, defense-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 defense is a necessary element 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 defense-in-depth, shall remain under the overall frequency-consequence curve.

- Based on the concept from IAEA INSAG 12: "All safety activities, whether organizational, behavioral or equipment related, are subject to layers of overlapping provisions, so that if a failure occurs it would be compensated for or corrected without causing harm to individuals or the public at large," the claim is that quantities calculated in PRA can be linked to specific levels of defense-in-depth, as defined in INSAG 12 and other IAEA publications.

In the international literature, determining the adequacy of defense-in-depth still remains a challenge. There is little to no criteria or guidance for determining the adequacy of defense-in-depth beyond general statements.

9.6 Observations from Other Agencies Regarding Defense-in-Depth

Based on the August 26 and 27, 2015 inter-agency workshop on defense-in-depth held by the Office on Nuclear Regulatory Research (RES), the following observations were made:

- Most agencies do not formally use the term “defense-in-depth” but many use similar concepts, or terms such as “resilience.”

- Defense-in-depth is an approach used to ensure the mission of each agency; e.g., public safety.

- Defense-in-depth is not the goal, but a tool that is used to achieve the mission.

- The amount of risk that is acceptable is dependent on the agency mission.

- Defense-in-depth implementation varies and is dependent on the actual missions of each agency.

- Defense-in-depth is achieved through implementation of a combination of design, operational and programmatic requirements.

- Quantitative risk goals to measure defense-in-depth may be difficult to develop.

- Relative risk estimates for comparison purposes are more credible than absolute quantification of risk.

- Prevention and mitigation are key principles of defense-in-depth, however, because of the agency mission, restoration (i.e., resilience) may also be a significant aspect of defense-in-depth.

- Design, operational and/or programmatic requirements are dependent on the phase of the mission; for example, whether you are building from the ground up (a new design) or working with an existing design.

- The balance between prevention and mitigation depends on the application.

- From a security perspective, it is not always possible to eliminate the risk (e.g., activity will occur).

From the various presentations, it can be gleaned that other agencies view defense-in-depth in a similar light. For example, there are uncertainties, and because of these uncertainties, the design and operation must consider both prevention and mitigation of potential adverse events. This consideration is implemented by identifying multiple layers of defense and providing for specific measures to accomplish the specific layers. However, like the NRC, how to determine or measure the adequacy of defense-in-depth is still a challenge.

9.7 Overall Observations on Characterization of Defense-in-Depth

In performing a historical review of defense-in-depth and providing observations based on the review regarding the purpose, goal, strategy, structure and definition, overall perspectives can be drawn regarding how defense-in-depth can be characterized.

- The purpose of defense-in-depth is to ensure that the risk of the regulated activity remains acceptably low regardless of lack of knowledge.

- The goal of defense-in-depth is to ensure that the public is protected from harm by preventing and mitigating accidents.

- The approach used for achieving defense-in-depth is to have multiple layers of defense incorporated into the design and operation of the regulated activities and to have these multiple layers address both prevention and mitigation.

- The actual layers are dependent on the posed threat.

- The actual protective measures (i.e., design, operational or programmatic features) that are used to achieve each layer of defense are dependent on both the layer of defense and the actual threat (reactor core versus a medical device).

- There is almost no guidance on criteria for determining adequacy of defense-in-depth. The literature does suggest that the elements (e.g., layer of defense) should be quantified, that risk can be used to assess each defense system (e.g., safety measure), that compensatory measures can be graded in order to reduce risk, that any sequence (given all defense layers have failed) remain under a frequency consequence curve, that redundancy and diversity is sufficient to ensure risk guidelines are met, and that the adequacy of defense-in-depth can be assessed via a process that uses measures of risk.

- Principles are developed to help guide implementation of defense-in-depth. The principles define what defense-in-depth is to achieve for the subject regulated activity (i.e., goals). Overall, defense-in-depth should ensure that each regulated activity has appropriate defense-in-depth measures (i.e., design, operational and administrative features) for prevention and mitigation of adverse events and accidents. For prevention, defense-in-depth principles could include: acceptable reliability and availability of equipment and human actions; design, operational and administrative features to prevent and/or respond to unacceptable equipment failures, human errors, natural phenomena and malicious acts; and safety and security not dependent upon a single element of design, construction, maintenance or operation. For mitigation, principles could include: design, operational and administrative features to contain unacceptable releases of radioactive material; design, operational, administrative features and response capability to limit exposure to radiation and/or radioactive materials to acceptable levels.

These observations can be captured in a generic framework on defense-in-depth, as illustrated in Figure 9-1.

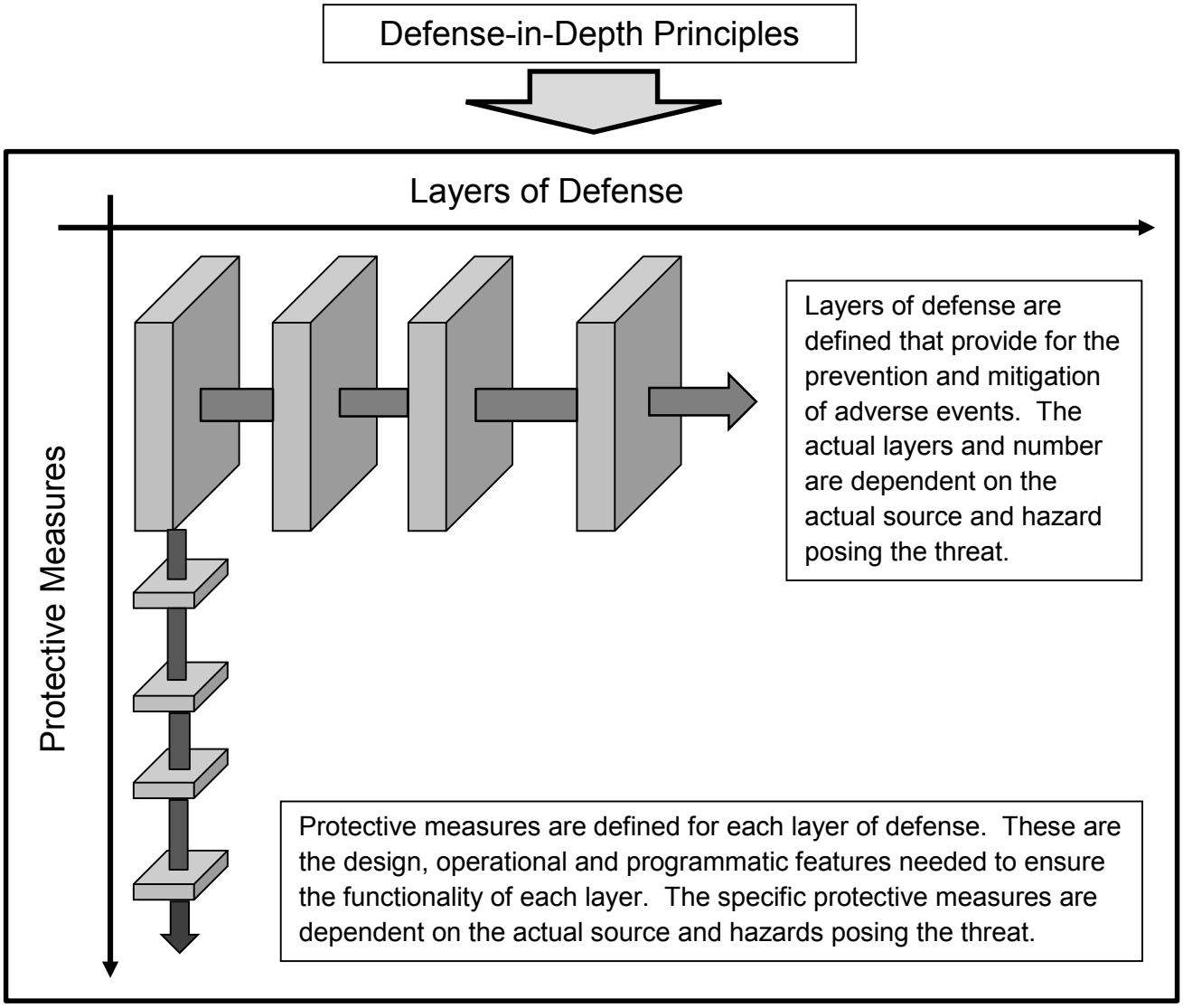

Figure 9-1 Defense-in-Depth Framework

- Regardless of the application, there are layers of defense-in-depth that provide for prevention and mitigation of the adverse event; however the actual layers and number of layers are dependent on the threat being averted.

- For each defense layer there are protective measures (i.e., design, operational and programmatic features) that serve to prevent and mitigate the adverse event. The actual measures are dependent on the threat being adverted.

- The layers of defense and their associated protective measures are guided by a set of principles.

10. REFERENCES

[ACRS] Advisory Committee on Reactor Safeguards letters: http://www.nrc.gov/reading-rm/doc-collections/acrs/letters/

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

[ACRS, 1999] Powers, D.A., ACRS letter to USNRC Chairman Jackson, "The Role of Defense in Depth in a Risk-Informed Regulatory System," May 19, 1999. (ADAMS Accession No. ML091280427)

[ACRS, 2000a] Advisory Committee on Reactor Safeguards, Advisory Committee on Nuclear Waste Meeting of the Joint ACRS/ACNW Subcommittee, January 13-14, 2000. (ADAMS Accession No. ML003678181 and ML003678024)

[ACRS, 2000b] 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. (ADAMS Accession No. ML003719182)

[AEC, 1956] U.S. Atomic Energy Commission, Letter to Senator Hickenlooper, March 14, 1956.

[AEC, 1957] 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.

[AEC, 1973] U.S. Atomic Energy Commission "The Safety of Nuclear Power Reactors and Related Facilities," WASH-1250, March 1973. (ADAMS Accession No. ML12143A280)

[AEC, 1971a] U.S. Atomic Energy Commission, Letter to Senator Pastore, Chairman of the Joint Committee on Atomic Energy, April 27, 1971.

[AEC, 1971b] U.S. Atomic Energy Commission, Public Rulemaking Hearings on Interim Acceptance Criteria for Emergency Core Cooling Systems (ECCS) for Light Water Power Reactors, December 28, 1971.

[ANS, 1999] 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.

[ANSI/ANS, 1998] American Nuclear Society, "Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors," September 9, 1998.

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

[CFR] Code of Federal Regulations, Title 10, Energy, Parts 1-50 and 51-99, Nuclear Regulatory Commission, Office of the Federal Register, National Archives and record Administration.

[Fleming, 2002] 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, Pages 205-225.

[FRN, 1983] *Federal Register* Notice, "Disposal of High-level Radioactive Wastes in Geologic Repositories Technical Criteria," Final Rule, Volume 48, Page 28194, June 21, 1983.

[FRN, 2000] *Federal Register* Notice, "Disposal of High-Level Radioactive Wastes in a Proposed Geologic Repository at Yucca Mountain, Nevada; Final Rule," Volume 66, No. 213, Page 55732 Nov 2, 2001

[IAEA, 1996a] International Nuclear Safety Advisory Group (INSAG), "Basic Safety Principles for Nuclear Power Plants," INSAG-3, International Atomic Energy Agency, Vienna, Austria, 1996.

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

[IAEA, 1996c] IAEA, "Basic Safety Principles for Nuclear Power Plants," INSAG- 12, International Atomic Energy Agency, Vienna, Austria, 1996.

[IAEA, 2005] IAEA, "Assessment of Defence in Depth for Nuclear Power Plants," Safety Reports Series No. 46, Vienna, Austria, February 2005.

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

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

[IAEA, 2009] IAEA Nuclear Energy Series, "Design Features to Achieve Defence in Depth in Small and Medium Sized Reactors," NP-T-2.2, June 2009.

[IAEA, 2011] IAEA, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities," INFCIRC/225/Revision 5, Nuclear Security Series, No. 13, Vienna, Austria, January 2011.

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

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

[JCAE, 1967] 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.

[JCAE, 1969] 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.

[NEA, 2014] Nuclear Energy Agency, Committee On Nuclear Regulatory Activities, “Challenges and Enhancements to Defence-in-Depth (DiD) in Light of the Fukushima Daiichi NPP Accident, Proceedings of a Joint CNRA/CSNI Workshop, Paris, France, 5 June 2013,” NEA/CNRA/R(2014)4, June 2014.

[NEA, 2016} Nuclear Energy Agency, Organization for Economic Co-Operation and Development, “Implementation of Defence-in-Depth at Nuclear Power Plants: Lessons Learnt from the Fukushima Daiichi Accident,” NEA No. 7248, 2016.

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

[NRC, 1975] U.S. Nuclear Regulatory Commission, “Annual Report 1975,” December 31, 1975. (ADAMS Accession No. ML090060072, not publicly available)

[NRC, 1976a] U.S. Nuclear Regulatory Commission, “Fact Sheet on Reactor Safety,” April 20, 1976.

[NRC, 1976b] U.S. Nuclear Regulatory Commission, “Recommendations Related to Browns Ferry Fire,” NUREG-0050, February 1976. (ADAMS Accession No. ML070520452)

[NRC, 1979a] U.S. Nuclear Regulatory Commission, “TMI Lessons Learned Task-Force Status Report and Short-Term Recommendations,” NUREG-0578, July 1979. (ADAMS Accession No. ML090060030)

[NRC, 1979b] U.S. Nuclear Regulatory Commission, “TMI-2 Lessons Learned Task Force Final Report,” NUREG-0585, October, 1979. (ADAMS Accession No. ML061430367)

[NRC, 1979] U.S. Nuclear Regulatory Commission, “Performance capabilities for fixed site physical protection systems,” 10 CFR §73.45, 1979.

[NRC, 1980] U.S. Nuclear Regulatory Commission, “Report on the Accident at the Chernobyl Nuclear Power Station,” NUREG/CR-1250, January 1987. (ADAMS Accession No. ML071690245)

[NRC, 1982] U.S. Nuclear Regulatory Commission, “Physical Protection for Transient Shipments,” Regulatory Guide 5.63, July 1982.

[NRC, 1983] U.S. Nuclear Regulatory Commission, “Safety Goals for Nuclear Power Plants,” NUREG-0880 Rev. 1, May 1983. (ADAMS Accession No. ML071770230)

[NRC, 1986] 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). (ADAMS Accession No. ML051580404)

[NRC, 1994a] U.S. Nuclear Regulatory Commission, “Perspectives on Reactor Safety,” NUREG/CR-6042, March 1994. (ADAMS Accession No. ML)

[NRC, 1994b] U.S. Nuclear Regulatory Commission, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” NUREG/CR-6303, December 1994. (ADAMS Accession No. ML071790509)

[NRC, 1995] 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. (ADAMS Accession No. ML021980535)

[NRC, 1996a] U.S. Nuclear Regulatory Commission, “Reactor Site Criteria,” 10 CFR Part 100, 1996.

[NRC, 1996b] U.S. Nuclear Regulatory Commission, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” NUREG-1537, February 1996. (ADAMS Accession No. ML12251A353)

[NRC, 1996c] U.S. Nuclear Regulatory Commission, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” Regulatory Guide 1.152, January 1996. (ADAMS Accession No. ML003740015)

[NRC, 1997a] U.S. Nuclear Regulatory Commission, “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,” NUREG-0800, Branch Technical Position (BTP) HICB-19, June 1997. (ADAMS Accession No. ML052500555)

[NRC, 1997b] U.S. Nuclear Regulatory Commission, “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.

[NRC, 1997c] U.S. Nuclear Regulatory Commission, “Proposed Strategy for Development of Regulations Governing Disposal of High-Level Radioactive Wastes in a Proposed Repository at Yucca Mountain, Nevada,” SECY-97-300, December 1997. (ADAMS Accession No. ML032830444)

[NRC, 1999a] U.S. Nuclear Regulatory Commission, “Risk-Informed and Performance-Based Regulation.” Commission White Paper, (ADAMS Accession No. ML15223A685)

[NRC, 1999b] U.S. Nuclear Regulatory Commission, “Staff Plan for Clarifying how Defense-in-Depth Applies to the Regulation of a Possible Geologic Repository at Yucca Mountain, Nevada,” SECY-99-186, July 1999. (ADAMS Accession No. ML040640782)

[NRC, 2000a] U.S. Nuclear Regulatory Commission, “Requirements for New Facilities or New Processes at Existing Facilities,” 10 CFR §70.64, 2000.

[NRC, 2000b] U.S. Nuclear Regulatory Commission, “Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors,” Regulatory Guide 1.183, July 2000. (ADAMS Accession No. ML003716792)

[NRC, 2000c] U.S. Nuclear Regulatory Commission, “Standard Review Plan for Spent Fuel Dry Storage Facilities,” NUREG-1567, March 2000. (ADAMS Accession No. ML003686776)

[NRC, 2002a] U.S. Nuclear Regulatory Commission, Revision 2, “Perspectives on Reactor Safety,” NUREG/CR-6042, March 2002. (ADAMS Accession No. ML091250169)

[NRC, 2002b] U.S. Nuclear Regulatory Commission, “Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979,” Appendix R to 10 C.F.R. pt. 50 (2012).

[NRC, 2003a] U.S. Nuclear Regulatory Commission, “Yucca Mountain Review Plan,” NUREG-1804, Rev. 2, July 2003. (ADAMS Accession No. ML032030389)

[NRC, 2003b] U.S. Nuclear Regulatory Commission, 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,"September 12, 2003. (ADAMS Accession No. ML032480751)

[NRC, 2004] U.S. Nuclear Regulatory Commission, 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. (ADAMS Accession No. ML041550865)

[NRC, 2006] U.S. Nuclear Regulatory Commission, "Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to their Safety Significance," Regulatory Guide 1.201, May 2006. (ADAMS Accession No. ML061090627)

[NRC, 2007a] U.S. Nuclear Regulatory Commission, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," NUREG-0800, Standard Review Plan (SRP), BTP 7-19, March 2007. (ADAMS Accession No. ML070550072)

[NRC, 2007b] U.S. Nuclear Regulatory Commission, "Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing," NUREG-1860, U.S. Nuclear Regulatory Commission, December 2007. (ADAMS Accession No. ML080440170)

[NRC, 2007c] U.S. Nuclear Regulatory Commission, "General Design Criteria for Nuclear Power Plants," Appendix A to 10 CFR Part 50, 2007.

[NRC, 2007d] U.S. Nuclear Regulatory Commission, "Requirements for reduction of risk from anticipated transients without SCRAM (ATWS) events for light-water-cooled nuclear power plants," 10 CFR §50.62, 2007.

[NRC, 2007e] U.S. Nuclear Regulatory Commission, "Combined License Applications for Nuclear Power Plants (LWR Edition)," Regulatory Guide 1.206, June 2007.

[NRC, 2007f] U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," NUREG-0800, 2007.

[NRC, 2008a] 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.

[NRC, 2008b] U.S. Nuclear Regulatory Commission, "Risk-Informed Decisionmaking for Nuclear Material and Waste Applications," February 2008. (ADAMS Accession No. ML080720238)

[NRC, 2009a] U.S. Nuclear Regulatory Commission, “Digital Instrumentation and Controls,” DI&C-ISG-02, June 2009. (ADAMS Accession No. ML091590268)

[NRC, 2009b] U.S. Nuclear Regulatory Commission, “Protection of Digital Computer and Communication Systems and Networks,” 10 CFR §73.54, 2009.

[NRC, 2009c] U.S. Nuclear Regulatory Commission, “Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage,” 10 CFR §73.55, 2009.

[NRC, 2009d] U.S. Nuclear Regulatory Commission, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,” Regulatory Guide 1.200, March 2009. (ADAMS Accession No. ML090410014)

[NRC, 2010a] U.S. Nuclear Regulatory Commission, “Cyber Security Programs for Nuclear Facilities,” Regulatory Guide 5.71, January 2010. (ADAMS Accession No. ML090340159)

[NRC, 2010b] U.S. Nuclear Regulatory Commission, “Standard Review Plan (SRP) for Dry Cask Storage Systems,” NUREG-1536, February 1996. (ADAMS Accession No. ML010040237)

[NRC, 2011a] U.S. Nuclear Regulatory Commission, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Regulatory Guide 1.174, Revision 2, May 2011. (ADAMS Accession No. ML100910006)

[NRC, 2011b] U.S. Nuclear Regulatory Commission, “The Near-Term Task Force Review of Insights from the Fukushima Dai-Ichi Accident,” July 12, 2011. (ADAMS Accession No ML111861807)

[NRC, 2012a] U.S. Nuclear Regulatory Commission, “A Proposed Risk Management Regulatory Framework,” NUREG-2150, April 2012. (ADAMS Accession No. ML12109A277)

[NRC, 2012b] U.S. Nuclear Regulatory Commission, “Nuclear Power Plant Safeguards Contingency Plans,” Appendix C to 10 CFR Part 73, 2012.

[NRC, 2012c] U.S. Nuclear Regulatory Commission, “Risk-informed Categorization and Treatment of Structures, Systems and Components for Nuclear Power Reactors,” 10 C.F.R. §50.69 (2012).

[NRC, 2012d] U.S. Nuclear Regulatory Commission, “Strategic Plan: Fiscal Years 2008–2013 (Updated)” NUREG-1614, Volume 5, February 2012.

[NRC, 2012e] U.S. Nuclear Regulatory Commission, “Performance requirements for industrial radiography equipment,” 10 CFR § 34.20, 2012.

[NRC, 2012f] U.S. Nuclear Regulatory Commission, “Program Specific Guidance About Portable Gauge Licensees,” NUREG-1556, Vol. 1, Rev. 2, Draft for Comment, May 2012. (ADAMS Accession No. ML12139A008)

[NRC 2013a] U.S. Nuclear Regulatory Commission, “Defense-in-Depth Observations and Detailed History,” SECY-13-132, Enclosure 3, December, 2013. (ADAMS Accession No. ML13277A421)

[NRC 2013b] U.S. Nuclear Regulatory Commission, “Staff Requirements – SECY-13-0132 - U.S. Nuclear Regulatory Commission Staff Recommendation for the Disposition of Recommendation 1 of the Near-Term task Force Report,” SRM to SECY-13-132, May 2014. (ADAMS Accession No. ML14137A104)

[NRC, 2013c] U.S. Nuclear Regulatory Commission, “Factors to be considered when evaluating sites,” 10 CFR §100.20, 2013.

[NRC, 2014a] U.S. Nuclear Regulatory Commission, “USNRC Strategic Plan Fiscal Years 2014-2018,” NUREG-1614, Volume 6, August 2014. (ADAMS Accession No. ML14246A439)

[NRC, 2014b] U.S. Nuclear Regulatory Commission, Public Website, Glossary, http://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth, 2015.

[NRC, 2014c] U.S. Nuclear Regulatory Commission, “Protection and safety systems,” 10 CFR 50.55a(h), 2014.

[NRC, 2015] U.S. Nuclear Regulatory Commission, “Standard Review Plan for Fuel Cycle Facilities License Applications,” NUREG-1520, Rev. 2, June 2015. (ADAMS Accession No. ML15176A258)

[Nuclear Safety, 1981] Breen, R.J., "Defense-in-Depth Approach to Safety in Light of the Three Mile Island Accident,” Nuclear Safety, Vol. 22, No.5, Sept.-Oct. 1981.

[RGs] U.S Nuclear Regulatory Commission, Regulatory Guide (RG) 1.152 ML102870022, RG 1.174 ML023240437, RG 1.175 ML003740149, RG 1.176 ML003740172, RG 1.177 ML100910008, RG 1.178 ML032510128, RG 1.183 ML003716792, RG 1.186 ML003754825, RG 1.189 ML092580550, RG 1.191 ML011500010, RG 1.195 ML031490640, RG 1.205 ML091960258, RG 4.2 ML003739519, RG 5.71 ML092670517

[OECD, 2013] Organisation for Economic Co-Operation and Development, “Challenges and Enhancements to Defence-in-Depth (DiD) in Light of the Fukushima Daiichi NPP Accident,” Proceedings of a Joint CNRA/CSNI workshop. Paris, France. June 5, 2013

[SECYs] U.S. Nuclear Regulatory Commission, Commission Paper SECY-77-0439 ML060260236, SECY-83-0269 ML101970113, SECY-93-0190 ML072360060, SECY-00-0022 ML 993630359, SECY-00-0077 ML003694288, SECY-00-0080 ML003675817, SECY-00-0086 ML003696258, SECY-00-0212 ML003757695, ML003760469, ML003759593, SECY-01-0009 ML003779058, SECY-01-0100 ML011450420, SECY-02-0030 ML020150056, SECY-03-0047 ML030160002, SECY-04-0236 ML042590576, SECY-05-0006 ML043560093, ML043560390, ML043560335, SECY-05-0172 ML051880303, SECY-06-0187 ML061910627, SECY-07-0205 ML073270114, SECY-09-0113 ML091970152, SECY-09-0140 ML092151078, SECY-10-0121 ML102230076, SECY-11-0014 ML102590196, ML102110167

[Sorenson, 1997] Sorenson, J.N., "Historical Notes on Defense in Depth," October 15, 1997. (ADAMS Accession No. ML082740322)

[SSM, 2015] Swedish Radiation Safety Authority, SSM, "DID-PSA: Development of a Framework for Evaluation of the Defence-in-Depth with PSA," January 2015

NRC FORM 335 (12-2010) NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER *(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)*
NUREG/KM-0009

2. TITLE AND SUBTITLE
Historical Review and Observations of Defense-in-Depth

3. DATE REPORT PUBLISHED

MONTH	YEAR
April	2016

4. FIN OR GRANT NUMBER

5. AUTHOR(S)
Mary Drouin, RES/PRB
Brian Wagner, RES/PRB
John Lehner, Brookhaven National Lab (BNL)
Vinod Mubayi, Brookhaven National Lab (BNL)

6. TYPE OF REPORT
Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Nuclear Sciences & Technology Department
Brookhaven National Laboratory
Bldg. 130,
Upton, NY 11973

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

10. SUPPLEMENTARY NOTES
Prepared in conjunction with BNL.

11. ABSTRACT (200 words or less)
This report is for use by NRC staff, the public, the nuclear and other high risk industries, and the international nuclear safety community. It is a summary of the history of defense-in-depth, specifically of the various descriptions, discussions, and definitions that have been used in the nuclear industry. It provides an overall historical perspective with insights and observations on the concept of defense-in-depth. This report builds on the information provided to the Commission to illustrate the rich history and demonstrate the various and similar perspectives and concepts on defense-in-depth in Enclosure 3 to SECY-13-0132, "U.S. Nuclear Regulatory Commission Staff Recommendation for the Disposition of Recommendation 1 of the Near-Term Task Force Report," related to lessons learned from the accident at Fukushima Dai-ichi Nuclear Power Plant. To meet the needs as a "knowledge management tool," this report more fully addresses the history on reactors, materials, waste, and security than Enclosure 3 to SECY-13-0132. The report includes information from other Federal agencies (e.g., Department of Energy, National Aeronautics and Space Agency, Federal Aviation Administration, Department of Defense) that regulate or oversee industries with significant risk impacts and from the international nuclear safety community.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)
Defense-in-Depth
Risk-informed decision-making
Fukushima Dai-ichi
Risk Management Regulatory Framework
Near-Term Task Force

13 AVAILABILITY STATEMENT
unlimited

14 SECURITY CLASSIFICATION
(This Page)
unclassified
(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS