SH2705 Simulation Course

Safety Margin, Single Failure & Acceptance Criteria

Sean Roshan

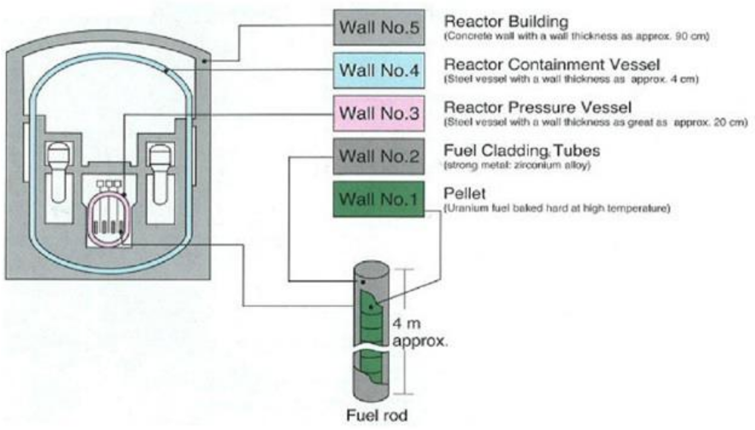
The Precautionary Principle

- Recognize and respect uncertainty of our knowledge,
- If anything can possibly go wrong, it will (Murphy’s law)
- Avoid assuming things that we do not know as safe

What do we really know?

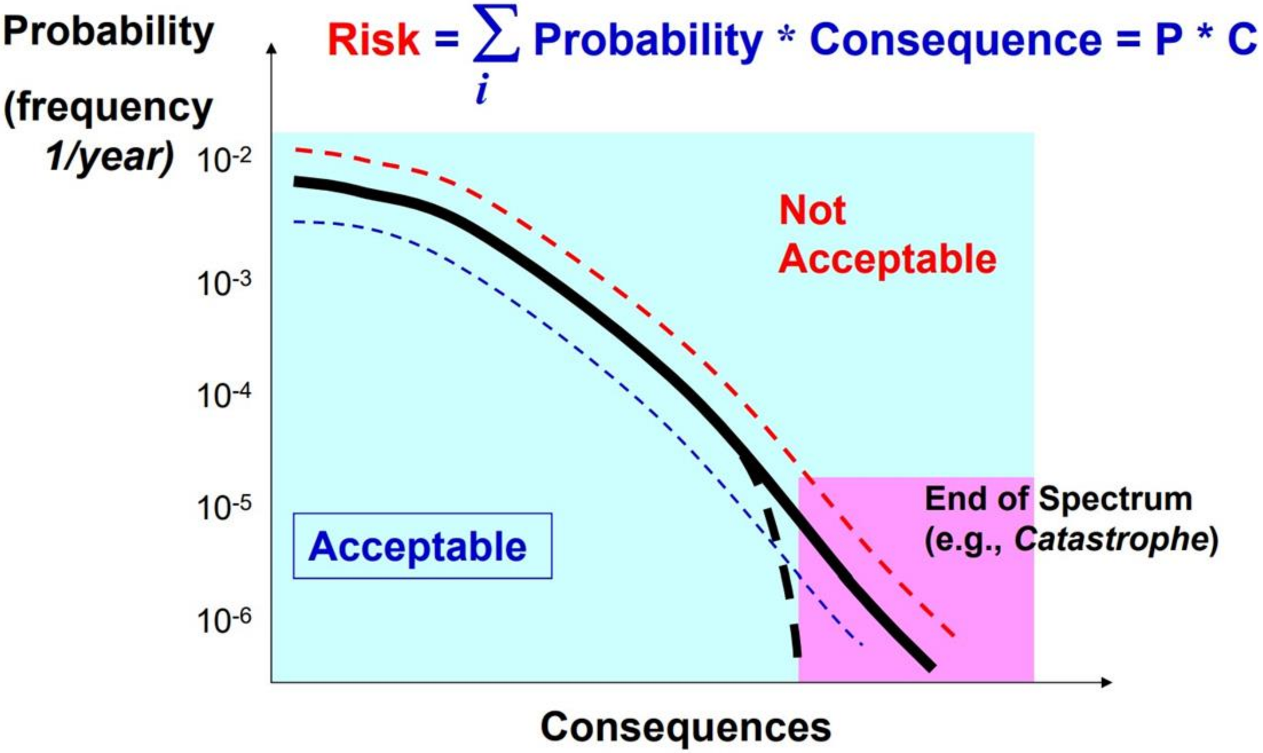
What is safe?

Defense in Depth


Wall No.5
Reactor Building
(Concrete wall with a wall thickness as approx. 90 cm)
Wall No.4
Reactor Containment Vessel
(Steel vessel with a wall thickness as approx. 4 cm)
Wall No.3
Reactor Pressure Vessel
(Steel vessel with a wall thickness as great as approx. 20 cm)
Wall No.2
Fuel Cladding Tubes
(strong metal: zirconium alloy)
Wall No.1
Pellet
(Uranium fuel baked hard at high temperature)
4 m approx.
Fuel rod

Five Walls of Protection

Probability – Consequence Curves



AEC Nuclear Safety Philosophy

"…it is never entirely assured that all accidents have been examined. It should be noted that search for credible accidents often contributes substantially to facility safety."

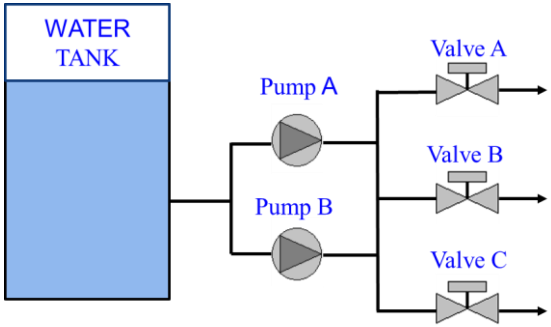
"In general, accidents would be considered credible if their occurrence might be caused by one single equipment failure or operational error, though clearly some considerations must be given to the likelihood of this failure or error."

It has been suggested that this criterion be extended to assignment of decreasing probabilities to accidents occasioned only by 2, 3, or more independent and simultaneous errors or malfunctions, with possibility that accidents requiring more than 3 or 4 such failures be considered incredible….this suggestion has not been found useful."

Single Failure Criteria

Redundancy and independence shall be sufficient to assure:

1. No single failure results in the loss of protective function..”
2. Removal from service of any component or channel does not result in loss of required minimum redundancy unless acceptable reliability of operation of protection system can be otherwise demonstrated.”
3. Protection system shall be designed for high functional reliability and in-service testability, to permit periodic testing of its functioning when reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.”



Acceptance criteria

To ensure that an adequate level of defence in depth is maintained by preventing damage to barriers and unacceptable radiological releases.

- Two levels:
  - Global/high level criteria related to doses to the public or prevention of consequential pressure boundary failure. Often defined in law or by the regulatory body.

  - Detailed criteria defined by regulatory, designer or analyst. Sufficient, but not necessary to meet the global ones.

Acceptance criteria (contd)

Detailed acceptance criteria could include:

- An event should not generate a subsequent more serious plant condition with occurrence of one further independent failure. (Single failure)
- No consequential loss of functions of the safety systems should hinder mitigation of the consequences of an accident.
- Systems for accident mitigation: designed to withstand loads, stresses and environmental conditions for the accidents.
- Pressure in primary and secondary systems should not exceed design limits.

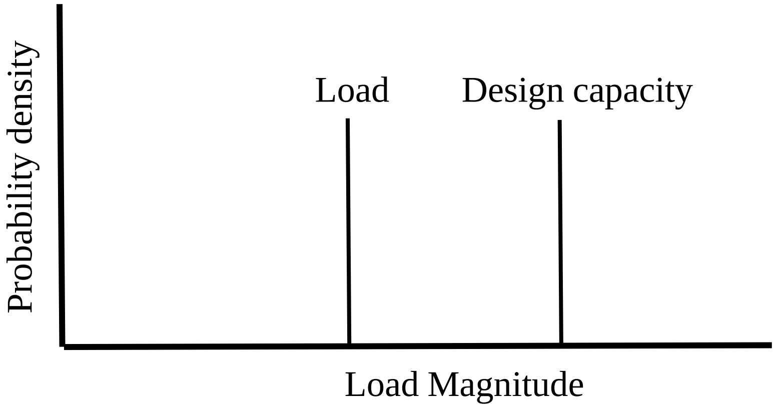
More strict criteria often applied for events with a higher frequency of occurrence.

Load vs Capacity

- Given some loading: “L” and design capacity “D”:

If L > D - the element will fail.

If L < D - the element will not fail.

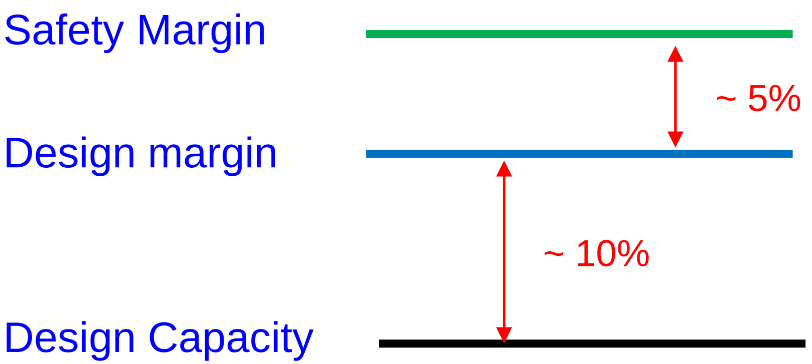


Load vs Capacity (contd)

- Design margin is defined as ‘the extent to which a parameter value exceeds what it needs to meet its functional requirements regardless of the motivation for which the margin was included. *
- Industrial Design Codes and Standards have defined conservative approaches to calculate Design Capacity.
- Use of conservative design codes and standards eliminates need of assessing individual component’s Design Margins.
- Examples include:
- ASME Boiler and Pressure Vessel Code
- IEEE, IEC Electrical Standards

* Eckert, C., Isaksson, O. & Earl, C.2012 Product property margins: An underlying critical problem of engineering design. Proceedings of TMCE 2012.

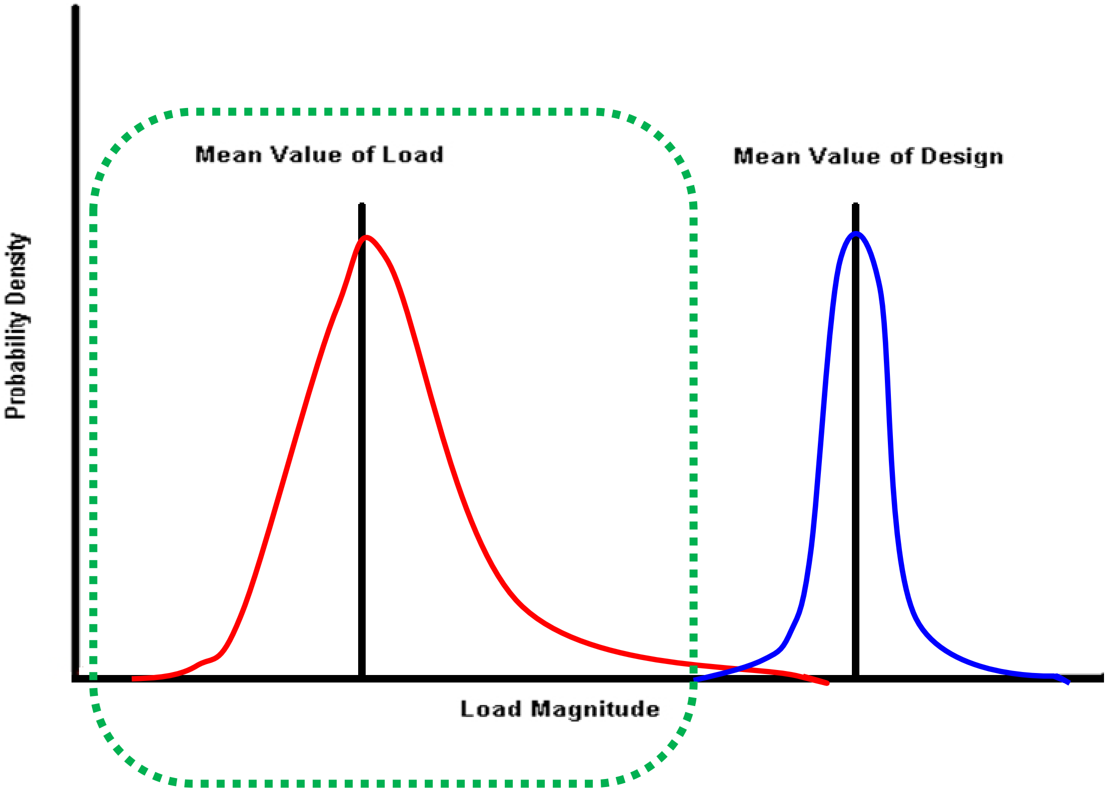
Capacity in industrial applications



Load vs Capacity (contd)

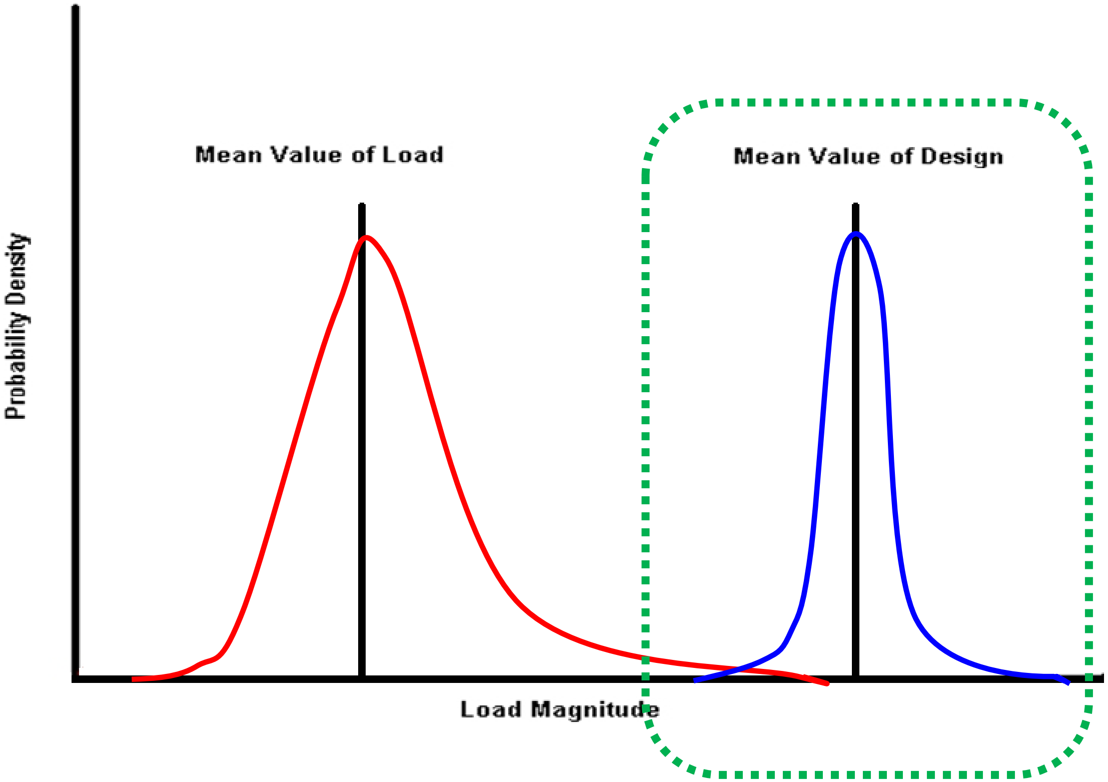
- By setting conservative definitions of Loads to be considered in design – problem of assuring Design Margins reduces considerably.
- Regulatory bodies did exactly this by issuing: Regulations.

Load vs Capacity (contd)



- L, D are actually random variables characterized by a mean value and some measure of uncertainty (density functions).
- Actual Loads can vary given circumstances and our understanding of them.
- Actual Design Capacity can vary due to manufacturing processes.

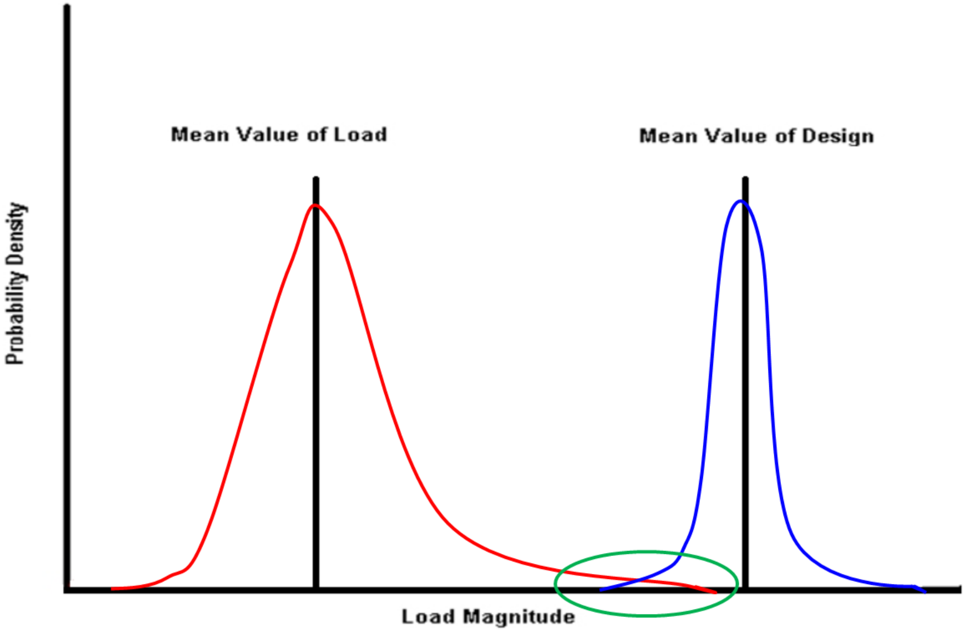
Load vs Capacity (contd)



- L, D are actually random variables characterized by a mean value and some measure of uncertainty.
- Actual Loads can vary given circumstances and our understanding of them.
- Actual Design Capacity can vary due to manufacturing processes.

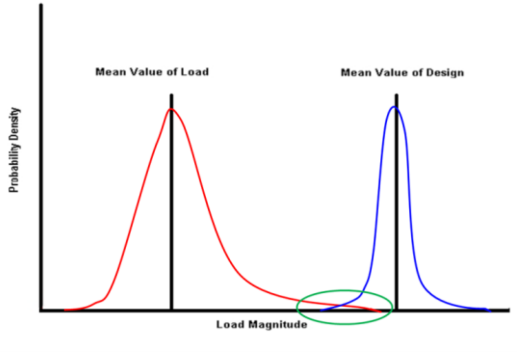
Marginal & Robust Design

- When overlap region of the "tails" is significant – a design is said to be "marginal".
- When overlap is minimal – design is said to be "robust" and not sensitive to uncertainties.
- Further analysis, integrated system testing, tends to reduce uncertainties associated with "Loads".
- Manufacturing QA programs, repeated qualification testing, tends to reduce uncertainties associated with "Design".



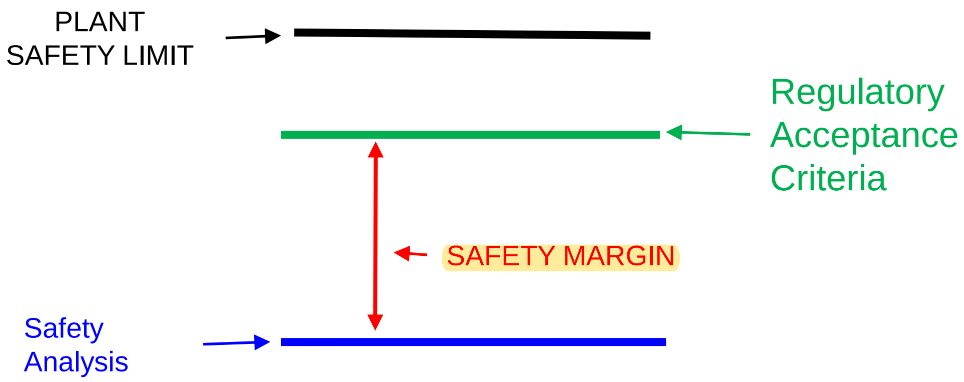
Overlapping region of load and capacity

- Usual technical problem is understanding shape of “tails” of $f_L(L+D)$ probability density function in the “overlap region” (aka how marginal is the design).



- For many general aspects of NPP design, DBA loads are used, and one sees:
  - DB earthquake (peak ground acceleration)
  - DBA LOCA (maximum diameter pipe rupture)
  - DB wind loading (maximum wind loading on buildings)
  - DB sea water temp

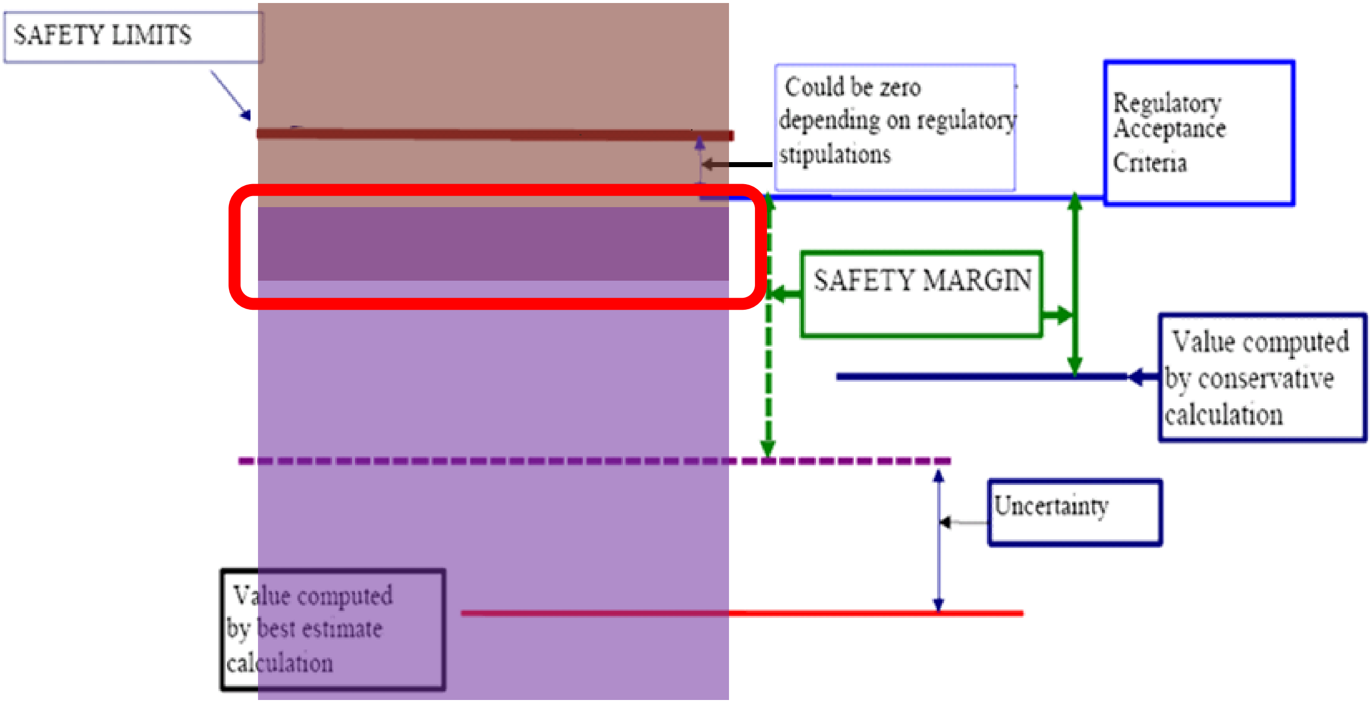
Acceptance criteria (contd)



Examples of acceptance criteria

- Allowed number of fuel cladding failures: established for each type of event to meet the global radiological criteria.
- LOCA criteria.
- Containment criteria.

Safety Margins


SAFETY LIMITS
Could be zero depending on regulatory stipulations
Regulatory Acceptance Criteria
SAFETY MARGIN
Value computed by conservative calculation
Uncertainty
Value computed by best estimate calculation

Acceptance criteria (contd)

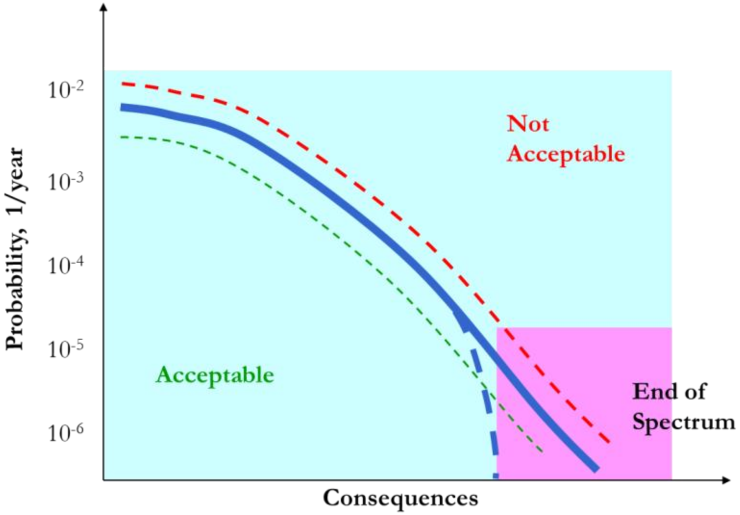
If

Risk = ∑ Probability * Consequence

then

All the AOOs and postulated accidents should produce about the same level of risk (i.e., the risk is approximately constant across the spectrum of AOOs and postulated accidents).

U.S NRC's general design criteria (GDC) generally prohibit relatively frequent events (AOOs) from resulting in serious consequences but allows the relatively rare events (postulated accidents) to produce more severe consequences.



Categorization of Transients and Accidents

Events are categorized based om Initiating or type of event,

- Initiating events are categorized according to:
  - Frequency (provides a basis for acceptance criteria)
    - AOO (accidents of moderate frequency US.NRC. RG 1.70, RG1.206, AKA ANS condition II &III)
    - Postulated and unanticipated occurrences (Not expected during the life of NPP, AKA ANS condition IV)
- Type (provides a basis for comparison between events to identify limiting cases)
  - Categorizes the events based on their effect on the plant, e.g., events that cause the RCS to pressurize and jeopardies its integrity.

Acceptance Criteria for AOOs

Condition I—normal operation and operational transients,

Pressure in the reactor coolant and main steam systems should be maintained below 110 % of the design values in accordance with the American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code.

I. Fuel cladding integrity shall be maintained by ensuring that the minimum departure from nucleate boiling ratio (DNBR) remains above the 95/95 DNBR limit for PWRs and that the critical power ratio (CPR) remains above the minimum critical power ratio (MCPR) safety limit for BWRs.

II. An AOO should not generate a postulated accident without other faults occurring independently or result in a consequential loss of function of the RCS or reactor containment barriers

- ○ The reviewer applies the third criterion, based on the ANS standards to ensure that there is no possibility of initiating a postulated accident with the frequency of occurrence of an AOO. Some of the questions that licensees must answer to justify making plant modifications without advance review (see 10 CFR 50.59) by the NRC staff reflect this concern.)

Acceptance Criteria for AOOs Condition II, III

Condition II events - faults of moderate frequency,

I. Same as above.

II. Same as above.

III. A Condition II incident cannot generate a more serious incident of the Condition III or IV category without other incidents occurring independently or result in a consequential loss of function of the RCS or reactor containment barriers.

Condition III events - infrequent faults,

I. Only small fraction of the fuel elements are damaged, although sufficient fuel element damage might occur to stop the operation for a considerable time.

II. For PWRs, the release of radioactive material may exceed guidelines of 10 CFR Part 20 but shall not be sufficient to interrupt or restrict public use of those areas beyond the exclusion radius.

For BWRs, the offsite release of radioactive material is limited to a small fraction of the guidelines of 10 CFR Part 100, which may be the result of the failure of a small fraction of the fuel elements in the reactor.

III. A Condition III incident shall not, by itself, generate a Condition IV fault or result in a consequential loss of function of the RCS or reactor containment barriers.

Acceptance Criteria for AOOs Condition IV

Condition IV—limiting faults.

A postulated accident could result in sufficient damage to preclude resumption of plant operation. Basic criteria necessary to meet the requirements of GDC for postulated accidents are:

I. Pressure in the RCS and main steam system should be maintained below acceptable design limits, considering potential brittle as well as ductile failures.

II. Fuel cladding integrity will be maintained if the minimum DNBR remains above the 95/95 DNBR limit for PWRs and the CPR remains above the MCPR safety limit for BWRs. If the minimum DNBR or MCPR does not meet these limits, then the fuel is assumed to have failed.

III. The release of radioactive material shall not result in offsite doses in excess of the guidelines of 10 CFR Part 100.

IV. A postulated accident shall not, by itself, cause a consequential loss of required functions of systems needed to cope with the fault, including those of the RCS and the reactor containment system

Acceptance Criteria for LOCA

For loss-of-coolant accidents (LOCAs), the following analysis acceptance criteria of 10 CFR 50.46 also apply:

I. The calculated maximum fuel element cladding temperature shall not exceed 2200 °F.

II. The calculated total oxidation of the cladding shall nowhere exceed 0.17 times the total cladding thickness before oxidation.

III. The calculated total amount of hydrogen generated from the chemical reaction of the cladding with water or steam shall not exceed 0.01 times the hypothetical amount that would be generated if all of the metal in the cladding cylinders surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react.

IV. Calculated changes in core geometry shall be such that the core remains amenable to cooling.

V. After any calculated successful initial operation of the emergency core cooling system (ECCS), the calculated core temperature shall should be maintained at an acceptably low value and decay heat shall be removed for the extended period of time required by the long-lived radioactivity remaining in the core.

Accident Doses Criteria

Accident or Case	EAB* and LPZ** Dose Criteria	Analysis Release Duration
LOCA	0.25 Sv TEDE***	30 days for all leakage pathways
BWR Main Steam Line Break - Fuel Damage or Pre-incident Spike - Equilibrium Iodine Activity	 0.25 Sv TEDE 0.025 Sv TEDE	Instantaneous puff, until MSIV isolation
BWR Rod Drop Accident	0.063 Sv TEDE	24 hours
Small Line Break Accident	0.025 Sv TEDE	Until isolation, if capable, or until cold shutdown is established
PWR Steam Generator Tube Rupture - Fuel Damage or Pre-incident Spike - Coincident Iodine Spike	 0.25 Sv TEDE 0.025 Sv TEDE	Affected SG: time to isolate; Unaffected SG(s): until cold shutdown is established
PWR Main Steam Line Break - Fuel Damage or Pre-incident Spike - Coincident Iodine Spike	 0.25 Sv TEDE 0.025 Sv TEDE	Until cold shutdown is established
PWR Locked Rotor Accident	0.025 Sv TEDE	Until cold shutdown is established
PWR Rod Ejection Accident	0.063 Sv TEDE	30 days for containment leakage pathway; Until cold shutdown is established for secondary pathway
Fuel Handling Accident or Cask Drop	0.063 Sv TEDE	2 hours

* EAB = exclusion area boundary
** LPZ = low population zone
*** TEDE = total effective dose equivalent