# IAEA SAFETY STANDARDS

## FOR DESIGN SAFETY

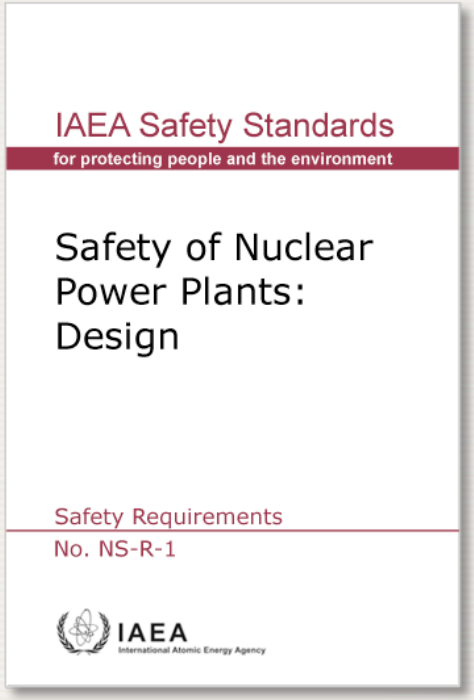
**May 2010**

**Mamdouh El-Shanawany**
Head of Safety Assessment Section
Division of Nuclear Installation Safety

IAEA
International Atomic Energy Agency

# Requirements for design of NPPs

To be implemented by the designer to fulfill the fundamental safety functions with the appropriate level of Defence in depth

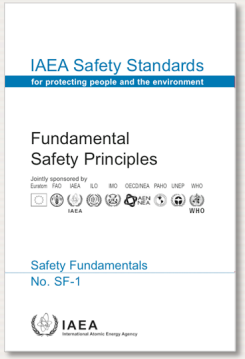


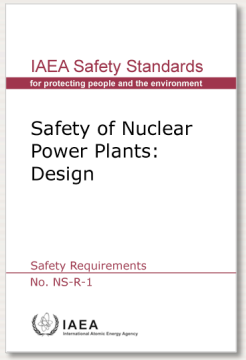

To be used by the reviewer of the design (e.g. Safety Authority) to assess the safety of the design

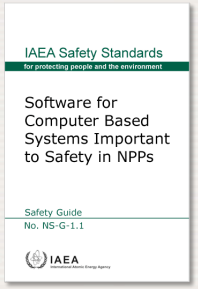
The revision of NS-R-1 is in progress
The draft has been submitted to all Member States of the IAEA for comments

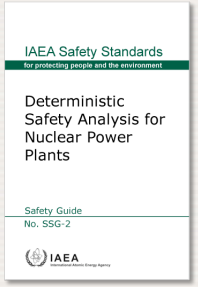
IAEA

# IAEA Safety Standards for Design of NPPs

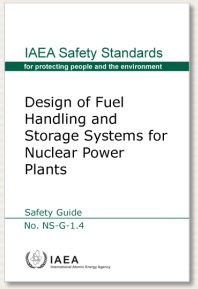


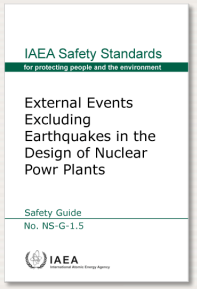



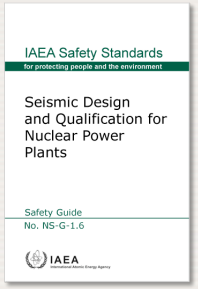



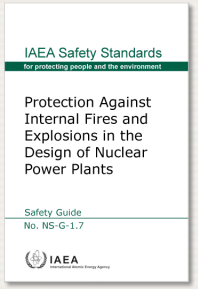



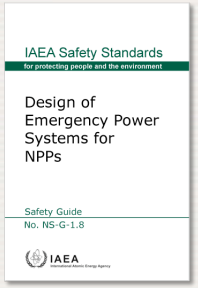


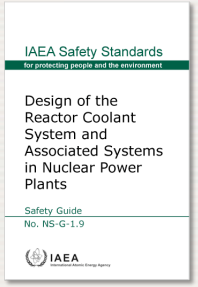


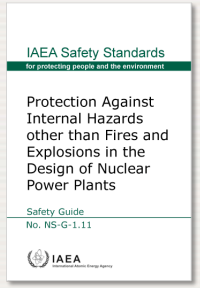



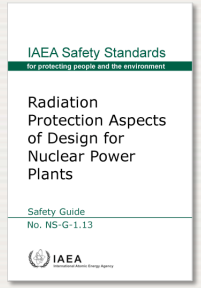












IAEA

# General safety approach

- THE GENERAL SAFETY APPROACH IS MAINLY BASED ON THE CONCEPT OF DEFENCE IN DEPTH
  - High quality, conservatism and safety margins
  - Plant deterministically designed against a broad set of postulated events according to established design criteria
  - Capability to deal with conditions that are not considered in the design basis
- THE DETERMINISTIC APPROACH IS COMPLEMENTED BY PROBABILISTIC EVALUATIONS

IAEA

# Examples of requirements for management of safety

- RESPONSIBILITY IN MANAGEMENT
  - The operating organization has overall responsibility for safety

- SAFETY ASSESSMENT
  - A comprehensive safety assessment shall be carried out to confirm that the design as delivered for fabrication, as for construction and as built meets the safety requirements set out at the beginning of the design process
  - The safety assessment shall be part of the design process….

# Examples of Principal Technical Requirements

- DEFENCE IN DEPTH
  - Defence in depth shall be incorporated in the design process
- ACCIDENT PREVENTION AND PLANT SAFETY CHARACTERISTICS
  - The design shall be such that its sensitivity to pies is minimized
  - The plant response to any pie shall be achieved through:
    (in order of importance)

    1. Inherent characteristics
    2. Passive systems
    3. Active safety systems
    4. Procedural actions

# Examples of Requirements for Plant Design

- SAFETY CLASSIFICATION OF SSCs
  - All structures systems and components that are items important to safety shall be identified and classified on the basis of their significance to safety
  - The significance to safety shall take into account:
    1. The safety function(s) to be performed
    2. The consequences of failure to perform its function
    3. The probability to be called upon to perform a safety function
    4. The time following a pie at which, or the period throughout which, it will be called upon to operate

# Requirements for Design of Plant Systems

- REACTOR CORE AND ASSOCIATED FEATURES
- REACTOR COOLANT SYSTEM
- CONTAINMENT SYSTEM
- INSTRUMENTATION AND CONTROL
- EMERGENCY CONTROL CENTRE
- EMERGENCY POWER SUPPLY
- WASTE TREATMENT AND CONTROL SYSTEMS
- FUEL HANDLING AND STORAGE SYSTEMS
- RADIATION PROTECTION

IAEA

# Examples of Requirement for Design of Plant Systems

- REACTOR CORE AND ASSOCIATED FEATURES
  - The means for shutting down the reactor shall consist of at least two different systems to provide diversity
- REACTOR COOLANT SYSTEM
  - Provisions shall be made for controlling the inventory and pressure of coolant to ensure that specified design limits are not exceeded in any operational state
- CONTAINMENT SYSTEM
  - Each line that penetrates the containment as part of the reactor coolant pressure boundary shall be automatically and reliably sealable in the event of design basis accident (…). these lines shall be fitted with at least two adequate isolation valves (…).

# Examples of Requirement for Design of Plant Systems

- INSTRUMENTATION AND CONTROL
  - Instrumentation shall be provided for measuring all the main variables that can affect the fission process, the integrity of the reactor core, the reactor cooling systems and the containment, and for obtaining any information from the plant necessary for its reliable and safe operation.
- EMERGENCY CONTROL CENTRE
  - An on-site emergency control centre, separated from the plant control room, shall be provided to serve as meeting place for the emergency staff who will operate from there in the event of an emergency. Information about important plant parameters and radiological conditions in the plant and its immediate surroundings should be available there.
- EMERGENCY POWER SUPPLY
  - The combined means to provide emergency power (…) shall have a reliability and form that are consistent with all the requirements of the safety systems to be supplied, and shall perform their functions on the assumption of a single failure.

# Examples of Requirement for Design of Plant Systems

- WASTE TREATMENT AND CONTROL SYSTEMS
  - Adequate systems shall be provided to treat radioactive liquid and gaseous effluents in order to keep the quantities and concentrations of radioactive discharges within prescribed limits. In addition, the ‘as low as reasonably achievable’ (ALARA) principle shall be applied.
- FUEL HANDLING AND STORAGE SYSTEMS
  - The handling and storage systems for irradiated fuel shall be designed to prevent criticality by physical means or processes, preferably by use of geometrically safe configurations even under conditions of optimum moderation.
- RADIATION PROTECTION
  - The shielding design shall be such that radiation levels in operating areas do not exceed the prescribed limits, and shall facilitate maintenance and inspection so as to minimize exposure of maintenance personnel. In addition, the ALARA principle shall be applied.

# Safety guides for the design of NPPs

- DESIGN FOR INTERNAL HAZARDS
  - **NS-G-1.7** - *Protection Against Internal Fires and Explosions in the Design of Nuclear Power Plants*
    - Approach to design for buildings (plant layout and construction, fire compartment and fire cells, analysis of fire hazards)
    - Design measures for fire prevention (control of combustible materials by design, control of explosions, lightning protection, control of ignition sources)
    - Provisions for fire detection and extinguishing
    - Mitigation of secondary effects
  - **NS-G-1.11** - *Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants*
    - Assessment of possible consequences of internal hazards
    - Prevention and mitigation of the internal hazards
    - Hazards considered are: Missiles, Collapse of Structures and falling objects, Pipe failures and their consequences, Pipe whip, Jet effects, Flooding

# Safety guides for the design of NPPs

- DESIGN FOR EXTERNAL HAZARDS
  - **NS-G-1.5** - *External Events Excluding Earthquakes in the Design of Nuclear Power Plants*
    - Derivation of the design basis from the site hazard evaluation
    - Design load derivation for :aircraft crash, external fire, explosions, asphyxiant and toxic gases, corrosive and radioactive gases and liquids, electromagnetic interference, floods, extreme winds, extreme meteorological conditions, biological phenomena, volcanism, collision of floating bodies with water intake and UHS components
  - **NS-G-1.6** - *Seismic Design and Qualification for Nuclear Power Plants*
    - Seismic design: seismic categorization for SSCs, combination of earthquake loads with operating conditions loads, seismic capacity, appropriate plant layout, geotechnical parameters, design of civil structures, design of piping and equipment.
    - Seismic qualification (by analysis, by testing, by indirect methods)
    - Seismic instrumentation

# Safety guides for the design of NPPs

- DESIGN OF PLANT SYSTEMS
  - **NS-G-1.1** - *Software for Computer Based Systems Important to Safety in Nuclear Power Plants*
    - Technical considerations for computer based systems
    - Computer systems design
    - Software design and implementation
    - Verification and analysis
    - Installation, commissioning and operation
  - **NS-G-1.3** - *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*
    - Design for reliability, failure modes, set points, equipment qualification, testing and testability
    - Safety systems, protection systems
    - Power supply
    - Digital systems
    - Human-machine interface

# Safety guides for the design of NPPs

- DESIGN OF PLANT SYSTEMS (Cont.)
  - **NS-G-1.4** - *Design of Fuel Handling and Storage Systems in Nuclear Power Plants*
    - Design of systems for the handling and storage of fresh fuel
    - Design of systems for the handling and storage of irradiated fuel and other core components
    - Handling of fuel casks
  - **NS-G-1.8** - *Design of Emergency Power Systems for Nuclear Power Plants*
    - General design: redundancy, independence and diversity, capacity and capability
    - Design and features of the electrical and non-electrical parts of the EPS
    - Inspection, testing and maintenance
  - **NS-G-1.9** - *Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants*
    - General design considerations (design basis, safety classification, layout, in-service inspections,
      testing and maintenance)
    - Design of: chemical and inventory control system, emergency boration system, emergency core cooling system, residual heat removal systems, steam and main feedwater system, auxiliary feedwater system, ultimate heat sink

# Safety guides for the design of NPPs

- **NS-G-1.10** - *Design of Reactor Containment Systems for Nuclear Power Plants*
  - Design of containment systems for operational states and design basis accidents (Structural design, energy management, management of radionuclides and combustible gases, mechanical features, materials, I&C, support systems)
  - Test and Inspections
  - Design for severe accidents
- **NS-G-1.12** - *Design of the Reactor Core for Nuclear Power Plants*
  - Neutronic, thermal-hydraulic and mechanical design
  - Fuel, coolant, moderator
  - Control of reactivity, reactor shutdown systems, core monitoring
  - Reactor core and associated structures
  - Qualification and testing

# Safety guides for the design of NPPs

- RADIATION PROTECTION
  - **NS-G-1.13** - *Radiation Protection Aspects of Design for Nuclear Power Plants*
    - Radiation protection aspects in design (sources, design approach for operational and accident conditions)
    - Protection of site personnel and the public during operation, decommissioning and accident conditions
    - Estimation of dose rates
    - Monitoring for radiation protection during plant operation and decommissioning
- SAFETY CLASSIFICATION
  - **DS 637** - *Safety Classification of Structures, Systems and Components for NPPs (in preparation)*
    - Rating of the importance to safety of SSCs
    - Classification scheme and implication on design of SSCs

IAEA

# Reviews and Services

## Application of Safety Assessment Methods and Tools

**IPSART** → International PSA Review Team

**GRSR** → Generic Reactor Safety Review

**RAMP** → Review of Accident Management Programme

**SAR** → Review of Safety Analysis Reports:

Accident Analysis

Chapter 4 (Fuel behavior)

Chapter 15 (Accidents Analysis) and

Chapter 19 (PSA and Severe Accidents)

IAEA

# IPSART

## International Probabilistic Assessment Review Team

### Mission Objectives

- To assess the adequacy of the treatment of analysis methods and data used in the PSA
- To assess whether specific conclusions and applications of the PSA are adequately supported by the underlying technical basis
- To assess the validity and applicability of the PSA models as a tool for risk management or specific applications

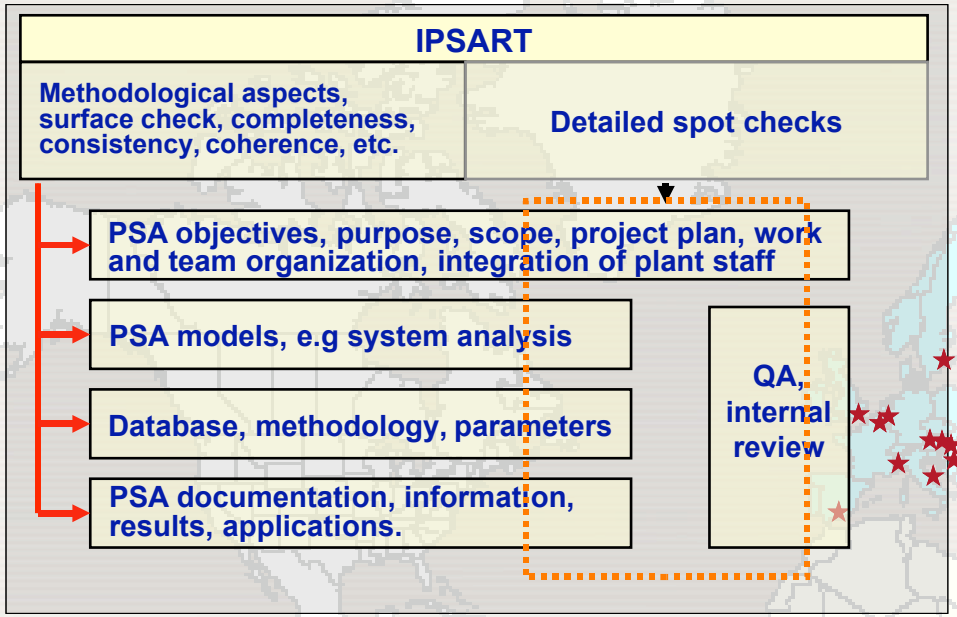
As many MSs have nearly completed their PSA programmes, and the emphasis of current and future missions is placed on applications, mostly by Licensees but also by RBs.

So far, we have addressed these needs with expert missions or workshops, e.g. on Risk Monitor implementation and use.

Hence, there is a need to make the service modular and application oriented, and to integrate it in other services,
e.g. OSART

IAEA

# Summary of IPSART missions




- **Whole coverage review:** The general and methodological aspects of all PSA areas within the scope of the mission are reviewed.
- **Detailed limited review:** Spot checks of the individual areas to verify application of processes and methods. Choice based on the relevance of particular aspects, expertise of the reviewers and the experience from previous missions. Identification of: isolated, endemic and general findings. Tendency to generalize the findings

IAEA

# RAMP

## Review of Accident Management Programmes

### Objectives:

- ✓ to explain to licensee personnel principles and possible approaches in effective implementation of AMP
- ✓ to perform an objective assessment of the status in various phases of AMP implementation
- ✓ To provide licensee with suggestions and assistance for improvements of AMP

### Review Area of RAMP

**Review of accident analysis for accident management**

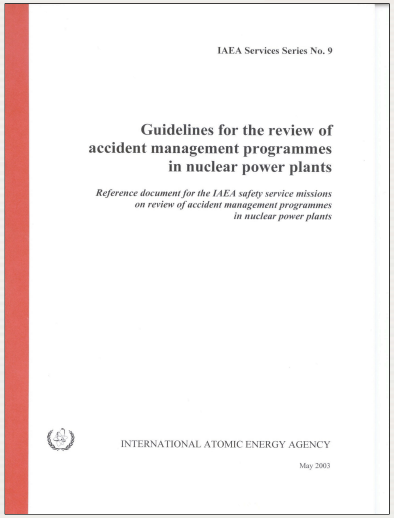
- *to check completeness and quality of accident*
- *analysis covering BDBA and severe accidents*

**Review of AMP (RAMP)**

- *to check quality, consistency and completeness of AMP*

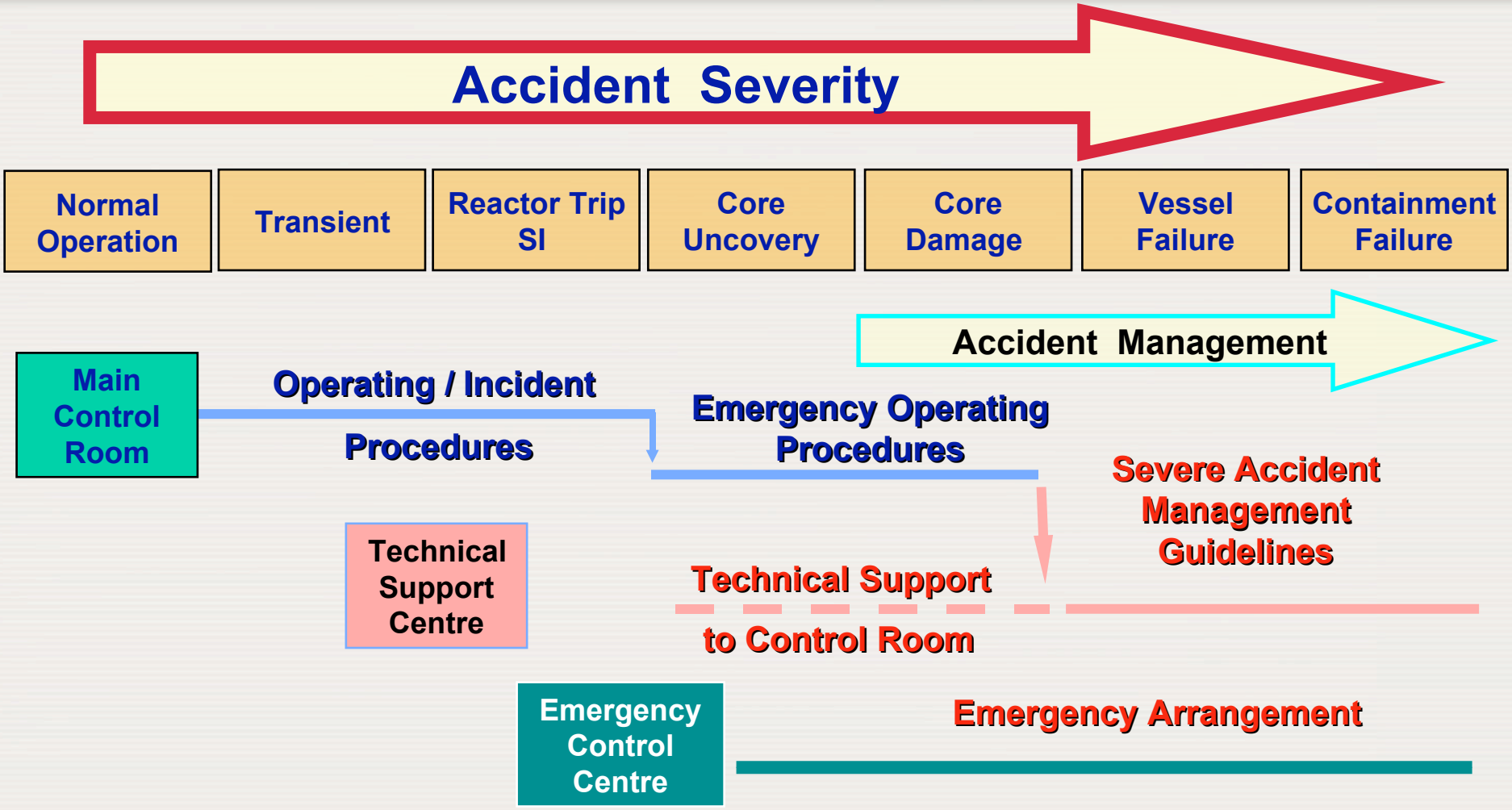
**ACCIDENT MANAGEMENT MEASURES AGAINST TERRORIST ATTACKS OR ATTACKS OF A MALEVOLENT NATURE**

An effort to enhance the protection of NPPs against acts of malevolent nature through consistent use of PSA and accident management strategy




IAEA

# What is Accident Management?




IAEA

# Generic Reactor Safety Review Projects (GRSR)

- NSNI has developed a tailored project framework to provide Member States with an early evaluation of a vendor's submission of a new nuclear power plant, against the IAEA Safety Standards at the fundamentals and requirements level.
- This review framework builds upon design review services which have been conducted by the IAEA over the last 20 years.
- In offering this support to its Member States, the IAEA fulfils the fundamental goal of promoting global nuclear safety by fostering the application of its Safety Standards and feedback.


IAEA

# Generic Reactor Safety Review - Summary

- Provides support to Member States according to NSNI mission.
- A review process based strictly on application of IAEA Safety Standards
- Flexible process as applied to mature designs as well as to concepts and also applicable to early evaluation of innovative reactors.
- Forms a solid basis for harmonization of safety approaches and possibly licensing activities of Member States.
- Valuable feedback for standards interpretation, clarification and future update
- Positively acknowledged by requesting Member States
- The IAEA Generic Reactor Safety Review should be considered for implementation as the foundation of the MDEP programme.

**Projects:**
**Ongoing and completed**

| | |
|---|---|
| **UK GRSR** | Screening of Four New Reactor Safety Cases submitted for the consideration of the UK Health and Safety Executive/ NII against DS348: ACR1000, AP1000, ESBWR, EPR *(completed)* |
| **ATMEA GRSR** | Screening of Conceptual Design Safety File against DS348 and NS-R-1 of new AREVA-MHI Reactor ATMEA1 *(in final stages)* |
| **AP1000 GRSR** | Screening of AP1000 Safety and Environmental Report against DS348 and NS-R-1 *(ongoing)* |
| **APR1400 GRSR** | Screening of KHNP APR1400 Safety and Environmental Report against DS348 and NS-R-1 *(in approval process)* |

IAEA

# Characteristics of a new Safety Approach

- UNDERSTANDABLE, TRACEABLE AND REPRODUCIBLE
  - Clearly stated basis, each step identified and described
- DEFENSIBLE
  - Assumptions, approximations and their impact are known and understood
- FLEXIBLE
  - New information and knowledge can be incorporated
- RISK-INFORMED
  - Blended approach that employs deterministic and probabilistic concepts
- PERFORMANCE-BASED
  - Less prescriptive than current safety approach

# Thank You for your attention

http://www-ns.iaea.org/tech-areas/safety-assessment

IAEA