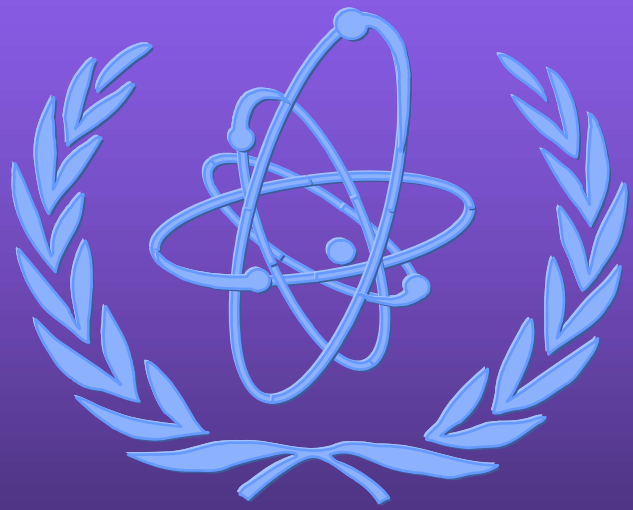
IAEA Training Course on Safety Assessment of NPPs to Assist Decision Making

Safety Assessment of General Design Aspects of NPPs (Part 1)



Lecturer
Lesson III 1_1

Workshop Information

IAEA Workshop

City , Country
XX - XX Month, Year

Items for Discussion

- Evolution of Nuclear Safety Concepts
- Defense in Depth
- Methods Used in Assessing Safety Margins
- Use of Codes and Standards in Assessing Safety Margins
- Hierarchy of Nuclear Safety Requirements

Evolution of Nuclear Safety

- Nuclear technology in US evolved from 1940's wartime environment in national laboratories.
- Computers did not exist.
- Calculations done by hand with "slide rules".
- Confirmatory test data did not exist.
- Accidents did occur – but no fatalities.
- Fear of "run-away nuclear chain reaction"
- Philosophy of "defense in depth"
- Use of conservative design parameters and multiple protective barriers.

Evolution of Nuclear Safety

- Concept of design and siting to cope with Maximum Credible Accident or MCA.
- In 1950's "run-away chain reaction" and "stability" concerns shifted to new concerns
- Release of radionuclide inventory from core
- Major unknowns included
- Fraction of core radionuclide inventory released
- Transport and uptake mechanisms
- Radioactive isotope toxicity effects

Evolution of Nuclear Safety

- Early demonstration reactor projects involved relatively small cores (< 50 MW).
- WASH-3 (1950) "rule of thumb" for Exclusion Zone:

$$R\ (\text{miles}) \sim 0.01 \times (\text{Power (KW)})^{0.5}$$

  -implications: 3000 MW $\rightarrow$ 17.3 miles!

- MCA Source Terms recognized as very pessimistic !
- Risks to public were controlled by:
  - Relatively small core radionuclide inventory
  - Low population density, remote sites

Evolution of Nuclear Safety

- 1954 Atomic Energy Act encouraged US government to: "promote the peaceful uses of atomic energy provided reasonable assurances exist that such uses would not result in undue risks to the health and safety of the public."
- Authorized private enterprises to build and operate NPPs.
- USAEC established as government agency to set regulations and issue licenses.
- NOTE: *USAEC reorganized as USNRC (1976).*

AEC Nuclear Safety Philosophy

- "If worst conceivable accidents are considered no site except one removed from populated areas by hundreds of miles would offer sufficient protection."

- "… if safeguards are included in facility design against all possible accidents having unacceptable consequences, then it could be argued that any site would be acceptable assuming that safeguards would not fail and that some dangerous accidents had not been overlooked."

- It is desired that "in plants finally approved for operation, there are really no credible potential accidents remain against which safeguards have not been provided to the extent that the calculated consequences to the public are unacceptable."

* *Taken from paper by Dr. Clifford Beck (USAEC) delivered to World Nuclear Congress of 1959 in Rome Italy.*

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."

From this Early Statement of Nuclear Safety Philosophy

Need to Consider nuclear safety implications of any credible single failure events:

- Any pipe break or seal leak in any location
- Any electrical fault
- Any mechanical component failure
- Single Operator Error
- Not to consider certain “incredible events”
- Catastrophic failure of the Reactor Pressure Vessel
- Multiple independent failure events

Evolution of Nuclear Safety

- Projection of commercial NPPs indicated need for 1000 - 3000 MW cores, located nearer to major electrical load centers
- ⇒1950's era simplified site criteria impractical.
- Concept of design and site selection for reactor based on Design Bases Accident or DBA Source Terms.
- 1960 revised Reactor Site Criteria proposed effects of ECCS, Containment, Air Scrubbing, etc, factored in to DBA Source Terms.
- Effects of Average Site Meteorology Considered.

Evolution of Nuclear Safety

- 1960 Siting Rulemaking report effort effectively changed exclusion zone "rule of thumb" from:

$$R\ (\text{miles}) \sim 0.01 \times (\text{Power (KW)})^{0.5}$$

to:

$$R\ (\text{miles}) \sim 0.00018 \times (\text{Power (KW)})^{0.61}$$

- Source terms changed from MCA to DBA
- Scenario of DBA limited by functioning of safeguards systems.

Evolution of Nuclear Safety

- Worst conceivable accident. (1940's)

⇓

- Maximum credible accident. (1950's)

⇓

- Design bases accident. (1960's)

Defense in Depth Concept

- Defense in Depth originated in 1940's - precise knowledge of design margins lacking.
- Defense in Depth consists of:
- Multiple functional and/or engineered barriers to preclude Single Failures and prevent release of radioactive materials.
- Incorporation of large Design Margins where possible.
- High Quality in design and manufacture.
- Operation within design limits.
- Testing/inspection to maintain Design Margins.

Example of LWR Defense in Depth

- Radioactive fission products in ceramic fuel pellets – operated at relatively low power density.
- Fuel pellets contained in hermetically sealed fuel rods cooled by reactor coolant system.
- Reactor coolant system contained in pressure tested RPV and Primary Coolant System.
- Piping subject to In-Service Inspection & NDT exams.
- Primary Coolant System leaks backed up by ECCS.
- Primary Coolant System contained in hermetically sealed and cooled Containment.
- All activities subject to Quality Assurance verifications.

Single Failure Criteria

- ".. protection system shall be designed for high functional reliability and inservice testability commensurate with safety functions performed."
- "Redundancy and independence designed into protection system 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."

Single Failure Criteria

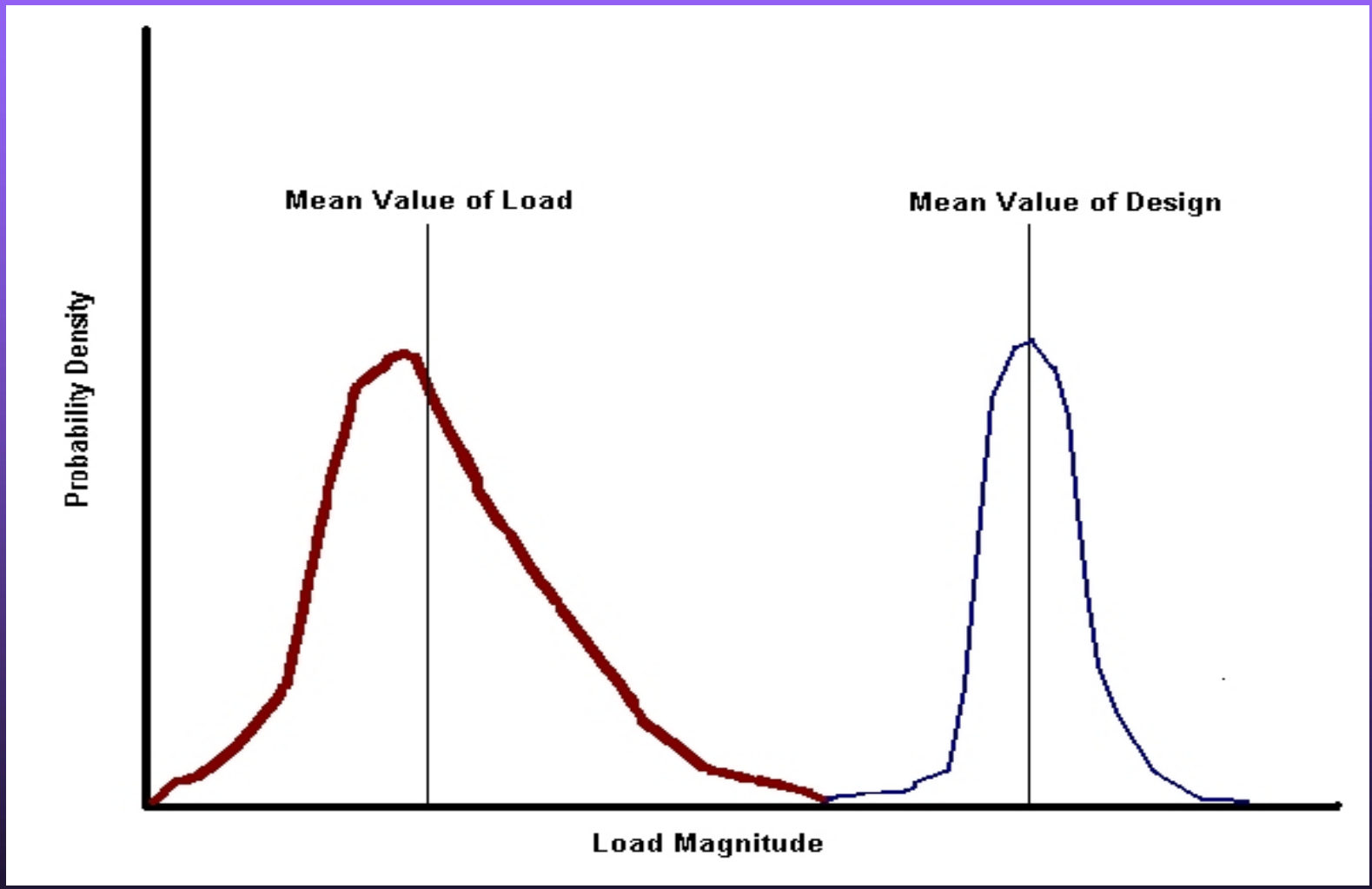
- "..protection system shall be designed to permit periodic testing of its functioning when reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred."

  Taken from US Title 10 Code of Federal Regulations, Part 50 Appendix A, General Design Criteria 21

Design Margins

- Given some loading: “L” and design capacity “D”:
- If $L > D$ - the element will fail.
- If $L < D$ - the element will not fail.
- 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.

Design Margins



Design Margins

- 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”.

Design Margins

- Design process seeks to provide high confidence that engineered system can withstand maximum credible load (e.g.: pressure, stress, heat flux….)
- Mathematically:

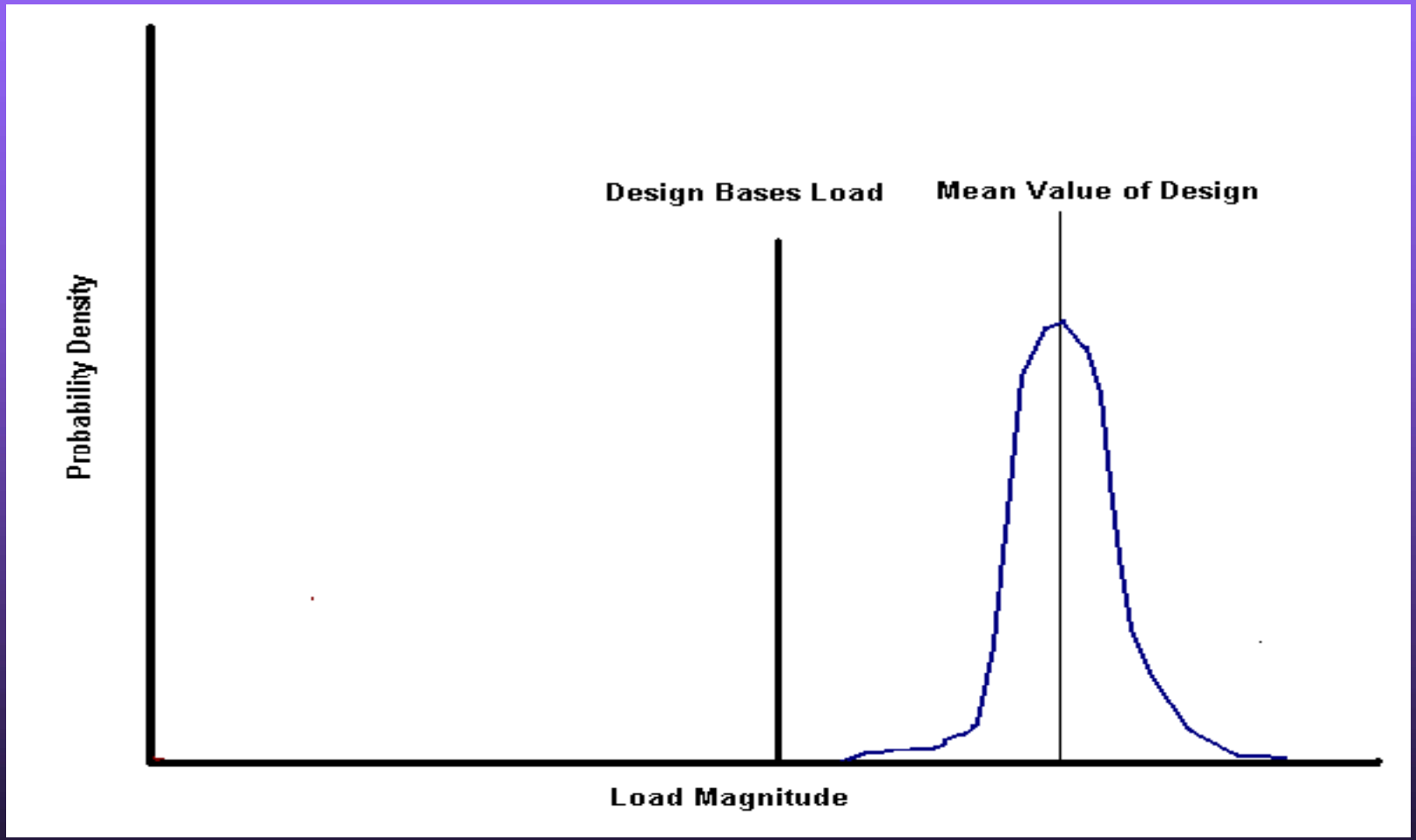
$$P_f = \text{Prob}[L>D] = \int_0^{\infty} \int_{-\infty}^{\infty} f_{LD}(L+D, D)\, dL\, dD$$

where: $f_{LD}(L+D,D) = f_L(L+D)f_D(D)$ via convolution

Design Margins

- Usual technical problem is understanding shape of "tails" of $f_L(L+D)$ probability density function in the "overlap region".
- For many general aspects of NPP design DBA loads used, and one sees:
- DB earthquake (peak ground acceleration)
- DBA LOCA (maximum diameter pipe rupture)
- DB wind loading (maximum wind loading on buildings)

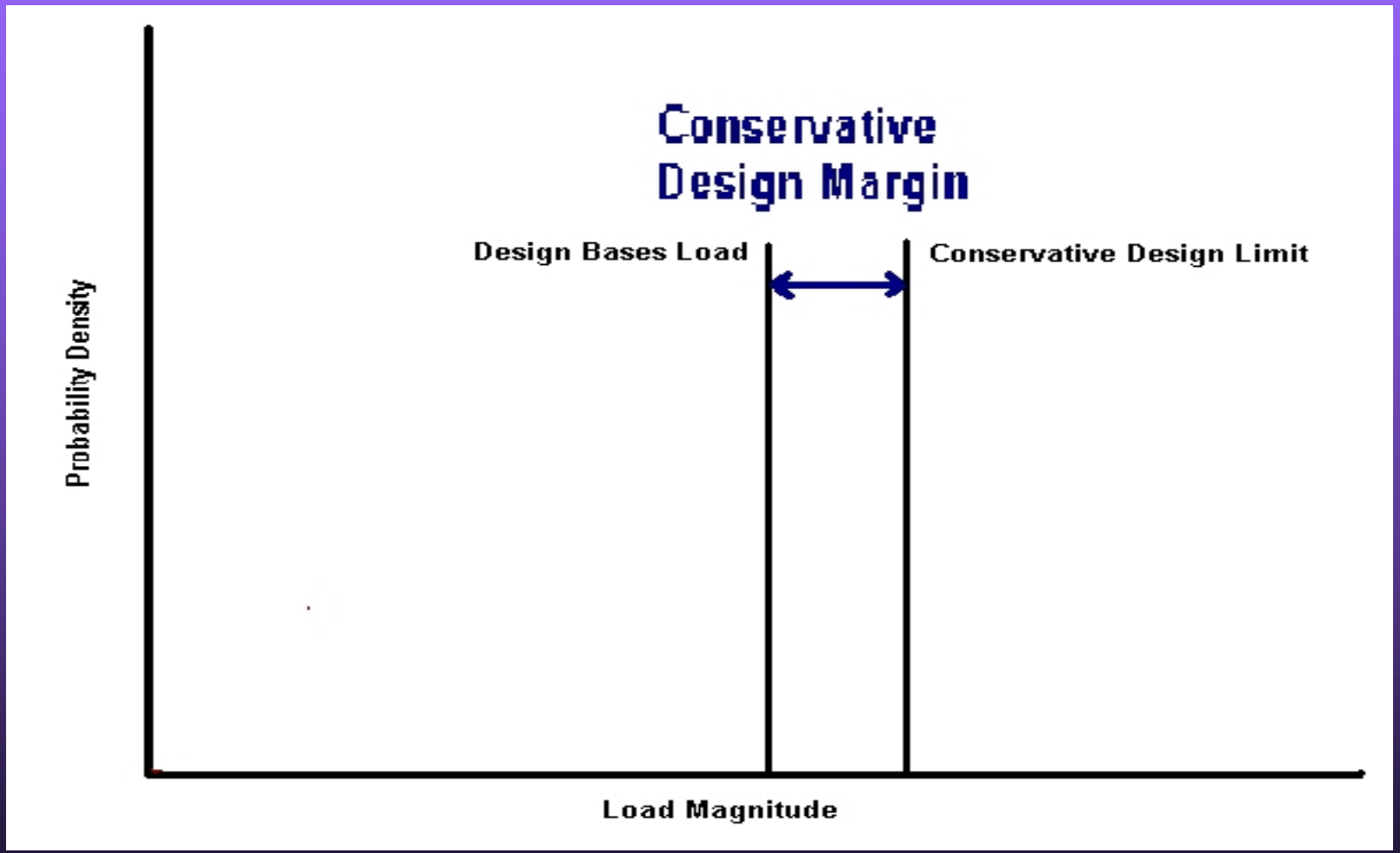
Design Margins



Design Margins

- 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.
- Why not extend this to Design Capacity?

Design Margins



Design Margins

- 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 Design Margins.
- Examples include:
- ASME Boiler and Pressure Vessel Code
- IEEE, IEC Electrical Standards

Regulations, Codes, Standards

Hierarchy of Safety Requirements Documents used to address Design Margins:

- **National Laws** – Obligatory (Policy)
  - Issued by Governments or Parliaments with inputs from Regulatory Body
- **Regulations** – Obligatory (General)
  - Issued by Regulatory Body, may reference Codes & Standards
- **Regulatory Guidance** – Suggested (Detailed)
  - Issued by Regulatory Body, defines accepted option, may reference Codes & Standards.
- **Codes & Standards** – "Optional?" (Detailed)
  - Issued by Professional Groups, defines acceptable option.

Insights and Practical Experience

- An NPP design involves millions of individual component design decisions impacting safety.
- Safety Assessment of these millions of design elements without Codes and Standards implies millions of individual issues to be assessed.
- Use of Codes and Standards reduces critical safety related design decisions on NPP Design Margins to re-produceable, “transparent”, and mutually accepted approaches.

Insights and Practical Experience

- Piping, Pressure Vessel, Containment, Seismic Structural support design limits (stress analyses) are historically performed based on conservative Industry Codes and Standards. (in most countries)
- Sizing of cabling, breakers, electrical components are historically based on Loads in conservative Industry Codes and Standards. (in most countries)
- Fuel Rod Critical Heat Flux Design Margins typically rely on detailed analysis of uncertainties.
- DBA LOCA has been replaced by Best Estimate LOCA which relies on detailed consideration of uncertainties.

Summary

- Safety Assessment of NPPs evolved to assessment of mitigated accident source terms based on assumption of working engineered safety systems.
- Safety Assessment of NPP safety systems involves assessment of both Reliability and Design Margins
- Assuring Reliability is based on Single Failure Criteria, and On-line Testability.
- Assuring Design Margins is based on either use of conservative Regulations, Codes, and Standards, or in a limited number of areas performing detailed margins analysis (Fuel Rod CHF limits, Best Estimate LOCA).