Annual CRA PSA / HFA Forum
Bristol, 13 – 14 September 2012

# Safety Assessment Challenges of the New Generation Reactors - Experience from the IAEA Generic Reactor Safety Reviews

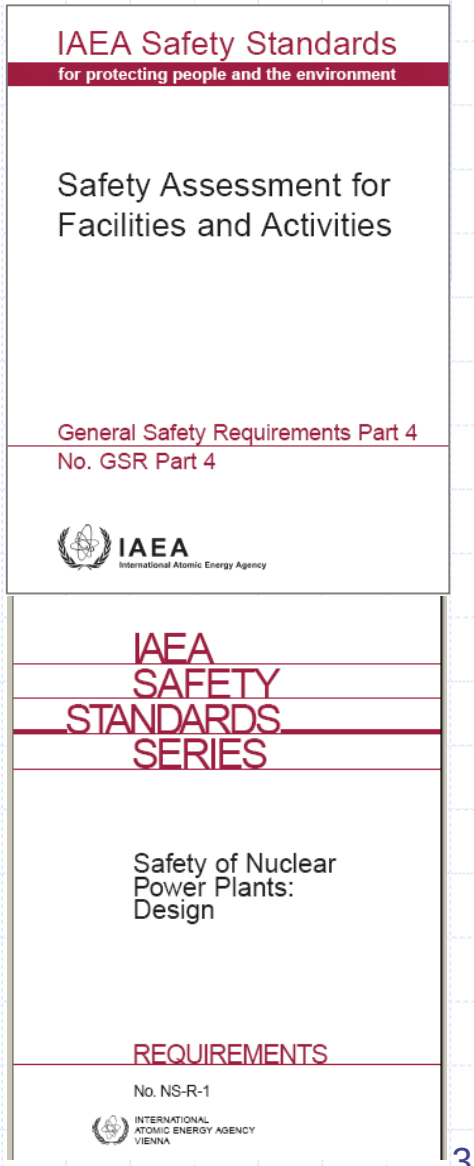
**Tomislav Bajs**
tomislav.bajs@enconet.hr
Enconet d.o.o., Zagreb, Croatia

# Overview

- Description of the Generic Reactor Safety Review Process
- Defence In Depth Characteristics of the New Reactor Designs
- Impact of New Reactors Design Features on Safety Analysis
- Observations from Generic Reactor Safety Review
- Examples of Deficiencies
- Conclusions

# IAEA Generic Reactor Safety Review (GRSR)

- Early evaluation of a vendor's submission of a safety case for new NPP design.
- Review against the IAEA Safety Standards at the requirements level.
- Harmonized review performed by the team of the international experts and the IAEA NSNI staff as secondary reviewers.
- The review does not make any comparisons with other reactor design safety cases – it focuses only on the reactor being reviewed.



# IAEA GRSR Objectives

- Determine whether the design follows the IAEA Fundamental Safety Principles (SF-1);
- Determine whether the safety requirements defined in GS-R-4 and SSR 2/1 (previously NS-R-1) have been addressed in the design safety case and identify omitted;
- Check consistency of the addressed requirements with the spirit of the IAEA standards and guides;
- For the omitted safety determine the relative significance and highlight importance within the safety case;
- Strengths as well as gaps or weaknesses of the safety case are identified in the context of the requirements.

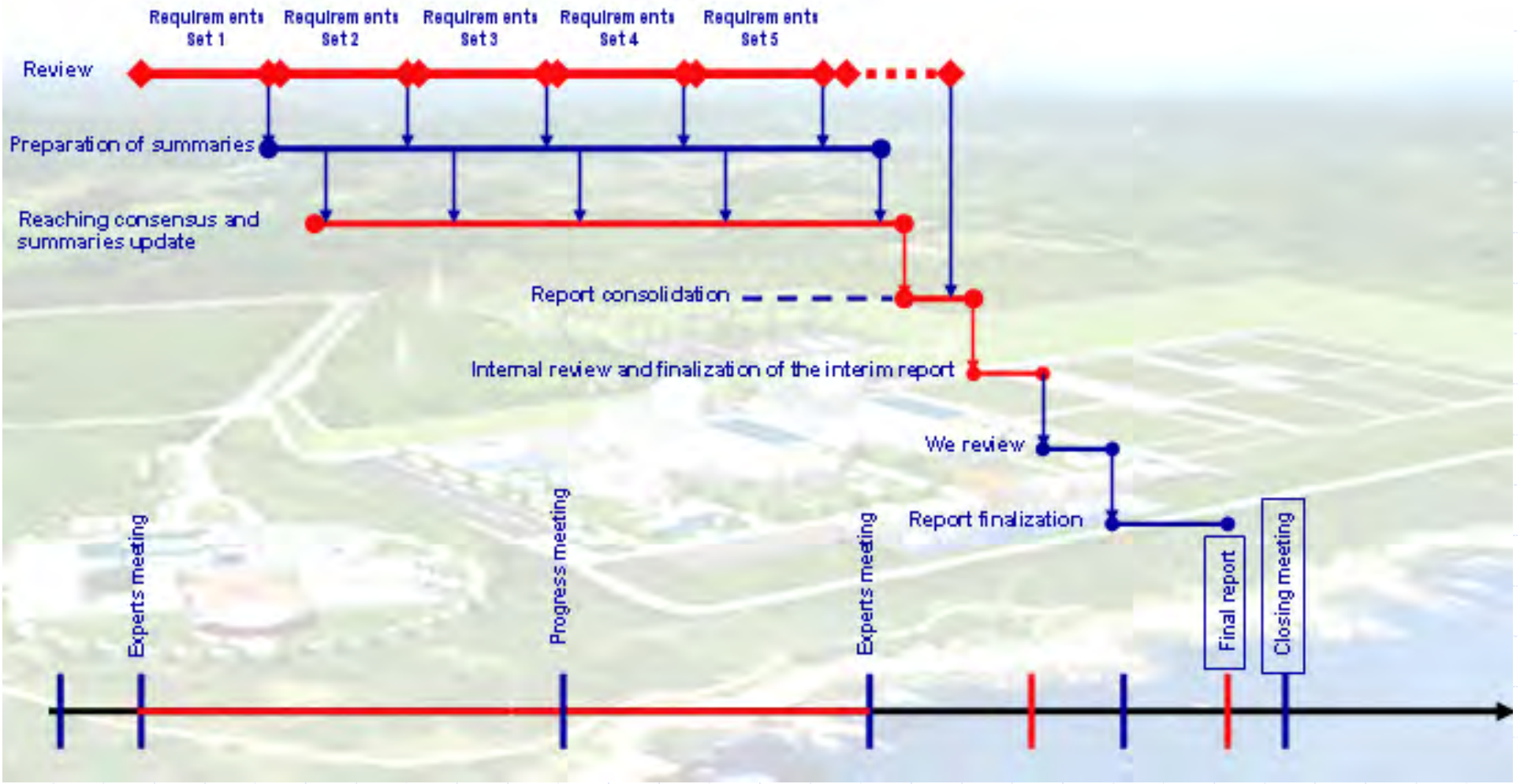
# IAEA GRSR Goals

- Completeness
  - Does the documentation provide sufficient information on the safety case or gaps exist;
  - Is there any indication of what is being done to fill the gaps?
  - Safety claims and arguments are substantiated?
- Comprehensiveness
  - Covered all modes of operation (e.g. start-up, power operation, shutdown, refuelling)?
  - Considered all major systems, structures and components e.g. spent fuel and radioactive waste storage?
  - Lifetime issues covered e.g. ALARA, ageing, provisions for radioactive waste minimisation, decommissioning?

# GRSR Project Concept

- Review Programme is developed and agreed with the requesting Member State.
- A team leader leads the review to consensus among the experts and prepares the Final Report.
- Assignments of topics/requirements are internally assigned within the team according to specialization.
- Review activities are structured sequentially and input from the team is collected in the form of the review sheets.
- A series of meetings are held to discuss and consolidate the views of all experts.
- Consolidated outcomes from the review sheets are summarized in the reports (Interim and Final).

# Example of the GRSR Project Timetable



# Scope of the GRSR GSR-4 Requirements

- Overall requirements for safety assessment (4.1 – 4.15)
- Specific requirements (generic, 4.16 – 4.18)
- Assessment of the potential radiation risks (4.19)
- Assessment of safety functions (4.20 – 4.21)
- Assessment of site characteristics ( 4. 22 – 4.23)
- Assessment of radiological protection provisions (4.24 – 4.26)
- Assessment of the engineering aspects (4.27 – 4.37)
- Assessment of human factors (4.38 - 4.41)
- **Defence in depth and safety margins (4.45 – 4.48)**
- **Scope of safety analysis (4.49 4.52)**
- **Approaches to safety analysis (4.53 – 4.56)**
- Criteria for judging safety (4.57)
- **Uncertainty and sensitivity analysis (4.58 – 4.59)**
- **Use of computer codes (4.60)**
- Use of data from operating experience (4.61)

# Scope of the GRSR NS-R-1 (SSR2/1) Requirements

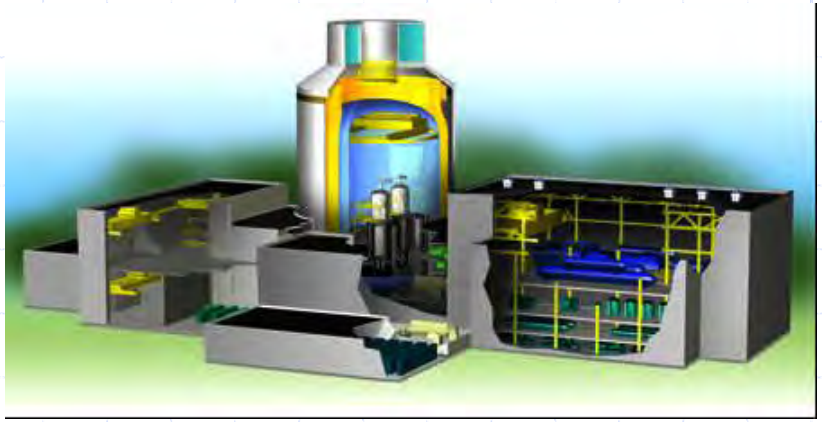
- Management of design (3.2-3.5)
- Proven engineering practices (3.6-3.8)
- **Safety assessment (3.10–3.12)**
- **Independent verification of the safety assessment (3.13)**
- Safety functions (4.5 – 4.7)
- Accident prevention and plant safety characteristics (4.8)
- Safety classification (5.1-5.3)
- General design basis (5.4-5.31)
- Design for reliability of structures, systems and components (5.32-5.42)
- Provision for in-service testing, maintenance, repair, inspection and monitoring (5.43-5.44)
- Equipment qualification (5.45-5.46)
- Ageing (5.47)
- Reactor core and associated features (6.1-6.20)
- Reactor coolant system (6.21-6.42)
- Containment system (6.43-6.67)
- Instrumentation and control (6.68-6.86)
- Emergency power supply (6.88-6.89)
- Waste treatment and control systems (6.90-6.95)
- Fuel handling and storage systems (6.96-6.98)

# History of GRSR Projects

- UK HSE New Reactor Safety Cases submitted for the consideration of the UK Health and Safety Executive/NII against GSR-4: ACR1000, AP1000, ESBWR, EPR
- AREVA-MHI Reactor ATMEA1 Conceptual Design Safety File and its innovative features against GSR-Part 4 and NS-R-1
- Westinghouse AP1000 Safety, Security and Environmental Report against GSR-Part 4 and NS-R-1
- KHNP APR1400 Standard Safety Analysis Report against GSR-Part 4 and NS-R-1
- KEPCO APR1000 Preliminary Standard Safety Analysis Report against GSR-Part 4 and NS-R-1
- Atomenergoproekt VVER-1200 AES2006 Preliminary Safety Analysis Report against GSR-Part 4 and SSR2/1

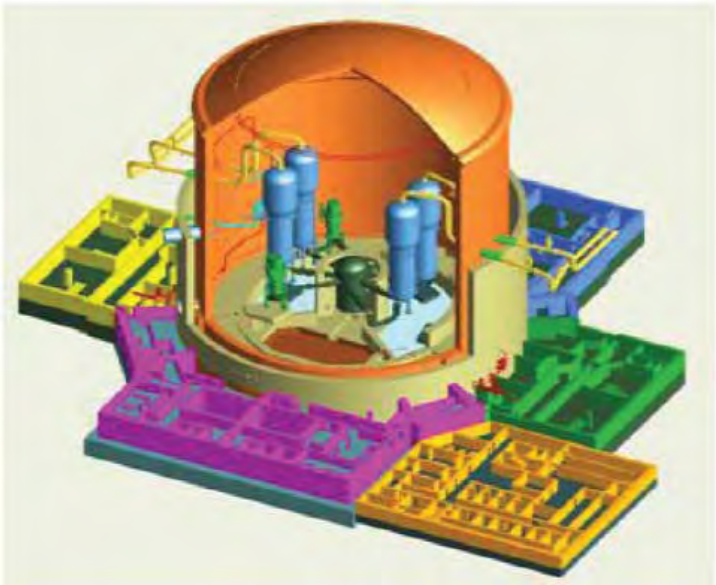
# Overview of the Defence in Depth Concepts

- Representative designs
  - EPR
  - AES 2006
  - AP1000



AP-1000

AES 2006



EPR

# Levels of Defence-in-Depth

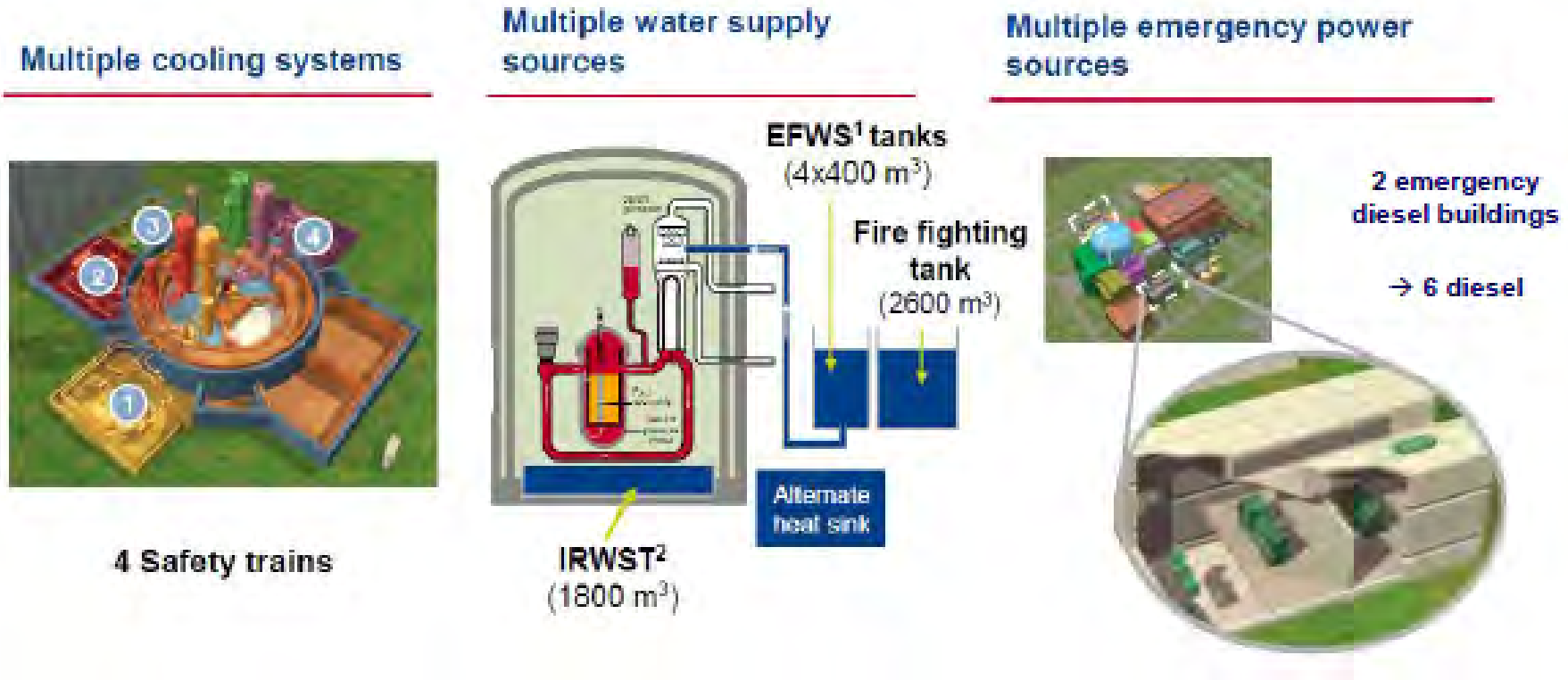
1. Prevention of abnormal operation and failures
2. Control of abnormal operation and detection of failures
3. Control of accidents within the design basis
4. Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents
5. Mitigation of radiological consequences of significant releases of radioactive materials

# Characteristics of the Level 1 and Level 2 Defence in Depth

- Typical extension of proved design considerations with advances in materials and components
- The design of the major components (steam generators, reactor coolant pumps, fuel, internals, turbine and generator) is based on equipment with successful operating experience.
- Advanced Plant Controls including man-machine interface, digital I&C

  Note from GRSR review: Reliability of the computer based systems, on classification of the software used in this system, and on the verification and validation (V&V) process for the systems were in reference reports that were not part of the IAEA study.

# EPR Level 3 Defence in Depth



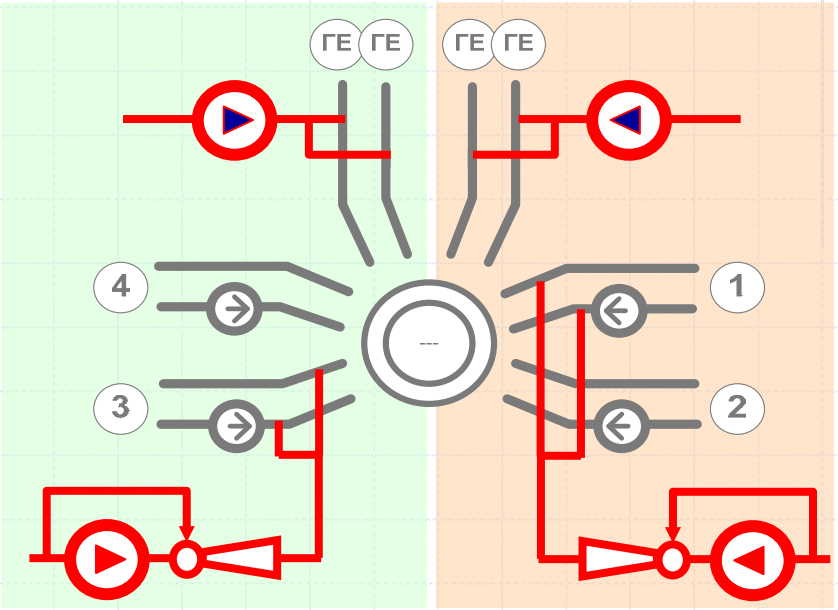

- High redundancy (4 safety trains, each train with double redundandant and diverse sub-systems)
- Alternate heat sink source
- Water reserves in 4 EFWS, large fire fighting tank, IRWST

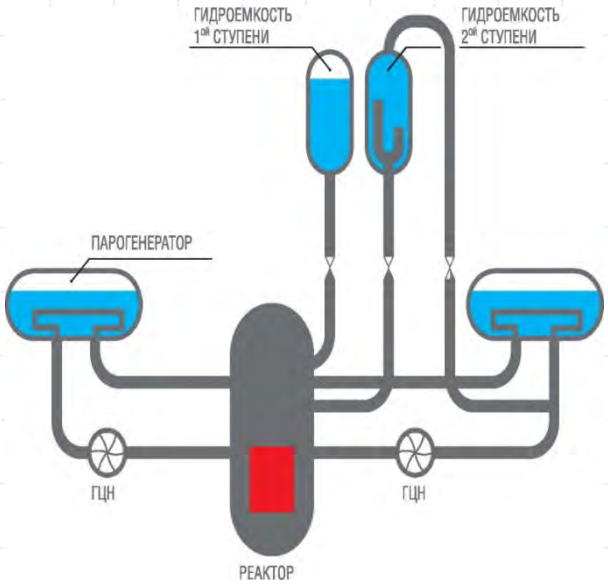
# AP 1000 Level 3 Defence in Depth

- Active Nonsafety-Related Systems
  - Reliably support normal operation
  - Redundant equipment powered by on-site diesels
- Passive Safety-Related Systems
  - Use “passive” process only, no active pumps, diesels, ....
    - One time alignment of valves
    - No support systems required after actuation
  - Reduced dependency on operator actions
  - Mitigate design basis accidents without nonsafety systems
- Sufficient indications to allow determination that the reactor is operating within the envelope of conditions considered by plant safety analysis

# AES-2006 Level 3 Defence in Depth

- Active safety systems:
  - High pressure ECCS (2 pumps)
  - Low pressure ECCS (2 pumps)
  - Emergency Feedwater (2 pumps)
- Passive safety systems:
  - Hydroaccumulators 1st stage (4)
  - Hydroaccumulators 2nd stage (8)
  - Passive Heat Removal System (PHRS) 4 trains

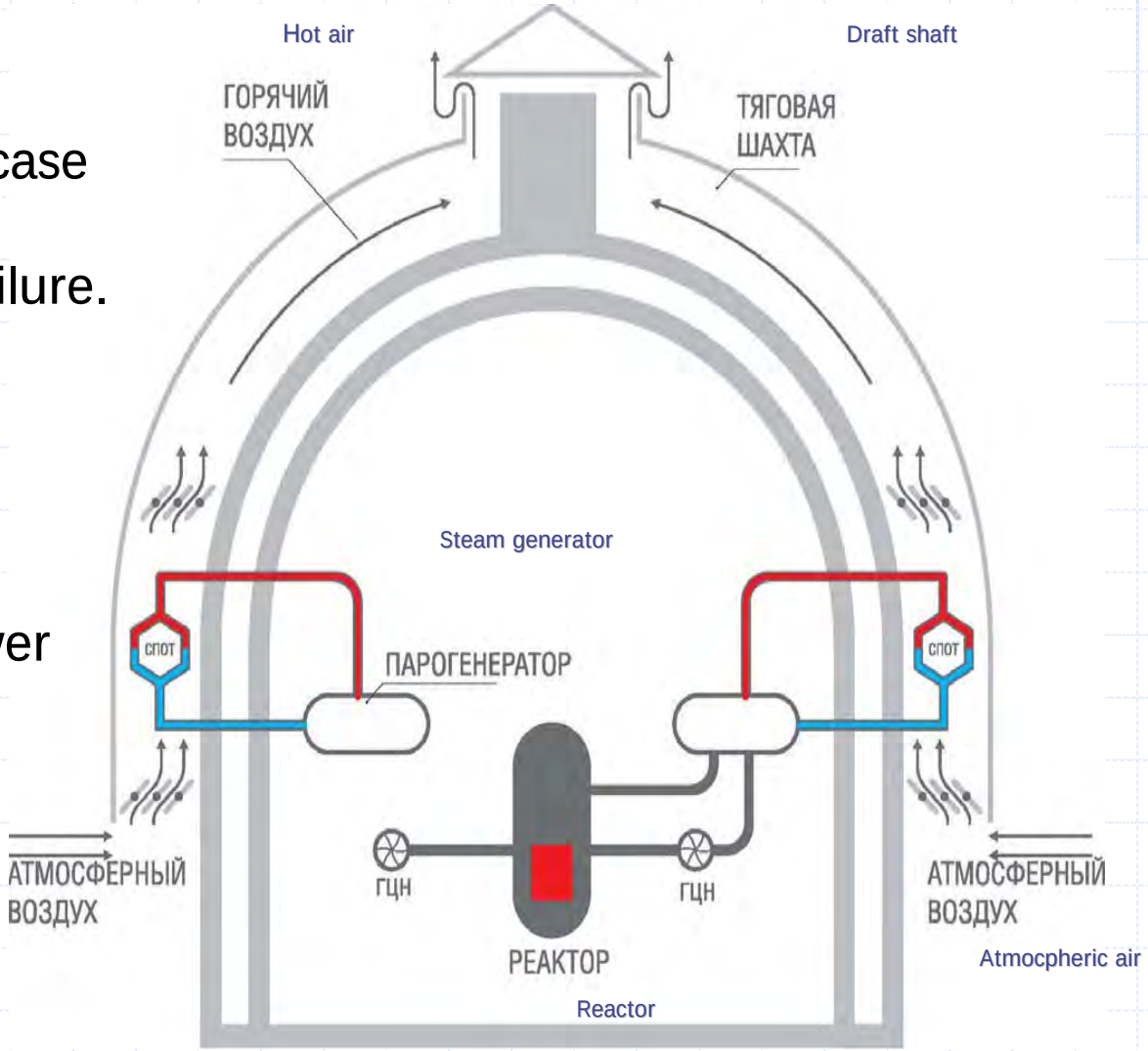


# AES 2006
# Passive Heat Removal System

Filtration system for uncontrolled leaks in case of the active annulus ventilation systems failure.

Continuous removal of residual heat without power

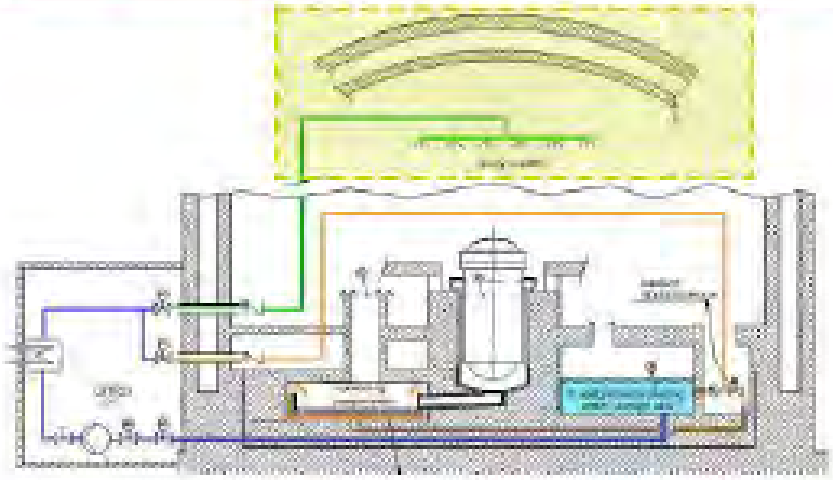


# EPR Level 4 Defence in Depth

## Short-term cooling

- The Core catcher protects the integrity of the containment basemat. It is designed to passively stabilize molten core:
  - Passive valve opening
  - Gravity-driven overflow of water

## Long-term cooling



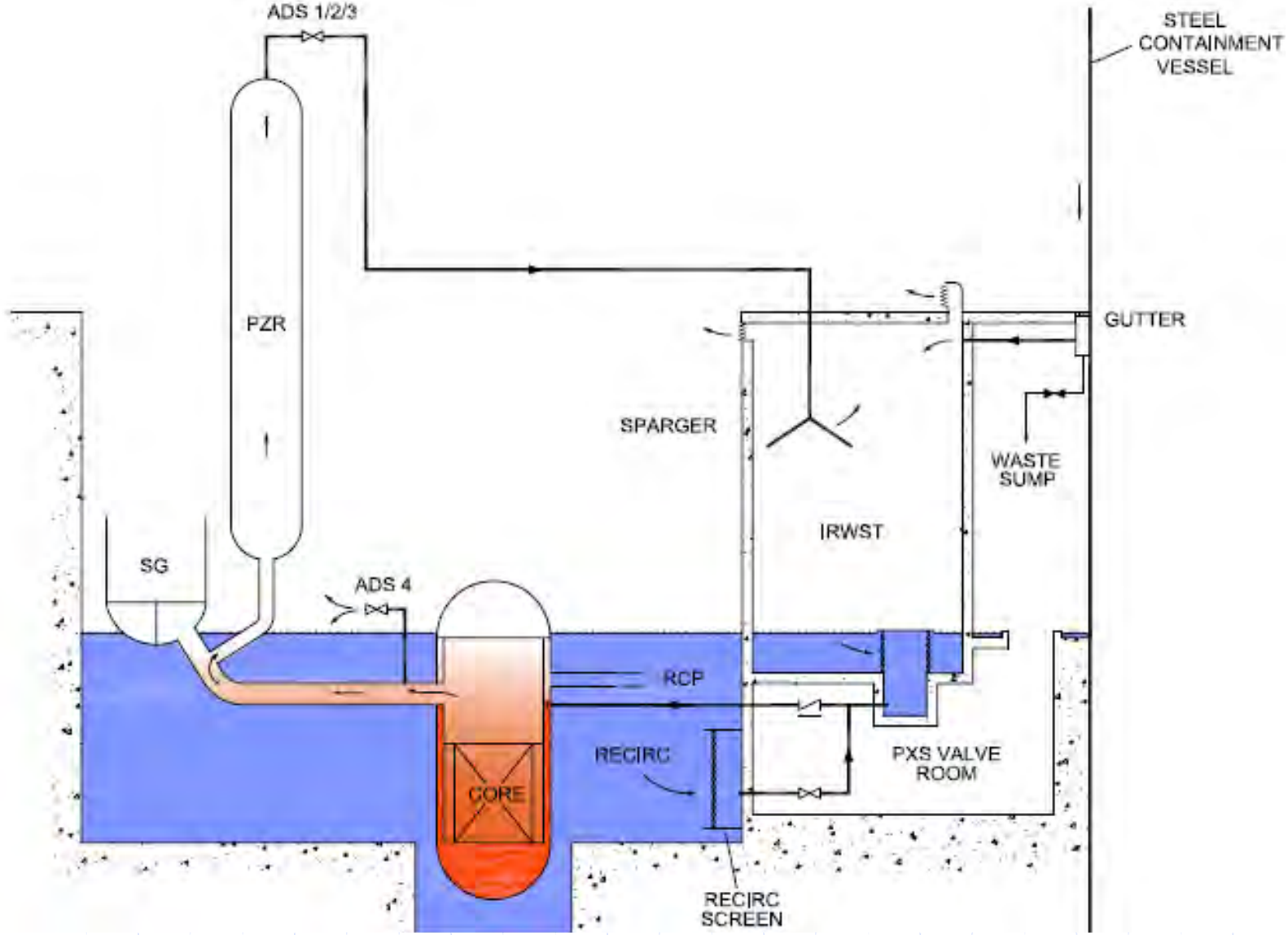
- Long-term core cooling is provided by the containment spray
- The grace period provided by the passive short term cooling allows ample time to recover active systems and ensure long-term

- Complementary active and passive systems for severe accident management strategy
- Prevention of highly energetic events (No H2 detonation, high pressure core melt or steam explosion)

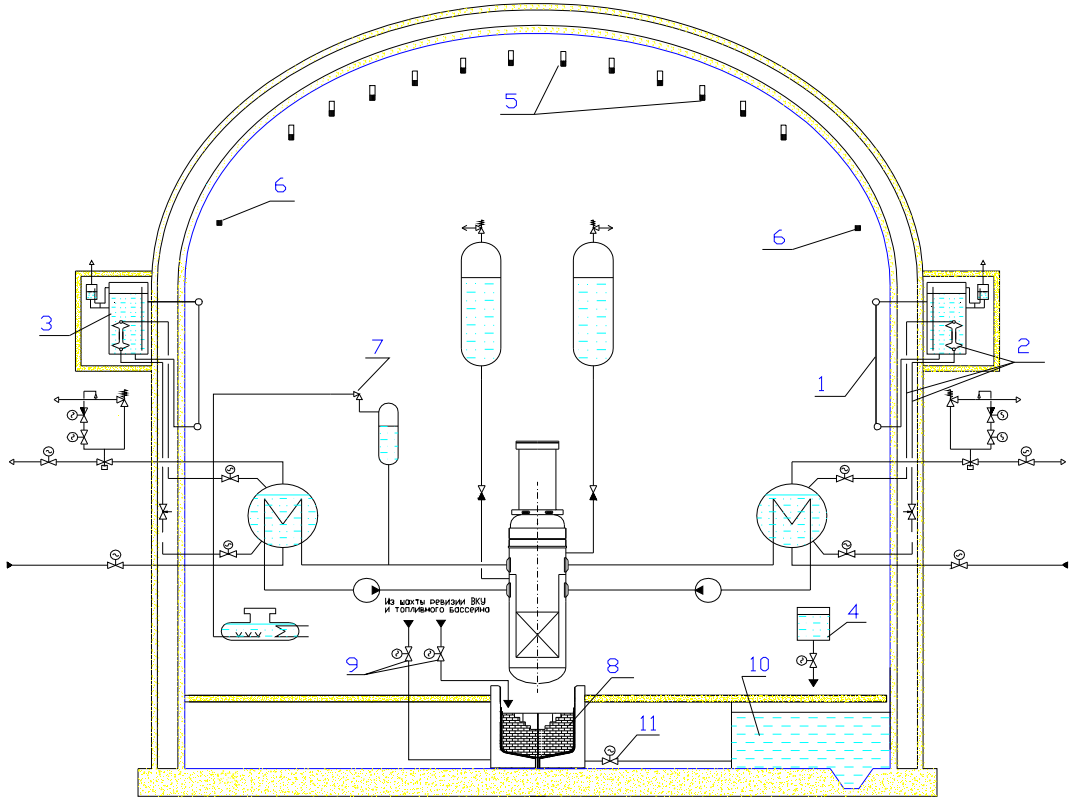
# AP 1000 Level 4 Defence in Depth

- Flood the reactor cavity during severe accidents with IRWST water and submerge the reactor vessel to prevent vessel failure.
  - The multi-stage RCS depressurization system results in low stresses on the vessel wall after the pressure is reduced.
  - The vessel lower head has no vessel penetrations to provide a failure mode for the vessel other than creep failure of the wall itself.
  - Hydrogen Detonation prevented by igniters and passive recombiners
- Retaining the debris in the reactor vessel protects the containment integrity by preventing ex-vessel severe accident phenomena, such as ex-vessel steam explosion and core-concrete interaction.

# AP 1000 In Vessel Retention



# AES-2006 Level 4 Defence in Depth




1 – Containment PHRS
2 – SG PHRS
3 – PHRS water tank
5 – H2 removal
7 – PRZ SV
8 – Core catcher
9 – System of water supply to core catcher
10 – Sump

- Systems for confining radioactive materials
  - Core Catcher
  - Double Containment
  - Spray System (3 trains)
  - Recombiners

# Impact of New Reactors Design Features on Safety Analysis

| | |
|---|---|
| Use of passive systems – low driving forces (gravitational) | → more detailed modelling necessary (two-phase flow!) reliability of passive systems |
| Increased dimensions of the main components | → importance of 3-D effects, revisiting scaling of results from experiments on the plant (calculation), additional validation of the codes |
| Large core dimensions | → multidimensional neutronic and thermal hydraulic space effects (coupled-code applications) |

# Impact of New Reactors Design Features on Safety Analysis (cont.)

Complex phenomena and dependence of response between different systems (primary, secondary, ECCS, containment)

→ control of transfer of information between the codes, validation of coupled codes

Load follow operation

→ modelling of control systems, consideration of effects on the core (localized burn-up effects)

# Impact of New Reactors Design Features on Safety Analysis (cont.)

| | | |
|---|---|---|
| High thermal power with flat power profile | → | vulnerability of fuel assemblies requires more exact prediction of failed fuel rods and associated source term |
| New material (MOX!), geometrical, neutronic and thermal-hydraulic properties of fuel | → | reconsideration (including experiments) and introduction of revised models in the core |
| Fuel burn-up increase, use of burnable absorbers, longer core cycles | → | more detailed modelling of fuel behaviour in steady-state, transients and accidents |

# Impact of Gen III Design Features on Safety Analysis (cont.)

| | | |
|---|---|---|
| Production, distribution, combustion and detonation of hydrogen in severe accidents is spatially dependent processes with potential for localized effects | → | detailed models for production, distribution and management of hydrogen needed |
| Severe accident management strategies (vessel retention, core catcher, PAR) | → | development of multidimensional models, experimental database, validation |
| Radiological acceptance criteria for operational states and for accidents, including severe accidents | → | elimination of unnecessary conservatism |

# Integration of Deterministic and Probabilistic Analysis

- Requirements
  - Probabilistic analysis used to balance the design and to identify factors mostly contributing to the risk
  - Broader use of probabilistic methods should also allow for more realistic approach in use of deterministic methods, in particular for determination of scenarios, assumptions for the analysis and for selection of acceptance criteria
  - PSA analysis shall cover all plant states and all significant internal initiating events including internal hazards as well as external hazards
  - Special attention for human factor reliability, modelling of common cause failures and modelling of passive systems

# Deterministic Safety Analysis Methodologies

time

New Designs

Future

| Selection of initiating events | Computer codes | Initial and boundary conditions | Plant systems availability | Evaluation of compliance with acceptance criteria |
|---|---|---|---|---|
| Few bounding cases (maximum credible accident) | Pessimistic models and codes | Pessimistic | Pessimistic | Some of calculated parameters compared to a set of limiting values |
| Spectrum of categorized events | Pessimistic (EM) | Pessimistic | Pessimistic | Graded criteria according frequency of initiating events |
| Spectrum of DBAs and BDBAs ( incl. severe accidents) | BE models and codes | Pessimistic | Pessimistic with some relaxation based on probabilities (LOOP, ATWS, BDBAs) | Graded criteria according frequency of initiating events; for BDBAs, probabilistic criteria used |
| Spectrum of transients, DBAs and BDBAs ( incl. severe accidents) | BE codes with uncertainties | Realistic data, with uncertainties | Pessimistic with some relaxation based on probabilities (LOOP, ATWS, BDBAs) | Uncertainty bands compared to a set of limiting values: graded criteria according frequency of initiating events; for BDBAs, probabilistic criteria typically used |
| Spectrum of transients, DBAs and BDBAs derived from their frequency | BE codes with uncertainties | Realistic data, with uncertainties | Availability of all systems in accordance with their failure probabilities | Calculated parameters (loads) with their probability distribution compared to a set of limiting values |
| Spectrum of transients, DBAs and BDBAs derived from their frequency | BE codes with uncertainties | Realistic data, with uncertainties | Availability of all systems in accordance with their failure probabilities | Calculated parameters (loads) with their probability distribution compared to a set of strengths with their distribution |

ENCONET

# Common Observations from GRSR (PSA, DSA)

- Deterministic and probabilistic analysis were used as two complementary methods.
- Use of conservative computer codes for safety analysis for design basis accidents.
- Quantification of uncertainties in safety analysis only for selected applications (LOCA, DNBR)
- Application of older methods for high burn-up issues may be inappropriate

# Common Observations from GRSR (passive systems, containment)

- Limited information provided on modelling of passive systems and the coupling with the heat removal by containment systems
- Additional selection and categorization of initiating events associated with passive safety systems failures needed
- Long term containment cooling sustainability

# Common Observations from GRSR (severe accidents and strategies)

- In-vessel retention strategy for molten corium stabilization considered (limited experimental evidence provided).
- Molten spread capability as an alternative mean considered in some designs (also presented with require limited supporting evidence).

# Observations on the Application of BE Tools

- Difficult to demonstrate that use of BE code in combination with conservative inputs and assumptions is done in a correct way:
  - Sensitivity calculations should confirm conservative selection of inputs (possible error if based on engineering judgment),
  - Intentional conservatisms may not always lead to conservative results since it can change during a course of the event, and may not be valid throughout the whole transient,
  - Conservatism may generate misleading sequences of events and unrealistic time-scales.
- Various aspects of the same initiating event when calculated in several steps by different computer codes:
  - Traceability of analyses questionable due to a lack of explanation how transfer of data between different steps is done
  - Transfer of data may mask some important phenomena.

# Observations on the Application of BE Tools (cont.)

- Approach to severe accident analysis is not harmonized. Varies from predominantly probabilistic approach used in USA to the concept of reference severe accidents with deterministic criteria typical for Europe.

- Lack of information on survivability of systems in case of severe accidents, especially in cases complete loss of normal and emergency power supply. Acceptability of the design should be demonstrated using only systems dedicated to severe accident mitigation.

# Examples of Deficiencies

- Omission of certain initiating events (usually accidents at shutdown operational modes or accidents in radwaste treatment systems or spent fuel management systems), or insufficient justification of selection or categorization of postulated initiating events
- Missing justification for categorization of initiating events
- Unclear application of the single failure criterion
- An explicit list of transients and accidents occurring during shutdown operational regimes not provided
- Missing analysis of plant normal operation conditions
- Missing analysis of events related to accidents related to the spent fuel pool

# Examples of Deficiencies (cont.)

- Assumptions used in safety analysis not presented in a clear and convincing way
- Limited presentation of plant data used in accident analysis (including reference values and uncertainties of plant parameters, set-points and system characteristics)
- Inadequate demonstration of codes validation or use of computer codes beyond the range of their validity (e.g. heat transfer correlations)
- Limited documentation of computer codes and demonstration of their validation status

# Examples of Deficiencies (cont.)

- State-of-the-art approaches and widely used international practices not followed, such as use of best estimate codes
- Sensitivity analyses not provided for selection of a bounding case or not adequately convincing
- Missing uncertainty and sensitivity calculations to prove adequate selection of conservative inputs, missing reference to such calculations
- Inconsistencies in transfer of data (without sufficient justification) from thermal-hydraulic analysis to containment analysis and to source term analysis
- Inconsistencies in use of plant data in analysis performed by different computer codes and in transfer of data between various stages of analysis.

# Examples of Deficiencies (cont.)

- Termination of analysis prior to reaching safe stable status of the plant
- Interpretation and evaluation of results made beyond the scope of performed analysis, in particular in cases when several acceptance criteria apply for the same event.
- Inadequate selection of acceptance criteria for high burn-up fuel
- No concise description of which global or detailed acceptance criteria have been used, including criteria associated with high burn-up issues.

# Examples of Deficiencies (cont.)

- Termination of analysis prior to reaching safe stable status of the plant
- Interpretation and evaluation of results made beyond the scope of performed analysis, in particular in cases when several acceptance criteria apply for the same event.
- Inadequate selection of acceptance criteria for high burn-up fuel
- No concise description of which global or detailed acceptance criteria have been used, including criteria associated with high burn-up issues.

# Examples of Deficiencies (cont.)

- Missing data important for evaluation of radiological status prior the accident (cladding defects, excessive coolant radioactivity, and leaking steam generator tubes)
- Unexpected rapid increase of doses in the environment with decreasing probability of occurrence in the range 1E-6 – 1.E-7/r.year
- Over-conservatism used in analysis of design basis accidents (e.g. postulation of a core melt) leading to the conclusion that radiological consequences of design basis accidents are more severe than of severe accidents
- No radiological criteria for design extension conditions have been established.

# Examples of Deficiencies (cont.)

- Missing assessment of doses to control room staff in case of severe accidents
- No separate analysis of a category of Beyond Design Basis Accident without severe core damage
- Inconsistencies in targets for severe accidents
- Unclear citeria for the scope of the severe accident analysis

# Examples of Deficiencies (cont.)

- Absence or limited scope of Level 2 PSA (or even Level 1 PSA)
- Limited scope or missing Low Power and Shutdown PSA
- PSA and Human Reliability Analysis (HRA) results are not used in developing the emergency procedures
- Use of old data sources, no evidence of analysing recent (national or international) operating experience (PIEs, failure rates)
- Missing or insufficient uncertainty & sensitivity studies, no display of uncertainty bands
- Insufficient documentation of phenomenological aspects
- Insufficient documentation of reliability data used
- Missing information on truncation criteria used

# Examples of Deficiencies (cont.)

- The time windows for several operator actions are not supported by thermal hydraulic calculations
- The thermal hydraulic analyses supporting the calculation of time windows for operator actions do not address all features of the accident sequences.
- Unusually low Core Damage Frequency or Large Release Frequency results
- Core Damage Frequency has been calculated for a time period of 24 h only. For reactors with passive safety features this is considered to be too short a time period.
- Cliff-edge effects (releases)  not analyzed
-

# Examples of Deficiencies (cont.)

- Need for review of fire PSA
- Insufficient documentation of application of THERP methodology
- Unusually large contributions from individual accident sequences
- Inconsistencies between tables reporting results
- Insufficient information about extrapolation of results from smaller to larger size reactors

# Conclusions

- The results of the review confirm that new reactor designs are developed to minimize potential risk to the public
- Harmonized evaluation of safety cases does not substitute any part of the licensing process but rather provides inputs for the more effective management of subsequent activities
- GRSR successfully detects gaps in the status of the documentation (completeness and comprehensiveness)
- Majority of design features of new reactor designs are evolutionary using proven technologies, but there are significant challenges that require careful consideration during safety assessment.

# Conclusions (cont.)

- Level of the integation of the PSA is limited by the approach that relies on predefined set of PIE.
- Acceptance criteria for the severe accidents and extended design basis conditions are not harmonized
- Surprisingly, although best-estimate codes have been widely used in the design, very limited use is observed in the safety cases.
- Best estimate safety analysis and quantification of uncertainties, should be more broadly used in demonstration of safety margins for new plant designs.
- Use of coupled codes with appropriate methodologies and validation might overcome limitations of the multi code-multi step approach that is still used in licensing of new designs.

# Acknowledgments

Work of the whole IAEA GRSR Team has been appreciated in the preparation of this presentation

Thank you for your attention!