

Background
Defense-in-Depth and Diversity Supporting Basis Including Single Failure Criterion
references and Risk-Informing Initiatives.

Regulations

10 CFR Part 50, Appendix A - General Design Criteria for Nuclear Power Plants

- Introduction - The development of these General Design Criteria is not yet complete ... Their omission does not relieve any applicant from considering these matters in the design of a specific facility and satisfying the necessary safety requirements. These matters include:

(4) Consideration of the possibility of systematic, non random, concurrent failures of redundant elements in the design of protection systems and reactivity control systems. (See Criteria 22, 24, 26, and 29.

- Definition - Single Failure

A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), result in a loss of the capability of the system to perform its safety function. (Note: single failures of passive components in electric systems should be assumed in the designing against a single failure. Fluid system considerations of passive failures are under development).

Criteria

Criterion 21, "Protection system Reliability and Testability," Redundancy and independence designed into the protection systems shall be sufficient to assure that (1) no single failure results in the loss of the protective function.

Criterion 22, "Protection System Independence," The protection system shall be designed to assure that the effects of natural phenomena, and normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

Criterion 24, "Separation of protection and Control Systems," The protection system shall be separated from the control system to the extent that failure of any single control system component or channel Common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection systems.

Criterion 25, "Protection System Requirements for Reactivity Control Malfunction," For any single malfunction for the reactivity control system, the protection system is designed to endure that fuel design limits are not exceeded.

Criterion 26, "Reactivity Control System Redundancy and Capability," Two independent reactivity control systems of different design principles shall be provided.

Criterion 29, "Protection against anticipated Operational Occurrences," The protection and reactivity control systems shall be designed to assure an extremely high reliability of accomplishing their safety functions in the event of anticipated operational occurrences.

Criterion 35, "Emergency Core Cooling," Suitable Redundancy ... shall be provided ... the system safety function can be accomplished, assuming a single failure.

Criterion 38, "Containment Heat Removal," Suitable redundancy ... shall be provided...the system safety function can be accomplished, assuming a single failure.

Criterion 44, "Cooling water," Suitable redundancy ... shall be provided...the system safety function can be accomplished, assuming a single failure.

10 CFR 50.62 - Requirements for Reduction of Risk From Anticipated Transients Without SCRAM (ATWS) Events for Light-Water-Cooled Nuclear Power Plants

- Requires, in part, diverse methods of responding to ATWS events for anticipated operational occurrences.

10 CFR Part 50 Appendix R - Fire protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979

- The fire protection system 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 structures, systems and components 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

10 CFR 50.55a(h) - Protection and Safety Systems

Protection and safety systems requirements of IEEE Std. 279 or IEEE Std. 603 incorporated by reference depending on construction permit dates. Standards provide minimum functional and design criteria for power, instrumentation and control portions of nuclear power plant safety systems including the single failure criteria (reference also IEEE Std. 379).

Standards

IEEE Std. 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating

Stations.” (10 CFR 50.55a(h) and RG 1.153, “Criteria for Safety Systems.”)

- IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
- Clause 5.1; The safety system shall perform all safety functions required for a design basis in the event of, (1) Any single detectable failure within the safety system concurrent with all identifiable but non-detectable failures, (2) All failures caused by the single failure, (3) All failures and spurious system actions that cause or are caused by the design basis event requiring safety functions

IEEE Std. 279 -1971, “Criteria for Protection Systems for Nuclear Generating Stations,” (10 CFR 50.55a(h) (RG 1.53, “Application of the Single-Failure Criterion to Safety Systems.”)

- Any single within the protection system shall not prevent proper protective action at the system level when required.

IEEE Std. 379, “ IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems.” (RG 1.53, “Application of the Single-Failure Criterion to Safety Systems.”)

- The safety systems shall perform all required safety functions for a design basis event in the presence of the following:

Any single detectable failure within the safety systems concurrent with all identifiable, but nondetectable failures.

All failures caused by the single failure.

All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety function.

Also discusses common-cause failures and their applicability to single failures and provisions to address common-cause failures including the use of design techniques such as diversity and defense-in-depth.

IEEE Std. 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems for Nuclear Power Generating Stations.” (RG 1.152, “Criteria for use of Computers in Safety Systems of Nuclear Power Plants.”)

Regulatory Guidance

Interim Staff Guidance (ISG), Revision 1, Task Working group 2, “Diversity and Defense-in-Depth Issues.” Dated September 26, 2007.

See <http://www.nrc.gov/reading-rm/doc-collections/isg/digital-instrumentation-ctrl.html>

Regulatory Guide (RG) 1.174, Revision 1, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” Dated November 2002.

- States that when implementing risk-informed decisionmaking, licensing basis changes are expected to meet a set of key principles, including defense-in-depth. RG 1.177 identifies a number of elements that can be used acceptance guidelines to determine whether the defense-in-depth principle has been met.

RG 1.177, “An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications,” Dated August 1998.

- States that when implementing risk-informed decisionmaking, licensing basis changes are expected to meet a set of key principles, including defense-in-depth. RG 1.177 identifies a number of elements that can be used as acceptance guidelines to determine whether the defense-in-depth principle has been met.

RG 1.53, “Application of the Single failure Criterion to Nuclear Plant Systems.”

RG 1.75, “Physical Independence of Electrical Systems.”

RG 1.152, “Criteria for Programmable Digital Computer System Software in Safety Related Systems of nuclear Power Plants.”

Generic Letters

Generic Letter 83-28, “Required Actions based on Generic Implications of Salem ATWS Event.”

NUREGs

NUREG-0737, “Clarification of TMI Action Plan Requirements”

II.K.3.44 Evaluation of anticipated transients with single failure to verify no fuel failure

Discusses anticipated transients combined with the worst single failure and demonstration that the core remains covered or that no significant fuel damage results from core uncover.

NUREG-0800, Standard Review Plan, Chapter 19.0, “Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors,” Revision 2, Dated June 2007

NUREG-0800, Standard Review Plan, Section 19.2, “Review of Risk Information Used to Support Permanent Plant Specific Changes to the Licensing basis: General Guidance,” Revision 0, Dated June 2007.

NUREG-0800, Standard Review Plan, Chapter 7.0, “Instrumentation and Controls – Overview of Review Process,” Revision 5, March 2007.

NUREG-0800, Chapter 7, Appendix 7-a, Branch Technical Position HICB-19, “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems.

NUREG-0493 - March 1979

- Defense-in-depth includes, as a general principle, design features providing for plant and public safety by the use of overlapping and redundant levels or echelons of defense so that failures in equipment and mistakes by people will be covered..

The ACRS subcommittee on July 24, 1978 and the full committee on August 1978 raised questions on the design of the RESAR-414 integrated protection system with emphasis on the interconnections between scram, the control system and the engineered safety features actuation system and common shared signals. The failures of concern to the staff and ACRS were postulated common cause failures of redundant functions and the propagation of the common cause failure to other systems/functions. NUREG0493 states that the traditional protection against a common cause failure is quality of design, manufacturing, operation and the use of diversity in the design to provide an alternative means to perform the safety function. The concerns as stated in NUREG-0493 are, (1) the possibility of a causal failure of more than one echelon of defense, (2) preventing an interdependence between echelons of defense, (3) the degree of interdependence acceptable to maintain an adequate level of safety. The common cause failure of concern is a failure that has not yet occurred or those that have not been considered. The problem is stated as one of specifying the degree of inter-dependence that is acceptable, determining methods to maintain an acceptable level of safety in spite of the presence of that degree of interdependence.

NUREG-0493 discusses evaluation approaches, types of common cause considered, recommended design basis events, and proposed diverse means and acceptance guidance.

NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems," Dated December 1994

Provides an update to NUREG-0493 including methods to evaluate diversity and defense-in-depth for digital systems implemented in nuclear power plants.

- 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 3 physical barriers to radiation release in a reactor - cladding, reactor pressure vessel, and containment - are an example of defense-in-depth.

NUREG/CR-6842, "Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants," Dated April 2004

- Provides a discussion on defense-in-depth approaches implemented internationally.

NUREG-1793, "Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design, Dated September 2004

NUREG-1462, "Final Safety Evaluation Report Related to the Certification of the Advance Boiling Reactor Design," Dated August 1994.

NUREG-1512, "Final Safety Evaluation Report Related to the Certification of the AP600 Standard Design," Dated September 1998.

NUREG-1503, "Final Safety Evaluation Report Related to the Certification of the System 80+ Design, Docket No. 52-002," Dated July 1994.

NUREG/CR-6042, "Perspective on Reactor Safety," Dated March 1994.

SECY Papers

SECY-77-439 - Information Report - Single failure Criterion

- The single failure criterion, as a design and analysis tool, has the direct objective of promoting reliability through the enforced provision of redundancy... application of the single failure criterion requires that a system which is designed to perform a defined safety function must be capable of meeting its objectives assuming the failure of any major component within the system or an associated system which supports its operation. The objective is to search for design weaknesses which could be overcome by increased redundancy, use of alternate systems or alternate procedures. *The single failure criteria must be supplemented by methods and criteria in the area of common mode assessments if improved reliability characteristics for safety systems are necessary.*

SECY-91-292 - Digital Computer Systems for Advanced Light Water Reactors, September 26, 1991

- Discusses issues with design implementation of digital I&C technology and the development of a review process for advanced light water reactors. 10 CFR Part 52 states that current NRC requirements referenced in the SRP are primarily the single failure criteria and redundancy and that new requirements are needed to address the potential for common-mode failure sources that are more likely to exist in digital systems. SECY-91-292 also noted that there were currently no regulatory requirements that adequately addressed potential safety concerns with digital I&C. Suggested regulatory requirement areas identified included assessment of diversity, engineering activities, design implementation and safety classification.

SECY 93-087 - Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, (Item II Q), April 2, 1993

- Defense against common-mode failures in digital I&C systems. Identifies staff concerns that hardware design error, software design error, or software programming may result in a safety significant common-mode failure of redundant equipment. The staff identified two principal factors for defense against common-mode failures - quality and diversity. Proposed four positions with respect to digital I&C and defense against common-mode failures.

SECY-98-144 - White Paper on Risk-Informed and Performance-Based Regulation

- Definition - Defense-in-Depth is an element of the Nuclear Regulatory Commission'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.

SECY-00-0198 - Status Report on Study of Risk-Informed Changes to the Technical Requirements of 10 CFR Part 50, to provide the staff's recommendations for risk-informed changes to 10 CFR 50.44 (Standards for Combustible Gas Control System in Light-Water-Cooled Power Reactors") that will both enhance safety and reduce unnecessary burden, and provide policy issues for Commission Decision.

- Discusses defense-in-depth, proposed definition and risk-informed approach.

SECY-03-0047 - Policy Issues Related to Licensing Non-Light-Water Reactor Designs

SECY-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.

- Proposes Definition of Defense-in-Depth to be incorporated into a policy statement.

SECY-05-130 - Policy Issues Related to New Plant Licensing and Status of the Technology Neutral Framework for new Plant Licensing

SECY-05-0138 - Staff Requirements - SECY-05-0138 - Risk-informed and Performance-Based Alternatives to the Single-Failure Criterion

- One of the principles of defense-in-depth is that accomplishing key safety functions should not depend upon a single element of design, construction, or operation. The single failure criterion addresses this requirement by providing a measure of redundancy to fulfill key safety functions. Redundancy enhances the reliability of independent means; diversity protects against dependent (common-cause) failures of multiple means, and, therefore, protection against the uncertainty in the mechanism of dependent failures. The SFC ensures redundancy, but not necessarily diversity. For example, two similar trains of ECCS provide redundancy, while one motor driven and one steam-driven source of injection offers redundancy and diversity; both satisfy the SFC. The SFC was supplemented to enhance levels of safety (e.g., by adding the requirements related to AFW, ATWS and SBO). RG 1.174 recognizes that redundancy, the central feature of the SFC, is an important element of the defense-in-depth philosophy.

SECY-06-0007 - Staff Plan to Make a Risk-Informed and Performance-based Revision to 10 CFR Part 50.

SECY-07-0101 - Staff Recommendations Regarding a Risk-informed and Performance-Based Revision to 10 CFR Part 50.

- Recommends that a policy statement on defense-in-depth for future plants be developed.

SRM to SECY 93-087 - Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, (Item II Q).

- Modified the staff positions first by stating that inasmuch as common mode failures are beyond design basis events and as such the analysis used should be on a best estimate basis. In addition, the safety grade requirement was removed from the fourth position.

SRM to SECY-98-144 - White Paper on Risk-Informed and Performance Based Regulation.

SRM to SECY-00-198 - Status Report on Study of Risk-Informed Changes to the technical Requirements of 10 CFR Part 50, to provide the staff's recommendations for risk-informed changes to 10 CFR 50.44 (Standards for Combustible Gas Control System in Light-Water-Cooled Power Reactors") that will both enhance safety and reduce unnecessary burden, and provide policy issues for Commission Decision.

SRM to SECY-03-047 - Policy Issues Related to Licensing Non-Light-Water Reactor Designs.

SRM to SECY-05-130 - Policy Issues Related to New Plant Licensing and Status of the Technology Neutral Framework.

SRM to SECY-05-138 - Risk-Informed and Performance-Based Alternatives to the Single Failure Criterion.

SRM TO SECY-06-0007 - Staff plan to Make Risk-Informed and Performance based Revision to 10 CFR Part 50.

SRM to SECY-07-0101 - Staff Recommendations Regarding a Risk-informed and Performance-Based Revision to 10 CFR Part 50.

ACRS References

ACRS Letter to the Chairman on "The Role of Defense-in-Depth in a Risk-Informed Regulatory System," Dated May 19, 1999.

ACRS Letter to the Chairman, "Technology-Neutral Framework for Future Plant Licensing," Dated April 20, 2007.

ACRS Letter to the Chairman, "Draft Commission Paper on Staff Plan Regarding a Risk Informed and Performance based Revision to 10 CAR Part 50," Dated May 16, 2007.

ACRS Letter to the Chairman, "Use of Defense-in- Depth in Risk-Informing NESS Activities," Dated May 25, 2000.

ACRS Letter to the Chairman, "Draft Commission Paper on "Risk-Informed Alternatives to the Single Failure Criterion," Dated June 10, 2005.

ACRS

Letter to the Chairman, Digital Instrumentation and Control Systems Project Plan and Interim Staff Guidance,” Dated October 16, 2007.

U.S. Atomic Energy Commission (USAEC)

“Nuclear Power Reactor Instrumentation Systems handbook, Volume 2, “ May 1974.

- Historical perspective concerning single failure, redundancy, common mode failures, independence, and diversity with regard to I&C systems protection systems (i.e., reactor trip and engineered safety features). Includes numerous additional references.

International Atomic Energy Agency

IAEA Safety Series No. 50-P-1, “Application of the Single Failure Criteria”, 1990.

- To determine the degree of system or component redundancy, to ensure adequate reliability of the safety function. Notes that the single failure criterion is only capable of dealing with random failures. Redundancy can be defeated by common cause failures which are the result of dependencies between components or systems (common cause).

IAEA Safety Series, No. 46, Dated 2005, “Assessment of Defense-in-Depth for Nuclear Power Plants.

- Describes a method for defense-in-depth including levels of defense-in-depth.

IAEA, INSAG -10, dated 1996, “Defense in Depth in Nuclear Safety.”

- Defense-in-Depth is stated as a two fold strategy: first to prevent accidents and, if prevention fails, limit the potential consequences and prevent an evolution to a more serious condition.
- Prerequisites are:

Conservatism, quality assurance and safety culture.
- Defense-in-depth is structured with four physical barriers and five levels as shown.
 1. Prevention of abnormal operation and system failures.
 2. Control of abnormal operation and detection of failures.
 3. Control of accidents within the design basis.
 4. Control of severe plant conditions, including accident progression and mitigation of the consequences of severe accidents.
 5. Mitigation of radiological consequences of significant releases of radioactive materials.

INSAG-10 also includes a defense-in-depth verification process which is to be performed throughout the lifetime of the plant.

IAEA-TECDOC-986, "Implementation of Defence-in-Depth for Next Generation Light Water Reactors, 1997.

Provides implementation guidance specifically for future reactors, but is consistent with INSAG-10. IAEA-TECDOC-986 provides discussion on grouping (screening) severe accident sequences (addressed in design or discounted as being of extremely low likelihood). Limited discussion on digital systems and the option of hard wired backup.

WCAP-7306 April 1969, "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors."

Provides an early example of a defense-in-depth analysis. Documents information provided to the AEC with respect failure modes changing from that of a single random failure to common-mode failures. A common mode failure stated as, "a failure mode that would adversely affect all redundant channels of a particular protective function in the protection system." The issues concerned single and multiple failures, channel independence, control and protection system independence, and the derivation of protection system inputs are evaluated.

Stated that to demonstrate diversity where protective action is needed to show combinations of two or more "barriers" as identified in WCAP-7306 for each accident.

- Tolerable consequences.
- Low Probability of the accident.
Considered but only in conjunction with the probable consequences.
- Control interlocks.
- Manual Action.
- Automatic Reactor Trip.
- Backup reactor trip - a second reactor trip function, of a diverse type is an additional barrier.

USAEC Report BAW-10019, "Babcock & Wilcox Co. Systematic Failure Study of Reactor Protection Systems," Dated September 1970.

CENPD-11, "Reactor Protection System Diversity Report, "Combustion Engineering, Dated February 1971.

WCAP-15775, "AP1000 Instrumentation and Control Defense-in-Depth and Diversity Report," dated March 2003.

- Discusses conformance to NUREG/CR-6303 and NUREG-0493.

National Research Council

National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants," National Academy Press, dated 1997.

Defense-in-Depth - Historical

AEC - 1967

1. Prevention of Initiating Events.
2. Safety Features to prevent accidents.
3. Consequence limiting systems to prevent large releases.

NRC - 1994

1. Accident Prevention.
2. Safety systems to prevent accidents.
3. Containment to limit releases.
4. Accident management.
5. Reactor siting and Emergency Planning.

IAEA - 1996

1. Prevention of abnormal operation and failures.
2. Control abnormal operation and detection of failures.
3. Control accidents within design basis using ESF and procedures.
4. Control of severe conditions by preventing accident progression, mitigation by accident management.
5. Mitigation of radiological consequences via emergency response.

NRC - 1998

RG Guide 1.174

1. A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
2. Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.
3. System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties.

4. Defenses against potential common cause failures are preserved, and the potential for introduction of new common cause failure mechanisms is assessed.
5. Independence of barriers is not degraded.
6. Defense against human error is preserved.
7. The intent of the GDCs in Appendix A to 10 CFR Part 50 is maintained.

NRC - 2000

Reactor Oversight Process

1. Initiating Events - Limit frequency (upset plant stability and challenge critical safety functions).
2. Mitigating Systems - Limit core damage probability – ensure the availability, reliability, and capability of systems designed to mitigate the effects of initiating events to prevent core damage.
3. Barrier Integrity - Limit release – barriers are fuel cladding, reactor coolant system boundary, and the containment.
4. Emergency Preparedness - Limit public health effects – ensure adequate protection of public health and safety during a radiological emergency.

NRC- 2003

Risk-informing part 50 - see above.

SAFETY EVALUATIONS

Turkey Point - Load Sequencer

Haddam Neck - RPS upgrade (Foxboro)

Sequoyah - Eagle 21 upgrade

Zion - Eagle 21 Upgrade

D.C. Cook RPS upgrade (Foxboro)

Diablo Canyon - Eagle 21 Upgrade

Palo Verde Nuclear Generating Station, Units 1, 2, and 3 - Issuance of Amendments on the Core Protection Calculator System Upgrade.

Safety Evaluation (SE) by The Electrical and Instrumentation and Controls Branch, Office of Nuclear Reactor Regulation Siemens Power Corporation Topical Report Emf-2110(np)
"Teleperm Xs: a Digital Reactor Protection System."

SE of Triconex Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 to Qualification Summary Report," Revision 1.

SE of Westinghouse Topical Report WCAP-15413, "Westinghouse 7300a ASIC-based Replacement Module Licensing Summary Report."

SE of CENPD-396-P, "Common Qualified Platform" and Appendices 1, 2, 3, and 4.

SE of TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications."

SE of TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."

SE of WCAP-15413, "Westinghouse 7300A ASIC Based Replacement Module Licensing Summary report."