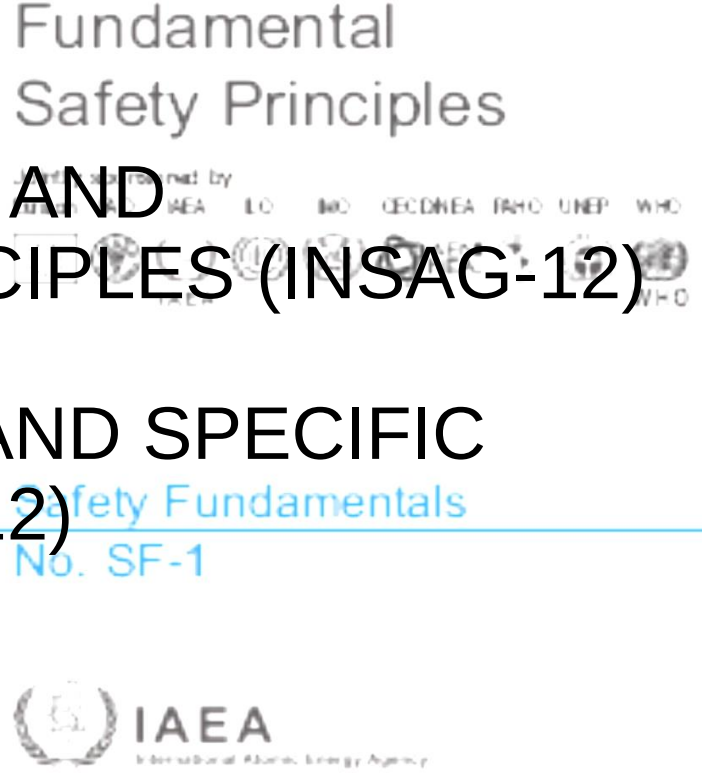
Joint KINS-IAEA-ANNuR/ANSN/FNRBA
BPTC Course on Nuclear Safety,
19 ~ 30 September 2022, KINS, Korea

SAFETY PRINCIPLES AND TECHNICAL ASPECTS

Hokee KIM

Korea Institute of Nuclear Safety

CONTENTS



□ 'Safety' from the IAEA glossary

- Protection of people and the environment against radiation risks
- Safety of facilities and activities that give rise to radiation risks
  - Include the safety of nuclear installations, radiation safety, the safety of radioactive waste management, and safety in the transport of radioactive material
  - Does not include non-radiation-related aspects of safety

✓ Safety, in general

- The state of being "safe"
  - The condition of being protected against types or consequences of failure, damage, accidents, or any other non-desirable event
- The control of recognized hazards to achieve an acceptable level of risk
  - The form of being protected from the event or from exposure to something that causes health or economical losses

□ Nuclear safety

- Achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards

□ Radiation risk

- Detrimental health effects of ionizing radiation exposure, or
- Any other safety related risks that might arise as a direct consequence of:
  - Exposure to radiation
  - Presence of radioactive material or its release to environment
  - Loss of control over a reactor core, chain reaction, radioactive source or any other source of radiation

□ Fundamental safety objective (SF -1)

Protect people and the environment from harmful effects of ionizing radiation

- Achieved without unduly limiting the operation of facilities or the conduct of activities that give rise to radiation risks
- So as to achieve the highest standards of safety that can be reasonably achieved
  - Control the radiation exposure and the release of radioactive material, restrict the likelihood of events that may lead to a loss of control, and mitigate the consequences
- Apply, the objective, for all facilities and activities, and for all stages over the lifetime

✓ *Balance between risks and benefits*

※ Conceptual criteria for balancing

- Measure of the probability and severity of an adverse effect to life, health, property, or the environment

✓ *De minimis non curat lex*

– *Rule that the law will not remedy an injury that is minimal*

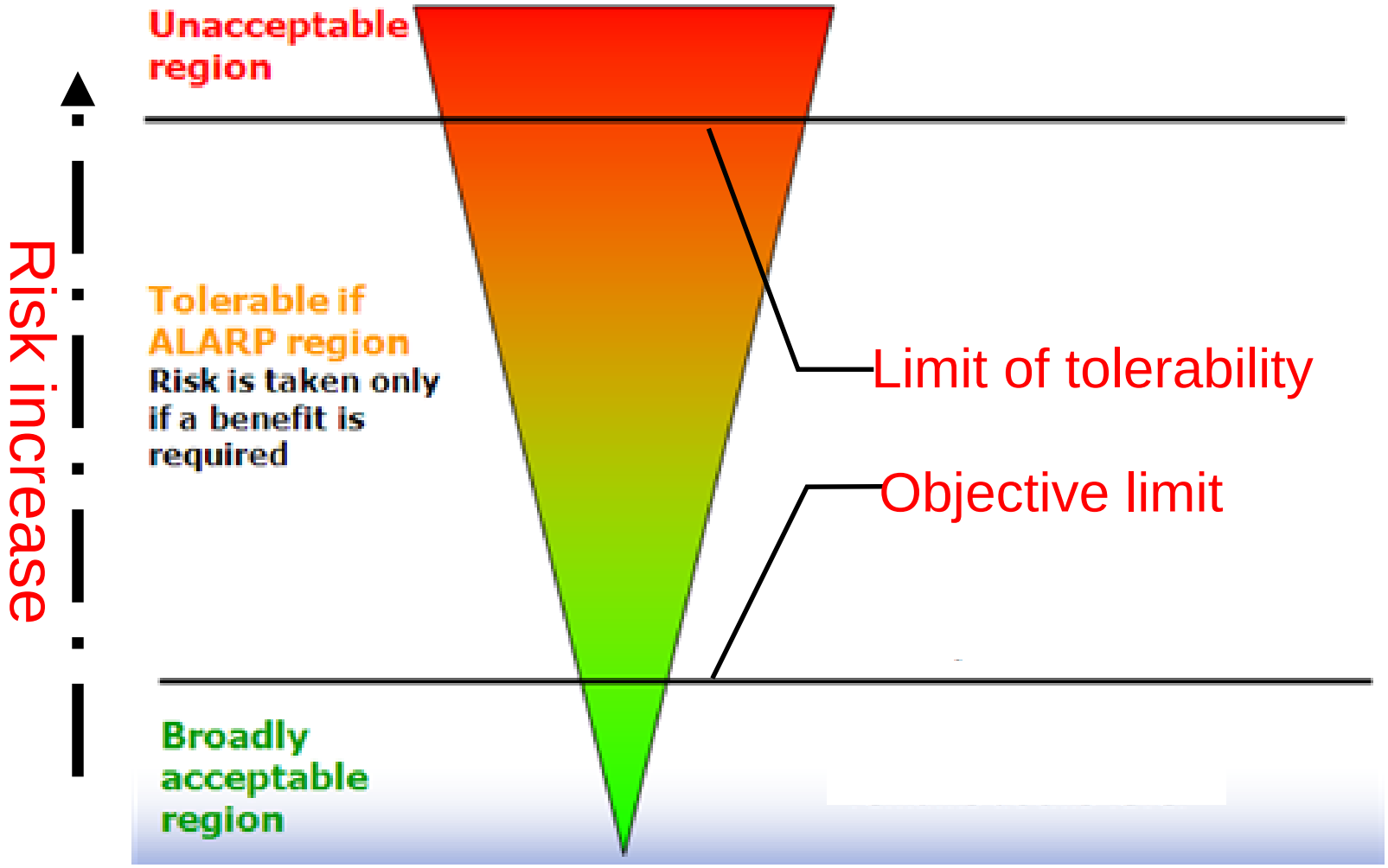
□ De minimis risks

– Those judged to be too small to be of social concern, or too small to justify the use of risk-management resources

- Those of too low a priority to regulate rather than the acceptable low risks
- Help set priorities for bringing regulatory attention to risk in a socially beneficial way

✓ Further reduction of risks is a waste of public resource

□ Risk framework



- Unacceptable risks
  - Unacceptable whatever the benefits, unless they are reduced or there are exceptional reasons

- Broadly acceptable risks
  - Risks, which for the purposes of life or work, everyone who might be impacted is prepared to accept assuming no changes in risk control mechanisms
    - Regarded as insignificant and adequately controlled, and would not usually require further reduction
  - Individual risk of death of one (1) in a million per annum (10^{-6})
    - Boundary between broadly acceptable and tolerable regions

✓ Comparable to everyday risks faced by the general public

- Tolerable risks between the 2 regions
  - Risks within a range that society can live with (1) so as to secure certain net benefits
  - It is (2) a range of risk that we do not regard as negligible or as something we might ignore, but rather as something we need to (3) keep under review and (4) **reduce it still further if and as we can**
  - People tolerate for benefits, in the expectation that:
    - Nature and level of the risks are properly assessed and the results are used properly to determine control measures
    - Residual risks are not unduly high and kept as low as reasonably practicable (the ALARP principle)
      - ✓ The risk of harm has to be balanced against the cost of preventive measure, until the costs are grossly disproportionate to the safety benefits
    - Risks are periodically reviewed to ensure that they still meet the ALARP principle

□ Legal systems for risks

- Have implications for the significance of the limit of tolerability and objective limit

- Civil law based system (e.g. Netherlands)
  - Risk assessment is to demonstrate risk reduction to meet the objective limit with a high level of confidence
  - Give confidence the owner of risk that he met legal obligations to reduce the risk
    - If reduced risk to barely meet an objective limit and convince the regulator that has been done so

    ✓ Role of regulator

- Common law based system (e.g. UK, US, Australia)
  - Generally, recognize tolerable risk as a goal for risk management
    - Ensure safety so far as is reasonably practicable (SFAIRP), to be as low as reasonably practicable (ALARP) or as low as reasonably achievable (ALARA)
    - Secure residual risk so that additional measures to reduce risk further are grossly disproportionate to the reduction
  - Limit of tolerability is a necessary but not necessarily a sufficient condition
    - ALARP is only defined retroactively as the result of a court judgement that considers whether or not the owner acted reasonably in all respects in a particular situation, and typically after a failure has occurred

✓ SFAIRP, ALARP, or ALARA as the conceptual tool for achieving nuclear safety

- *Interpretation in each legal background?*

□ 10 Safety Principles (must)

① Responsibility for safety

The prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risks

– The licensee retains the prime responsibility for safety throughout the lifetime of facilities and activities, and this responsibility cannot be delegated

② Role of government

An effective legal and governmental framework for safety, including an independent regulatory body, must be established and sustained

– Governments and regulatory bodies have an important responsibility in establishing standards and establishing the regulatory framework for protecting people and the environment against radiation risks

③ Leadership and management for safety

Effective leadership and management for safety must be sustained in organizations concerned with, and facilities and activities that give rise to, radiation risks

- **Leadership in safety matters** has to be demonstrated at the highest levels in an organization, to achieve safety by means of an **effective management system**
- This system has to integrate all elements of management so that requirements for safety are established and applied coherently with other requirements, including those for human performance, quality and security, and so that safety is not compromised by other requirements or demands
- The management system also has to ensure the promotion of a safety culture, the regular assessment of safety performance and the application of lessons learned from experience

④ Justification of facilities and activities

Facilities and activities that give rise to radiation risks must yield an overall benefit

- For facilities and activities to be considered justified, the benefits that they yield must outweigh the radiation risks to which they give rise
- To assess benefit and risk, all significant consequences of the operation of facilities and the conduct of activities have to be taken into account

⑤ Optimization of protection

Protection must be optimized to provide the highest level of safety that can reasonably be achieved

- To determine whether radiation risks are ALARA, all such risks, whether arising from normal operations or from abnormal or accident conditions, must be assessed (using a graded approach) a priori and periodically reassessed throughout the lifetime of facilities and activities

⑥ Limitation of risks to individuals

Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm

- **Both** the optimization of protection and the limitation of doses and risks to individuals are necessary to achieve the desired level of safety

⑦ Protection of present and future generations

People and the environment, present and future, must be protected against radiation risks

- Safety standards apply not only to local populations but also to populations remote from facilities and activities
- Where effects could span generations, subsequent generations have to be adequately protected without any need for them to take significant protective actions
- Radioactive waste must be managed in such a way as to avoid imposing an undue burden on future generations

⑧ Prevention of accidents

All practical efforts must be made to prevent and mitigate nuclear or radiation accidents

- To ensure that the likelihood of an accident having harmful consequences is extremely low, measures have to be taken:
  - To prevent the occurrence of failures or abnormal conditions that could lead to such a loss of control
  - To prevent the escalation of any such failures or abnormal conditions that do occur
  - To prevent the loss of, or the loss of control over, a radioactive source or other source of radiation
- The primary means of preventing and mitigating the consequences of accidents is 'defense in depth'
- Defense in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused
- Accident management procedures must be developed

⑨ Emergency preparedness and response

Arrangements must be made for emergency preparedness and response for nuclear or radiation incidents

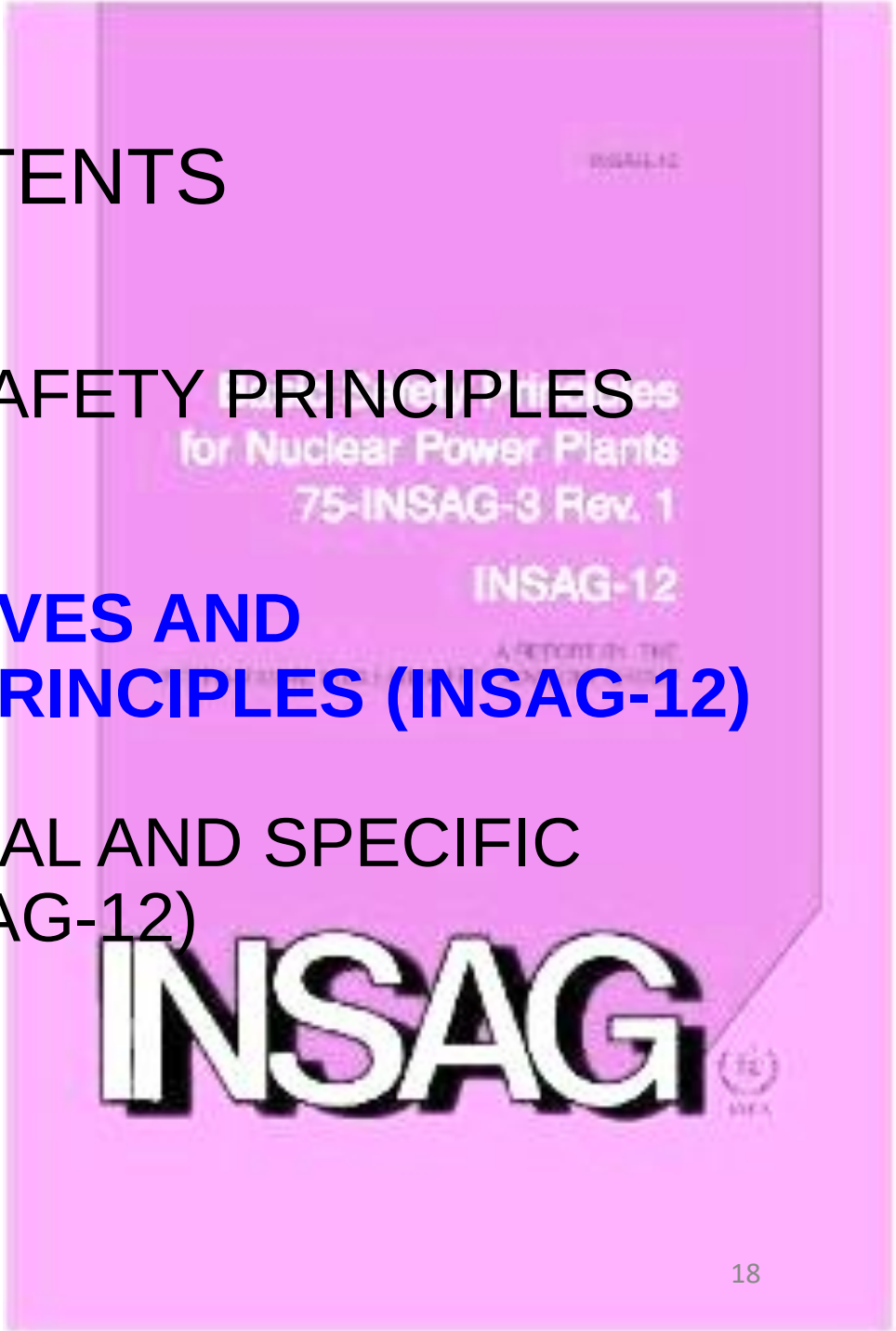
- Licensee, employer, regulatory body and government have to establish, in advance, arrangements for preparedness and response for a nuclear or radiation emergency

⑩ Protective actions to reduce existing or unregulated radiation risks

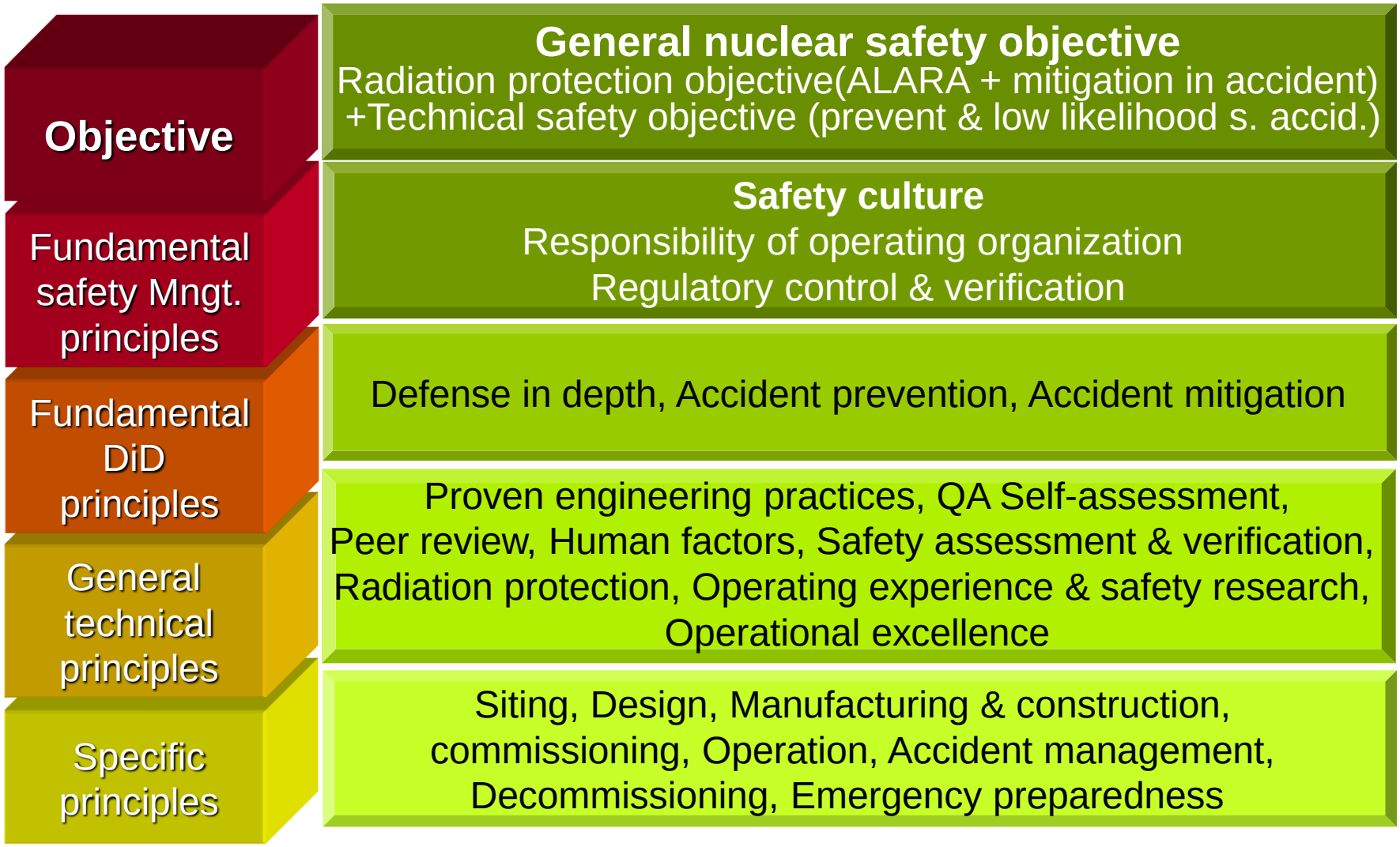
Protective actions to reduce existing or unregulated radiation risks must be justified and optimized

- Radiation of essentially natural origin (radon gas or daughter)
- Exposure that arises from human activities conducted in the past that were not subject to regulatory control, or that were subject to an earlier, less rigorous regime of control (radioactive residues from former mining operations)

CONTENTS



Safety objectives and principles for NPP



1. Safety objectives

General safety objective

To protect individuals, society and the environment by establishing & maintaining in NPPs an effective defense against radiological hazard

Radiation protection objective

- To ensure in normal operation that radiation exposure within the plant and due to any release of radioactive material from the plant is ALARA
- To ensure mitigation of the extent of radiation exposure due to accidents

Technical safety objective

- To prevent with high confidence accidents in NPPs
- To ensure that, for all accidents considered in plant design, even those of very low probability, radiological consequences, if any, would be minor
- To ensure that the likelihood of severe accidents with serious radiological consequences is extremely small

□ General nuclear safety objective

- When the objective is fulfilled, the level of risk due to NPPs does not exceed that due to competing energy sources, and is generally lower
- If another means of electricity generation is replaced by a NPP, the total risk will generally be reduced

  ✓ *Quantitative risk*

※ *Risk*

- *The potential of losing something of value, such as physical health, social status, emotional well being or financial wealth*
- *Intentional interaction with uncertainty, which is potential, unpredictable, unmeasurable and uncontrollable outcome*
- *Since 1950s up to now to estimate risk*
  - *Risk = probability of occurrence X magnitude of damage*
  - *Nuclear, aerospace and chemical industries*

□ Radiation protection objective

✓ *ALARA during normal operation and exposure mitigation for accidents*

- Radiation protection is provided in NPPs under normal conditions and separate measures would be available under accident circumstances
- Keep doses sufficiently low to prevent harmful effects of ionizing radiation
  - Deterministic effects are precluded and the probability of stochastic effects is limited to the levels deemed tolerable
- In preparation for any potential accident, safety provisions in the plant are planned and countermeasures outside the plant are prepared to mitigate harm to individuals, populations and the environment

□ Technical safety objective

- Take all reasonably practicable measures to prevent accidents in NPPs and to mitigate their consequences
  - Ensure with a high confidence that, for all possible accidents taken into account in the design of NPP, any radiological consequences would be minor and below prescribed limits
  - Ensure that the likelihood of accidents with serious radiological consequences is extremely low
- All these objectives should be satisfied in the processes of siting, design & construction, commissioning, operation, maintenance, and decommissioning
- Always pay attention to the strategy of defense-in-depth

2. 3 fundamental management principles

① Safety culture

An established safety culture governs the actions and interactions of all individuals and organizations engaged in activities related to nuclear power

- Safety culture refers to the personal dedication and accountability of all individuals engaged in any activity which has a bearing on the safety of NPPs
- Policies fostering the environment of safety consciousness are established and implemented
- Clear lines of responsibility, communication, and authority are established
- Sound procedures are developed and strict adherence to the procedures is demanded
- Internal reviews are performed of safety activities
- Staff training and education emphasize the reasons behind the safety practices established

② Responsibility of the operating organization

The ultimate responsibility for the safety of a NPP rests with the operating organization.

This is in no way diluted by the separate activities and responsibilities of designers, suppliers, contractors, constructors and regulators

- The organization is in complete charge of the plant, with full responsibility and commensurate authority for activities of electricity production
- Establish policy for adherence to safety requirements
- Establish procedures for safe control of the plant under all conditions, including maintenance and surveillance
- Retain a competent, fit and fully trained staff
- Ensure that responsibilities are well defined and documented and that the resources and facilities for the tasks of its staff are in place

③ Regulatory control and independent verification

The government establishes the legal framework for a nuclear industry and an independent regulatory organization which is responsible for licensing and regulatory control.

The separation between the responsibilities of the regulatory organization and those of other parties is clear, so that the regulators retain their independence as a safety authority and are protected from undue pressure

- Regulatory body makes provision for:
  - Specification and development of standards and regulations for safety
  - Issue of licenses: assessments of safety, the financial viability of the applicant and its organizational capabilities
  - Inspection, monitoring and review of the safety performance
  - Requiring corrective actions of licensee where necessary, and taking any necessary enforcement actions
  - Advocacy of safety research
  - Dissemination of safety information

□ Suwon Hwaseong fortress, Korea (1872)

3. Strategy of defense in depth

□ Defense-in-Depth

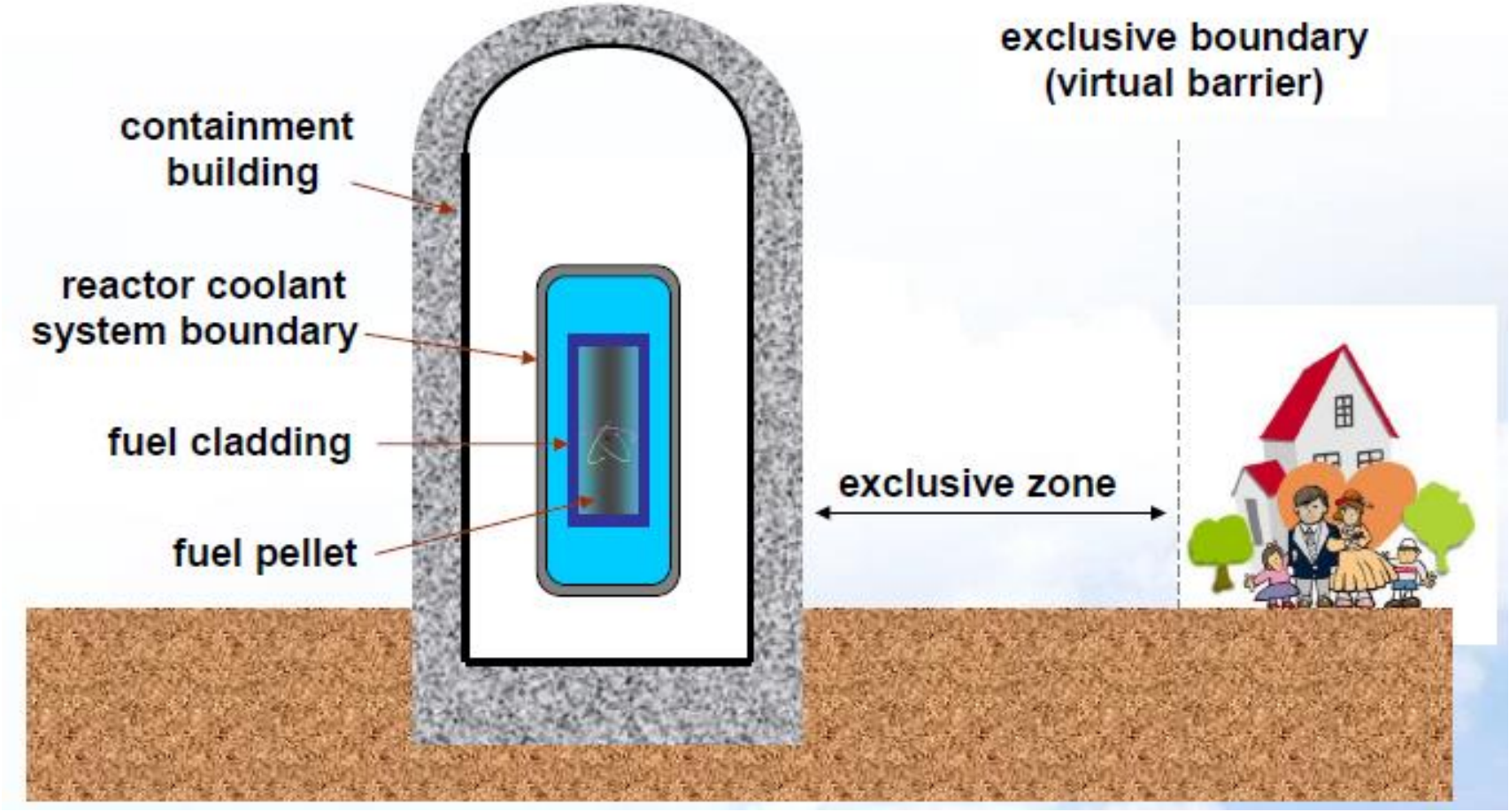
- Underlie the safety technology of NPP
  - An overall strategy for safety measures and features of NPPs to prevent accident
  - ✓ Multiple levels of protection to provide a graded protection against a wide variety of transients, incidents and accidents
- A hierarchical deployment of different levels of equipment and procedures
  - To maintain the effectiveness of physical barriers placed between a radiation source or radioactive materials and workers, the public or the environment, in operational states and, for some barriers, in accident conditions
- Help to preserve 3 fundamental safety functions
  - Control of reactivity
  - Removal of heat from the core
  - Confinement of radioactive material

- The objectives
  - To compensate for potential human and component failures
  - To maintain the effectiveness of the barriers by averting damage to the facility and to the barriers themselves
  - To protect the public and the environment from harm in the event that these barriers are not fully effective
- Assumptions
  - There will be errors in design
  - Equipment will occasionally fail
  - People will occasionally make mistakes
- Twofold strategy
  - To prevent accidents
  - If prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions

- Generally structured in 4 physical barriers and 5 successive levels
  - If one barrier or level were to fail, the subsequent comes into play
  - Special attention to hazards that could potentially impair several levels of defense, such as fire, flooding or earthquakes
  - Basic prerequisites to all measures of the 5 levels: appropriate conservatism, quality assurance and safety culture in safe design and operation
  - Ensure that no single human or equipment failure would lead to harm to the public, and even combinations of failures that are only remotely possible would lead to little or no harm
  - The independence of different levels of defense is a key element

✓ *Assessment of the effectiveness of DiD is an important means of assessing general plant safety*

- **Multiple barriers** against radioactive release



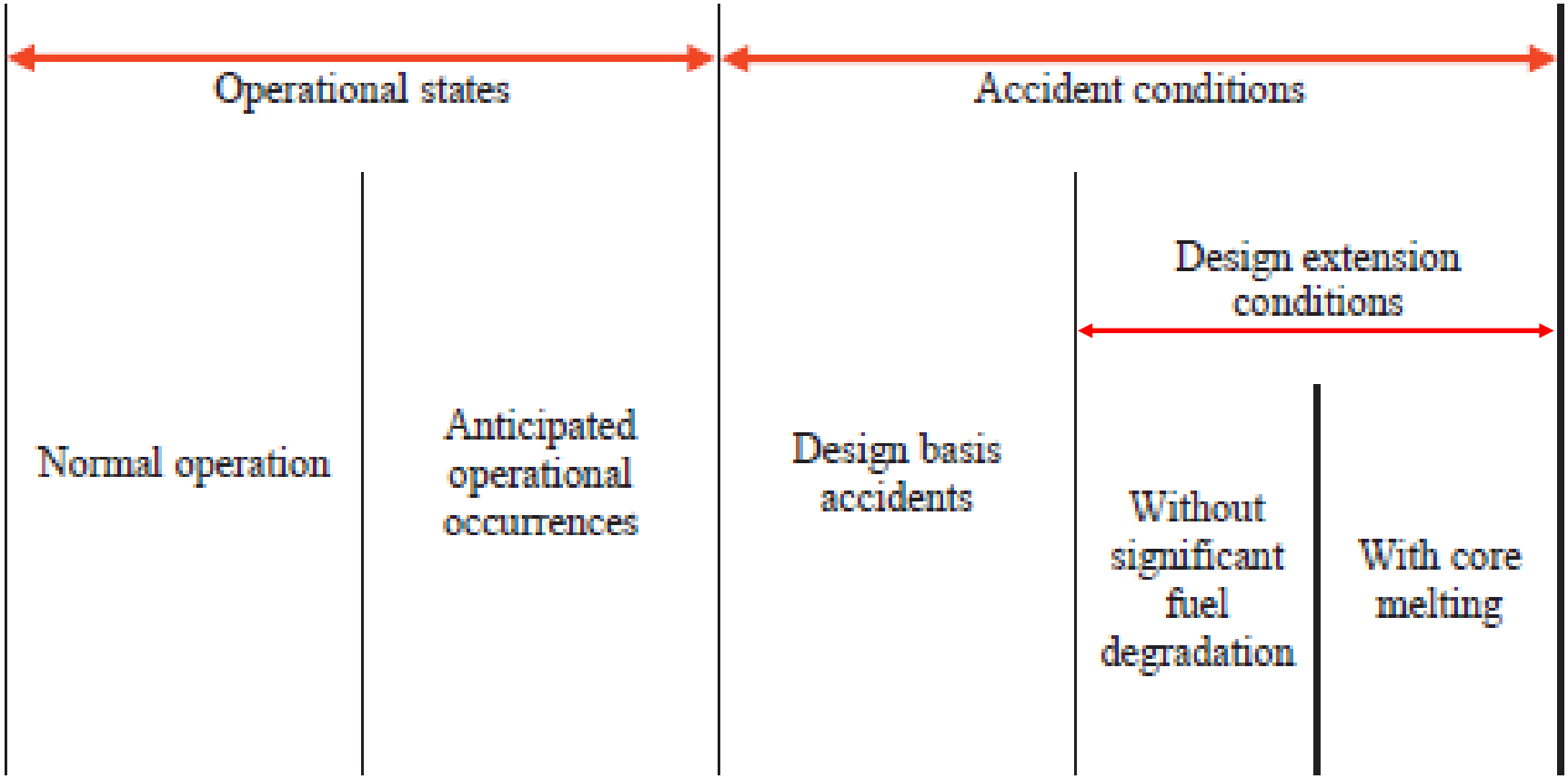
- For the physical barriers:
  - The reliability is enhanced by applying the concept of defense in depth to them
    - Design conservatively, check its quality to ensure that the margins against failure are retained, monitor its status, and control and monitor all plant processes capable of affecting it in operation
  - Human aspects to protect the integrity of the barriers:
    - Quality assurance
    - Administrative controls
    - Safety reviews
    - Independent regulation
    - Operating limits
    - Personnel qualification and training
    - Safety culture

- Levels of DID

	Definition	Means (HW, SW and control)
Level 1	• *Prevention* of abnormal operation and failures - *to confine radioactive material and minimize deviation from normal operation*	• Robust rules & regulations • Conservative design • High quality construction, operation, & maintenance • OEF & Safety Culture
Level 2	• *Control of abnormal operation* and detection of failures - *to bring the pant back to normal operating condition ASAP*	• Auto control & protection system • Monitoring facilities
Level 3	• *Control of accidents* within the design basis - *to prevent core damage*	• ESF • EOP
Level 4	• *Control of severe plant conditions*, preventing accident progression and mitigating the consequences - *to protect the confinement*	• Containment Building • SAMG
Level 5	• *Mitigation of radiological consequences* of significant releases of radioactive material	• Exclusion Area • Radiation Emergency Plan

※ DiD after Fukushima Daiichi accident

✓ *IAEA SSR-2/1(Rev.1), Safety of NPPs: Design*



✓ *Accident conditions*

- *Less frequent and more severe than AOOs*
- ***Design basis accidents***

  A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the NPP to withstand, without acceptable limits for radiation protection being exceeded

  – *Analysed in a conservative manner:*

    - *Postulating certain failures in safety systems,*
    - *Specifying design criteria, and*
    - *Using conservative assumption, models and input parameters*

- ***Design extension conditions (DECs)***

  A set of DECs shall be derived on the basis of engineering judgment, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the NPP by enhancing the plants capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures

  These DECs shall be used to identify the additional accident scenario to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences if they do occur

- *Prevent accident conditions not considered in DBA conditions and to mitigate their consequences, as far as is reasonably practicable*
- *Require additional safety features or extension of the capability of safety systems to maintain the integrity of containment*
  - *To manage accident conditions where there is a significant amount of radioactive materials in the containment*
- *Design the pant so that it can be brought into a controlled state and the containment function can be maintained*
  - *To practically eliminate DECs leading significant radioactive releases*
  - *If not, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures*
  - *Best estimate approach to analyse the effectiveness of provisions to ensure the functionality of containment*

※ *Vienna declaration in Feb. 2015*

1. New nuclear power plants are to be designed, sited, and constructed, consistent with the objective of preventing accidents in the commissioning and operation and, should an accident occur, mitigating possible releases of radionuclides causing long-term off site contamination and avoiding early radioactive releases or radioactive releases large enough to require long-term protective measures and actions.

2. Comprehensive and systematic safety assessments are to be carried out periodically and regularly for existing installations throughout their lifetime in order to identify safety improvements that are oriented to meet the above objective. Reasonably practicable or achievable safety improvements are to be implemented in a timely manner.

3. National requirements and regulations for addressing this objective throughout the lifetime of nuclear power plants are to take into account the relevant IAEA Safety Standards and, as appropriate, other good practices as identified inter alia in the Review Meetings of the CNS.

□ Accident prevention

Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents, particularly any which could cause severe core damage

- Means to prevent accidents:
  - Strive for high quality in design, construction and operation of the plant so that deviations from normal operational states are infrequent
  - Use safety systems as a backup to feedback in process control to prevent deviations
    - Redundancy, diversity, physical separation of parallel components, regular inspection and test to reveal any degradation, and detection of abnormal conditions by monitoring system
  - Foster a questioning attitude from the staff and promote discussion of what could go wrong prior to initiating activities

- The prevention of accidents depends on:
  - Conservatively designed equipment and good operational practices to prevent failure
  - Quality assurance to verify the achievement of the design intent
  - Surveillance to detect degradation or incipient failure during operation
  - Steps to ensure that a small perturbation or incipient failure would not develop into a more serious situation

□ Accident mitigation

In-plant and off-site mitigation measures are available and are prepared for that would substantially reduce the effects of an accidental release of radioactive material

- Provisions for accident mitigation extend the DiD concept beyond accident prevention
- 3 kinds of provisions
  - **Accident management** includes preplanned and ad hoc operational practices to restore the plant to a safe state
  - **Engineered safety features** act to confine any radioactive material released from the core so that discharges to the environment would be minimal
  - **Off-site countermeasures** are available to compensate for the remote possibility that safety measures might fail

CONTENTS

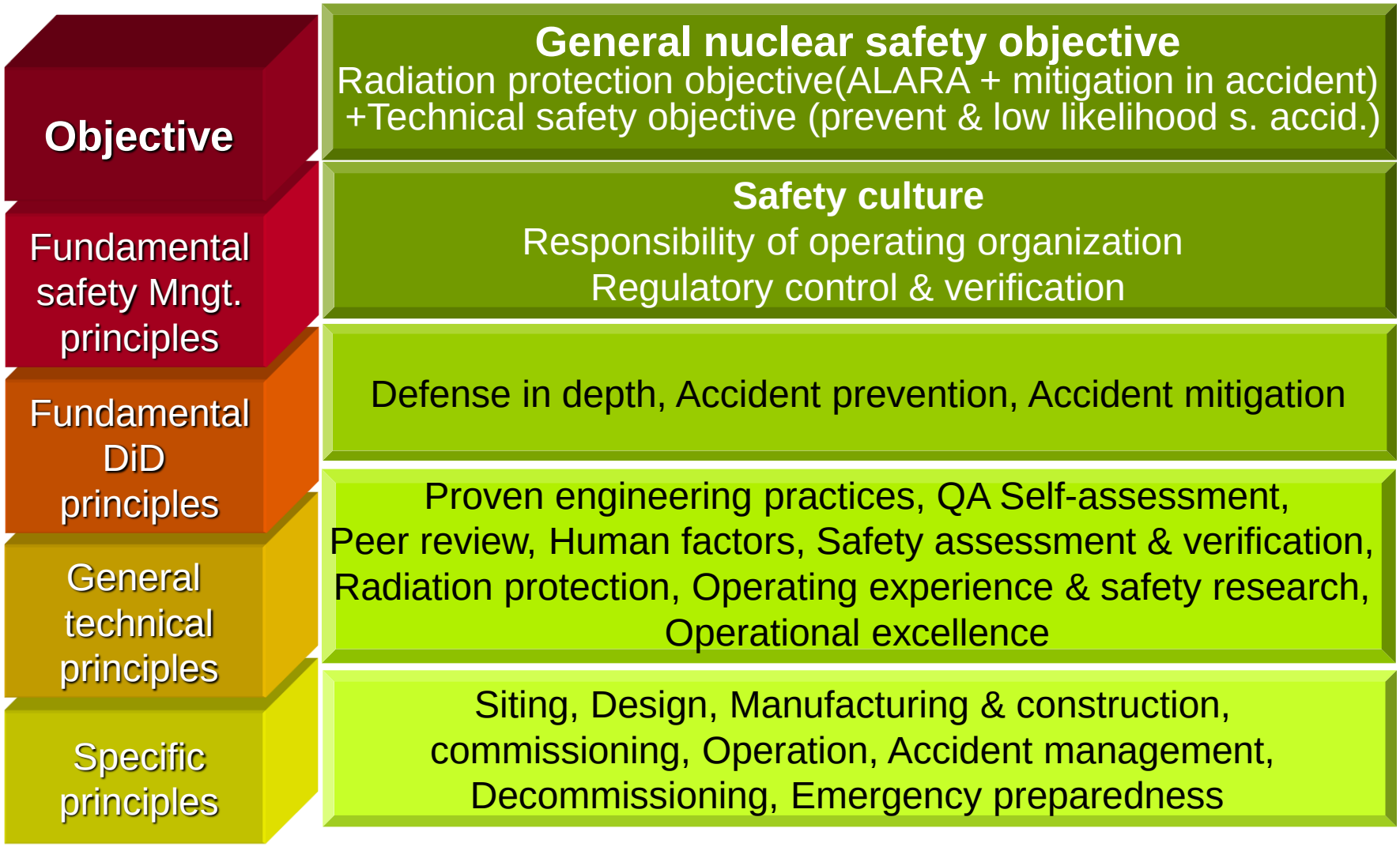
I. FUNDAMENTAL SAFETY PRINCIPLES (SF-1)

II. SAFETY OBJECTIVES AND FUNDAMENTAL PRINCIPLES (INSAG-12)

III. SAFETY TECHNICAL AND SPECIFIC PRINCIPLES (INSAG-12)

IV. REMARKS

Safety objectives and principles for NPP



1. General technical principles

① Proven engineering practices

Nuclear power technology is based on engineering practices that are proven by testing and experience, and which are reflected in approved codes and standards and other appropriately documented statements

- Codes and standards proven by research, past application, testing and dependable analysis
- New types of plants based on the experience from earlier operating plants, the results of research program, or the operation of prototypes
- Standardization can offer economic advantages by concentrating the resources of designers, regulators and manufacturers, but the risk of generic problems (vs. evolutionary improvements)

② Quality Assurance (QA)

QA is applied throughout activities at a NPP as part of a comprehensive system to ensure with high confidence that all items delivered and services and tasks performed meet specified requirements

- QA programmes provide a framework for the analysis of tasks, development of methods, establishment of standards, and identification of necessary skills and equipment
- QA practices cover: validation of designs; procurement; supply and use of materials; manufacturing, inspection and testing methods; and operational and other procedures to ensure that specifications are met
- Essential component of QA is the documentary verification: the completeness of tasks, identification and correction of deviations, and measures to prevent recurrence of errors

③ Self-assessment

Self-assessment for all important activities at a NPP ensures the involvement of personnel performing line functions in detecting problems concerning safety and performance and solving them

Self-assessments are used for:

- Single reviews in depth to find the basic causes of poor safety and performance
- Periodic reviews of specific activities or programmes by teams of experienced in-house personnel and outside technical experts
- Comparison of plant performance with existing management expectations and with best industry practices
- Frequent or continuous monitoring of activities at all levels of the entire organization

④ Peer reviews

Independent peer reviews provide access to practices and programmes employed at plants performing well and permit their adoption at other plants

- 'Peer reviews' are conducted by a team of independent experts with technical competence and experience in the areas of evaluation
- Judgements are based on the combined expertise of the team members
- Reviews comprise a comprehensive comparison of the practices applied by organizations with existing and internationally accepted good practices, and an exchange of expert judgements
- Reviews are aimed at increasing the effectiveness of practices and procedures of the organization being reviewed

⑤ Human factors

Personnel engaged in activities bearing on nuclear plant safety are trained and qualified to perform their duties.

The possibility of human error in NPP operation is taken into account by facilitating correct decisions by operators and inhibiting wrong decisions, and by providing means for detecting and correcting or compensating for error

- Twofold approach to reduce the human error component of events and accidents
  - Through the design (automation) and through improved human performance
- Human factor improvements
  - Plant hardware (ergonomic layout), plant procedures, training and other areas to help prevent or mitigate human error
  - Simplify the information reaching the operators for a clear understanding and control

✓ KINS simulator

⑥ Safety assessment and verification

Safety assessment is made before construction and operation of a plant begin.

The assessment is well documented and independently reviewed.

It is subsequently updated in the light of significant new safety information

- Safety assessment includes systematic critical review of the ways in which SSCs might fail, and identifies the consequences of such failures
- The assessment is undertaken expressly to reveal any underlying design weaknesses
- The results are documented in detail to allow independent audit of the scope, depth and conclusions of the critical review

⑦ Radiation protection

A system of radiation protection practices, consistent with recommendations of the ICRP and the IAEA, is followed in the design, commissioning, operational and decommissioning phases of NPPs

- Take measures to protect workers and the public against the harmful effects of radiation in normal operation, AOOs and accidents
- The system includes:
  - Control of the sources of radiation, including radioactive releases and waste
  - Provision and continued effectiveness of protective barriers and personal protective equipment
  - Provision of administrative means for controlling exposures

⑧ Operating experience and safety research

Organizations concerned ensure that operating experience and the results of research relevant to safety are exchanged, reviewed and analyzed, and that lessons are learned and acted on

- Develop a program to gather and use information specific to the plant safety to improve the plant performance
  - Reported plant events, errors, near misses, problems, observations, and suggestions for improvement
- Establish a process to track the various assessments and corresponding corrective actions and to determine unfavorable trends, including management involvement

⑨ Operational excellence

Operational excellence is achieved in present and future NPP operations by:

- *Augmenting safety culture and DiD*
- *Improving human performance*
- *Maintaining excellent material condition and equipment performance*
- *Using self-assessments and peer reviews*
- *Exchanging operating experience and other information around the world*
- *Increasing application of PSA*
- *Extending the implementation of severe accident management*

2. Specific principles

① Siting

□ External factors affecting the plant

The choice of site takes into account the results of investigations of local factors that could adversely affect the safety of the plant

- Natural factors
  - Geological and seismological characteristics, and the potential for hydrological and meteorological disturbances
- Human made hazards
  - Those arising from chemical installations, the release of toxic and flammable gases, and aircraft impact (e.g. 9/11)

□ Radiological impact on the public and the local environment

Sites are investigated from the standpoint of the radiological impact of the plant in normal operation and in accident conditions

- Pathways for the possible transport of radioactive material to humans
  - Air, food-chains and water supplies
- Site characteristics that can influence the pathways
  - Physical characteristics such as topography, meteorology and hydrology
  - Environmental characteristics such as type of vegetation and animal life
  - Use of land and water resources
  - Population distribution around the site

□ Feasibility of emergency plans

The site selected for a NPP is compatible with the offsite countermeasures that may be necessary to limit the effects of accidental releases of radioactive substances, and is expected to remain compatible with such measures

- Review the features of the site and its surroundings for the feasibility of emergency plan at the initial site review stage (e.g. Shoreham NPP)

□ Ultimate heat sink provisions

The site selected for a NPP has a reliable long term heat sink that can remove energy generated in the plant after shutdown, both immediately after shutdown and over the longer term

- Withstand any extreme events such as earthquakes, floods and tornadoes

② Design

□ Objective

- SSCs of the plant have the appropriate characteristics, specifications and material composition, and are combined and laid out to meet the plant performance specifications

□ Safety design objective

- Protect against the release and dispersal of radioactive materials

□ 3 fundamental functions in safety design

- Controlling reactor power
- Cooling the fuel
- Confining radioactive materials within the appropriate physical barriers

□ Design process

- Design management
  - *The assignment and subdivision of responsibility for safety are kept well defined throughout the design phase*
- Proven technology
  - *Technologies incorporated into design have been proven by experience and testing*
  - *Significant new design features or new reactor types are introduced only after thorough research and prototype testing*

✓ Balance between proven and innovation

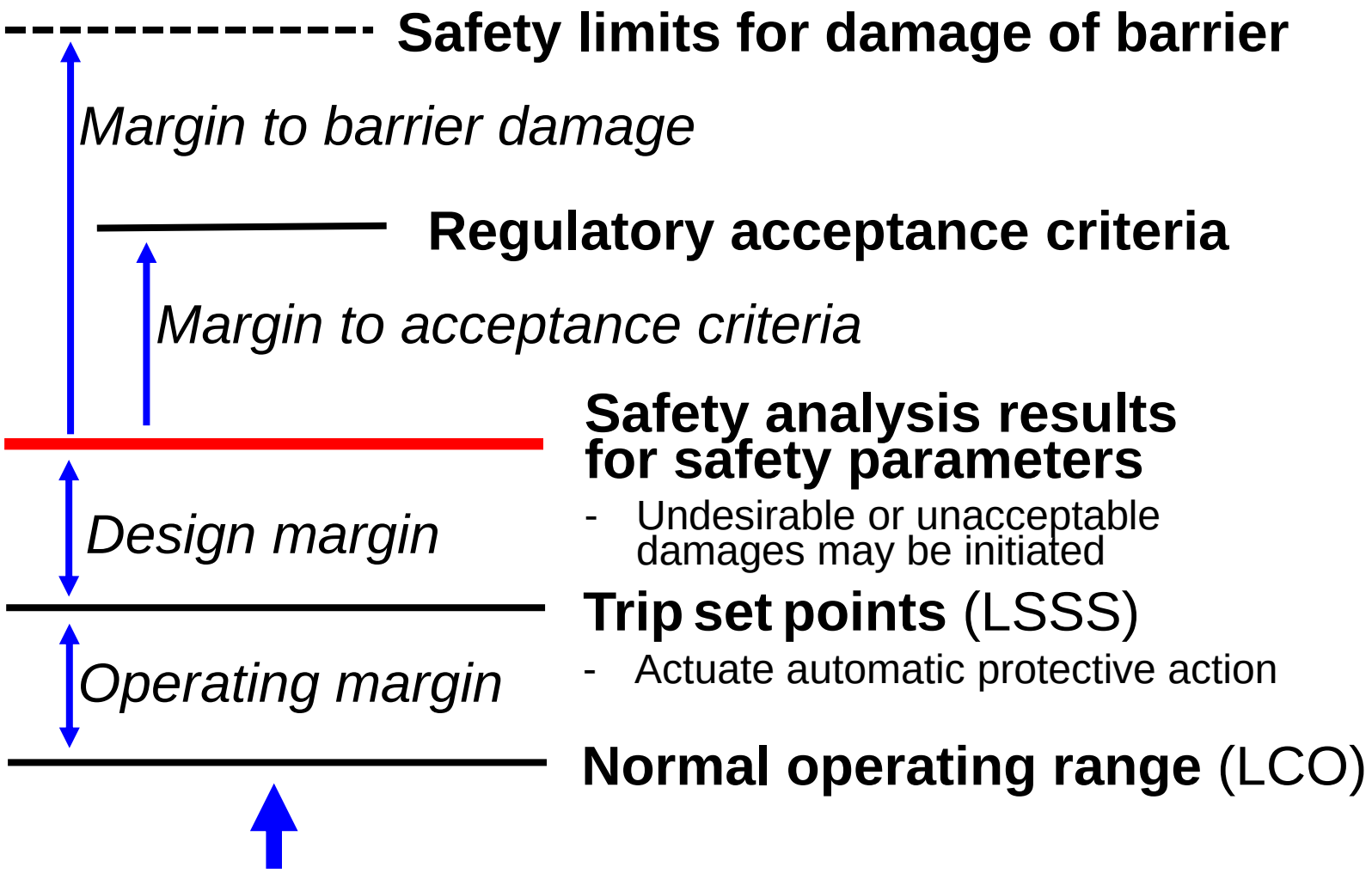
- Passive safety system: Independence from support systems, simplicity and reliability **vs.** lower driving heads in fluid system and reduced flexibility in abnormal condition

- General basis for design
  - *A nuclear power plant is designed to cope with a set of events including normal conditions, anticipated operational occurrences, extreme external events and accident conditions*
  - *For this purpose, conservative rules and criteria incorporating safety margins are used to establish design requirements*
  - *Comprehensive analyses are carried out to evaluate the safety performance or capability of the various components and systems in the plant*

□ **General features** affecting the design of NPP

- Plant process control systems
  - *Normal operation and AOOs are controlled so that plant and system variables remain within their operating ranges. This reduces the frequency of demands on safety systems*
    - Assign operating ranges, trip setpoints and safety limits for important plant neutronic and thermal-hydraulic variables
    - Safety limits are extreme values of the variables at which conservative analysis indicates that undesirable or unacceptable damage to the plant may be initiated
    - Trip set points are at less extreme values of the variables which would actuate an automatic plant protective action

✓ Safety criteria and margins



- Automatic safety systems
  - *Automatic systems are provided that would safely shut down the reactor, maintain it in a shut down and cooled state, and limit any release of fission products that might possibly ensue, if operating conditions were to exceed predetermined set points*
    - Cope with events that exceed the protective capabilities of normal plant control systems
    - Engineered safety features (ESFs) are incorporated to ensure that plant damage, *especially damage to the reactor core*, would be limited even in the most severe DBAs
    - Achieve the reliability of ESFs with the use of fail-safe design; protection against common cause failures; and independence between safety systems and plant process systems

- Reliability targets
  - *Reliability targets are assigned to safety systems or functions*
    - To ensure performance on demand and operation throughout the required duration of performance
  - *The targets are established on the basis of the safety objectives and are consistent with the roles of the systems or functions in different accident sequences*
  - *Provision is made for testing and inspection of components and systems for which reliability targets have been set*

- Dependent failures
  - *Design provisions seek to prevent the loss of safety functions due to damage to several SSCs resulting from a common cause*
    - Use the methods of physical separation by barriers or distance, protective barriers, redundancy linked with diversity and qualification to withstand the damage
- Equipment qualification
  - *Safety components and systems are chosen that are qualified for the environmental conditions that would prevail if they were required to function*
  - *The effects of ageing on normal and abnormal functioning are considered in design and qualification*

- Inspectability of safety equipment
  - *Safety related SSCs are designed and constructed so that they can be inspected throughout their operating lifetimes to verify their continued acceptability for service with an adequate safety margin*
    - Provision for in-service inspection access, and for the ease and frequency of inspection
- Radiation protection in design
  - *At the design stage, radiation protection features are incorporated to protect plant personnel from radiation exposure and to keep emissions of radioactive effluents within prescribed limits*
    - All plant components containing radioactive material are adequately shielded and radioactive material is suitably contained

□ **Specific features** for safety

- Protection against power transient accidents
  - *The reactor is designed so that reactivity induced accidents are protected against, with a conservative margin of safety*
    - Achieved by the combination of inherent feedback features (negative reactivity feedback), reactivity control systems and shutdown systems with a satisfactory margin (neutron absorber)
- Reactor core integrity
  - *The core is designed to have mechanical stability*
    - *Tolerate an appropriate range of anticipated variations in operational parameters*
    - *The expected core distortion or movement during an accident would not impair the effectiveness of the reactivity control or the safety shutdown systems or prevent cooling of the fuel*

- Automatic shutdown systems
  - *Rapidly responding and highly reliable reactivity reduction for safety purposes is designed to be independent of the equipment and processes used to control the reactor power (reactivity control sys.)*
  - *Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are being intentionally taken or whenever a chain reaction might be initiated accidentally*

✓ ATWS, Anticipated Transients Without **Scram**

- Failure of an automatic shut down system, causing an excessive increase in reactivity, an excessive primary circuit pressure, excessive fuel temperatures or some other potential cause of damage to the plant
- Demonstrate that the pressure boundary of the reactor coolant will not fail, the pressure suppression system will not fail, safe long term shutdown is reached and heat removal capacity is sufficient

- Normal heat removal
  - *Heat transport systems are designed for highly reliable heat removal in normal operation*
  - *They would also provide means for the removal of heat from the reactor core during anticipated operational occurrences and during most types of accidents that might occur*

- Startup, shutdown, and low power operation
  - *SSCs used during startup, low power and shutdown operations are designed to maintain or restore the reactivity control, decay heat removal, and the integrity of the fission product barriers, so as to prevent the release of radioactive material resulting from accidents*

- Emergency heat removal
  - *Provision is made for alternative means to restore and maintain fuel cooling under accident conditions, even if normal heat removal fails or the integrity of the primary cooling system boundary is lost*
    - Residual heat removal systems and emergency core cooling systems
    - Emergency feedwater systems to ensure the capability of heat removal on the secondary side

- Reactor coolant system integrity
  - *Codes and standards for nuclear vessels and piping are supplemented by additional measures to prevent conditions arising that could lead to a rupture of the primary coolant system boundary at any time during the plant lifetime*
    - Require careful attention to design, materials, fabrication, installation, inspection and testing
    - Analysis to demonstrate structural integrity under the extreme load conditions expected,
    - Multiple inspections of ultrasonic, radiographic and surface methods, and
    - Hydraulic pressure test

- Confinement of radioactive material
  - *The plant is designed to be capable of retaining the bulk of the radioactive material that might be released from fuel, for the entire range of accidents considered in the design*
- Protection of confinement structure
  - *If specific and inherent features of a NPP would not prevent detrimental effects on the confinement structure in a severe accident, special protection against the effects of such accidents is provided, to the extent needed to meet the general safety objective*
    - Containment structure is designed to withstand the internal pressure resulting from DBA
    - Hydrogen igniter, autocatalytic recombiner, filtered vent and area spray system, fuel debris retainer

- Monitoring of plant safety status
  - *Parameters to be monitored in the control room are selected, and*
  - *Their displays are arranged to ensure that operators have clear and unambiguous indications of the status of plant conditions important for safety,*
  - *Especially for the purpose of identifying and diagnosing the automatic actuation and operation of a safety system or the degradation of DiD*

- Preservation of control capability
  - *The control room is designed to remain habitable under normal operation, AOOs and DBAs*
  - *Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control room for circumstances in which main control room may be uninhabitable or damaged* (e.g. remote shutdown panel)
- Station blackout
  - *NPPs are so designed that the simultaneous loss of on- and off-site AC power (a station blackout, dominant component of the total risk) will not soon lead to fuel damage*
    - Backup power supplies of direct drive DG, direct drive steam turbines and batteries for instruments, and other DC components (AAC, mobile DG)

- Control of accidents within the design basis
  - *Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents*
    - Provided with appropriate safety equipment, instrumentation and operating procedures for response to and control of accidents
    - Designed to restore normal conditions with the feedback characteristics of neutronic and process controls, shutdown, continued cooling and protection against the release of radioactive materials, and automatic actuation of ESFs

- New and spent fuel storage
  - *Plant designs provide for the handling and storage of new and spent fuel in such a way as to ensure protection of workers and to prevent the release of radioactive material*

- Plant physical protection
  - *The design and operation of a NPP provide adequate measures to protect the plant from damage and to prevent the unauthorized release of radioactive material arising from unauthorized acts by individuals or groups, including trespass, unauthorized diversion or removal of nuclear materials, and sabotage of the plant*

③ Manufacturing and construction

□ Safety evaluation of design

- *Construction of a NPP is begun only after the operating organization and the regulatory organization have satisfied themselves by appropriate assessments*:
  - The main safety issues have been satisfactorily resolved
  - The remainder are amenable to solution before operations are scheduled to begin

□ Achievement of quality

- *The plant manufacturers and constructors discharge their responsibilities for the provision of equipment and construction of high quality by using well proven and established techniques and procedures supported by quality assurance practices*

④ Commissioning

□ Verification of design and construction

- *The commissioning programme is established and followed to demonstrate that the entire plant, especially items important to safety and radiation protection, has been constructed and functions according to the design intent, and to ensure that weaknesses are detected and corrected*

□ Validation of operating and functional test procedures

- *Procedures for normal plant and systems operation and for functional tests to be performed during the operating phase are validated as part of the commissioning programme*

□ Collecting baseline data

- *During commissioning tests, detailed diagnostic data are collected on components having special safety significance and the initial operating parameters of the systems are recorded*

□ Pre-operational plant adjustments

- *During the commissioning programme, the as-built operating characteristics of safety and process systems are determined and documented*
- *Operating points are adjusted to conform to design values and to safety analyses*
- *Training procedures and limiting conditions for operation are modified to reflect accurately the operating characteristics of the systems as built*

⑤ Operation

□ Organization, responsibilities and staffing

- *The utility exerts full responsibility for the safe operation of a NPP through a strong organizational structure under the line authority of the plant manager*
- *The plant manager ensures that all elements for safe plant operation are in place, including an adequate number of qualified and experienced personnel*

□ Safety review procedures

- *Safety review procedures are maintained by the utility to provide a continuing surveillance and audit of plant operational safety and to support the plant manager in the overall safety responsibilities*
  - Safety review independent of the pressures of plant operation

□ Conduct of operations

- *Operation of the plant is conducted by authorized personnel, according to strict administrative controls and observing procedural discipline*

□ Training

- *Programmes are established for training and retraining operations and maintenance, technical support, chemistry and radiation protection personnel to enable them to perform their duties safely and efficiently*
- *Training is particularly intensive for control room staff, and includes the use of plant simulators*

□ Operational limits and conditions

- *A set of operational limits and conditions is defined to identify safe boundaries for plant operation*
- *Minimum requirements are also set for the availability of staff and equipment*

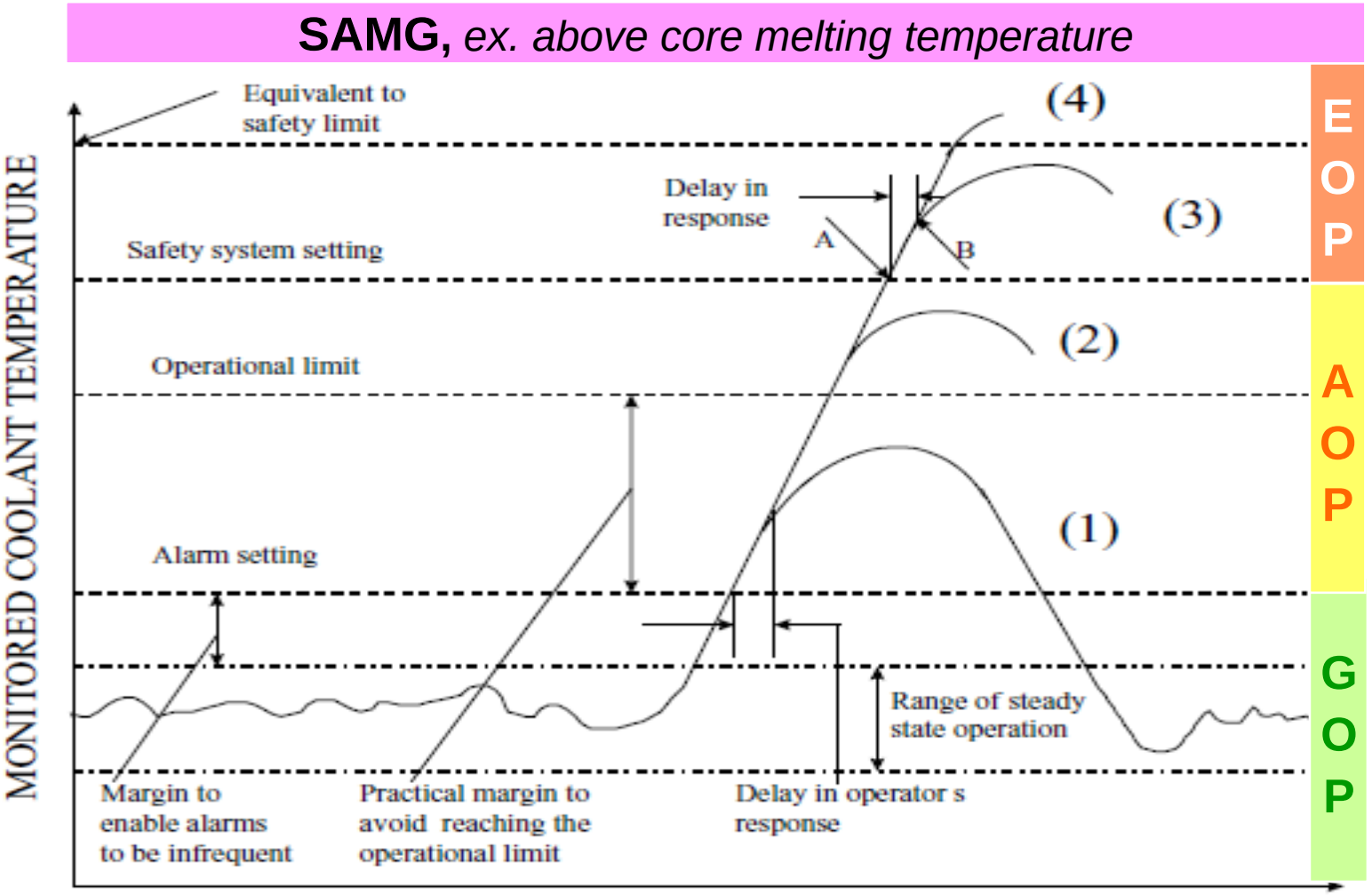
□ Normal operating procedures

- *Normal plant operation is controlled by detailed, validated and formally approved procedures*

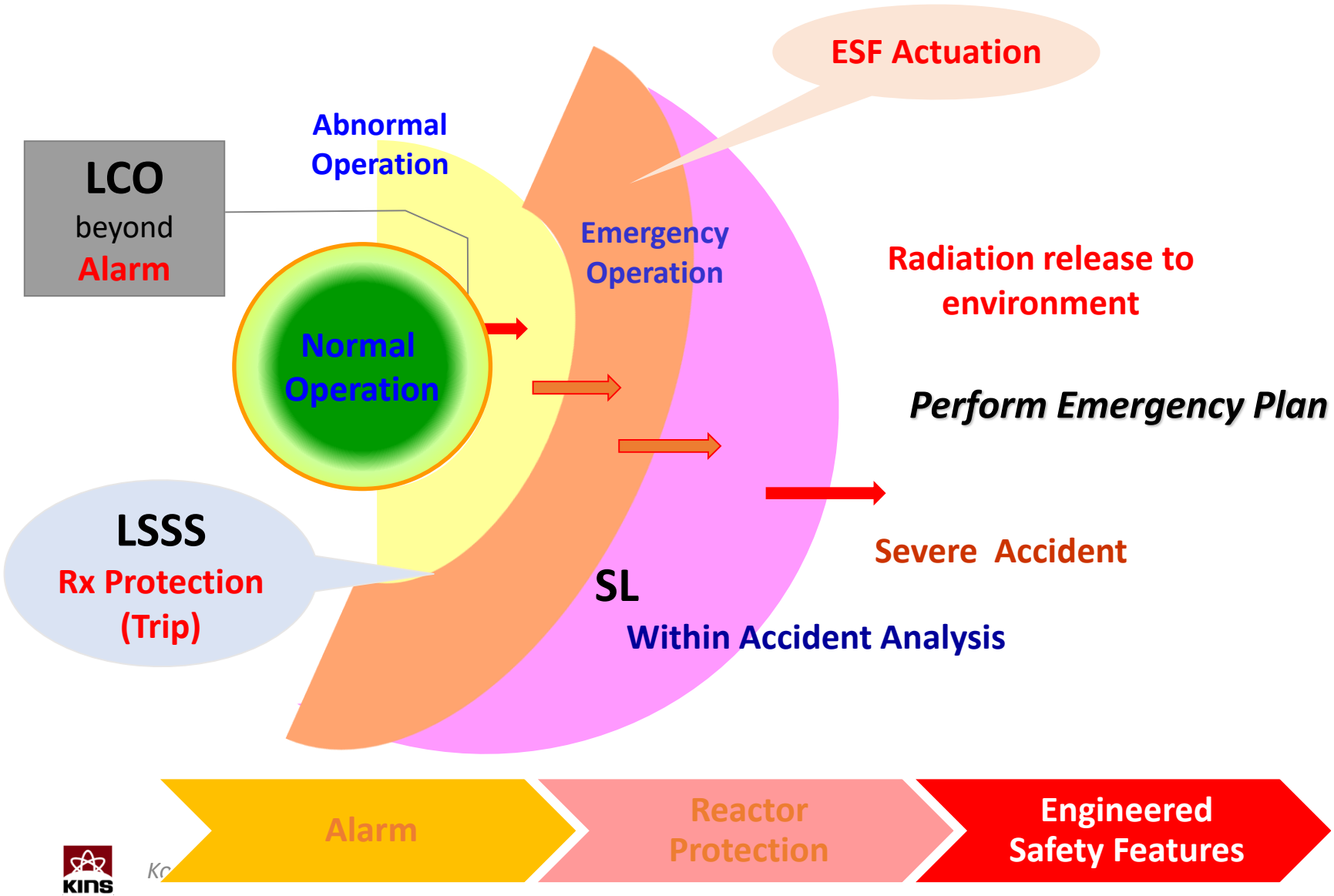
□ Emergency operating procedures

- *Emergency operating procedures are established, documented and approved to provide a basis for suitable operator response to abnormal events*

- SL, LSSS, OL, and alarm setting & operation range



□ Operational concept and space



□ Radiation protection procedures

- *The radiation protection staff of the operating organization establish written procedures for the control, guidance and protection of personnel, carry out routine monitoring of in-plant radiological conditions, monitor the exposure of plant personnel to radiation, and also monitor releases of radioactive effluents*

□ Engineering and technical support of operations

- *Engineering and technical support, competent in all disciplines important for safety, is available throughout the lifetime of the plant*

□ Feedback of operating experience

- *Plant management institutes measures to ensure that events significant for safety are detected and evaluated in depth, and that any necessary corrective measures are taken promptly and information on them is disseminated*
- *The plant management has access to operational experience relevant to plant safety from other NPPs around the world*

□ Maintenance, testing and inspection

- *Safety related SSCs are the subject of regular preventive and predictive maintenance, inspection, testing and servicing when needed, to ensure that they remain capable of meeting their design requirements throughout the lifetime of the plant*
- *Such activities are carried out in accordance with written procedures supported by quality assurance measures*

□ Quality assurance in operation

- *An operational QA programme is established by the utility to assist in ensuring satisfactory performance in all plant activities important to plant safety*

⑥ Accident management

□ Strategy for accident management

- *The analysis results of plant response to potential accidents beyond the design basis are used in preparing guidance on an accident management strategy*

□ Training & procedures for accident management

- *Nuclear plant staff are trained and retrained in the procedures to follow if an accident occurs that exceeds the design basis of the plant*

□ Engineered features for accident management

- *Equipment, instrumentation and diagnostic aids are available to operators, who may at some time be faced with the need to control the course and consequences of an accident beyond the design basis* (e.g. hardened core of EU)

⑦ Decommissioning

- *Consideration is given in design and plant operations to facilitating eventual decommissioning and waste management*
- *After the end of operations and the removal of spent fuel from the plant, radiation hazards are managed so as to protect the health of workers and the public during plant decommissioning*

⑧ Emergency preparedness

□ Emergency plans

- *Emergency plans are prepared before the startup of the plant, and are exercised periodically to ensure that protection measures can be implemented in the event of an accident which results in, or has the potential for, significant releases of radioactive materials within and beyond the site boundary*
- *Emergency planning zones defined around the plant allow for the use of a graded response*

□ Emergency response facilities

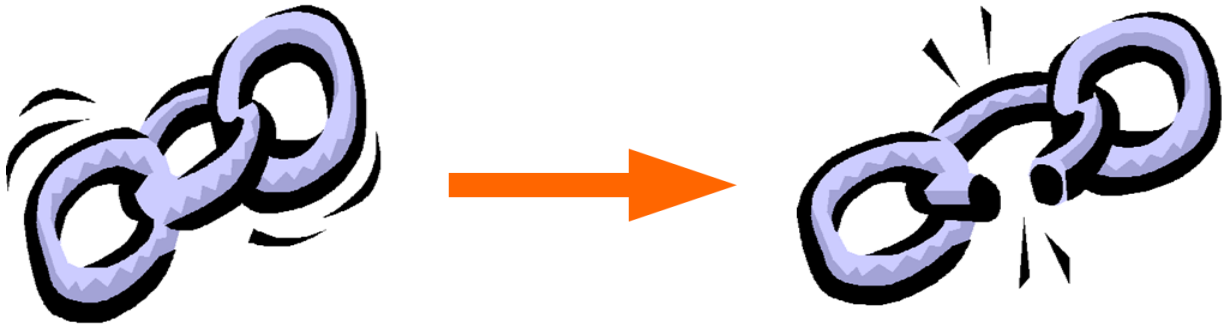
- *A permanently equipped emergency center is available off the site for emergency response*
- *On the site, a similar center is provided for directing emergency activities within the plant and communicating with the off-site emergency organization*

□ Assessment of accident consequences and radiological monitoring

- *Means are available to the responsible site staff to be used in early prediction of the extent and significance of any release of radioactive materials if an accident were to occur*
  - For rapid and continuous assessment of the radiological situation
  - For determining the need for protective measures

CONTENTS

Safety is a relative concept



A chain is strong as its weakest link

How to secure safety?

The devil is in the details

Safety First KINS,
trusted by the public

Thank You

한국원자력안전기술원
KINS KOREA INSTITUTE OF NUCLEAR SAFETY