NARSIS Workshop
Training on Probabilistic Safety Assessment for Nuclear Facilities
September 2-5, 2019, Warsaw, Poland

Identification of critical elements within NPPs

Screening and ranking methods

Andrija Volkanovski, Andrej Prošek

Jožef Stefan Institute

Content

- Nuclear safety fundamentals
- Deterministic classification of SSC
- PSA description
- Definition of RISC Categories and utilization for identification of NPP critical elements

1. Nuclear safety fundamentals

"Nuclear safety"

- IAEA definition: The achievement of proper *operating conditions*, prevention of *accidents* and mitigation of *accident* consequences, resulting in protection of workers, the public and the environment from undue radiation risks.
- The prime purpose of the nuclear safety is prevention of the release of radioactive materials formed in the fuel, ensuring that the operation of nuclear power plants does not contribute significantly to individual and societal health risk.

INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: 2018 Edition, IAEA, Vienna (2019).

Nuclear safety (cont'd)

- Prevention of radiation risk is achieved by:
  - Preventing major damage of the reactor core or the used nuclear fuel bundles,
  - If this is not successful, preventing release of radioactive nuclides from the damaged core to the environment.

Safety functions

- **Control of reactivity** - preventing uncontrolled reactor power increase and shutting down the reactor when needed
- **Removal of heat from the reactor and from the fuel store** - cooling of shutdown reactor and used nuclear fuel
- **Confinement of radioactive material** - preventing significant radioactive releases to the environment

Safety functions (cont'd)

Fundamental (basic) safety functions:

- Shall be assured in **all situations**
- Preferably by means of **inherent safety** features relying on the laws of nature, and
- As the second alternative by **reliable active safety systems** designed to carry out these functions (high quality, redundancy, diversity)

Safety functions (cont'd)

- The systems and structures providing the basic safety functions shall be protected from **HAZARDS** that may threaten their integrity and intended function.
- **Hazard**: The physical effects of a natural phenomenon such as flooding, tornado, or earthquake that can pose potential danger [ANSI/ ANS-58.21-2003]

Protection of safety functions from hazards

10 CFR 50, Appendix A:

- Criterion 2—Design bases for protection against natural phenomena
- Criterion 3—Fire protection
- Criterion 4—Environmental and dynamic effects design bases

CFR – Code of Federal Regulations (in United States)

10 CFR 50 Appendix A

Title 10: Energy

Part 50 (0-199): Rules for license application, facility design requirements, and reporting of events to the NRC

10 CFR 50 APPENDIX A

Code of Federal Regulations

Code of Federal Regulations, Title 10, "Energy," Part 50, "Licensing of Production and Utilization Facilities," Appendix A, "General Design Criteria for Nuclear Power Plants".

General Design Criteria for NPP

Criterion 2

Criterion 2 - Design bases for protection against natural phenomena

- "Structures, systems, and components important to safety **shall be designed** to withstand the effects of natural phenomena such as **earthquakes**, tornadoes, hurricanes, floods, ***tsunami***, and seiches without loss of capability to perform their safety functions."

Criterion 2 (cont'd)

"The design bases for these structures, systems, and components shall reflect:

(1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with **sufficient margin** for the limited accuracy, quantity, and period of time in which the historical data have been accumulated,

(2) appropriate **combinations** of the effects of normal and accident conditions with the effects of the natural phenomena and

(3) the importance of the safety functions to be performed."

Criterion 3

Criterion 3 - Fire protection

- "Structures, systems, and components important to safety **shall be designed** and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions."
  - noncombustible and heat resistant materials used, fire detection and fighting systems provided

Criterion 4

Criterion 4 - Environmental and dynamic effects design bases

- "Structures, systems, and components important to safety **shall be designed** to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. "

Final Safety Analysis Report (FSAR)

- FSAR is submitted with each application for an operating license and includes a description of the facility, the design bases and limits on its operation and a safety analysis of the structures, systems and components (SSCs) of the facility.
- FSAR demonstrates the applicant's qualifications; capability, and planned controls to assure safe plant operation within the constraints of plant design, operating limitations and regulatory requirements.

FSAR (cont'd)

- Description and Safety Assessment of Site (10 CFR 100)
- Description of the Facility Design and Design Bases (10 CFR 50, Appendix A - ANSI 18.2A, Safety Classes)
- Accident Analysis (10 CFR 50.46, ECCS Acceptance Criteria) (ANSI 18.2, Conditions for Design)
- Technical Specification (10 CFR 50.36)
  - Technical specifications (TS) establish minimum operating criteria for the facility. The basis for tje criteria established in TS is the analyses and evaluations included in the FSAR.
- Description of Quality Assurance Program (10 CFR 50, Appendix B)
- The requirements for having an FSAR and minimum information is established in the 10 CFR 50.34(b)

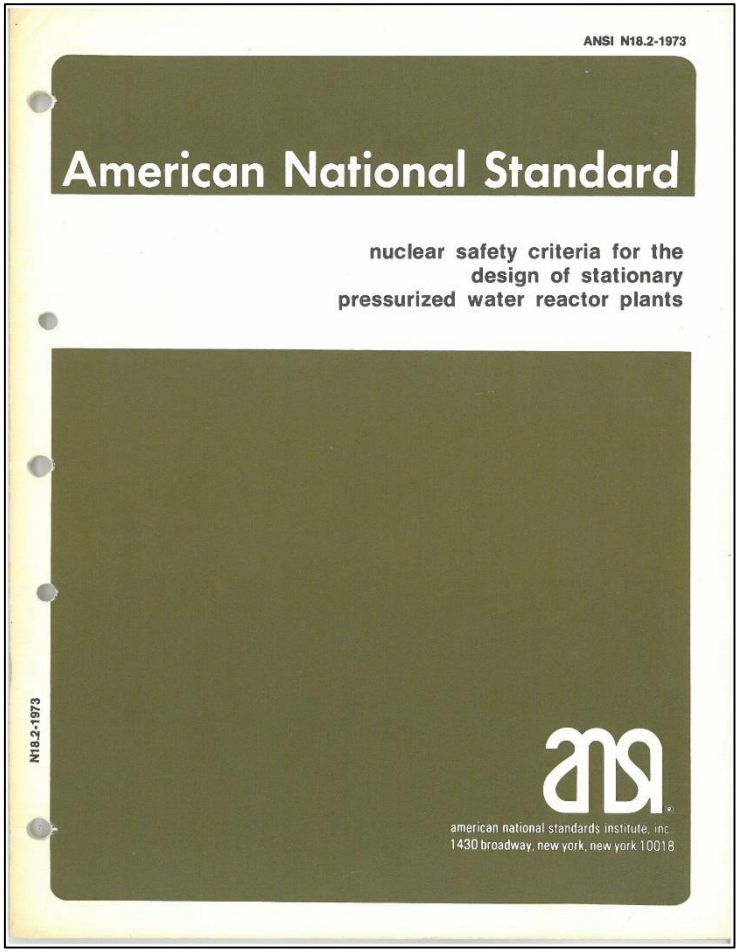
Codes and Standards

- CFR is written in general terms
- Supplementary documentation is necessary
- 10 CFR 50.55a Codes and standards
- Systems and components of BWR/PWR: ASME Boiler and Pressure Vessel Code
- Protection & safety systems: IEEE Std.603-1991

BWR – Boiling Water Reactor; PWR – Pressurized Water Reactor; ASME – American Society of Mechanical Engineers; IEEE – Institute of Electrical and Electronics Engineers

ANSI Standard 18.2

- Establishes the nuclear safety criteria and functional design requirements of SSC of stationary PWR power plants. Operations, maintenance, and testing requirements are covered only to the extent that they affect design provisions.



ANSI – American National Standards Institute

ANSI Standard 18.2 (cont'd)

- A methodology is given for identifying and categorizing into one of **four Plant Conditions** the normal operations and events for which the plant shall be designed. Acceptance criteria are given for each Plant Condition. These design conditions and requirements are analyzed for each plant, and the results are documented in the facility's FSAR.

ANSI Standard 18.2 (cont'd)

- Specific design criteria are given for systems in a typical pressurized water reactor (PWR) plant. These requirements are related to other, more specific design standards and are intended to amplify the criteria given in 10CFR50, Appendix A.
  - systems: reactor core assembly, reactivity control capability, protection systems and safety instrumentation and control, reactor plant fluid systems, enigineered safety features, radioactive waste disposal system, fuel handling sytem, electrical power systems.

ANSI Std. 18.2: Conditions For Design

ANSI Std. 18.2: Conditions For Design:

- Condition I - Normal Operation
- Condition II - Moderate Frequency Incidents
- Condition III - Infrequent Incidents
- Condition IV - Limiting Faults

Each condition defined by the expected frequency of occurrence and its probability of deteriorating to a worse case condition.

ANSI Std. 18.2 Condition I - Normal Operation

ANSI Std. 18.2 **Condition I** - Normal Operation:

- Condition I occurences are operations that are expected frequently or regularly in the course of power operation, refueling, maintenance, or maneuvering of the plant.
  - Examples: startup, shutdown, standby, power operation from partial load to maximum anticipated power level.
- Design Requirement. Condition I occurrences shall be accommodated *with margin* between any plant parameter and the value of that parameter which would require either automatic or manual protective action.

ANSI Std. 18.2 Condition II - Moderate Frequency Incidents

ANSI Std. 18.2 **Condition II** - Incidents of Moderate Frequency:

- Condition II occurences includes incidents, any of which may occur during a calendar year for a particular plant.
  - Examples: loss of normal feedwater, loss of off-site power, inadvertent control rod group withdrawal, steam generator tube leaks…
- Design Requirement. Condition II incidents shall be accommodated with, at most, a shutdown of the reactor with the plant capable of returning to operation after corrective action.

ANSI Std. 18.2 Condition III - Infrequent Incidents

ANSI Std. 18.2 **Condition III** - Infrequent Incidents:

- Condition III occurences include incidents, any of which may occur during the lifetime of a particular plant.
  - Examples: insertion of unexplained reactivity, gas decay tank rupture..
- Design Requirements. Condition III incidents shall not cause more than a small fraction of the fuel elements in the reactor to be damaged, although sufficient fuel element damage might occur to preclude resumption of operation for a considerable outage time.

ANSI Std. 18.2 Condition IV - Limiting Faults

ANSI Std. 18.2 **Condition IV** - Limiting Faults:

- Condition IV occurences are faults that are not expected to occur, but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material. Condition IV faults are the most drastic that must be designed against, and thus represent the limiting design case.
  - Examples: major rupture of a pipe containing reactor coolant up to and including double-ended rupture of the largest pipe in the reactor coolant pressure boundary, ejection of any single control rod, single reactor coolant pump locked rotor.
- Design Requirements. Condition IV faults shall not cause a release of radioactive material that results in an undue risk to public health and safety exceeding the guidelines of 10 CFR 100, "Reactor Site Criteria.„ A single Condition IV fault shall not cause a consequential loss of required functions of systems needed to cope with the fault including those of the reactor coolant system and the reactor containment system.

2. Deterministic classification of SSC

ANSI Std. 18.2a Safety Classifications

- A methodology is given for classifying all equipment into one of **three Safety Classes** according to its importance to nuclear safety or into a **Non-Nuclear Safety Class**.
- ANSI Standard 18.2a defines safety classes used to designate safety systems and components in accordance with their importance to nuclear safety.
- ANSI 18.2a defines a safety system as any system that is necessary to:
  - shut down the reactor,
  - cool the core,
  - cool another safety system, or
  - cool the reactor containment after an accident.
- In addition, any system that contains, controls, or reduces radioactivity released in an accident is a safety system.

ANSI Std. 18.2 Safety Classifications (cont'd)

Safety Class I, SC-I applies to components whose failure could cause a Condition III or Condition IV loss of reactor coolant.

ANSI Std. 18.2 Safety Classifications (cont'd)

Safety Class 2, SC-2 applies Safety Class 2 generally applies to reactor containment and RCS pressure boundary components not in Safety Class 1.

Also included in Safety Class 2 are:

- safety systems that remove heat from the reactor or reactor containment,
- circulate reactor coolant, or
- control radioactivity or
- hydrogen in containment.

ANSI Std. 18.2 Safety Classifications (cont'd)

Safety Class 3, SC-3, applies to those components not in SC-1 or SC-2:

1. Provide or support any safety system function,
2. Control outside the reactor containment airborne radioactivity released, or
3. Remove decay heat from spent fuel

Non-nuclear safety (NNS) applies to those components not in SC-1, SC-2 or SC-3 (example turbine-generator).

ANSI/ANS-51.1-1983

- ANSI/ANS-51.1-1983 (revision and combination of N18.2-1973(ANSI51.1 and N18.2a-1975/ANS-51.8); R1988; W1998: Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants
  - major systems: reactor core and internals; reactivity control systems; protection systems; reactor coolant system; shutdown heat removal system; reactor coolant auxiliary systems; cooling water systems; emergency core cooling systems, primary containment, emergency secondary heat removal systems, containment auxiliary systems, safety-related area cooling systems, fuel storage and handling, electrical power systems, fire protections systems, control complex, radioactive waste processing systems, other structures, power conversion system, multi-unit stations.

ANSI – American National Standards Institute; ANS – American Nuclear Society

ASME Code Classification

American Society of Mechanical Engineers (ASME) Code Classification

- Code Classes 1, 2, and 3 for fluid system components and Code Class MC for reactor containment components (design and quality assurance requirements)

Safety Class (SC)	Code Class
SC-1	1
SC-2 for reactor containment components	MC
SC-2 for other than reactor containment components	2
SC-3	3

IEEE standards

Institute of Electrical and Electronic Eng. (IEEE) Std.

- IEEE standards are used in the design, operation, and testing of nuclear power plant electrical, and instrumentation components and systems.
- IEEE standards define as **Class IE**, electrical equipment and systems that are **essential** to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

IEEE standards (cont'd)

Institute of Electrical and Electronic Eng. (IEEE) Std.

- 279-1971 - IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations
- 379-2000 - IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems
- 308-2001 - IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations

3. PSA description

Probabilistic Safety Assessment (PSA/PRA)

Probabilistic Safety Assessment (PSA/PRA)

- A systematic method for assessing "risk“:

(1) What can go wrong,

(2) How likely it is, and

(3) What its consequences might be.

PSA provides insights into the strengths and weaknesses of the design and operation of a nuclear power plant.

PSA/PRA (cont'd)

Probabilistic Safety Assessment (PSA/PRA)

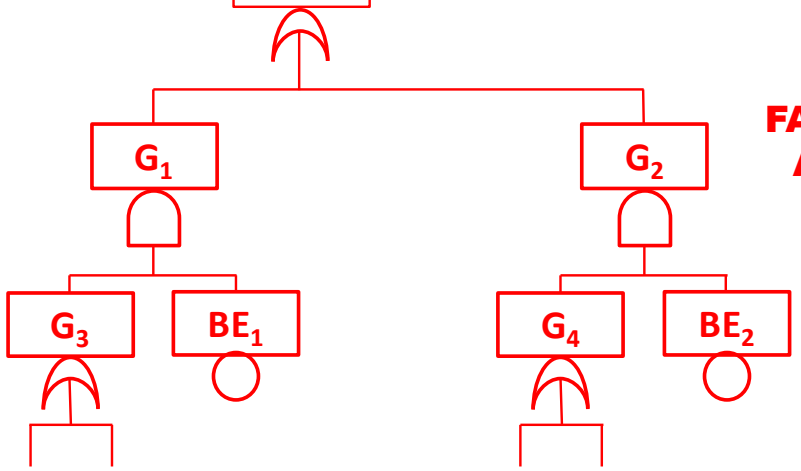
- Level 1 PSA estimates the frequency of accidents that cause damage to the nuclear reactor core. This is commonly called core damage frequency (CDF).
- Level 2 PSA, which starts with the Level 1 core damage accidents, estimates the frequency of accidents that release radioactivity from the nuclear power plant.
- Level 3 PSA, which starts with the Level 2 radioactivity release accidents, estimates the consequences in terms of injury to the public and damage to the environment.

PSA level 1

PSA level 1

EVENT TREE ANALYSIS

INITIATING EVENT (IE)	SAFETY SYSTEM 1 (SS1)	SAFETY SYSTEM 2 (SS2)	SAFETY SYSTEM 3 (SS3)	No.	Frequency	State
4E-5 /yr	SS1 succeeds	SS2 succeeds	SS3 succeeds	1	3.92E-5 /yr	OK
			1.11E-2 SS3 fails	2	4.39E-7 /yr	CD
		1.01E-2 SS2 fails		3	4.00E-7 /yr	CD
	1.10E-4 SS1 fails			4	4.40E-9 /yr	CD



FAULT TREE ANALYSIS

PSA/PRA (cont'd)

Probabilistic Safety Assessment (PSA/PRA)

- Qualitative results include:
  - Minimal cut sets (how systems, NPP fail)
  - Qualitative importance (qualitative rankings of contributions)
  - Common cause potentials (MCS susceptibility to CCF).
- The quantitative results include:
  - Numerical probabilities/frequencies (CDF/LERF)
  - Quantitative importance (Importance measures)
  - Sensitivity evaluations

MCS – minimal cut sets, CCF – common cause failure, LERF – large early release frequency

Decision criteria in PSA applications, NKS-44, 2001, Finland

Risk measure	criteria
RRW - Risk Reduction Worth	
• System level - significant importance	> 1.05
• Component level – significant importance	> 1.005
RAW - Risk Achievement Worth	
• significant importance	> 2
• very safety severe	> 10
• safety severe	> 1.05
FV - Fussel-Vesely Importance	
• System level - significant importance	> 0.05
• Component level – significant importance	> 0.005

Birnbaum Importance
Fussel-Vesely Importance

$$BI(i) = Qs(Qi=1) - Qs(Qi=0)$$

The Birnbaum importance (BI) is a well-known measure that evaluates the relative contribution of components to system reliability.

$$FV(i) = \frac{Qs(Qi) - Qs(Qi=0)}{Qs(Qi)}$$

Fussell-Vesely Importance (F-V)
Fussell-Vesely Importance of a modeled plant feature (usually a component, train, or system) is defined as the fractional decrease in total risk level (usually CDF) when the plant feature is assumed perfectly reliable (failure rate = 0.0). If all the sequences comprising the total risk level (e.g. CDF) are minimal, the F-V also equals the fractional contribution to the total risk level of all sequences containing the (failed) feature of interest. Note that F-V = 1-1/RRW. (See Risk Reduction Worth.)

Qs … system unavailability
Qi … unavailability of component i
Qs(Qi=0) … system unavailability when unavailability of component i is 0
Qs(Qi=1) … system unavailability when unavailability of component i is 1

Risk Achievement Worth
Risk Reduction Worth

$$RAW(i) = \frac{Qs(Qi=1)}{Qs(Qi)}$$

Risk Achievement Worth (RAW)
Risk Achievement Worth (RAW) of a modeled plant feature (usually a component, train, or system) is the increase in risk if the feature is assumed to be failed at all times. It is expressed in terms of the ratio of the risk with the event failed to the baseline risk level.

$$RRW(i) = \frac{Qs(Qi)}{Qs(Qi=0)}$$

Risk Reduction Worth (RRW)
Risk Reduction Worth (RRW) of a modeled plant feature is the decrease in risk if the feature is assumed to be perfectly reliable. It is expressed in terms of the ratio of the baseline risk level to the risk with the feature guaranteed to succeed. See Fussell-Vesely Importance.

Qs … system unavailability
Qi … unavailability of component i
Qs(Qi=0) … system unavailability when unavailability of component i is 0
Qs(Qi=1) … system unavailability when unavailability of component i is 1

4. Definition of RISC Categories and utilization for identification of NPP critical elements

10CFR50.69

10CFR50.69:

- 10CFR50.69: Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors
- Risk-informed process for categorizing SSCs according to their safety significance
- Focusing of resources on safety significant components thereby allowing for the reduction in undue burden while focusing on safety improvement and enhanced equipment reliability

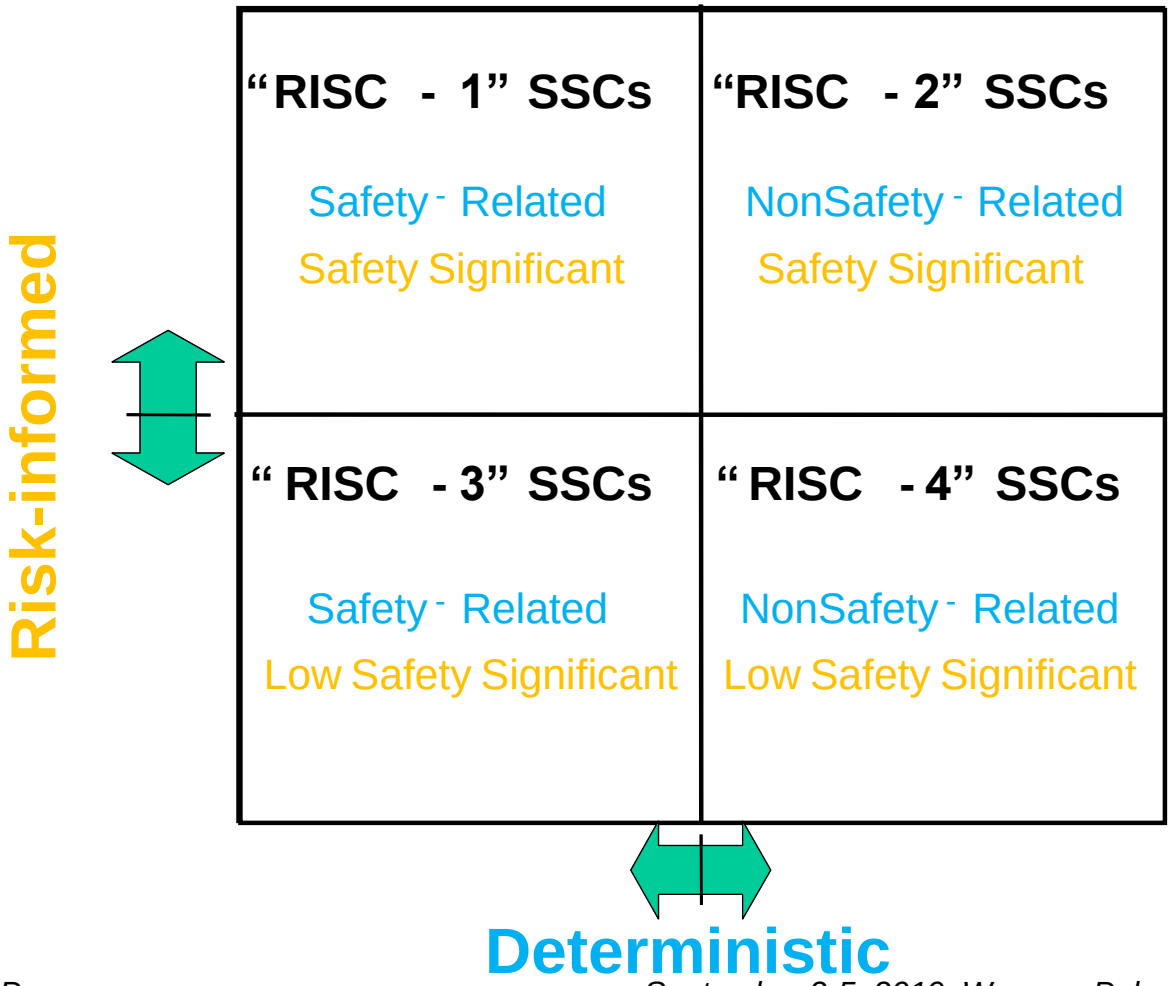
10CFR50.69 (cont'd)

10CFR50.69:

- Safety significance of SSCs is determined by an integrated decision-making process, incorporating risk and traditional engineering insights
- Safety significant function: function whose degradation or loss could result in a significant adverse effect on defense-in-depth, safety margin, or risk
- Four risk-informed safety class (RISC)

10CFR50.69 (cont'd)

10 CFR 50.69 RISC Categories



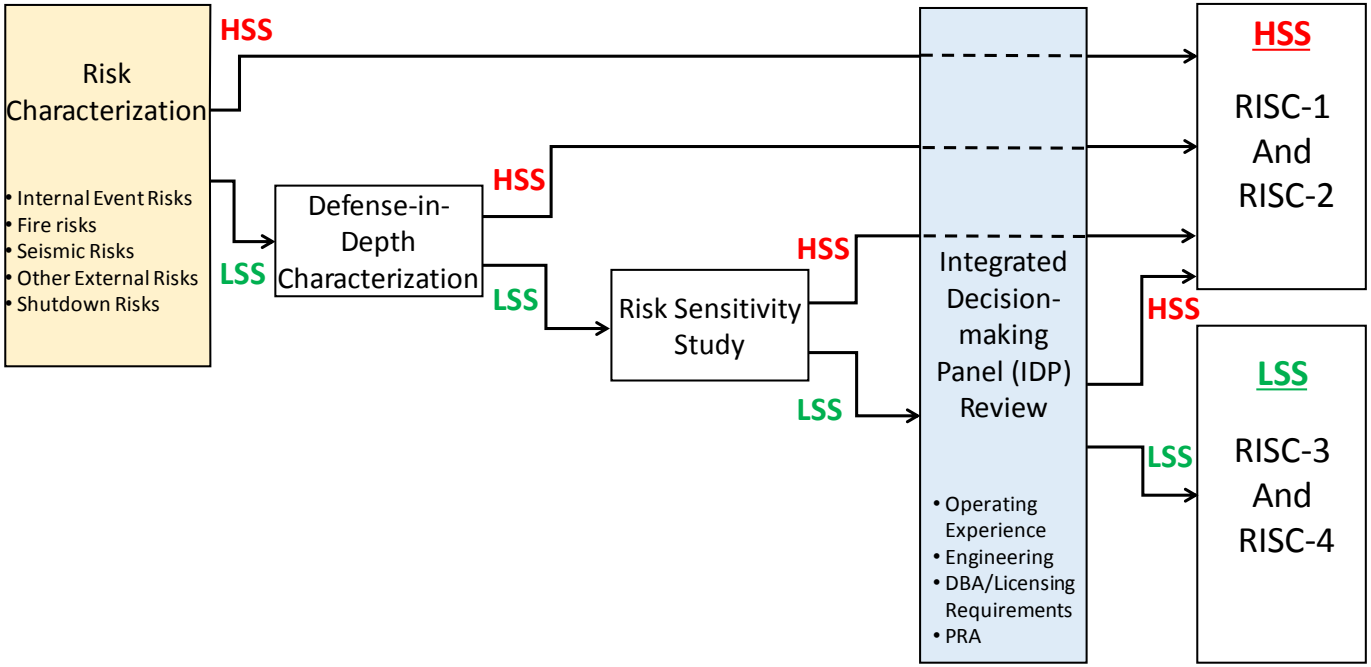
10CFR50.69 (cont'd)

- **10CFR 50.2 Definitions**
- Safety-related SSCs: those that are relied upon to remain functional during and following design basis events to assure:
  - The integrity of the reactor coolant pressure boundary
  - The capability to shut down the reactor and maintain it in a safe shutdown conditions or
  - The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guidelines exposures

NEI-00-04

➢ NEI-00-04 (10CFR50.69 SSC Categorization Guideline)

- ❑ Industry developed categorization process that utilizes a series of evaluations to determine the proper risk-informed safety classification for SSCs



NEI-00-04 (cont'd)

- **The importance measure criteria used to identify candidate safety significance are:**
  - **Sum of F-V for all basic events modeling the SSC of interest, including CCF > 0.005**
  - **Maximum of component basic event RAW > 2**
  - **Maximum of applicable common cause basic events RAW > 20.**
- **If any of these criteria are exceeded it is considered candidate safety significant SSCs**

NEI-00-04 (cont'd)

Example NEI-00-04

COMPONENT FAILURE MODE	F-V	RAW	CCF RAW
1) Valve 'A' Fails to Open	0.002	1.7	n/a
2) Valve 'A' Fails to Remain Closed	0.00002	1.1	n/a
3) Valve 'A' In Maintenance (Closed)	0.0035	1.7	n/a
4) Common Cause Failure of Valves 'A', 'B' & 'C' to Open	0.004	n/a	54
5) Common Cause Failure of Valves 'A' & 'B' to Open	0.0007	n/a	5.6
6) Common Cause Failure of Valves 'A' & 'C' to Open	0.0006	n/a	4.9
Component Importance	0.01082 (sum)	1.7 (max)	54 (max)
Criteria	> 0.005	>2	>20
Candidate Safety-significant?	**Yes**	**No**	**Yes**