



UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
ADVISORY COMMITTEE ON NUCLEAR WASTE
WASHINGTON, D.C. 20555

MEMORANDUM

OFFICE OF
ACRS/ACNW

TO: ACRS Members

FROM:  J. N. Sorensen

DATE: October 15, 1997

SUBJECT: Historical Notes on Defense in Depth

Attached for your information is a memorandum I prepared for Dr. Kress on the history of the term "defense in depth." This memo documents the preparation done for the August 27, 1997 meeting of the Subcommittee on Regulatory Policies and Practices, and adds some new material to the discussion of the use of the term "defense in depth" in Commission policy statements.

Attachment: As stated

cc w/attachment: ACRS/ACNW Staff
J. T. Larkins
R. P. Savio

MEMORANDUM

TO: T. S. Kress

FROM:  J. N. Sorensen

SUBJECT: Historical Notes on Defense in Depth

DATE: October 9, 1997

The ACRS has been discussing the concept of defense in depth and its impact on the design, operation and regulation of nuclear power plants in a number of contexts during the past year. The basic questions that have been formulated appear to revolve around two concerns: (1) how is defense in depth defined and (2) how can it be determined that specific design or regulatory requirements are necessary or sufficient to achieve defense in depth? The purpose of this memo is to document the historical research done to support discussion of those two issues.

The term "defense in depth" occurs frequently in the documented history of nuclear reactor safety. In fact, it is used so frequently that its evolution, meaning(s) and function in the design and regulatory processes are not always clear. For example, the term "defense in depth" does not appear in Title 10 of the Code of Federal Regulations except in Appendix R of Part 50, 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:

- o To prevent fires from starting;
- o To detect rapidly, control, and extinguish promptly those fires that do occur;
- o 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."

Note the choice of words, ". . . extend the concept of defense-in-depth . . ." This phrase implies that the concept of defense in depth is well understood at this point in the document, and

that it has been used in other sections of the regulations. In fact, the term itself is not defined in Title 10, and has no prior or subsequent appearances. The concept of defense in depth permeates the General Design Criteria in 10 CFR 50 Appendix A, and underlies other Title 10 requirements as well. One might reasonably conclude from this that the only requirements to implement defense in depth are those that are implicit in other, explicitly stated, requirements. (Perhaps defense in depth should properly be thought of as a response to specific design and regulatory requirements, since it does not appear to be a regulatory requirement per se. A configuration management perspective suggests that this may be an important thought. I will return to it in a later memo.)

Joint Committee on Atomic Energy Hearings, 1967

The earliest definition of defense in depth that I found (with the assistance of NRC historian Sam Walker) was in an April 1967 statement submitted by Clifford Beck, then Deputy Director of Regulation, to the Joint Committee on Atomic Energy. The following two pages quote extensively from the paper because there may be some significance in how narrowly Beck defines defense in depth relative to the extremely broad view he takes of contributors to reactor safety. In discussing the system of safety protection for power reactors, the statement reads:

"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."

The broad picture Beck draws is of "three basic lines of defense." Within the "first line," he illustrates "the principle of defense-in-depth" by example, choosing the multiple physical barriers of fuel matrix, clad, primary system and containment. He then goes on to describe what he calls the second and third lines of defense, namely, accident prevention and limiting the consequences of accidents. Does he mean the term "defense-in-depth" to apply to his three broad "lines of defense"? It does not seem so. For example, within his discussion of the first line of defense, he lists and apparently intends to differentiate among the attributes "fail safe design, redundancy and backup, defense in depth, and extra margins of safety." If we accept this reading at face value, then he has defined defense in depth very narrowly and not very clearly by his example. (The example is clear, but its extension is not.) On the other hand, how could one avoid interpreting "three levels of defense" as "defense in depth"?

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 ACRS, and the Atomic Safety and Licensing Board Panel. The Group considered the general questions of (1) the adequacy of the protection of the health and safety of the public and (2) whether regulatory procedures and requirements have adversely affected the development of the industry. 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."

Two things seem evident from the preceding discussion. The first is that the issue of "balance," and a relationship between balance and defense in depth, had already been identified. The second is that the writers considered the "first line of defense" as described by Clifford Beck to be one element of defense in depth.

ECCS Hearings, 1971

The third 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 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 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."

The subsection goes on to list conservatisms that the authors apparently consider to be an addition to, but not part of, defense-in-depth.

"Further, the design of the ECCS is required to be adequate to provide this protection in spite of additional conservative assumptions such as non-availability of offsite power, single failures of redundant components, and partial loss of cooling water. Still further, in evaluating the suitability of a site proposed for a light-water power reactor, the AEC requires an analysis to be made of the potential offsite effects of a postulated LOCA. Additional elements of conservatism are included in this analysis, including assumptions of high release fractions of fission products from the fuel, containment leakage continuously for 30 days, and unfavorable meteorology."

And in a subsection titled "Conclusions":

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

In this document, the writers clearly equate the "three levels of defense" discussed earlier by Beck, with "defense-in depth." Beck made no such equation. They also appear to distinguish between "defense-in-depth" and "margin" as reflected by conservatisms introduced in analyzing the consequences of accidents.

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 PWR plants and among 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."

Thus, the authors draw a distinction between multiple barriers against the release of fission products and defense in depth, by associating the latter term with protection of the barriers against off-normal occurrences. The discussion then goes on to say that defense in depth can be conveniently described by discussing it in the broader concept of "three levels of safety." Those three levels are then described as: (1) design for unquestionable safety in normal operation, (2) assume incidents will occur and provide safety systems accordingly, and (3) provide additional safety systems to protect against hypothetical accidents where level two safety systems are assumed to fail. These three levels of safety clearly equate to the three lines of defense described by Clifford Beck in his 1967 paper. Also like Beck, the term "defense in depth" is not associated directly with those levels of safety. There are differences, however. While Beck treats defense in depth as a subsidiary element of the first line of defense, and cites the four fission product barriers as an example, WASH-1250 treats defense in depth as the things that are done to protect the barriers, rather than the barriers themselves. The Internal Study Group, on the other hand, equates defense in depth with the lines of defense (Beck's term) or levels of safety (WASH-1250 term). Similarly, the AEC staff testimony in the ECCS hearings firmly equates defense in depth with the same "three lines of defense" described by Beck.

Other Documents Examined

One of the interesting aspects of the history of "defense in depth" is that it often does not appear where it logically might be expected. Title 10, as described earlier, is one example. I could find no occurrences of the term in the Statements of Consideration of 10 CFR 50 Appendix A, although it does occur in the SOC for the final rule on Disposal of High Level Radioactive Wastes in Geologic Repositories, 10 CFR 60 (48 FR 28194-28299). It is interesting to note that both Appendix R and Part 60 were added to Title 10 at about the same time, early 1980s, and are thus relatively recent additions.

The occurrence, or more precisely the lack of occurrence, of "defense-in-depth" in other historical documents is equally interesting. David Okrent's history of light water reactor safety covers the time period from the early 1960's to 1977. As far as I could determine, the only appearance of the term is in a quotation from a 1977 document prepared by the United Kingdom's Nuclear Installation Inspectorate. That document, in describing generic pressurized water reactor safety issues, refers to the containment as "the last of a series of defenses in depth . . .". In Okrent's discussion of AEC and ACRS activities there are references to "several levels of safety," but the term defense in depth is not used. Similarly, the "Report of the Advisory Task Force on Power Reactor Emergency Cooling," the so-called Ergen Committee report, completed in 1967, does not use the term defense in depth. There is a discussion of the same three levels of safety discussed in Clifford Beck's paper, and later in WASH-1250, but "defense in depth" is not used.

The term "defense in depth" appears ten times in the section of the Standard Review Plans on fire protection (Section 9.5.1) and only twice in the section on containments (Section 6.2). In the latter case it is simply used to describe the containment as the "final barrier in the defense in depth concept," in two different places.

The term occurs in three Commission Policy Statements: the Final PRA Policy Statement, the Safety Goal Policy Statement and the Advanced Nuclear Power Plant Policy Statement. None of these documents offer a definition of defense in depth, except by example or implication. The implied definitions in all three policy statements are somewhat different, but not inconsistent with other historical examples. For example, the Commission Policy on Regulation of Advanced Reactors contains the following statement: "Among the attributes that could assist in establishing the acceptability or licensability of a proposed advanced reactor design . . . are . . . [d]esigns that incorporate defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for and consequences of severe accidents."

The Safety Goal Policy Statement associates defense-in-depth with compensating for uncertainty in probabilistic analyses. The policy states, in part, ". . . it is necessary that proper

attention be given not only to the range of uncertainty surrounding probabilistic estimates, but also to the phenomenology that most influences uncertainties. . . . The results of sensitivity studies should be displayed showing, for example, the range of variation together with the underlying science or engineering assumptions that dominate this variation. [J]udgements can be made by the decisionmaker about the degree of confidence to be given to these estimates and assumptions. . . . This defense in depth approach is expected to continue to ensure the protection of public health and safety."

The PRA policy statement stipulates that the use of PRA technology should support the "NRC's traditional defense-in-depth philosophy." The policy statement recognizes 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 . . ." The policy statement specifically recognizes "the philosophy of a multiple-barrier approach against fission product release," and notes that such barrier principles are mandated by the Nuclear Waste Policy Act of 1982.

10 CFR Part 60, Statements of Consideration

As noted earlier, "defense in depth" does appear in the statements of Consideration for 10 CFR 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 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 . . ." The description here clearly includes the concept of defense in depth as multiple barriers.

Post-TMI Definitions and Examples

In approximately the same time frame that Part 60 was published, R.J. Breen, Deputy Director of EPRI's Nuclear Safety Analysis Center, published a paper titled "Defense in Depth Approach to Safety in Light of the Three Mile Island Accident (Nuclear Safety, Vol. 22, No. 5, Sept.-Oct. 1981). 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 appears to accept without question 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 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.

Two aspects of this paper are worthy of note relative to the questions currently being considered regarding defense in depth. The first is that Breen believed that defense in depth should be quantifiable. He saw PRA as one way of doing the quantification,

but he also identified alternatives that were available at the time. The second point is that Breen's definition of defense in depth was essentially the same as that used in WASH-1250, the 1969 Internal Study Group report, and the AEC staff's testimony in the Interim Acceptance Criteria for Emergency Core Cooling Systems.

Addressing Limitations

Another paper that appeared about the same time as the Breen article mentioned above was one by Stan Kaplan, "Safety Goals and Related Questions," Reliability Engineering, 1982. Although the paper deals with "safety goals" as opposed to "defense in depth," I believe it states a principle that cannot be ignored when we are trying to determine what limits should be placed on requirements in the name of defense in depth. Kaplan argues that the question of "how safe is safe enough" can never be answered without consideration of all available alternatives, including the costs, benefits, and damages for each alternative. The essential point is that evaluation of a proposed safety requirement, in the name of defense in depth or some other high principle, ultimately must consider the question of cost.

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

A recent summary of the history and application of defense in depth is contained in NUREG/CR-6042, "Perspectives on Reactor Safety," by F. E. Haskin (University of New Mexico) and A. L. Campbell (Sandia National Laboratory), 1994. The document describes a one week course in reactor safety concepts offered by the NRC Technical Training Center. It is significant in the context of examining the issue of defense in depth for two reasons. The first is that the authors, in developing their discussion of defense in depth and in coming to their conclusions, examined that same history that has been partially recounted here. The second is that it represents what is being taught to NRC employees regarding the definition and application of defense in depth.

NUREG/CR-6042 introduces defense in depth by listing ". . . the key elements of an overall safety strategy that began to emerge in the early 1950s and has become known as defense in depth." The key elements listed are accident prevention, safety systems,

containment, accident management, and siting and emergency plans. This picture of defense in depth is consistent with that described in WASH-1250 and other documents which considered defense in depth as "multiple levels of safety." NUREG/CR-6042 also associates defense in depth with multiple barriers or layers, as opposed to the systematic view just mentioned. The barriers identified, each with an associated function, are: ceramic fuel pellets, metal cladding, reactor vessel and piping, containment, exclusion area, low population zone and evacuation plan, and population center distance.

INSAG -3, 1988

Finally, in considering the history and definition of defense in depth, it is worth noting the description by the International Nuclear Safety Advisory Group in INSAG-3, "Basic Safety Principles for Nuclear Power Plants," IAEA, 1988. INSAG-3 states, "All safety activities, whether organizational, behavioural 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: "To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred 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." The preceding definition appears to be entirely consistent with what one might derive from the history recounted in this memorandum.

Chairman Jackson has also recently provided her thoughts on defense in depth. In a July 22, 1997 talk at the MIT Nuclear Power Reactor Safety Course, she states, "The defense-in-depth concept should be viewed as complementary to risk-informed,

performance-based approaches, as opposed to a competitive process. . . . Defense-in-depth is a design and operational concept that ensures that successive compensatory measures are incorporated to mitigate potential failures. . . . The notion of Probabilistic Risk Assessment results being used to compromise the defense-in-depth concept is related to the issue of uncertainty (emphasis in original). The magnitude of a single number cannot be used to eliminate safety barriers without due consideration of uncertainty. Multiple barriers provide assurance against catastrophic events."

Conclusions

There are a number of conclusions and some inferences one can draw from the preceding historical perspective. While acknowledging that many of them already have been stated by other writers, I include them here for the sake of completeness.

First, there is no "best" or "most acknowledged" definition for defense in depth. The closest one comes to a common definition is the "three levels of safety" described by a number of authors relative (primarily) to nuclear power plant design: (1) design, build and operate so the probability of an accident is small, (2) provide protection systems for unexpected behavior, (3) provide engineered safety features to mitigate consequences of postulated accidents. However, few writers firmly equate defense in depth with these three levels; rather these levels are used to set the context for discussing defense in depth. All the "definitions," discussions, and examples are similar, yet each is a little different.

The concept of "multiple barriers" is frequently cited as an example or illustration of defense in depth. Most often, the reference is to the fission product barriers in a nuclear power plant: fuel matrix, clad, primary coolant system, and containment. Other examples are mentioned where the barriers are at least in part systematic as well as physical.

Defense in depth is most often characterized as a concept, an approach, a philosophy, or a principle, and is most frequently defined by example.

None of the discussions, definitions or examples of defense in depth which were reviewed contained any element of limitation. Limits on what can be or should be demanded in the name of defense in depth were not mentioned.

Distribution:

ACRS

ACNW

Staff

Fellows



UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
ADVISORY COMMITTEE ON NUCLEAR WASTE
WASHINGTON, D.C. 20555

MEMORANDUM

OFFICE OF
ACRS/ACNW

TO: ACRS Members

FROM: *J. N. Sorensen*
J. N. Sorensen

DATE: October 15, 1997

SUBJECT: Historical Notes on Defense in Depth

Attached for your information is a memorandum I prepared for Dr. Kress on the history of the term "defense in depth." This memo documents the preparation done for the August 27, 1997 meeting of the Subcommittee on Regulatory Policies and Practices, and adds some new material to the discussion of the use of the term "defense in depth" in Commission policy statements.

Attachment: As stated

cc w/attachment: ACRS/ACNW Staff
J. T. Larkins
R. P. Savio
Fellows

MEMORANDUM

TO: T. S. Kress

FROM: J. N. Sorensen

SUBJECT: Historical Notes on Defense in Depth

DATE: October 9, 1997

The ACRS has been discussing the concept of defense in depth and its impact on the design, operation and regulation of nuclear power plants in a number of contexts during the past year. The basic questions that have been formulated appear to revolve around two concerns: (1) how is defense in depth defined and (2) how can it be determined that specific design or regulatory requirements are necessary or sufficient to achieve defense in depth? The purpose of this memo is to document the historical research done to support discussion of those two issues.

The term "defense in depth" occurs frequently in the documented history of nuclear reactor safety. In fact, it is used so frequently that its evolution, meaning(s) and function in the design and regulatory processes are not always clear. For example, the term "defense in depth" does not appear in Title 10 of the Code of Federal Regulations except in Appendix R of Part 50, 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:

- o To prevent fires from starting;
- o To detect rapidly, control, and extinguish promptly those fires that do occur;
- o 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."

Note the choice of words, ". . . extend the concept of defense-in-depth . . ." This phrase implies that the concept of defense in depth is well understood at this point in the document, and

that it has been used in other sections of the regulations. In fact, the term itself is not defined in Title 10, and has no prior or subsequent appearances. The concept of defense in depth permeates the General Design Criteria in 10 CFR 50 Appendix A, and underlies other Title 10 requirements as well. One might reasonably conclude from this that the only requirements to implement defense in depth are those that are implicit in other, explicitly stated, requirements. (Perhaps defense in depth should properly be thought of as a response to specific design and regulatory requirements, since it does not appear to be a regulatory requirement per se. A configuration management perspective suggests that this may be an important thought. I will return to it in a later memo.)

Joint Committee on Atomic Energy Hearings, 1967

The earliest definition of defense in depth that I found (with the assistance of NRC historian Sam Walker) was in an April 1967 statement submitted by Clifford Beck, then Deputy Director of Regulation, to the Joint Committee on Atomic Energy. The following two pages quote extensively from the paper because there may be some significance in how narrowly Beck defines defense in depth relative to the extremely broad view he takes of contributors to reactor safety. In discussing the system of safety protection for power reactors, the statement reads:

"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."

The broad picture Beck draws is of "three basic lines of defense." Within the "first line," he illustrates "the principle of defense-in-depth" by example, choosing the multiple physical barriers of fuel matrix, clad, primary system and containment. He then goes on to describe what he calls the second and third lines of defense, namely, accident prevention and limiting the consequences of accidents. Does he mean the term "defense-in-depth" to apply to his three broad "lines of defense"? It does not seem so. For example, within his discussion of the first line of defense, he lists and apparently intends to differentiate among the attributes "fail safe design, redundancy and backup, defense in depth, and extra margins of safety." If we accept this reading at face value, then he has defined defense in depth very narrowly and not very clearly by his example. (The example is clear, but its extension is not.) On the other hand, how could one avoid interpreting "three levels of defense" as "defense in depth"?

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 ACRS, and the Atomic Safety and Licensing Board Panel. The Group considered the general questions of (1) the adequacy of the protection of the health and safety of the public and (2) whether regulatory procedures and requirements have adversely affected the development of the industry. 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."

Two things seem evident from the preceding discussion. The first is that the issue of "balance," and a relationship between balance and defense in depth, had already been identified. The second is that the writers considered the "first line of defense" as described by Clifford Beck to be one element of defense in depth.

ECCS Hearings, 1971

The third 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 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 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."

The subsection goes on to list conservatisms that the authors apparently consider to be an addition to, but not part of, defense-in-depth.

"Further, the design of the ECCS is required to be adequate to provide this protection in spite of additional conservative assumptions such as non-availability of offsite power, single failures of redundant components, and partial loss of cooling water. Still further, in evaluating the suitability of a site proposed for a light-water power reactor, the AEC requires an analysis to be made of the potential offsite effects of a postulated LOCA. Additional elements of conservatism are included in this analysis, including assumptions of high release fractions of fission products from the fuel, containment leakage continuously for 30 days, and unfavorable meteorology."

And in a subsection titled "Conclusions":

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

In this document, the writers clearly equate the "three levels of defense" discussed earlier by Beck, with "defense-in depth." Beck made no such equation. They also appear to distinguish between "defense-in-depth" and "margin" as reflected by conservatisms introduced in analyzing the consequences of accidents.

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 PWR plants and among 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."

Thus, the authors draw a distinction between multiple barriers against the release of fission products and defense in depth, by associating the latter term with protection of the barriers against off-normal occurrences. The discussion then goes on to say that defense in depth can be conveniently described by discussing it in the broader concept of "three levels of safety." Those three levels are then described as: (1) design for unquestionable safety in normal operation, (2) assume incidents will occur and provide safety systems accordingly, and (3) provide additional safety systems to protect against hypothetical accidents where level two safety systems are assumed to fail. These three levels of safety clearly equate to the three lines of defense described by Clifford Beck in his 1967 paper. Also like Beck, the term "defense in depth" is not associated directly with those levels of safety. There are differences, however. While Beck treats defense in depth as a subsidiary element of the first line of defense, and cites the four fission product barriers as an example, WASH-1250 treats defense in depth as the things that are done to protect the barriers, rather than the barriers themselves. The Internal Study Group, on the other hand, equates defense in depth with the lines of defense (Beck's term) or levels of safety (WASH-1250 term). Similarly, the AEC staff testimony in the ECCS hearings firmly equates defense in depth with the same "three lines of defense" described by Beck.

Other Documents Examined

One of the interesting aspects of the history of "defense in depth" is that it often does not appear where it logically might be expected. Title 10, as described earlier, is one example. I could find no occurrences of the term in the Statements of Consideration of 10 CFR 50 Appendix A, although it does occur in the SOC for the final rule on Disposal of High Level Radioactive Wastes in Geologic Repositories, 10 CFR 60 (48 FR 28194-28299). It is interesting to note that both Appendix R and Part 60 were added to Title 10 at about the same time, early 1980s, and are thus relatively recent additions.

The occurrence, or more precisely the lack of occurrence, of "defense-in-depth" in other historical documents is equally interesting. David Okrent's history of light water reactor safety covers the time period from the early 1960's to 1977. As far as I could determine, the only appearance of the term is in a quotation from a 1977 document prepared by the United Kingdom's Nuclear Installation Inspectorate. That document, in describing generic pressurized water reactor safety issues, refers to the containment as "the last of a series of defenses in depth . . .". In Okrent's discussion of AEC and ACRS activities there are references to "several levels of safety," but the term defense in depth is not used. Similarly, the "Report of the Advisory Task Force on Power Reactor Emergency Cooling," the so-called Ergen Committee report, completed in 1967, does not use the term defense in depth. There is a discussion of the same three levels of safety discussed in Clifford Beck's paper, and later in WASH-1250, but "defense in depth" is not used.

The term "defense in depth" appears ten times in the section of the Standard Review Plans on fire protection (Section 9.5.1) and only twice in the section on containments (Section 6.2). In the latter case it is simply used to describe the containment as the "final barrier in the defense in depth concept," in two different places.

The term occurs in three Commission Policy Statements: the Final PRA Policy Statement, the Safety Goal Policy Statement and the Advanced Nuclear Power Plant Policy Statement. None of these documents offer a definition of defense in depth, except by example or implication. The implied definitions in all three policy statements are somewhat different, but not inconsistent with other historical examples. For example, the Commission Policy on Regulation of Advanced Reactors contains the following statement: "Among the attributes that could assist in establishing the acceptability or licensability of a proposed advanced reactor design . . . are . . . [d]esigns that incorporate defense-in-depth philosophy by maintaining multiple barriers against radiation release, and by reducing the potential for and consequences of severe accidents."

The Safety Goal Policy Statement associates defense-in-depth with compensating for uncertainty in probabilistic analyses. The policy states, in part, ". . . it is necessary that proper

attention be given not only to the range of uncertainty surrounding probabilistic estimates, but also to the phenomenology that most influences uncertainties. . . . The results of sensitivity studies should be displayed showing, for example, the range of variation together with the underlying science or engineering assumptions that dominate this variation. [J]udgements can be made by the decisionmaker about the degree of confidence to be given to these estimates and assumptions. . . . This defense in depth approach is expected to continue to ensure the protection of public health and safety."

The PRA policy statement stipulates that the use of PRA technology should support the "NRC's traditional defense-in-depth philosophy." The policy statement recognizes 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 . . ." The policy statement specifically recognizes "the philosophy of a multiple-barrier approach against fission product release," and notes that such barrier principles are mandated by the Nuclear Waste Policy Act of 1982.

10 CFR Part 60, Statements of Consideration

As noted earlier, "defense in depth" does appear in the statements of Consideration for 10 CFR 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 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 . . ." The description here clearly includes the concept of defense in depth as multiple barriers.

Post-TMI Definitions and Examples

In approximately the same time frame that Part 60 was published, R.J. Breen, Deputy Director of EPRI's Nuclear Safety Analysis Center, published a paper titled "Defense in Depth Approach to Safety in Light of the Three Mile Island Accident (Nuclear Safety, Vol. 22, No. 5, Sept.-Oct. 1981). 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 appears to accept without question 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 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.

Two aspects of this paper are worthy of note relative to the questions currently being considered regarding defense in depth. The first is that Breen believed that defense in depth should be quantifiable. He saw PRA as one way of doing the quantification,

but he also identified alternatives that were available at the time. The second point is that Breen's definition of defense in depth was essentially the same as that used in WASH-1250, the 1969 Internal Study Group report, and the AEC staff's testimony in the Interim Acceptance Criteria for Emergency Core Cooling Systems.

Addressing Limitations

Another paper that appeared about the same time as the Breen article mentioned above was one by Stan Kaplan, "Safety Goals and Related Questions," Reliability Engineering, 1982. Although the paper deals with "safety goals" as opposed to "defense in depth," I believe it states a principle that cannot be ignored when we are trying to determine what limits should be placed on requirements in the name of defense in depth. Kaplan argues that the question of "how safe is safe enough" can never be answered without consideration of all available alternatives, including the costs, benefits, and damages for each alternative. The essential point is that evaluation of a proposed safety requirement, in the name of defense in depth or some other high principle, ultimately must consider the question of cost.

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

A recent summary of the history and application of defense in depth is contained in NUREG/CR-6042, "Perspectives on Reactor Safety," by F. E. Haskin (University of New Mexico) and A. L. Campbell (Sandia National Laboratory), 1994. The document describes a one week course in reactor safety concepts offered by the NRC Technical Training Center. It is significant in the context of examining the issue of defense in depth for two reasons. The first is that the authors, in developing their discussion of defense in depth and in coming to their conclusions, examined that same history that has been partially recounted here. The second is that it represents what is being taught to NRC employees regarding the definition and application of defense in depth.

NUREG/CR-6042 introduces defense in depth by listing ". . . the key elements of an overall safety strategy that began to emerge in the early 1950s and has become known as defense in depth." The key elements listed are accident prevention, safety systems,

containment, accident management, and siting and emergency plans. This picture of defense in depth is consistent with that described in WASH-1250 and other documents which considered defense in depth as "multiple levels of safety." NUREG/CR-6042 also associates defense in depth with multiple barriers or layers, as opposed to the systematic view just mentioned. The barriers identified, each with an associated function, are: ceramic fuel pellets, metal cladding, reactor vessel and piping, containment, exclusion area, low population zone and evacuation plan, and population center distance.

INSAG -3, 1988

Finally, in considering the history and definition of defense in depth, it is worth noting the description by the International Nuclear Safety Advisory Group in INSAG-3, "Basic Safety Principles for Nuclear Power Plants," IAEA, 1988. INSAG-3 states, "All safety activities, whether organizational, behavioural 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: "To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred 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." The preceding definition appears to be entirely consistent with what one might derive from the history recounted in this memorandum.

Chairman Jackson has also recently provided her thoughts on defense in depth. In a July 22, 1997 talk at the MIT Nuclear Power Reactor Safety Course, she states, "The defense-in-depth concept should be viewed as complementary to risk-informed,

performance-based approaches, as opposed to a competitive process. . . . Defense-in-depth is a design and operational concept that ensures that successive compensatory measures are incorporated to mitigate potential failures. . . . The notion of Probabilistic Risk Assessment results being used to compromise the defense-in-depth concept is related to the issue of uncertainty (emphasis in original). The magnitude of a single number cannot be used to eliminate safety barriers without due consideration of uncertainty. Multiple barriers provide assurance against catastrophic events."

Conclusions

There are a number of conclusions and some inferences one can draw from the preceding historical perspective. While acknowledging that many of them already have been stated by other writers, I include them here for the sake of completeness.

First, there is no "best" or "most acknowledged" definition for defense in depth. The closest one comes to a common definition is the "three levels of safety" described by a number of authors relative (primarily) to nuclear power plant design: (1) design, build and operate so the probability of an accident is small, (2) provide protection systems for unexpected behavior, (3) provide engineered safety features to mitigate consequences of postulated accidents. However, few writers firmly equate defense in depth with these three levels; rather these levels are used to set the context for discussing defense in depth. All the "definitions," discussions, and examples are similar, yet each is a little different.

The concept of "multiple barriers" is frequently cited as an example or illustration of defense in depth. Most often, the reference is to the fission product barriers in a nuclear power plant: fuel matrix, clad, primary coolant system, and containment. Other examples are mentioned where the barriers are at least in part systematic as well as physical.

Defense in depth is most often characterized as a concept, an approach, a philosophy, or a principle, and is most frequently defined by example.

None of the discussions, definitions or examples of defense in depth which were reviewed contained any element of limitation. Limits on what can be or should be demanded in the name of defense in depth were not mentioned.

Distribution:

ACRS

ACNW

Staff

Fellows