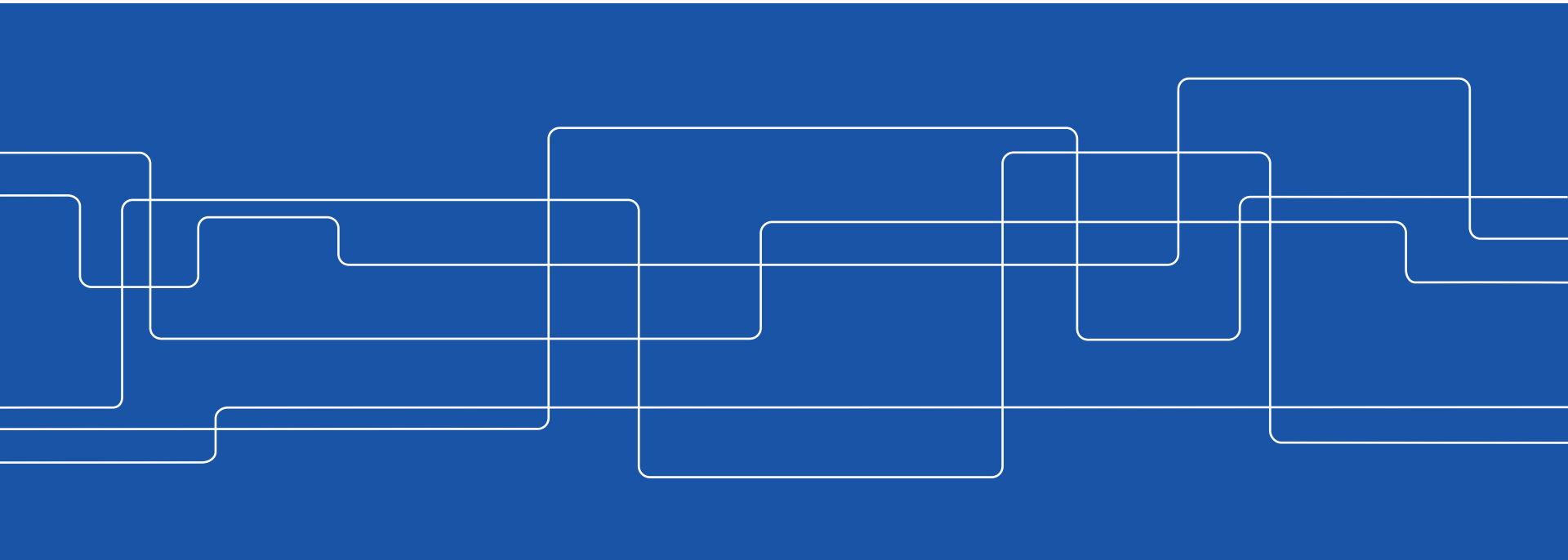
SH2705 Simulation Course

Safety Assessment and Safety Analysis

Sean Roshan



Safety Assessment

Assessment of all aspects of a practice that are relevant to protection and safety; for an authorized facility, this includes siting, design and operation of the facility.

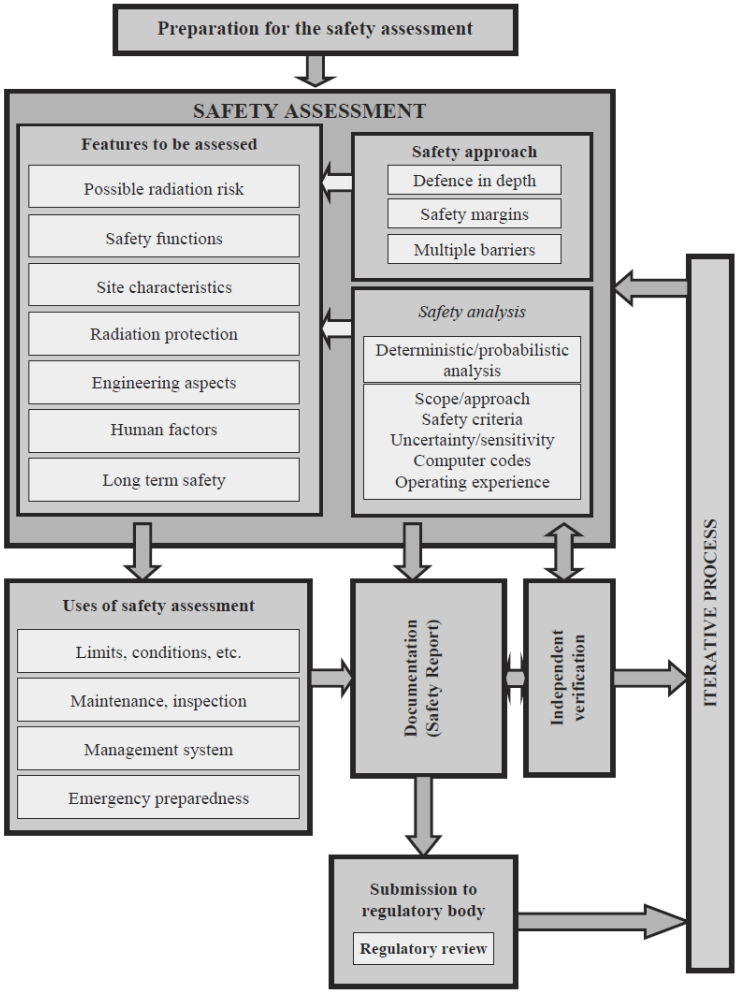
Analysis to predict the performance of an overall system and its impact, where the performance measure is the radiological impact or some other global measure of the impact on safety

I.A.E.A

Safety Assessment (contd.)

- Safety assessment is undertaken as a means of evaluating compliance with safety requirements (and thereby the application of the fundamental safety principles) for an energy transformation plant (e.g. an NPP) to determine the measures that need to be taken to ensure safety.
- Its is the assessment of all aspects of the plant that are relevant to protection and safety. This includes siting, design and operation of the plant.
- Safety assessment is the systematic process that is carried out throughout the lifetime of the plant to ensure that all the relevant safety requirements are met by the proposed (or actual) design.
- Safety assessment includes, but is not limited to, the formal safety analysis.

Safety Assessment (contd.)



Overview of safety assessment process for an NPP

Needs for Safety Assessment

Safety assessment is used for:

- Licensing of a new plant and/or renewing the license of an operating plant,
- Safety review, periodic safety review,
- Plant modification, upgrading and modernization projects,
- Assessment of operational experience,
- Final safety analysis report, updating of safety analysis report,
- Determining and updating of operational limits and conditions,
- Updating the safety relevant programs and procedures

Safety Assessment is performed by:

- Designer safety assessment
- Licensee safety assessment
- Regulatory safety assessment and review

Safety Assessment during lifetime of a facility

Safety assessment is carried out during different stages of a facility's lifetime:

- Site evaluation for the facility or activity;
- Development of the design;
- Construction of the facility or implementation of the activity;
- Commissioning of the facility or of the activity;
- Commencement of operation of the facility or conduct of the activity;
- Normal operation of the facility or normal conduct of the activity;
- Modification of the design or operation;
- Periodic safety reviews;
- Life extension of the facility beyond its original design life;
- Changes in ownership or management of the facility;
- Decommissioning of a facility;
- Closure of a disposal facility for radioactive waste and the post-closure phase;
- Remediation of a site and release from regulatory control.

Insights and Practical Experience

- An NPP design involves millions of individual components 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-producible, “transparent”, and mutually accepted approaches.

Insights and Practical Experience

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.

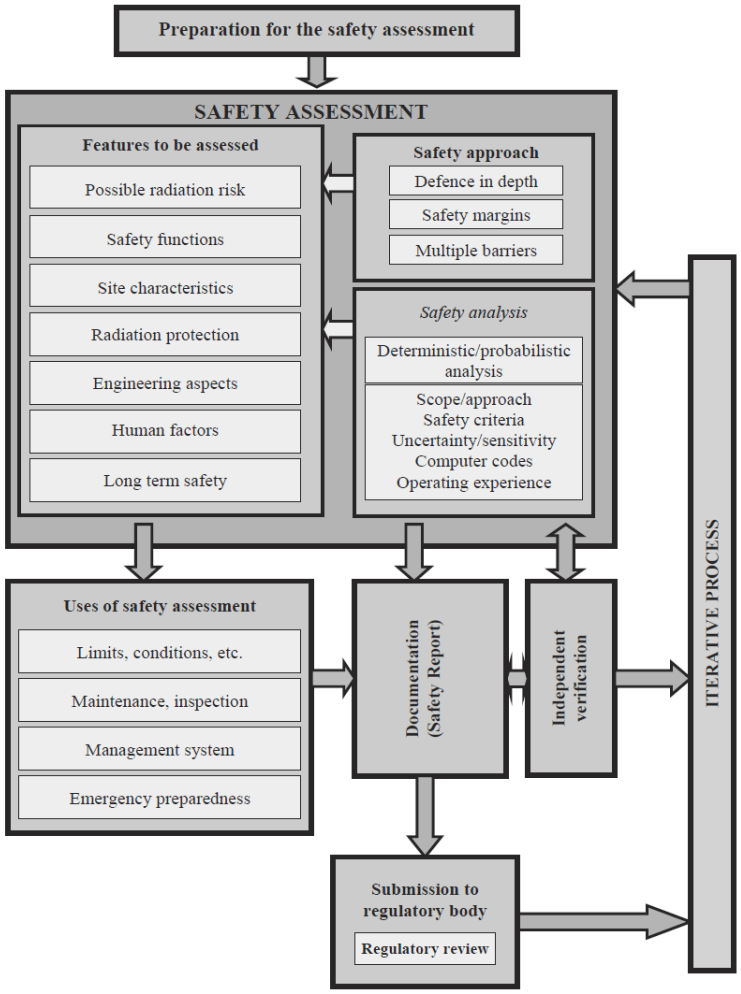
Insights and Practical Experience (contd.)

Regulations, Codes, Standards

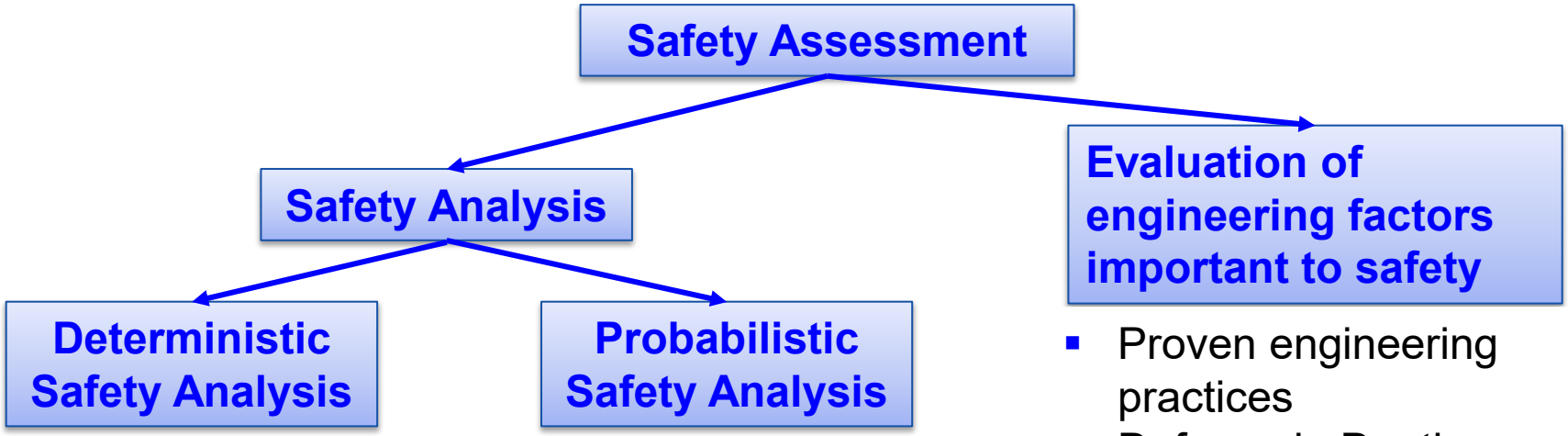
- Piping, Pressure Vessel, Containment, Seismic Structural support design limits (stress analyses) are historically performed based on conservative Industry Codes and Standards. (in most countries)
- Sizing of cabling, breakers, electrical components are historically based on Loads in conservative Industry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

Overview of Safety Assessment

- Safety Assessment of NPPs has evolved to assess 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 Safety 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).



Safety Assessment Hierarchy



- Predict the response to postulated events with predetermined assumptions
- Checks fulfilment of acceptance criteria

Combines the
- likelihood of initiating scenarios
- and their consequences

Into estimation of
- Core damage frequency
- Source term release
- Overall risk

- Proven engineering practices
- Defence in Depth
- Radiation protection
- Safety classification
- Protection against internal and external hazards
- Combination of loads
- Selection of materials
- Single failure criterion
- Redundancy, diversity
- Equipment qualification
- Ageing
- Man – machine interface

…

Safety Analysis

- Evaluation of the potential hazards associated with the operation of a facility or the conduct of an activity.
- The formal safety analysis is part of the overall safety assessment; that is, it is part of the systematic process that is carried out throughout the design process (and throughout the lifetime of the facility or the activity) to ensure that all the relevant safety requirements are met by the proposed (or actual) design.

Safety Analysis (contd.)

Applying methods of deterministic and probabilistic analysis, shall be provided which establishes and confirms the design basis for the items important to safety and demonstrate that overall plant design is capable of meeting the prescribed and acceptable limits for radiation doses and releases for each plant condition category and that defense- in-depth is achieved

Safety Analysis (contd.)

- Safety analysis is an essential element of a safety assessment. It is an analytical study used to demonstrate how safety requirements are met for a broad range of operating conditions and various initiating events.
- Safety analysis involves deterministic and probabilistic analyses in support of the siting, design, commissioning, operation or decommissioning of an NPP.

Safety Analysis (contd.)

Safety analysis is the study of how the reactor behave during abnormal conditions.

- as a step in the design process
- an essential part of the safety assessment in the licensing process

Deterministic safety analysis employs calculational models which describe the physical processes in reactor/plant systems to examine the plant's behavior after an assumed initial event or malfunction.

- "Deterministic" is because of one result (one sequence) at a time.

Probabilistic safety analysis studies the reliability of the safety systems and identifies event sequences which can lead to core melting (Level 1), containment failure (Level 2) and off-site consequences (Level 3).

Goal of Safety Analyses

Identify hidden failures or weakness in safety functions (backdoors in the system)

- Instability events
- Steam line blockage
- Pressure control failure
- Control rod insertion by electrical motors
- Fuel damage because of dryout
- …

Safety Landscape is *very complex*, appropriate methods for analysis should be developed to define the boundary of this landscape

Safety Analysis: Deterministic approach

Deterministic approach: analyze plant behavior under specific predetermined operational states and accident conditions, with specific set of rules in judging design adequacy (conservative approach is often used for design purposes)

A **deterministic** model does not include elements of randomness. Every time you run the model with the same initial conditions you will get the same results

Safety Analysis: Probabilistic approach

Probabilistic approach: determining all significant contributors to risk and evaluating the balance of the overall system configuration

A **probabilistic** model includes elements of randomness. Every time you run the model, you are likely to get different results, even with the same initial conditions. A probabilistic model is one which incorporates some aspect of random variation.

Deterministic and Probabilistic analysis are two complementary approaches to be used

Safety Analysis Report

- A Safety Analysis Report (SAR) is a document which enables the regulatory body to assess the safety of a nuclear power plant.
  - Preparing a preliminary SAR (PSAR) is part of the licensing process for new build of nuclear power plants.
  - Final SAR (FSAR) is part of for operating license.
  - Revision of a FSAR is usually part of the process of extending a license.

Deterministic Safety Analysis

- The mechanistic thinking era
- Determinism, everything has a cause and can be explained why it happened
- Knowing everything that can happen when dealing with a machine
- Analysis to know how things work

Deterministic Safety Analysis (contd.)

- DSA answers the question; if a reactor design is adequate and licensable?
- DSA is a tool in developing plant protection and control systems, set points and control parameters, and the technical Specifications of the plant.

Why "deterministic"? :

- Traditionally:
  - No randomness (probabilities) in the calculation (in principle)
  - Results are single numerical values with probability 1 (this is not true for "best-estimate" analyses)

Deterministic Safety Analysis (contd.)

DSA is used to:

- Demonstrates the effectiveness of the equipment incorporated to prevent escalation of AOOs and DBAs to severe accidents and to mitigate their effects.
- Demonstrates that the safety systems can:
  - Shutdown the reactor and maintain it in safe shutdown condition during and after DBA.
  - Remove residual heat from the core after reactor shutdown from all operational states and DBA conditions.
  - Ensure that radioactive releases during DBA are below acceptable limits.

Deterministic Safety Analysis (contd.)

DSA for normal operation of the plant:

- Ensures that normal operation is safe (with radiological doses and releases of radioactive materials within acceptable limits. Also checking if they are ALARA) and with plant parameters not exceeding operating limits.

- Should establish the conditions and limitations for safe operation, including:
  - Safety limits for reactor protection and control and other engineered safety systems.
  - Operational limits and reference settings for the control system.
  - Procedural constraints for operational control of processes.
  - Identification of allowable operating configurations.

Requirements for deterministic methodology

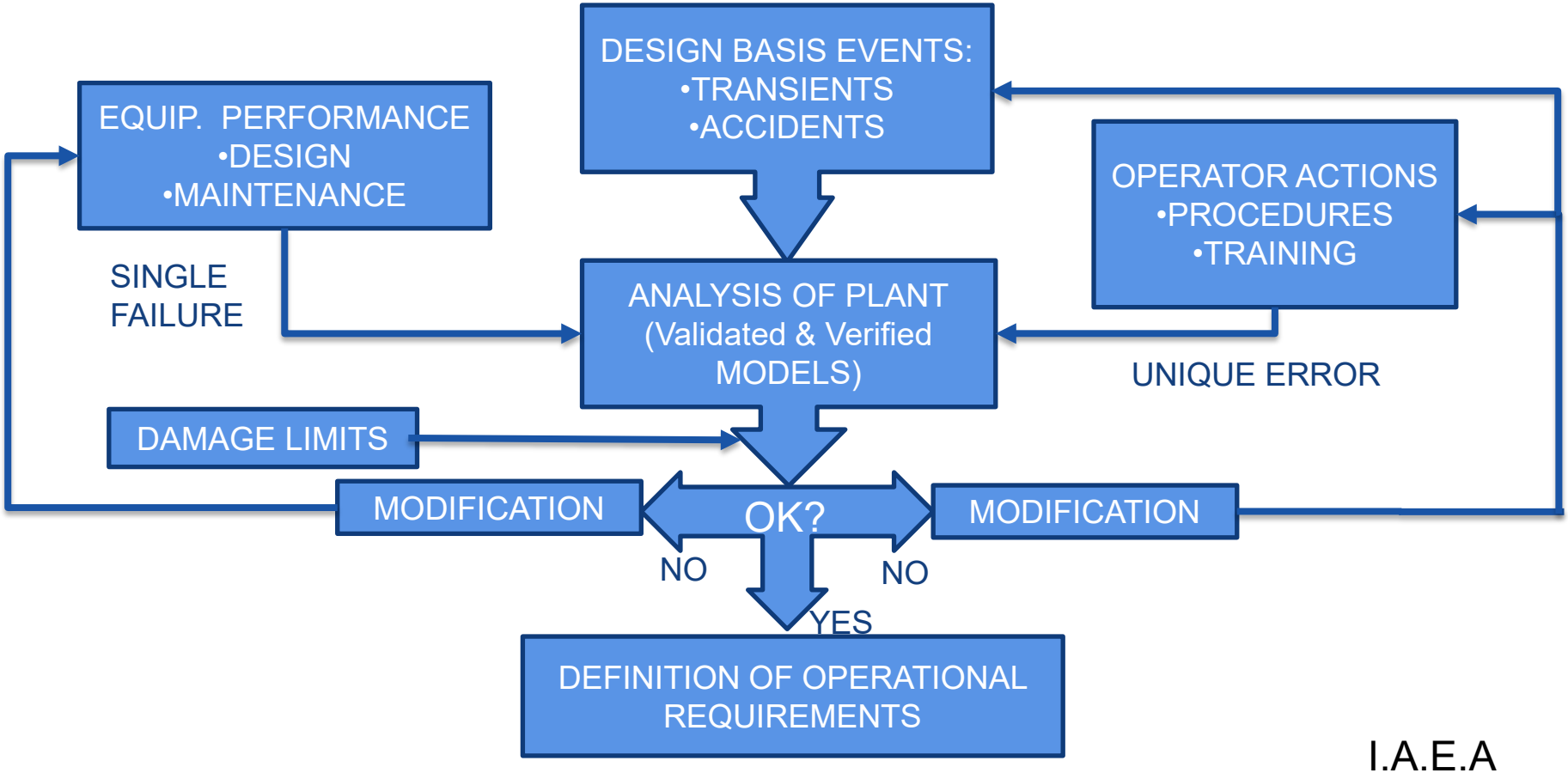
- Compliance of operational limits in the assumptions
- PIEs appropriate for the design and the site
- Analysis of the events sequences resulting from PIEs
- Compliance with acceptance criteria
- Assessment of the degree of conservatism
- Uncertainty method together with the best estimate methodology

The Deterministic Approach

We need to limit the scope and extent of the deterministic safety analysis:

- simplifying assumptions and bounding situations
- design basis events
- single failures
- actions taken to fulfill the assumptions made in the safety analysis
- unique error of the operator

The Deterministic Approach (contd.)



I.A.E.A

The Objectives of DSA

- Confirm that the design of an NPP meets design and safety requirements
- Derive or confirm operational limits and conditions that are consistent with the design and safety requirements for the NPP
- Assist in establishing and validating accident management procedures and guidelines
- Assist in demonstrating that safety goals, which may be established to limit the risks posed by the NPP, are met

DSA Applications

- DSA establish and confirm the DB for items important to safety, ensuring that the plant design meets safety and radiological criteria (integrity of barriers).
- As part of the Safety Assessment with the aim to determine the effectiveness of "defense barriers".

DESIGN BASIS (DB): the range of conditions and events taken explicitly into account in the design of a plant, so that the plant can withstand them w/o exceeding authorized limits, by the planned operation or safety systems.

DSA Applications (contd.)

- **Design Applications**
  - Designer: as part of the design and construction process
  - Operating organization, to confirm the design

DSA must be parallel to the design process, with iteration between them.

- **Licensing Applications**
  - Calculations for Final Safety Analysis Report (FSAR)
  - Fuel reload analysis
  - Periodic SA of an operating plant
  - Safety justification of a design modification

The final SA must reflect the final plant design. DSA is also used for evaluating design changes, supporting decision-making processes, revealing new issues, etc.

- **Regulatory Applications**
  - Audit calculations
  - Evaluation of emergency operating procedures
  - Review of significant events and incidents
  - Evaluation of emergency operating procedures
  - Unresolved Safety Issues Evaluation

Types of DSA

DSA can be conservative or best- estimate:

- Conservative: use pessimistic or worst-case assumptions and models. Most of the analysis presented to regulatory bodies follow this approach.

- Best-estimate or realistic: most of assumptions and models are realistic (some conservatisms are maintained), include uncertainty analysis.

Conservatism

The concept of conservatism was introduced to the analyses, when:

- the capabilities (physical knowledge and modelling, experimental database and the computer capacity) were insufficient for the realistic calculations.
- to account for the statistical character of the plant data
- to account for equipment failures.

By using pessimistic assumptions and simplifications concerning the initial conditions, boundary conditions and the physical models, it was believed that the limiting results could be obtained for the chosen bounding cases.

One of the basic difficulties of that approach is that too many and too coarse assumptions may result in very unrealistic sequences, which in the worst cases may turn out not to be conservative, since the real progression might lead to more limiting results.

Best-estimate

- **Best-estimate or realistic DSA:**
  - Started to develop when the capabilities for simulating the phenomenology originated by accidents increased.
  - Try to unbiasedly reproduce the real plant behavior during an accident or transient.
  - Realistic models and assumptions.
  - Must include an uncertainty analysis for the important results, that must be given with an "error interval".

Best Estimate Approaches

The BE codes are best estimate in the sense that the physical modelling applied uses the best knowledge of the phenomena available. In such areas, as severe accident analysis, the BE methods have been striven for from the beginning.

The basic elements of successful application of the BE methods are:

- the codes are carefully validated against the existing database,
- the code users are well educated,
- the associated uncertainties can be quantified or are at least qualitatively understood and managed.

The code users should be experienced in performing complex system analysis. The validation calculations against the experimental database from various facilities and successful simulation of the plant experience from the real transients and accidents are efficient means for user training

Best Estimate Approaches (contd.)

- **Uncertainty evaluation in DSA:**
  - In principle, being realistic is harder that being pessimistic. Conservative models can be simple.
  - Need for robust demonstration that there are large safety margins.
  - In both approaches you must know the accuracy of your models and assumptions. But in the BE approach you must quantify such accuracy (uncertainty study).
  - Given an accident scenario in a plant, a conservative analysis can make use of only one or some few computer code runs. But in a BE Plus Uncertainty (BEPU) analysis you need "many" computer runs, in order to carry out the uncertainty analysis.

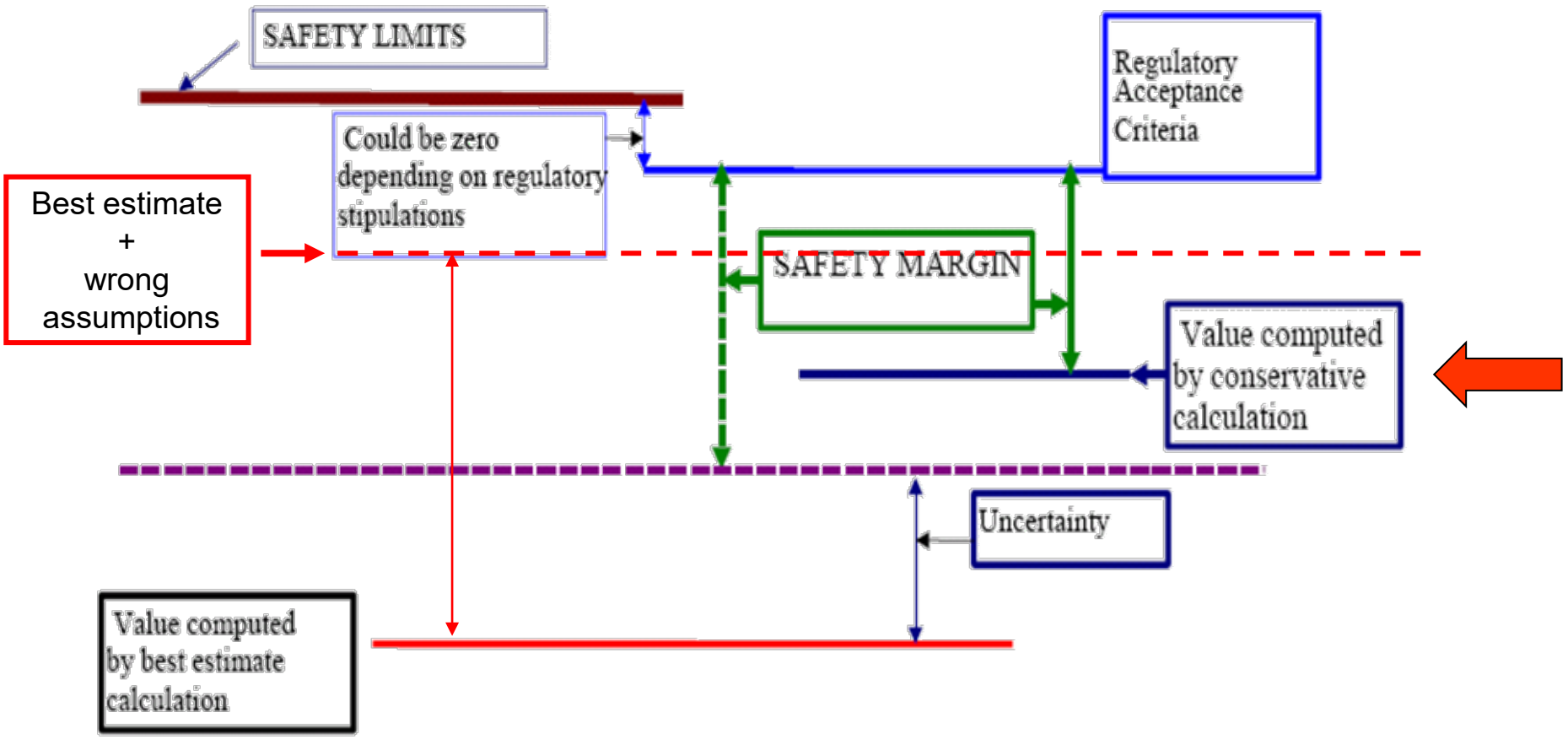
Evolution of DSA

Applied codes	Input & BIC (boundary and initial conditions)	Assumptions on systems availability	Approach
Conservative codes	Conservative input	Conservative assumptions	Deterministic*
Best estimate (realistic) codes	Conservative input	Conservative assumptions	Deterministic
Best estimate codes + Uncertainty	Realistic input + Uncertainty	Conservative assumptions	Deterministic
Best estimate codes + Uncertainty	Realistic input + Uncertainty	PSA-based assumptions	Deterministic + probabilistic

Best Estimate Approaches (contd.)

- **The advantages of a realistic DSA:**
  - You look for the "real" performance of your plant. Conservative methodologies use to be physically unrealistic (misleading sequences of events, unrealistic time scales, missing of physical phenomena). BE calculations can provide guidance in developing accident management plans.
  - Lower margins: real safety margins adopted for a plant with a conservative approach may be unnecessarily large. BEPU margins may permit augment reactor power.
  - You have a precise idea about the sensitivity of the calculations to variables and parameters.

Regulatory Acceptance Criteria



Conservative vs. Best-estimate approaches

- Deterministic Safety Analysis has been traditionally carried out with a conservative or pessimistic bias.
- Conservative DSA makes use of pessimistic assumptions everywhere, so that the results of the analyses are expected to be “worse” than realistic ones (“bounding”):
  - Conservative initial and boundary conditions.
  - Models in the computer codes are chosen as conservative.

Conservative vs. Best-estimate approaches

- Conservative DSA have been very popular, because it is relatively "easy" to perform. But the convenience of such an approach does not "excuse" the analyst from being unaware of the accuracy of the models and assumptions.
- A very characteristic example of conservative analysis: LOCA analysis for LWR according to section 46 and appendix K of the 10 CFR 50. The conservativeness imposed by the appendix K requirements is very large, because some parameters/models are given overwhelmingly pessimistic values.

CONSERVATIVE VS. BEST-ESTIMATE
LOCA Analysis

LOCA analysis for LWR section 46 and appendix K to 10 CFR 50

- Conservatisms imposed by the Appendix K to 10 CFR 50:
  - Stored energy: initial steady temperatures chosen so as to maximize the stored energy in the fuel.
  - Decay heat: heat generation rate from radioactive decay are 1.2 times the 1971 ANS Standard (this is an overestimation of about five standard deviations !!!).
  - Metal-water reaction: conservative Baker-Just model. If cladding ruptures, both inner and outer surfaces are assumed to react.

CONSERVATIVE VS. BEST-ESTIMATE
LOCA Analysis (contd.)

- Discharge from break: critical flow is based on the conservative Moody model multiplied by discharge coefficients (from 0.6 to 1.0) that lead to the worst results.
- ECCS bypass: during most of the blowdown period for a PWR cold leg break, the ECCS water is assumed to be ineffective in refilling the system.
- No return to nucleate or transition boiling: once Critical heat flux (CHF) has occurred in the blowdown period, no return to nucleate or transition boiling is allowed during blowdown; it must be postponed until the reflood period.

CONSERVATIVE VS. BEST-ESTIMATE
LOCA Analysis (contd.)

- Film boiling correlations, chosen to under predict data.
- Single failure: it is assumed that one of the ECCS components fails.
  - The failure leading to the highest damage is chosen.

CONSERVATIVE VS. BEST-ESTIMATE
LOCA Analysis (contd.)

Acceptance criteria for a LOCA Analysis (after 10 CFR 50.46)

- Peak cladding temperature (PCT) lower than 2200 ºF.
- Maximum cladding oxidation lower than 0.17 times the total cladding thickness before oxidation. If cladding rupture is predicted, the inside surfaces will participate in the oxidation
- Maximum hydrogen generation resulting from the cladding oxidation: lower 0.01 times the amount that would be generated if all the cladding metal were to react.
- Core geometry will remain amenable to cooling.
- Long-term cooling.

CONSERVATIVE VS. BEST-ESTIMATE
LOCA Analysis (contd.)

Best-estimate LOCA analysis:

- Makes use of realistic assumptions and codes: TRACE, RELAP5, APROS, POLKA-T, SIMULATE, TRAC-P, TRAC-B,…that incorporate state-of-the-art models.
- Must include an uncertainty analysis.
- Drops out the Appendix K requirements.
- Regulatory door open:
  - SECY-83-472
  - 1988 revision of 10 CFR 50
  - Regulatory Guide 1.157 (1989)
  - CSAU Methodology (1989)

Contents of Safety Analysis Report

- **USNRC Regulatory Guide 1.70** *
  1. Introduction and general description of plant
  2. Site characteristics
  3. Design of structures, components, equipment and systems
  4. Reactor
  5. Reactor coolant system and connected systems
  6. Engineered safety features
  7. Instrumentation and control
  8. Electrical power
  9. Auxiliary systems
  10. Steam and power conversion system

* For new reactors see RG 1.206 issued in 2007

- ***IAEA Safety Standards, No. SSG-61***
  1. *Introduction and general considerations*
  2. *Site characteristics*
  3. *Safety objectives and design rules for structures, systems and components*
  4. *Reactor*
  5. *Reactor coolant system and associated systems*
  6. *Engineered safety features*
  7. *Instrumentation and control*
  8. *Electrical power*
  9. *Auxiliary systems and civil structures,*
     - *A. Auxiliary systems,*
     - *B. Civil engineering works and structures*
  10. *Steam and power conversion systems*

Contents of Safety Analysis Report cont.

- **USNRC Regulatory Guide 1.70** *

11. Radioactive waste management
12. Radioactive protection
13. Conduct of operation
14. Initial test program and Inspections, ITAAC-design (Tests, Analyses, and Acceptance Criteria) certification
15. Accident analysis
16. Technical specifications
17. Quality assurance
18. Human factors engineering
19. Severe accidents

* For new reactors see RG 1.206 issued in 2007

- *IAEA Safety Standards, No. SSG-61*

11. *Management of radioactive waste*
12. *Radiation protection*
13. *Conduct of operation*
14. *Plant construction and commissioning*
15. *Safety analysis*
16. *Operational limits and conditions for safe operation*
17. *Management for safety*
18. *Human factors engineering*
19. *Emergency preparedness and response*
20. *Environmental aspects*
21. *Decommissioning and end of life aspects*

U.S. NRC standard review plans (SRP)

- The U.S. NRC has several standard review plans (SRP) for staff use in reviewing proposed licensing actions. These actions may relate to
  - nuclear facility
    - constructing,
    - operating,
    - decommissioning.
  - nuclear materials or waste
    - possessing,
    - using,
    - storing,
    - transporting.
- The SRP establish criteria to use in evaluating applications to construct and operate nuclear power plants.
- The SRP is not a substitute for the NRC's regulations, and compliance with it is not required, However, the applicant must show that they are complying with the regulation U.S. NRC and full fill the acceptance criteria

Review of Safety Analysis Reports for Nuclear Power Plants : LWR Edition (NUREG-0800)

Chapter 1, Introduction and Interfaces
Chapter 2, Sites Characteristics and Site Parameters
Chapter 3, Design of Structures, Components, Equipment, and Systems
Chapter 4, Reactor
Chapter 5, Reactor Coolant System and Connected Systems
Chapter 6, Engineered Safety Features
Chapter 7, Instrumentation and Controls
Chapter 8, Electric Power
Chapter 9, Auxiliary Systems
Chapter 10, Steam and Power Conversion System
Chapter 11, Radioactive Waste Management
Chapter 12, Radiation Protection
Chapter 13, Conduct of Operations
Chapter 14, Initial Test Program and ITAAC-Design Certification
Chapter 15, Transient and Accident Analysis
Chapter 16, Technical Specifications
Chapter 17, Quality Assurance
Chapter 18, Human Factors Engineering
Chapter 19, Severe Accidents

NUREG-0800, Chapter 15, Transient and Accident Analysis

1. Steam System Piping Failures Inside and Outside of Containment (PWR)
2. Decrease in Feedwater Temperature, Increase in Feedwater Flow, Increase in Steam Flow, and Inadvertent Opening of a Steam Generator Relief or Safety Valve
3. Radiological Consequences of Main Steam Line Failures Outside Containment of a PWR
4. Loss of External Load; Turbine Trip; Loss of Condenser Vacuum; Closure of Main Steam Isolation Valve (BWR); and Steam Pressure Regulator Failure (Closed)
5. Loss of Nonemergency AC Power to the Station Auxiliaries
6. Loss of Normal Feedwater Flow
7. Feedwater System Pipe Breaks Inside and Outside Containment (PWR)
8. Loss of Forced Reactor Coolant Flow Including Trip of Pump Motor and Flow Controller Malfunctions
9. Reactor Coolant Pump Rotor Seizure and Reactor Coolant Pump Shaft Break
10. Uncontrolled Control Rod Assembly Withdrawal from a Subcritical or Low Power Startup Condition
11. Uncontrolled Control Rod Assembly Withdrawal at Power

NUREG-0800, Chapter 15, Transient and Accident Analysis (contd)

12. Control Rod Misoperation (System Malfunction or Operator Error)
13. Startup of an Inactive Loop or Recirculation Loop at an Incorrect Temperature, and Flow Controller Malfunction Causing an Increase in BWR Core Flow Rate
14. Inadvertent Decrease in Boron Concentration in the Reactor Coolant System (PWR)
15. Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position
16. Spectrum of Rod Ejection Accidents (PWR)
17. Radiological Consequences of a Control Rod Ejection Accident (PWR)
18. Spectrum of Rod Drop Accidents (BWR)
19. Radiological Consequences of Control Rod Drop Accident (BWR)
20. Inadvertent Operation of ECCS and Chemical and Volume Control System Malfunction that Increases Reactor Coolant Inventory
21. Inadvertent Opening of a PWR Pressurizer Pressure Relief Valve or a BWR Pressure Relief Valve