Deterministic Safety Analyses

Overview, PIEs, Acceptance Criteria, Conservative vs Best Estimate Analysis

S. Michael Modro

Joint IAEA-ICTP Essential Knowledge Workshop on Nuclear Power Plant Design Safety-Updated IAEA safety Standards

9-20 October 2017

Trieste, Italy

Content

- Overview of DSA
- Determination of PIEs
- Acceptance Criteria
- Conservative vs BE methods

Safety Analysis Objectives

- Safety analysis must demonstrate the following:
  - NPPs can withstand abnormal or accidental conditions with acceptable consequences to environment and population
- Safety analysis should confirm the following:
  - Protective barriers and safety system design are adequate to mitigate the abnormal or accident situation either automatically or with justified operator intervention
- While the analysis should demonstrate safety of the public and environment, the intent is not to demonstrate that the plant will be able to operate again after the accident (of course, this depends on category of an event)

Objective of DSA

- The objective of deterministic safety analysis for nuclear power plants is to confirm that safety functions and the needed systems, structures and components, in combination where relevant with operator actions, are capable and sufficiently effective, with adequate safety margins, to keep the releases of radioactive material from the plant within acceptable limits.
- Deterministic safety analysis is aimed to demonstrate that barriers to the release of radioactive material from the plant will maintain their integrity to the extent required.

Goals of Deterministic Safety Analysis

- Establishment and confirmation of the design basis
- Characterization of the appropriate Postulated Initiating Events (PIEs)
- Analysis and evaluation of the event sequences resulting from the PIEs against acceptance criteria
- Confirming that operational limits and conditions are in compliance with the design assumptions
- Verification of analytical assumptions, methods and extent of conservatism
- Updating to account for changes, and for improvement in knowledge

Scope of DSA

- The deterministic safety analyses performed **for different plant states** is aimed to demonstrate adequacy of the engineering design in combination with the envisaged operator actions by demonstrating compliance with established acceptance criteria.
  - Typically, these analyses focus on neutronic, thermal-hydraulic, thermal mechanic, structural and radiological aspects, which are often analysed with different computational tools. Computational simulations are carried out specifically for predetermined operating modes and plant states.

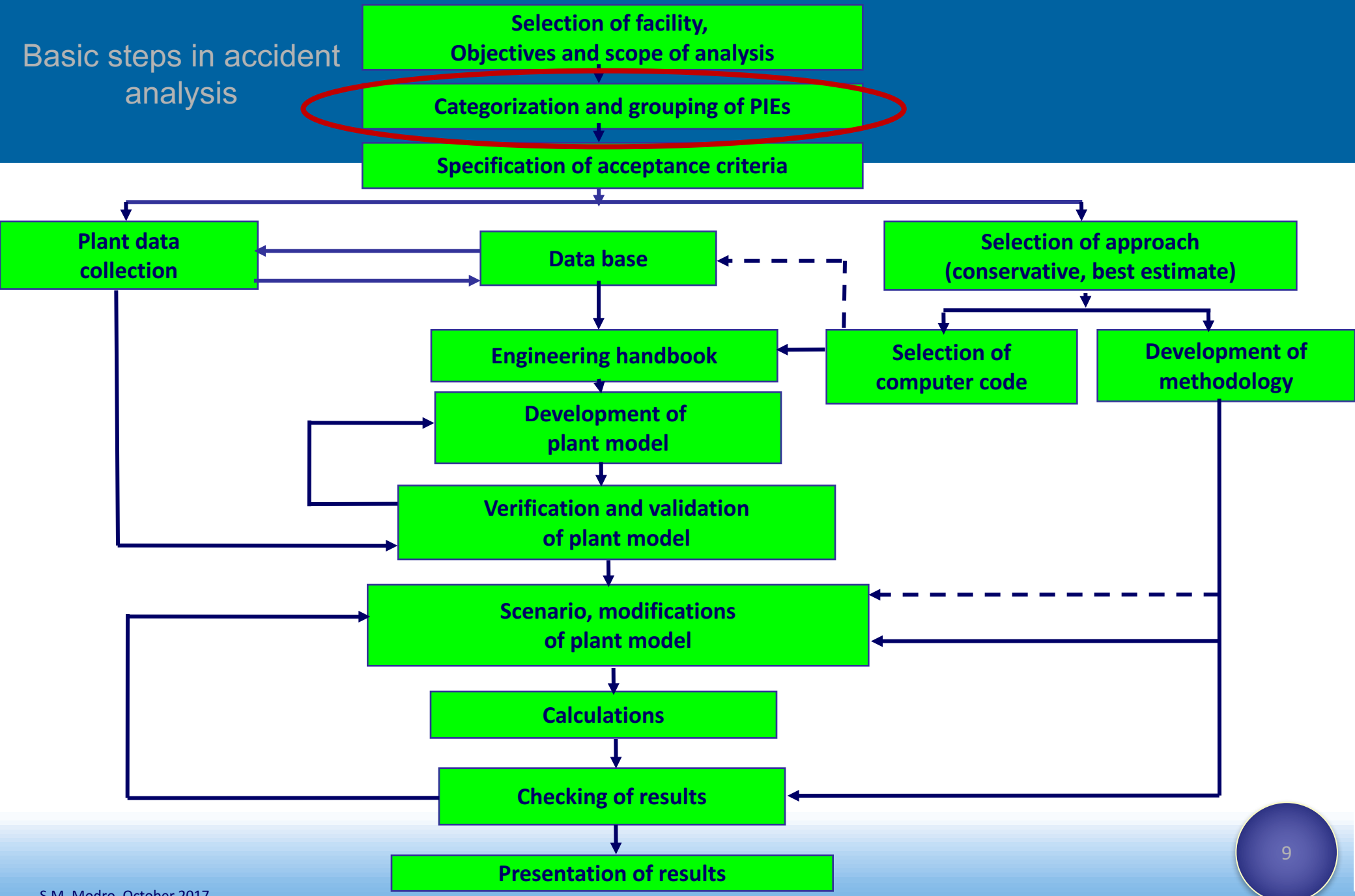
NPP states
according to the IAEA Safety Standards (SSR-2/1)

Operational States		**Accident Conditions**		
Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents	Design Extension Conditions	**Practically Eliminated Conditions**

Accident conditions - Terminology

- **Accident conditions** mean deviations from normal operation that are less frequent and more severe than anticipated operational occurrences, and which include design basis accidents and design extension conditions.
- **Design basis accident** is an accident causing accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits.
- **Design extension conditions** are accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.
- **Severe accident** means accident conditions more severe than a design basis accident and involving significant core degradation; for light water reactor it is synonymous for core melt accidents

Basic steps in accident analysis



POSTULATED INITIATING EVENTS

Postulated initiating Events

- An initiating event is an event that creates a disturbance in the plant and has a potential to lead to core damage, depending on the successful operation of the various mitigating systems of the plant
- The starting point for the safety analysis is the set of postulated initiating events that need to be addressed. A PIE is defined as an “identified event that leads to anticipated operational occurrences or accident conditions”.
- PIEs include events such as equipment failure, human errors and human induced or natural external events (hazards). The deterministic safety analysis and the PSA should normally use a common set of PIEs

Postulated Initiating Events

- An initiating event is an event that creates a disturbance in the plant and has a potential to lead to core damage, depending on the successful operation of the various mitigating systems of the plant
- The starting point for the safety analysis is the set of postulated initiating events that need to be addressed. A PIE is defined as an “identified event that leads to anticipated operational occurrences or accident conditions”.
- PIEs include events such as equipment failure, human errors and human induced or natural external events (hazards). The deterministic safety analysis and the PSA should normally use a common set of PIEs

PIEs – general guidance (1/8)

- The deterministic safety analysis should consider the postulated initiating events originated in any part of the plant potentially leading to a radioactive release to the environment, with consideration also of additional failures, e.g. in the control and limitation systems and the associated safety functions.
  - This includes events that can lead to a release of radioactivity not only from the reactor core but from other relevant sources such as fuel elements stored at the plant and systems dealing with radioactive material.
- Where applicable, it should be considered that a single cause can simultaneously initiate postulated initiating events in several or even all reactors, spent fuel storage and any other sources of potential radioactive releases on the given site.
- The DSA should address postulated initiating events that can occur in all modes of normal operation.
  - Initial conditions should consider a controlled plant mode with normal operation equipment operating prior to the initiating event.

PIEs – general guidance (2/8)

- Every configuration of shutdown modes including refuelling and maintenance should be considered.
- For these modes of operation, contributors potentially increasing risk should be considered, such as the
  - inability to start some safety systems automatically or manually;
  - disabled automation systems;
  - equipment in maintenance or in repair;
  - reduced amounts of coolant in the primary circuit as well as in the secondary circuit for some modes;
  - instrumentation switched off or non-functional and measurements not made;
  - open primary circuit and open containment.
- For PIEs related to the spent fuel pool, specific operating modes related to fuel handling and storage should be considered.
- PIEs taking place during plant operating modes with negligible duration in time may be excluded from DSA after careful analysis and quantitative assessment of its potential of contribution to the overall risk, including to conditions arising that could lead to an early radioactive release or a large radioactive release. Nevertheless, the need to prevent or mitigate these events with appropriate procedures or means should be addressed on a case by case basis.

PIEs – general guidance (3/8)

- A comprehensive list of PIEs should be prepared for ensuring that the analysis of the behaviour of the plant is as complete as possible so that 'all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.
- The list of postulated initiating events should take due account of operational experience feedback, which includes, depending on availability of relevant data, operating experience from the actual or from similar nuclear power plants.
- The set of postulated initiating events should be defined in such a way that covers all credible failures, including:
  - Failures of structures, systems and components of the plant (partial failure if relevant), including possible spurious actuation;
  - Failures initiated by operator errors, which could range from faulty or incomplete maintenance operations to incorrect settings of control equipment limits or wrong operator actions;
  - Failures of structures, systems and components of the plant arising from internal and external hazards.

PIEs – general guidance (4/8)

- All consequential failures that a given postulated initiating event could originate in the plant should be considered in the analysis of the plant response as a part of the postulated initiating event. These should include the following:
  - If the initiating event is a failure of part of an electrical distribution system, the anticipated operational occurrences, design basis accidents or design extension conditions analysis should assume the unavailability of all the equipment powered from that part of the distribution system;
  - If the initiating event is an energetic event, such as the failure of a pressurized system that leads to the release of hot water or pipe whip, the definition of the anticipated operational occurrences, design basis accidents or design extension conditions should consider potential failure of the equipment which could be affected;
  - For internal hazards such as fire or flood or external hazards such as earthquakes the definition of the induced postulated initiating event should include failure of all the equipment that is neither designed to withstand the effects of the event nor protected from it.
- Additional failures are assumed in deterministic safety analysis for conservatism e.g.
  - single failure criterion in design basis accidents
  - common cause failure for the purpose of defence in depth

PIEs – general guidance (5/8)

- Distinction should be made between these additional failures and failures that are part of, or directly caused by, the postulated initiating event.
- Further failures may be added to bound a set of similar events, limiting the number of analyses.
- The postulated initiating events should only include those failures (either initial or consequential) that directly lead to challenging safety functions and eventually to a threat to barriers against radioactive releases.
- Hazards, either internal or external (natural or human induced) should not be considered as postulated initiating events by themselves.
  - loads associated with these hazards should be considered a potential cause of postulated initiating events, which includes resulting multiple failures.

PIEs – general guidance (6/8)

- Where the results of engineering judgement, deterministic assessments and probabilistic assessments indicate that combinations of independent events could lead to anticipated operational occurrences or to accident conditions, such combinations of events should be considered to be design basis accidents or should be included as part of design extension conditions, depending mainly on their complexity and frequency of their occurrence.
- The set of postulated initiating events should be identified in a systematic way. This should include a structured approach to the identification of the postulated initiating events such as:
  - Use of analytical methods such as hazard and operability analysis (HAZOP), failure modes and effects analysis (FMEA), engineering judgement and master logic diagrams;
  - Comparison with the list of postulated initiating events developed for safety analysis of similar plants (ensuring that prior flaws or deficiencies are not propagated);
  - Analysis of operating experience data for similar plants;
  - Use of probabilistic safety analysis insights and results.

PIEs – general guidance (7/8)

- Certain limiting faults (e.g. large break loss of coolant accidents, main steam or feedwater pipe breaks and control rod ejection in pressurized water reactors or rod drop in boiling water reactors) are traditionally considered in deterministic safety analysis as design basis accidents. These accidents should be considered because they are representative of a kind of risk the reactor has to be protected from.
  - They should not be excluded from this category of accidents without careful analysis and quantitative assessment of its potential of contribution to the overall risk, including to conditions arising that could lead to an early radioactive release or a large radioactive release.
- Failures occurring in the supporting systems that impede the operation of systems necessary for normal operation should be also considered as postulated initiating events if such failures eventually require the actuation of the reactor protection systems or safety systems.

PIEs – general guidance (8/8)

- The set of postulated initiating events should be reviewed as the design and safety assessments proceed and should involve an iterative process between these two activities.
- The postulated initiating events should also be periodically reviewed throughout plant life to ensure that they remain valid, for example as part of a periodic safety review.

Identification and grouping of PIEs (1/14)

- PIEs should be subdivided into representative groups of event sequences taking into account physical evolution of the postulated initiating events.
- These groups gather event sequences that lead to a similar threat to the safety functions and barriers and the need for similar mitigating systems to drive the plant to a safe state.
  - They can be bound by a single representative sequence
  - Then these groups are also categorized according to their frequency of occurrence.
  - This approach allows the selection of the same acceptance criteria and initial conditions and the application of the same assumptions and methodologies to all postulated initiating events grouped under the same representative event sequence.
  - Example: “stop of a Main Feed Water (MFW) pump”, “stop of all MFW pumps” and “isolable break on MFW system” are all typically grouped under a single representative event sequence such as “Loss of MFW”.

Identification and grouping of PIEs (2/14)

- Representative event sequences can also be grouped by type of sequences with focus on reduced core cooling and RCS pressurization, containment pressurization, radiological consequences, or pressurized thermal shocks. The PIEs associated with AOOs and DBAs should reflect the specifics of the design
  - Increase or decrease of the heat removal from the reactor coolant system;
  - Increase or decrease of the reactor coolant system flow rate;
  - Anomalies in reactivity and power distribution in the reactor core or anomalies in reactivity in the fresh or spent fuel storage;
  - Increase or decrease of the reactor coolant inventory;
  - Leaks in reactor coolant system with potential containment by-pass;
  - Leaks outside containment;
  - Reduction or loss of cooling of the fuel in the spent fuel storage pool;
  - Loss of cooling to fuel during on-power refuelling (pressurized heavy water reactor);
  - Release of radioactive material from a subsystem or component (typically from treatment or storage systems for radioactive waste).

Identification and grouping of PIEs (3/14)

- For analysis of the source term, specific grouping of postulated initiating events may be appropriate to adequately address different pathways to the releases of radioactive material to the environment.
- Within each group of postulated initiating events, the representative event sequences should also be subdivided into categories depending on the frequency of the most frequent postulated initiating event in the group.

Plant state	Alternative names used in some States	Indicative frequency range (year^{-1})
Anticipated operational occurrences	Faults of moderate frequency, DBC[5]-2, PC-2	f >1E-2
Design basis accidents	Infrequent faults, DBC-3, PC-3	1E-2 > f > 1E-4
	Limiting faults, DBC-4, PC-4	1E-4 > f > 1E-6[6]

Identification and grouping of PIEs (4/14)

- Typical examples of PIEs leading to event sequences categorized as AOOs should include:
  - Increase in reactor heat removal: inadvertent opening of steam relief valves; pressure control malfunctions leading to an increase in steam flow rate; feedwater system malfunctions leading to an increase in the heat removal rate;
  - Decrease in reactor heat removal: feed water pump trips; reduction in the steam flow rate for various reasons (control malfunctions, main steam valve closure, turbine trip, loss of external load and other external grid disturbances, loss of power, loss of condenser vacuum);
  - Increase in reactor coolant system flow rate: start of a main coolant pump;
  - Decrease in reactor coolant system flow rate: trip of one or more coolant pumps; inadvertent isolation of one main coolant system loop (if applicable);
  - Reactivity and power distribution anomalies in the reactor core: inadvertent control rod (or control rod bank) withdrawal; boron dilution due to a malfunction in the chemical and volume control system (for a pressurized water reactor); wrong positioning of a fuel assembly;
  - Reactivity anomalies in the fresh or spent fuel storage: dilution in spent fuel pool;
  - Loss of moderator circulation or decrease or loss of moderator heat sink (in pressurized heavy water reactor);

Identification and grouping of PIEs (5/14)

- Increase in reactor coolant inventory: malfunctions of the chemical and volume control system; excessive feedwater flow in boiling water reactors; inadvertent operation of emergency core cooling;
- Decrease in reactor coolant inventory: very small loss of coolant due to the failure of an instrument line;
- Reduction or loss of fuel cooling in the fuel pools: loss of off-site power; malfunctions in decay heat removal system; leaking of pool coolant;
- Release of radioactive material due to leak in reactor coolant system, with potential containment bypass;
- Release of radioactive material due to leak from a subsystem or component: minor leakage from a radioactive waste system or effluents system.

Identification and grouping of PIEs (6/14)

- Typical examples of postulated initiating events leading to event sequences categorized as design basis accident should include
  - Increase in reactor heat removal: steam line breaks;
  - Decrease in reactor heat removal: feedwater line breaks;
  - Decrease in reactor coolant system flow rate: seizure or shaft break of main coolant pump; trip of all coolant pumps;
  - Reactivity and power distribution anomalies: uncontrolled control rod (or control rod bank) withdrawal; control rod ejection (pressurized water reactor); rod drop accident (boiling water reactor); boron dilution due to the startup of an inactive loop (for a pressurized water reactor);
  - Decrease in reactor coolant inventory: a spectrum of possible loss of coolant accidents; inadvertent opening of the primary system relief valves; leaks of primary coolant into the secondary system;
  - Reduction or loss of fuel cooling in the fuel pools: decrease of coolant inventory due to the break of piping connected to the water of the pool;
  - Loss of cooling to fuel during on-power refuelling (pressurized heavy water reactor);
  - Loss of moderator circulation or decrease or loss of moderator heat sink for a pressurized heavy water reactor;

Identification and grouping of PIEs (7/14)

- Release of radioactive material due to leak in reactor coolant system, with potential containment bypass, or from a subsystem or component: overheating of or damage to used fuel in transit or storage; break in a gaseous or liquid waste treatment system;
- End-shield cooling failure (pressurized heavy water reactor).
- Loss of cooling to fuel during on-power refuelling (pressurized heavy water reactor);
- Loss of moderator circulation or decrease or loss of moderator heat sink for a pressurized heavy water reactor;
- Release of radioactive material due to leak in reactor coolant system, with potential containment bypass, or from a subsystem or component: overheating of or damage to used fuel in transit or storage; break in a gaseous or liquid waste treatment system;
- End-shield cooling failure (pressurized heavy water reactor).

Identification and grouping of PIEs (8/14)

- PSA should be used as a support to justify the categorization of postulated initiating events according to their frequency of occurrence.
  - The calculation of the frequency should take account of the relative frequencies of plant operational states according to its occurrence, such as full power or hot shutdown.
  - It should especially be checked that a transient with potential effects on integrity of barriers has a category consistent with the possible damages on the barriers.
- A reasonable number of limiting cases, which are referred to as bounding or enveloping scenarios, should be selected from each category of events.
  - These bounding or enveloping scenarios should be chosen so that they present the greatest possible challenge to the relevant acceptance criteria and are limiting for the performance parameters of safety related equipment.
  - The safety analysis should confirm that the grouping and bounding of initiating events is acceptable.

Identification and grouping of PIEs (9/14)

- It should be taken into account that a single event should in some cases be analysed from different points of view with different acceptance criteria.
  - A typical example is a loss of coolant accident, which should be analysed for many aspects:
    - ✓ degradation of core cooling,
    - ✓ containment pressure build–up,
    - ✓ radioactivity transport and environmental releases,
    - ✓ leakage of primary coolant to the steam generator by-passing the containment (PWR),
    - ✓ pressurized thermal shock and boron dilution (reactivity accident)
- Handling accidents with both fresh and irradiated fuel should also be evaluated. Such accidents can occur both inside and outside the containment.

Identification and grouping of PIEs (10/14)

- PIEs that would result in a release of radioactive material outside the containment and whose source term should be evaluated include
  - A reduction in or loss of cooling of the fuel in the spent fuel pool when the pool is located outside the containment;
  - Reactivity anomalies in the fresh or spent fuel;
  - An accidental discharge from any of the other auxiliary systems that carry solid, liquid or gaseous radioactive material;
  - A failure in systems or components such as filters or delay tanks that are intended to reduce the level of discharges of radioactive material during normal operation;
  - An accident during reload or maintenance where the reactor or containment might be open.

Identification and grouping of PIEs (11/14)

- A deterministic list of design extension conditions without significant fuel degradation should be developed. These include:
  - PIEs that could lead to situations beyond the capability of safety systems that are designed for design basis accidents (e.g. multiple tube rupture in a steam generator of a pressurized water reactor);
  - AOOs or frequent DBAs combined with multiple failures (e.g. common cause failures in redundant trains) that prevent the safety systems from performing their intended function to control the postulated initiating event (e.g. loss of coolant accident without actuation of the safety injection.
- The failures of supporting systems are implicitly included among the causes of failure of safety systems.
- The identification of these sequences should result from a systematic analysis of the effects on the plant of a total failure of any safety system credited in the safety analysis, for each anticipated operational occurrence or design basis accident (at least for the most frequent ones);
- Credible multiple failures causing the loss of a safety system while this system is used to fulfil its function as part of normal operation.

Identification and grouping of PIEs (12/14)

- Design extension conditions without significant fuel degradation may include
  - Very low frequency initiating events typically not considered as design basis accidents
    - ✓ Uncontrolled heterogeneous boron dilution (PWR);
    - ✓ Multiple steam generator tube ruptures (PWR, PHWR);
    - ✓ Main steam line break and induced steam generator tube ruptures (PWR, PHWR);
  - AOOs or design basis accidents combined with multiple failures in safety systems
    - ✓ ATWS: AOOs combined with the failure of rods to insert;
    - ✓ Station blackout: loss of offsite power combined with the failure of the emergency diesel or alternative emergency power supply;
    - ✓ Total loss of feed water: loss of main feedwater combined with total loss of emergency feedwater;
    - ✓ Loss of coolant accident together with the complete loss of one type of emergency core cooling feature (either the high pressure or the low pressure part of the emergency core cooling system);
    - ✓ Loss of required safety systems in the long term after a postulated initiating event;

Identification and grouping of PIEs (13/14)

- Multiple failures postulated initiating events
  - ✓ Total loss of the component cooling water system or of the essential service water system;
  - ✓ Loss of the residual heat removal system during cold shutdown or refuelling;
  - ✓ Loss of the cooling systems designed for normal cooling and for design basis accidents in the spent fuel pool;
  - ✓ Loss of normal access to the ultimate heat sink.

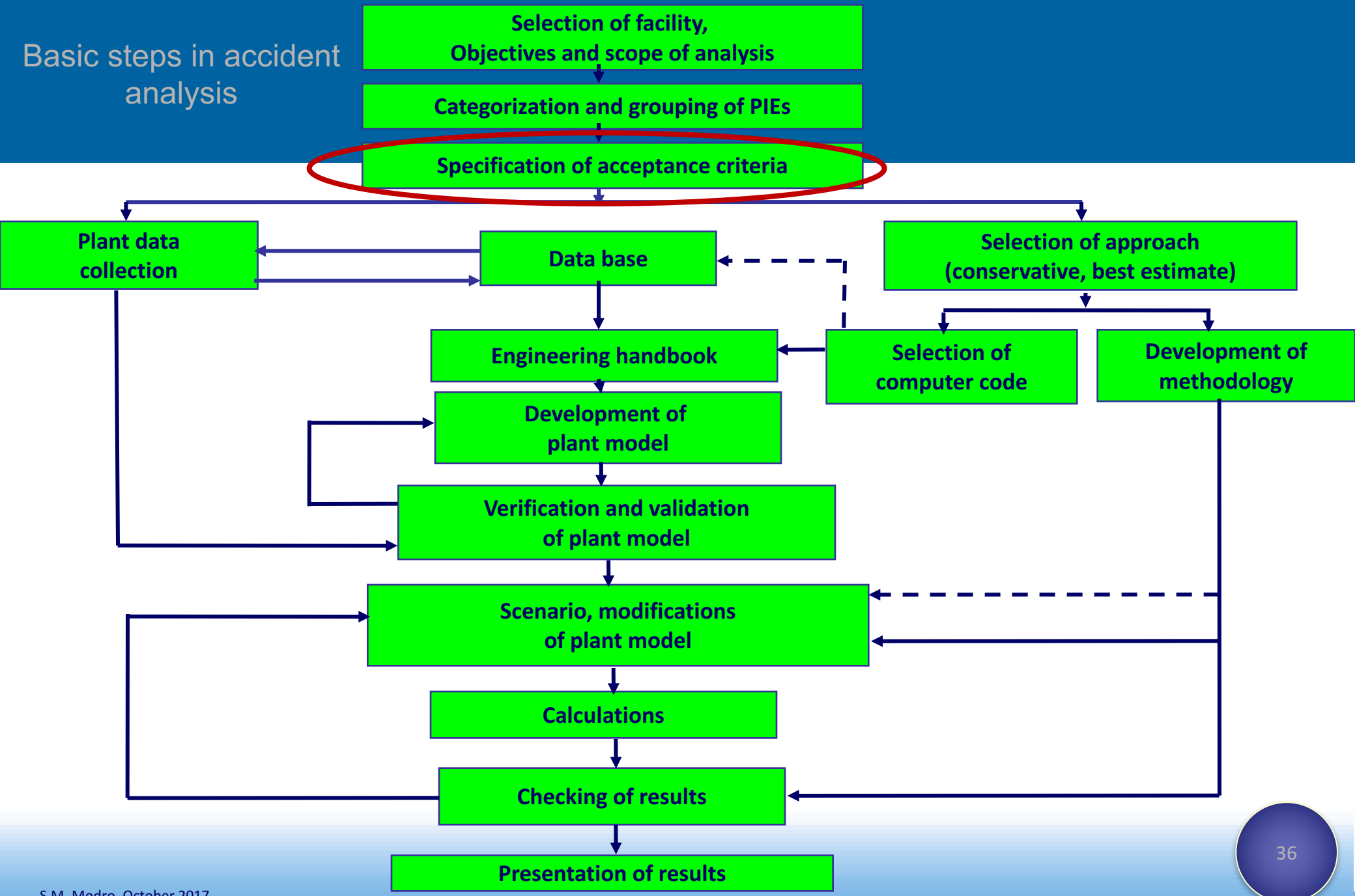
- For the identification of DECs without significant fuel degradation, specific attention should be paid to auxiliary and support systems (e.g. ventilation, cooling, electrical supply) as some of these systems may have the potential of causing immediate or delayed consequential multiple failures in both operational and safety systems.
- Different DEC sequences without significant fuel degradation associated with similar safety challenges should be grouped. Each group should be analysed through a bounding scenario that presents the greatest challenge to the relevant acceptance criteria.
- Multiple failures considered in each sequence of DECs without significant fuel degradation should be specifically listed.

Identification and grouping of PIEs (14/14)

- Determination of PIEs should consider effects and loads from events caused by relevant site specific internal and external hazards.
- In determination of PIEs caused by site specific hazards for multiple unit plant sites the possibility to impact several or even all units on the site simultaneously should be taken into account. (e.g., the effects from losing the electrical grid, those from losing the ultimate heat sink and the failure of shared equipment)
- The analysis of hazards which is performed by using probabilistic methods or appropriate engineering methods should demonstrate that either:
  - Such hazard can be screened out due to its negligible contribution to risk; or
  - The nuclear power plant design is robust enough to prevent any transition from the load into an initiating event; or
  - The hazard causes an initiating event considered in the design.
- In cases where an initiating event is caused by a hazard, the analysis should only credit structures, systems and components that are qualified or protected for the hazard.

ACCEPTANCE CRITERIA

Basic steps in accident analysis



Deterministic Acceptance Criteria: Definition

- **IAEA Safety glossary** explains the acceptance criteria as:
  - **'Specified bound on the value of a functional indicator or condition indicator used to assess the ability of a structure, system or component to perform its design function.'**
- Acceptance criteria can be expressed **quantitatively or qualitatively**
- Acceptance criteria should be established **separately for each category of plant states** (NO, AOOs, DBAs, BDBAs, ...)
- **More stringent criteria should be applied for events with a higher frequency of occurrence**

Acceptance criteria

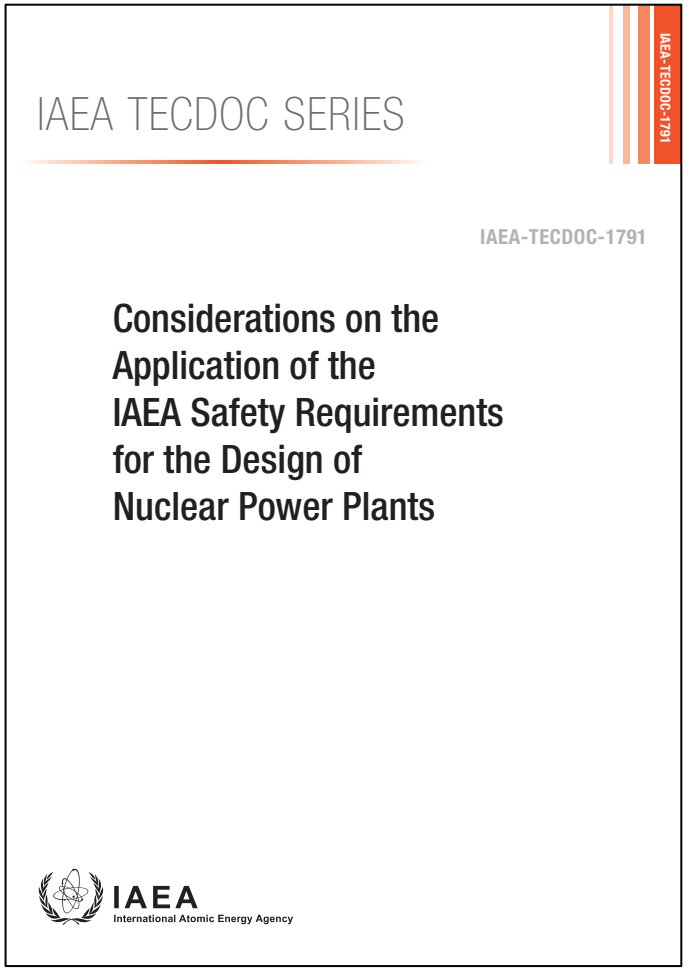
- Acceptance criteria are used in deterministic safety analysis for judgment of acceptability of the demonstration of safety of a nuclear power plant.
- The acceptance criteria can be expressed either in general, qualitative terms or as quantitative limits.
- Categories of acceptance criteria
  - **Safety criteria: these are criteria either directly related to the consequences of operational states or accident conditions or to the integrity of barriers against releases of radioactive material;**
  - **Design criteria: design limits for individual structures, systems and components, that are part of the design basis as important preconditions for meeting safety criteria**; and
  - Operational criteria: these are rules to be followed by operator during normal operation and anticipated operational occurrences; they provide preconditions for meeting the design criteria and ultimately the safety criteria.

- Acceptance criteria should be related to the frequency of the relevant conditions. Conditions that occur more frequently, such as normal operation or anticipated operational occurrences should have acceptance criteria that are more restrictive than those for less frequent events such as design basis accidents or design extension conditions.
- Acceptance criteria should be established at two levels as follows:
  - **High level (radiological) criteria which relate to radiological consequences of plant operational states or accident conditions. They are usually expressed in terms of activity levels or doses typically defined by law or by regulatory requirements;**
  - **Detailed/derived technical criteria which relate to integrity of barriers (fuel matrix, fuel cladding, reactor coolant system pressure boundary, containment) against radioactive releases. They are defined by regulatory requirements, or proposed by the designer subject to regulatory acceptance, for use in the safety demonstration.**

- The radiological acceptance criteria should be expressed in terms of effective doses, equivalent doses or dose rates to nuclear power plant staff, the general public or the environment, including non human biota, as appropriate. The doses are required to be within prescribed limits and as low as reasonably achievable in all plant state.
- Radiological acceptance criteria expressed in terms of doses may be conveniently transformed into acceptable activity levels for different radioactive isotopes in order to decouple nuclear power plant design features from the characteristics of the environment.
- Radiological acceptance criteria for normal operation should be typically expressed as effective dose limits for the plant staff and for the members of the public in the plant surroundings, or acceptable planned radioactive releases from the plant.
- The radiological acceptance criteria for anticipated operational occurrences should be more restrictive than for design basis accidents since their frequencies are higher.

Global Acceptance Criteria

Examples of high level acceptance criteria for different plant states are provided in:



Level of defence	Objective	Associated plant state	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences

Level of defence	Objective	Associated plant state	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences
Level 1	Prevention of abnormal operation and failures	Normal operation	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are bounded by the general radiation protection limit for the public (1 mSv /year[20] commensurate with typical doses due to natural background), typically in the order of 0.1 mSv/year.
Level 2	Control of abnormal operation and detection of failures	Anticipated operational occurrence	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are similar as for normal operation, limiting the impact per event and for the period of 1 year following the event (0.1 mSv/y)

Level of defence	Objective	Associated plant state	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences
Level 3a	Control of design basis accidents (DBAs)	Design basis accident	No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel	No or only minor radiological impact beyond immediate vicinity of the plant, without the need for any off-site emergency actions. Acceptable effective dose limits are typically in the order of few mSv.
Level 3b	Control of DECs without significant fuel degradation (prevention of accident progression into severe accident)	Design extension condition without significant fuel degradation	No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel.	The same or similar radiological acceptance criteria as for the most unlikely design basis accidents

Level of defence	Objective	Associated plant state	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences
Level 4	Control of DECs with core melt (mitigation of consequences of severe accidents)	Design extension condition with core melt (severe accident)	Maintaining containment integrity	Only emergency countermeasures that are of limited scope in terms of area and time are necessary[21]
Level 5	Mitigation of radiological consequences of significant releases	Accident with releases requiring implementation of emergency countermeasures	Containment integrity severely impacted, or containment disabled or bypassed	Off-site radiological impact necessitating emergency countermeasures

Detailed Acceptance Criteria Associated with Integrity of Barriers

Technical acceptance criteria (1/8)

- Technical acceptance criteria should be set in terms of the variable or variables that govern the physical processes that **challenge the integrity of a barrier**.
- It is a common engineering practice to make use of surrogate variables related to the integrity of the barriers to establish an acceptance criterion or a combination of criteria for ensuring the integrity of the barrier.
  - When defining these acceptance criteria, a sufficient conservatism should be included to ensure that there are adequate safety margins to the loss of integrity of the barrier.

Technical acceptance criteria (2/8)

- Technical acceptance criteria related to integrity of barriers should be more restrictive for conditions with higher frequency of occurrence.
  - For anticipated operational occurrences there should be no consequential failure of any of the physical barriers (fuel matrix, fuel cladding, reactor coolant pressure boundary or containment) and no fuel damage (or no additional fuel damage if minor fuel leakage, within operational limits, is authorized in normal operation).
  - For design basis accidents, and for design extension conditions without significant fuel degradation barriers to the release of radioactive material from the plant should maintain their integrity to the extent required.
  - For design extension conditions with core melting, containment integrity should also be maintained and containment by-pass prevented to ensure prevention of an early radioactive release or a large radioactive release.

Technical acceptance criteria (3/8)

- The range and conditions of applicability of each specific criterion should be clearly specified.
  - For example, specification of fuel melting temperature or fuel enthalpy rise should be associated with specification of fuel burn-up and content of burnable absorbers. (Similarly, for limitation of radioactive releases, duration of the releases should be specified.)
- Acceptance criteria can vary significantly depending on conditions. Therefore, acceptance criteria should be associated with sufficiently detailed conditions and assumptions to be used for safety analysis.
- In addition to all pertinent physical quantities, the evaluation of stresses and strains should consider the environmental conditions resulting from each loading, each loading combination and appropriate boundary conditions.

Technical acceptance criteria (4/8)

- The acceptance criteria should adequately reflect the prevention of consequential failure of structures or components needed to mitigate the consequences of the events which are correlated to the assumed loading.
- For postulated initiating events occurring during shutdown operational regimes or other cases with disabled or degraded integrity of any of the barriers, more restrictive criteria should be preferably used, e.g. avoiding boiling of coolant in open reactor vessel or in the spent fuel pool, or avoiding uncovering of fuel assemblies.

Technical acceptance criteria (5/8)

- For specification of a set of criteria depending on specific design solutions the following groups and examples of criteria should be considered as appropriate:
  - Criteria related to integrity of nuclear fuel matrix:
    - ✓ maximum fuel temperature,
    - ✓ maximum radially averaged fuel enthalpy (both values with their dependence on burn-up and composition of fuel / additives like burnable absorbers);
  - Criteria related to integrity of fuel cladding:
    - ✓ minimum departure from nucleate boiling ratio,
    - ✓ maximum cladding temperature,
    - ✓ maximum local cladding oxidation;

Technical acceptance criteria (6/8)

- Criteria related to integrity of the whole reactor core:
  - adequate subcriticality,
  - maximum production of hydrogen from oxidation of claddings,
  - maximum damage of fuel elements in the core,
  - maximum deformation of fuel assemblies (as required for cooling down, insertion of absorbers, and de-assembling),
  - calandria vessel integrity (pressurized heavy water reactor);
- Criteria related to integrity of nuclear fuel located outside the reactor:
  - adequate subcriticality,
  - adequate water inventory above the fuel assemblies and
  - adequate heat removal;

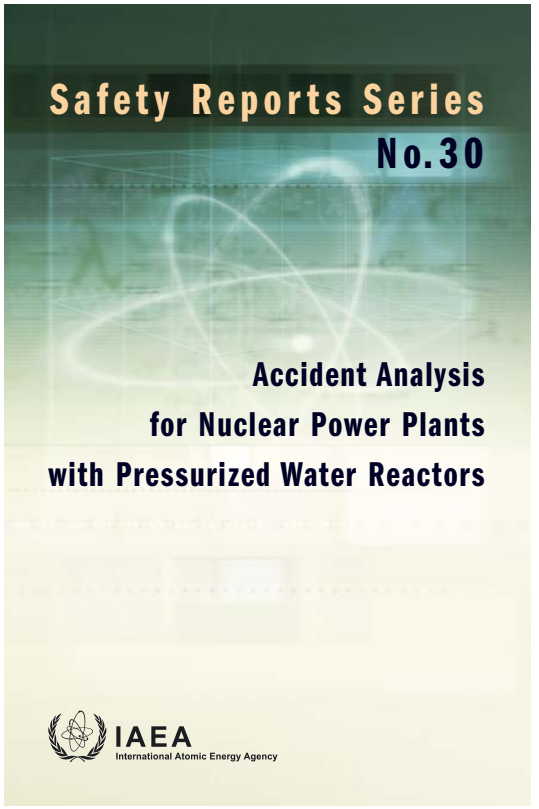
Technical acceptance criteria (7/8)

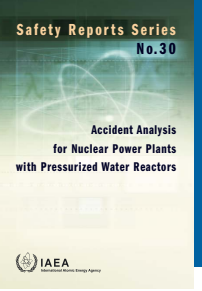
- Criteria related to integrity of the reactor coolant system:
  - ✓ maximum coolant pressure,
  - ✓ maximum temperature,
  - ✓ pressure and temperature changes and resulting stresses-strains in the coolant system pressure boundary,
  - ✓ no initiation of a brittle fracture or ductile failure from a postulated defect of the reactor pressure vessel;
- Criteria related to integrity of the secondary circuit (if relevant):
  - ✓ maximum coolant pressure,
  - ✓ maximum temperature, pressure and temperature changes in the secondary circuit equipment;

Technical acceptance criteria (8/8)

- Criteria related to integrity of the containment and limitation of releases to the environment:
  - ✓ duration and value of maximum and minimum pressure,
  - ✓ maximum pressure differences acting on containment walls,
  - ✓ leakages,
  - ✓ concentration of flammable/explosive gases,
  - ✓ acceptable working environment for operation of systems, maximum temperature in the containment;
- Criteria related to integrity of any other component needed to limit radiation exposure, such as end shield in pressurized heavy water reactors:
  - ✓ pressure,
  - ✓ temperature and
  - ✓ heat-up rate.

Acceptance criteria for PWRs from:



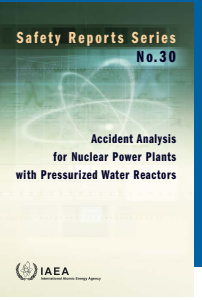


Examples of Technical Acceptance Criteria IAEA SRS-30 TRANSIENTS

- For transients (AOO) it has to be demonstrated that the intrinsic features of the design and the systems automatically actuated by the instrumentation, particularly the reactor trip system, are sufficiently effective to ensure that:
  1. The probability of a boiling crisis anywhere in the core is low. This criterion is typically expressed by the requirement that there is a 95% probability at the 95% confidence level that the fuel rod does not experience a departure from nucleate boiling (DNB).The DNB correlation used in the analysis needs to be based on experimental data that are relevant to the particular core cooling conditions and fuel design
  2. The pressure in the reactor coolant and main steam systems is maintained below a prescribed value (typically 110% of the design pressure)
  3. There is no fuel melting anywhere in the core
- For DBAs it has to be demonstrated that the design specific engineered safety features are sufficiently effective to ensure that:

  4. The radially averaged fuel pellet enthalpy does not exceed the prescribed values (the values differ significantly among different reactor designs and depend also on fuel burnup) at any axial location of any fuel rod. This criterion ensures that fuel integrity is maintained and energetic fuel dispersion into the coolant will not occur (specific to RIAs)

  5. The fuel rod cladding temperature does not exceed a prescribed value (typically 1200° C). This criterion ensures that melting and embrittlement of the cladding are avoided



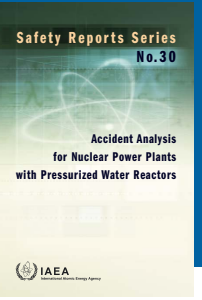
Examples of Technical Acceptance Criteria
IAEA SRS-30
DESIGN BASIS ACCIDENTS

- For DBAs it has to be demonstrated that the design specific engineered safety features are sufficiently effective to ensure that:

6. Fuel melting at any axial location of any fuel rod is limited (typically, no fuel melt is allowed or a maximum 10% melt of the fuel volume at the hot spot is accepted). This criterion ensures that substantial volumetric changes of fuel and a release of radioactive elements will not occur

7. The pressure in the reactor coolant and in the main steam system is maintained below a prescribed value (typically 135% of the design value for ATWSs and 110% for other DBAs).This criterion ensures that the structural integrity of the reactor coolant boundary is maintained

8. Calculated doses are below the limits for DBAs, assuming an event generated iodine spike and an equilibrium iodine concentration for continued power operation, and considering actual operational limits and conditions for the primary and secondary coolant activity



Examples of Technical Acceptance Criteria
IAEA SRS-30
DESIGN BASIS ACCIDENTS

- In addition to criteria 4–8, particularly for design basis LOCAs, short term and long term core coolability should be ensured by fulfilling the following five criteria:

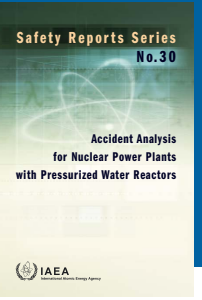
  9. The fuel rod cladding temperature should not exceed a prescribed value (typically 1200° C); the value is limiting from the point of view of cladding integrity following its quenching and is also important for avoiding a strong cladding–steam reaction, thus replacing criterion (5) which is valid for other accidents

  10. The maximum local cladding oxidation should not exceed a prescribed value (typically 17–18% of the initial cladding thickness before oxidation)

  11. The total amount of hydrogen generated from the chemical reaction of the cladding with water or steam should not exceed a prescribed value (typically 1% of the hypothetical amount that would be generated if all the cladding in the core were to react)

  12. Calculated changes in core geometry have to be limited in such a way that the core remains amenable to long term cooling, and the CRs need to remain movable

  13. There should be sufficient coolant inventory for long term cooling

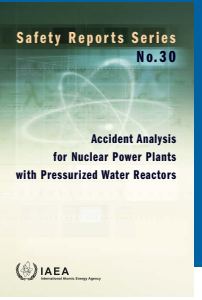


Examples of Technical Acceptance Criteria
IAEA SRS-30
ALL ACCIDENTS – CONTAINMENT PRESSURIZATION

- In addition to the previous relevant criteria, the following criteria apply:

14. The calculated peak containment pressure needs to be lower than the containment design pressure and the calculated minimum containment pressure needs to be higher than the corresponding acceptable value

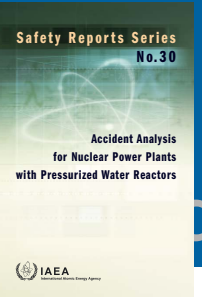
15. Differential pressures, acting on containment internal structures important for containment integrity, have to be maintained at acceptable values



Examples of Technical Acceptance Criteria
IAEA SRS-30
PRESSURIZED THERMAL SHOCK ANALYSIS OF ACCIDENTS

- Specific acceptance criteria for PTS analysis should apply, as follows:

16. There will be no initiation of a brittle fracture or ductile failure from a postulated defect of the reactor pressure vessel (RPV) during the plant design life for the whole set of anticipated transients and postulated accidents



Examples of Technical Acceptance Criteria
IAEA SRS-30
CEPTANCE CRITERIA FOR ACCIDENTS OCCURRING DURING SHUTDOWN

- The operational modes considered have several barriers partially degraded (reactor pressure vessel closed or open, containment closed or open). Besides generally applicable criteria, such as (8), the following specific (more stringent in the case of degraded barriers) criteria have to apply:

17. If both the reactor and the containment are closed, the fuel cladding temperature and oxidation have to be limited to the same values as those for a LOCA.

18. If one of the barriers (either reactor or containment) is open while the other is closed, uncovery of the fuel in the reactor needs to be avoided.

19. If both barriers (reactor and containment) are open, both coolant boiling in the core and fuel uncovery need to be avoided

Example of acceptance criteria: Integrity of the fuel and cladding

- Objective is to ensure that the fuel rods retain their geometries and hold the fuel in its inteded configuration so that fractured portions of the rods would not fall to the bottom of the core and inhibit coolability and there would be no release of the radioactive products into primary circuit

Example of acceptance criteria - PCT

- Peak cladding temperature (PCT) < 2200ºF (1204ºC)
  - Maximum calculated temperature allowable by any portion of the fuel rod cladding during the loss of coolant accident (LOCA)
- No more than 17% of the cladding wall thickness may be oxidized during the loss of coolant accident (LOCA)
  - To ensure that the cladding will retains adequate ductility to resist fracture or shattering caused by the thermal shock loads upon quenching during the reflood phase

Regulatory review of acceptance criteria

- Review process includes
  - How acceptance criteria were established and how the critical values were defined or calculated
  - Check if acceptance criteria are complete
  - Review each individual PIE and check if acceptance criteria correspond to the probability of the event
  - Review each individual PIE and check if acceptance criteria were fulfilled
  - Make assessment of safety margins
  - Document the review process and results of the review!

…Thank you for your attention