International Atomic Energy Agency

Basic Principles of Nuclear Safety

L.W. Deitrich

IAEA Consultant

(deirichlw@earthlink.net)

Contents

- Safety-related Characteristics of Nuclear Reactors
- Nuclear Safety Objectives
- Safety Fundamentals: The Safety of Nuclear Installations
- Defence-in-Depth

Safety-Related Characteristics of Nuclear Reactors

Safety-related Characteristics of Nuclear Reactors

- **Unique Characteristics:**
  - **A very large quantity of radioactive material is present in the core of a nuclear reactor after any significant period of power operation;**
  - **Significant energy release continues for a very long time after shutdown;**
  - **A reactor has no 'natural' or 'intrinsic' power level, and rapid power excursions are possible.**

- **Basic Safety Functions:**
  - **Confinement of radioactive materials, control of operational discharges, and limitation of accidental releases;**
  - **Removal of residual heat from the core;**
  - **Control of the reactivity.**

Radioactive Materials Inventory

- The radioactive inventory in a reactor comes from:
  - Fission products;
  - Activation products; and
  - Transuranics.
- Fission products are the largest radioactive component. Most fission products are retained in the fuel. Decay of fission products is the principal source of radiation hazard for times of several hundred years, and decay heat from reactor fuel for times up to about 60 years.

Radioactive Materials Inventory

- Some fission products emit delayed neutrons, which are extremely important in reactor kinetics and control.
- Activation products arise from neutron absorption in structural materials or in fission products.
  - Activation of stainless steel, Inconel and Zircaloy is a major contributor.
  - Neutron absorption in fission products is important in reactor operations due to large cross sections of Xe-135 (2E6 barns) and Sm-149 (6E4 barns).

Radioactive Materials Inventory

- **Transuranics arise from non-fissile capture of neutrons in fuel and fertile materials, primarily U-235 and U-238. Plutonium, Americium and Curium are the elements of principal interest.**
- **Most transuranics are alpha-emitters with long half-lives. They are a significant contributor to the radioactive hazard at times longer than a few hundred years and to the decay heat at times longer than about 60 years.**

Radioactive Materials Inventory

- **The radioactive material inventory depends on:**
  - **Reactor power and operating history;**
  - **Neutron flux and energy distribution;**
  - **Fission product yields and decay schemes;**
  - **Neutron cross-sections for important nuclides and reactions.**
- **The concentration of various fission products will reach saturation in a few half-lives of operation.**

Fission Product Decay Heat

- Radioactive fission products release energy in decay to a stable state.
- The decay heat depends on:
  - The fuel and fertile materials;
  - The time of irradiation and the power density;
  - The time after shutdown;
  - The reactor neutron spectrum.
- Since fission products are retained within the cladding, cooling must be sufficient to guard against cladding degradation or failure.

Fission Product Decay Heat
Long Time Operation, LWR, Uranium Fuel

Time after reactor shutdown:	Fraction of operating power:
1 second	17%
1 minute	5 %
1 hour	1.5 %
1 day	0.5%
1 week	0.3%
1 month	0.15%
1 year	0.03%
10 years	0.003%

Fission Product Decay Heat

- A standard for calculation of decay heat is available:
  - ANSI/ANS-5.1 – 2005, “Decay Heat Power in Light Water Reactors.”
  - Supersedes ANSI/ANS-5.1 – 1994.

Fission Product Decay Heat
Fuel Cooling Considerations

- **Adequate cooling must be maintained at all times to remove decay heat and prevent cladding failure in the reactor or in spent fuel storage.**
- **Decay heat is the thermal driving force in most accidents in LWRs.**
- **Water is an excellent heat sink. However, water quality must be maintained to guard against corrosion.**

Reactivity Control Requirements

- Control the reactor power level in operation and provide for shutdown under normal and off-normal conditions.
- Compensate for reactivity changes due to core configuration, experiments, burnup, or temperature changes.
- Compensate for transient poisoning effects, primarily from Xe and Sm.
- Provide for rapid shutdown if necessary, and maintain the reactor subcritical, including in accident conditions.

Reactivity Control

- **Some typical reactivity control mechanisms include:**
  - **Moveable control rods or blades.**
  - **Control drums at the edge of the core.**
  - **Moveable fuel.**
  - **Chemical means, such as boric acid in coolant.**
  - **Burnable poisons, such as Gadolinium.**
  - **Removable poison plates or curtains.**

Reactivity Control

- **Some typical reactivity feedback mechanisms include:**
  - **Fuel temperature – a prompt effect, which must be negative;**
  - **Doppler broadening of resonance absorption in U-238 or other materials – a prompt effect;**
  - **Moderator temperature – normally subject to heat transfer delay;**
  - **Coolant void formation – can be positive or negative.**

Fundamental Safety Principles

Principal Reference Documents

- **Draft Safety Fundamentals: Fundamental Safety Principles, Draft Safety Standard DS298 (June 2006).**
- **Safety Fundamentals: The Safety of Nuclear Installations, IAEA Safety Series No. 110 (1993).**
- **Defence in Depth in Nuclear Safety, INSAG-10 (1996).**
- **Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3, Rev.1, INSAG-12 (1999).**

Safety Objective

- **The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.**

Safety Objective (cont'd.)

- **Measures must be taken to:**
  - **Control the radiation exposure of people and the release of radioactive material to the environment;**
  - **Restrict the likelihood of events that might lead to loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;**
  - **Mitigate the consequences of such events if they were to occur.**

Safety Principle 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.**
  - **This prime responsibility cannot be delegated.**

Safety Principle 1
Responsibility for Safety

- **The responsible party must:**
  - **Establish and maintain the necessary competencies and provide adequate training and information;**
  - **Establish procedures and arrangements to maintain safety at all times;**
  - **Verify design and quality of facilities, activities and equipment;**
  - **Ensure control of radioactive material and waste.**

Safety Principle 2
Role of Government

- **An effective legal and governmental framework for safety, including an independent regulatory body, must be established and maintained.**
  - **Government authorities must prepare programs to reduce radiation risks, including in emergencies, monitor releases and for disposal of radioactive waste.**
  - **They must provide for control over sources for which no one else has responsibility.**

Safety Principle 2
Role of Government

- **The regulatory body must:**
  - **Have adequate legal authority, competence and resources to fulfill its responsibilities;**
  - **Be effectively independent;**
  - **Set up appropriate means of providing information about safety, health and environmental aspects of facilities and activities, and about regulatory processes.**
  - **Consult, as appropriate, in an open and inclusive process.**

Safety Principle 2
Role of Government

- **Comments:**
  - **The regulatory body must have the statutory authority, competence and resources to:**
    - **Set safety standards;**
    - **License and inspect installations;**
    - **Set, monitor and enforce license conditions; and**
    - **Ensure that corrective actions are taken whenever unsafe or potentially unsafe conditions are detected.**
  - **Although the operating organization may delegate authority to carry out functions on its behalf, it cannot delegate the prime responsibility for safety.**

Safety Principle 3
Leadership and Management for Safety

- **Effective leadership and management for safety must be established and sustained in organizations concerned with, and facilities and activities that give rise to, radiation risks.**
  - **Leadership in safety must be demonstrated at the highest levels in an organization.**
  - **Safety must be achieved and maintained by an effective management system that integrates all requirements so that safety is not compromised by other demands.**
  - **The management system must promote a strong safety culture.**

Safety Principle 3
Leadership and Management for Safety

- **Comments:**
  - **The principles of safety management apply broadly to all organizations having safety responsibilities.**
  - **Management must create an atmosphere of rigor and thoroughness throughout the operating organization to ensure that all safety objectives are met. There can be no complacency about safety matters. There must be a learning attitude and an open exchange of information both upwards and downwards.**
  - **Quality must be verified with a disciplined approach, but the basic responsibility for quality rests with the performer, not the verifier.**

Safety Principle 4
Justification of Facilities and Activities

- **Facilities and activities that give rise to radiation risks must yield an overall benefit.**
  - **For facilities or activities to be justified, the benefits that they yield must outweigh the risks to which they give rise.**

Safety Principle 5
Optimization of Protection

- **Protection must be optimized to provide the highest level of safety that can reasonably be achieved.**
  - **Optimization: Achieving the highest reasonable level of safety without unduly limiting utilization.**
  - **Risks must be periodically reassessed.**
  - **Resources devoted to safety must be commensurate with the magnitude of the risk and the possibility of control.**

Safety Principle 6
Limitation of Risks to Individuals

- **Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.**
  - **Justification and optimization do not guarantee that no individual bears an unacceptable risk of harm. Doses and radiation risks must be controlled within specific limits.**
  - **Optimization and limitation of individual doses and risks are both necessary to achieve the desired level of safety.**

Safety Principle 7
Protection of Present and Future Generations

- **People and the environment, present and future, must be protected against radiation risks.**
  - **Safety standards apply to local and remote populations.**
  - **Future generations must be protected without any need for them to take significant protective measures.**
  - **Radioactive waste must be managed to avoid an undue burden on future generations.**

Safety Principle 8
Prevention of Accidents

- **All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.**
  - **Prevent occurrence of failures, abnormal conditions (including breach of security) that could lead to loss of control.**
  - **Prevent escalation of any such failures or abnormal conditions that do occur.**
  - **Prevent loss of control over any source of radiation.**
  - **The primary means of preventing and mitigation the consequences of accidents is defense-in-depth.**

Safety Principle 9
Emergency Preparedness and Response

- **Arrangements must be made for emergency preparedness and response in case of nuclear or radiation incidents.**
  - **Ensure that arrangements are in place for an effective response at the scene, and as appropriate, at the local, regional, national and international levels.**
  - **Ensure that radiation risks are minor for reasonably foreseeable incidents.**
  - **Prepare practical measures to mitigate any consequences to human life or health or the environment.**

Safety Principle 9
Emergency Preparedness and Response

- **Emergency preparedness and response involves the operating organization, regulatory body, and appropriate branches of government at the local, regional and national, and possibly international levels.**
- **Emergency plans must include criteria for different protective actions, and provide for the capability to protect and inform people at the scene and the public.**
- **Emergency plans must be exercised periodically.**

Safety Principle 10
Protective Actions to Reduce Existing or Unregulated Radiation Risks

- **Protective actions to reduce existing or unregulated radiation risks must be justified and optimized.**
  - **Mitigation of radiation of essentially natural origin.**
  - **Exposure arising from past human activities never subject to regulatory control, such as residue from mining operations.**
  - **Remediation measures following an uncontrolled release of radionuclides to the environment.**

Safety Fundamentals:
The Safety of Nuclear Installations

Definitions

- **Nuclear safety: The 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.**
  - **Safety is primarily concerned with maintaining control over sources of radiation.**
  - **Protection is primarily concerned with controlling exposure to radiation and its effects.**

Nuclear Safety Objectives

General Nuclear Safety Objective:

- To protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defences against radiological hazards.

Radiation Protection Objective:

- To ensure that in all operational states radiation exposure within the installation or due to any planned release of radioactive material from the installation is kept below prescribed limits and as low as reasonably achievable, and to ensure mitigation of the radiological consequences of any accidents.

Nuclear Safety Objectives

Technical Safety Objective:

- To take all reasonably practicable measures to prevent accidents in nuclear installations and to mitigate their consequences should they occur;
- To ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and
- To ensure that the likelihood of accidents with serious radiological consequences is extremely low.

Nuclear Safety Objectives

Comments:

- **Nuclear installations must be designed and operated to keep all sources of radiation under strict technical and administrative control.**
- **Limited exposures of people and release of legally authorized quantities of radioactive materials are not precluded, but must be strictly controlled and in compliance with operational limits and radiation protection standards.**
- **Measures must be taken to control operational exposures to ALARA levels and minimize the likelihood of loss of normal control of the sources of radiation.**

Nuclear Safety Objectives

Comments:

- **Accidents can happen.**
- **Measures to mitigate accident consequences are required.**
- **Such measures may include on-site accident management procedures, and off-site intervention measures.**
- **The greater the potential hazard from an uncontrolled radioactive release, the lower its likelihood must be.**

Technical Aspects of Safety - Siting

- ***The site selection shall take into account relevant features that might affect the safety of the installation, or be affected by the installation, and the feasibility of carrying out emergency plans. All aspects shall be evaluated for the projected lifetime of the installation and re-evaluated as necessary to ensure the continued acceptability for safety of site-related factors.***

Technical Aspects of Safety
Design and Construction

- ***The design shall ensure that the nuclear installation is suited for reliable, stable and easily manageable operation. The prime goal shall be the prevention of accidents.***
- ***The design shall include the appropriate application of the defence-in-depth principle so that there are several levels of protection and multiple barriers to prevent releases of radioactive materials, and to ensure that failures or combinations of failures that might lead to significant radiological consequences are of very low probability.***

Technical Aspects of Safety Design and Construction

- ***Technologies incorporated in a design shall be proven or qualified by experience or testing or both.***
- ***The systematic consideration of the man-machine interface and human factors shall be included in all stages of design and in the associated development of operational requirements.***
- ***The exposure to radiation of site personnel and releases of radioactive materials to the environment shall be made by design as low as reasonably achievable.***

Technical Aspects of Safety Design and Construction

- ***A comprehensive safety assessment and independent verification shall be carried out to confirm that the design of the installation will fulfil the safety objectives and requirements, before the operating organization completes its submission to the regulatory body.***

Technical Aspects of Safety
Design and Construction

Comments:

- **Design and operation must ensure:**
  - **Limitation of radiation exposures, radioactive releases and production of radioactive wastes;**
  - **Prevention of accidents;**
  - **Limitation and mitigation of the consequences of accidents if they do occur.**

Technical Aspects of Safety Design and Construction

Comments:

- The design must provide:
  - SSCs with high reliability;
  - Proven technology, meeting conservative criteria with appropriate safety margins;
  - Appropriate engineered and inherent safety features;
  - Consideration of minimizing personnel exposures.

Technical Aspects of Safety Design and Construction

Comments:

- **Design principles:**
  - **No single equipment failure or human action should disable a safety function;**
  - **The possibility of common cause failure should be minimized by diversity of equipment;**
  - **Redundant systems should function independently;**
  - **Fail-safe design concepts should be used.**

Technical Aspects of Safety Design and Construction

Comments:

- Minimize likelihood and impact of human error by including:
  - Engineered systems;
  - Automatic control, protection and alarm systems;
  - Elimination of human actions that could jeopardize safety;
  - Clear presentation of data and reliable communications.

Technical Aspects of Safety Commissioning

- ***Specific approval by the regulatory body shall be required before the start of normal operation on the basis of an appropriate safety analysis and a commissioning program. The commissioning program shall provide evidence that the installation as constructed is consistent with design and safety requirements. Operating procedures shall be validated to the extent practicable as part of the commissioning program, with the participation of the future operating staff.***

Technical Aspects of Safety Operation and Maintenance

- ***A set of operational limits and conditions derived from the safety analysis, tests and subsequent operational experience shall be defined to identify safe boundaries for operation. The safety analysis, operating limits and procedures shall be revised as necessary if the installation is modified.***
- ***Operation, inspection, testing and maintenance and supporting functions shall be conducted by sufficient numbers of adequately trained and authorized personnel in accordance with approved procedures.***

Technical Aspects of Safety Operation and Maintenance

- ***Engineering and technical support, with competence in all disciplines important for safety, shall be available throughout the lifetime of the installation.***
- ***The operating organization shall establish documented and approved procedures as a basis for operator response to anticipated operational occurrences and accidents.***
- ***The operating organization shall report incidents significant to safety to the regulatory body. The OO and the RB shall establish complementary programs to analyse operating experience to ensure that lessons are learned and acted upon. Such experience shall be shared with relevant national and international bodies.***

Technical Aspects of Safety
Radioactive Waste Management and Decommissioning

- ***The generation of radioactive waste, in terms of both activity and volume, shall be kept to the minimum practicable by appropriate design measures and operating procedures. Waste treatment and interim storage shall be strictly controlled in a manner consistent with the requirements for safe final disposal.***
- ***The design of an installation and the decommissioning program shall take into account the need to limit exposures during decommissioning to ALARA. Prior to initiation of decommissioning activities, the decommissioning program shall be approved by the regulatory body.***

Verification of Safety

- ***The operating organization shall verify by analysis, surveillance, testing and inspection that the physical state of the installation and its operation continue in accordance with operational limits and conditions, safety requirements and the safety analysis.***
- ***Systematic safety reassessments of the installation in accordance with the regulatory requirements shall be performed throughout its operational lifetime, with account taken of operating experience and significant new safety information from all relevant sources.***

Defence-in-Depth

Defense-in-Depth

- Several Levels of Protection
  - Including successive barriers preventing the release of radioactive material to the environment.

- Defense-in-depth is the key concept on which all of nuclear safety is based.
- The independence of different levels of defense is a key element.

Defense-in-Depth (Cont'd)

- **Objectives of Defense-in-Depth**
  - **To compensate for potential human and component failures,**
  - **To maintain the effectiveness of the barriers by averting damage to the facilities and to the barriers themselves, and**
  - **To protect the public and the environment from harm in the event that these barriers are not fully effective.**

Defense-in-Depth (Cont'd)

- **Strategy of Defense-in-Depth**
  - **To prevent accidents:**
    - **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.**
  - **To mitigate the consequences of accidents:**
    - **In-plant and off-site mitigation measures are available and are prepared that would substantially reduce the effects of an accidental release of radioactive material.**

Defense-in-depth is generally structured in five levels.

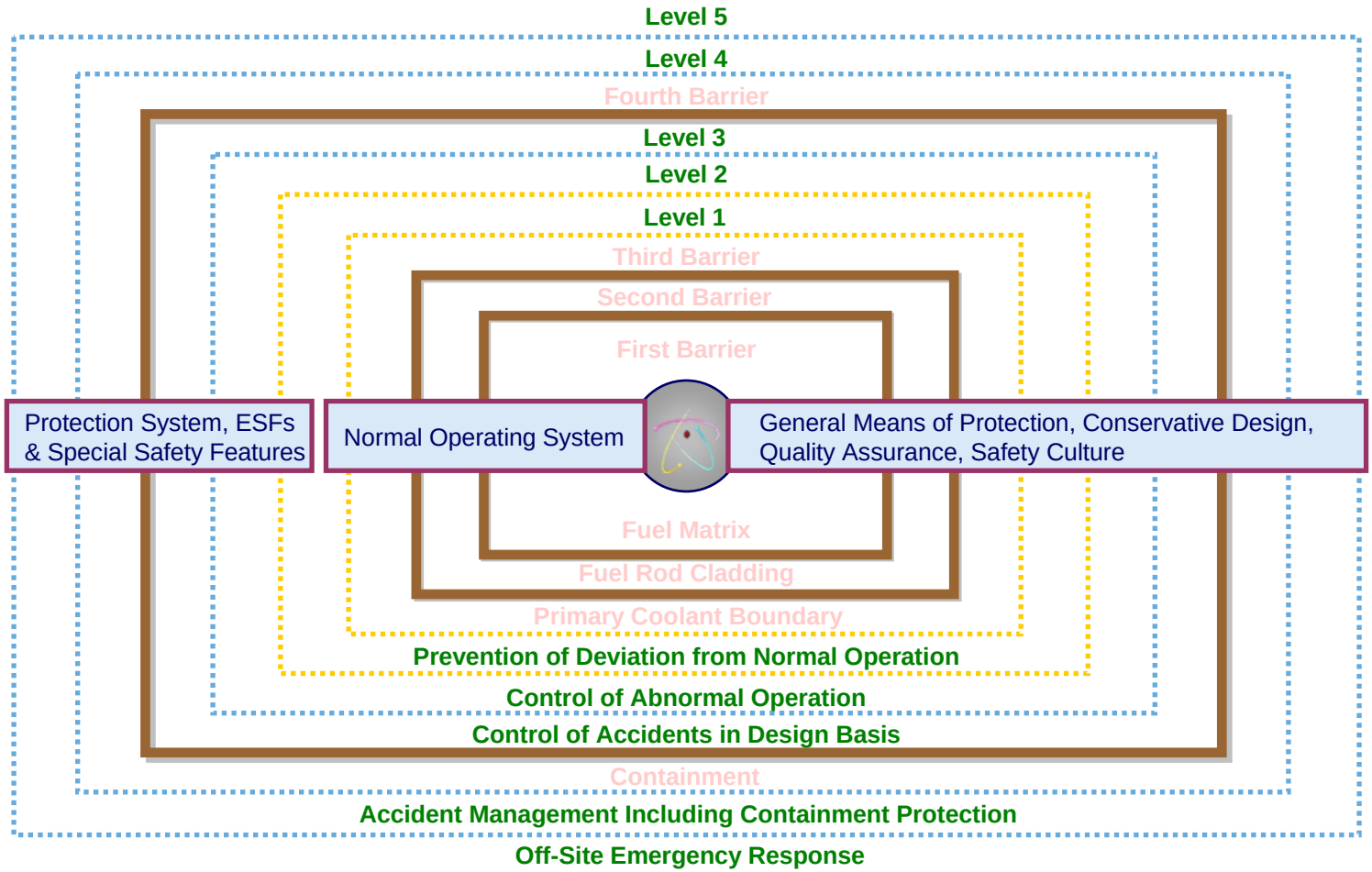
Levels of Defense-in-Depth

Level 1	**Objective**	Prevention of abnormal operation and failures
	Means	**Conservative design and high quality in construction and operation**
Level 2	**Objective**	Control of abnormal operation and detection of failures
	Means	**Control, limiting and protection system and other surveillance features**
Level 3	**Objective**	Control of accidents within the design basis
	Means	**Engineered safety features and accident procedures**
Level 4	**Objective**	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents
	Means	**Complementary measures and accident management**
Level 5	**Objective**	Mitigation of radiological consequences of significant releases of radioactive materials
	Means	**Off-site emergency response**

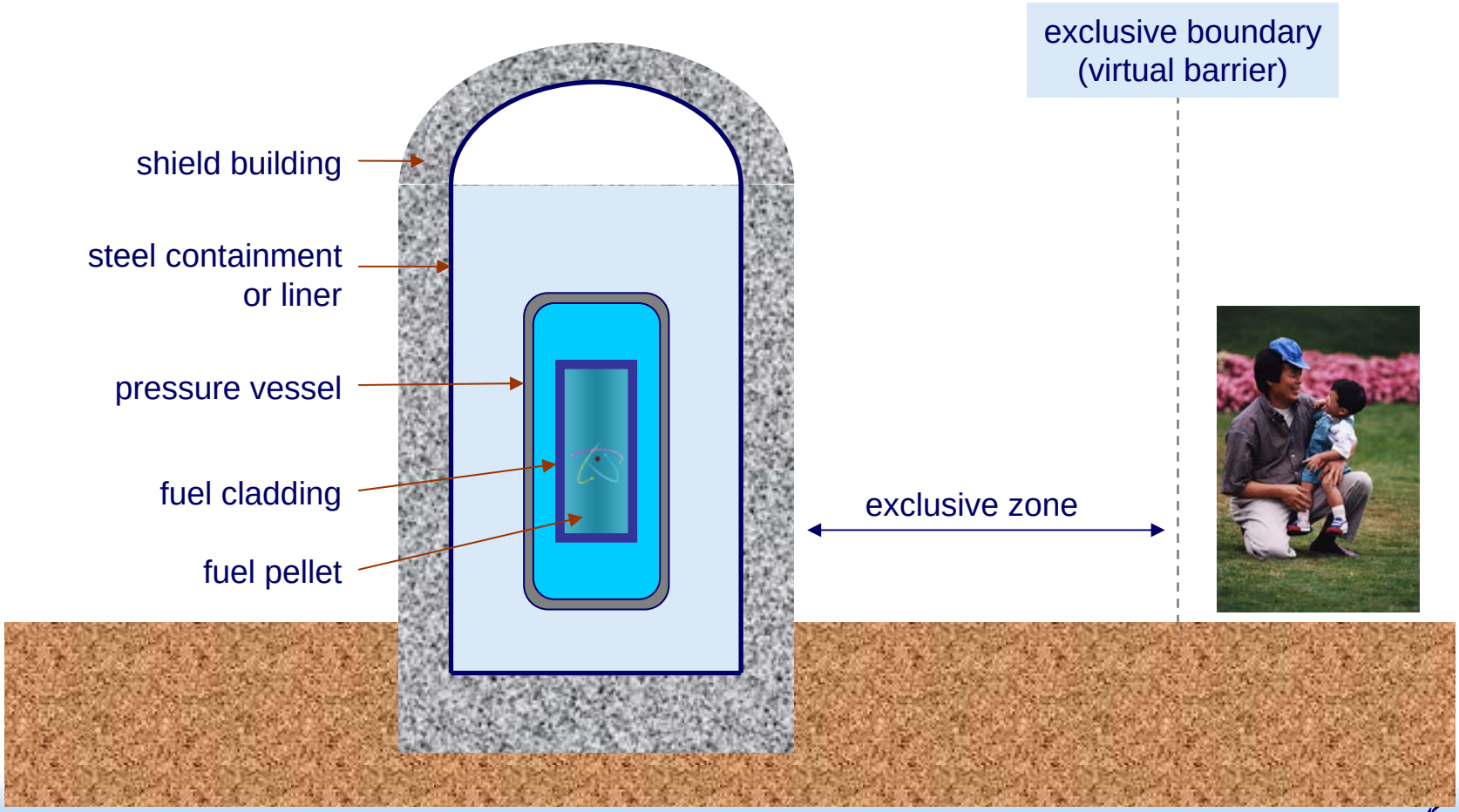
Prevention of accidents

Prevention of severe core damage

Relation between Multiple Barriers and Levels in Defense-in-Depth



Multiple Barriers against Radioactive Release



Application of Defense-in-Depth in Reactor Design

- Level 1 Application (Normal Operation)
  - Conservative design and high quality SSCs:
    - Minimize the need to take measures at Level 2 and 3.
  - Adequate operation and surveillance.
  - Comprehensive preventive maintenance.
  - Adequate consideration for human factors:
    - Adequate time for operator actions, appropriate man-machine interface, comprehensive training, and stress reduction.

Application of Defense-in-Depth in Reactor Design (Cont'd)

- **Level 2 Application (Abnormal Operation)**
  - **Reliable control, and protection system to restore normal operating conditions.**
    - **Inherent design features;**
    - **Core stability and system thermal inertia;**
    - **Prevention and mitigation features.**
  - **Adequate detection of failures.**
    - **Ongoing surveillance of quality;**
    - **In-service inspection and periodic testing of SSCs important to safety.**

Application of Defense-in-Depth in Reactor Design (Cont'd)

- **Level 3 Application (DBA)**
  - **Engineered Safety Features (ESFs):**
    - **Systems dedicated to safety for maintaining integrity of the barriers and preventing core damage;**
    - **Designed on the basis of postulated accidents representing the limiting loads resulting from sets of similar events, derived from conservative deterministic accident analyses.**
  - **Principles for ESF Design:**
    - **Redundancy, independence, and diversity;**
    - **Environmental qualification;**
    - **Automation to reduce vulnerability to human failure; and**
    - **Testability to ensure system availability and performance.**

Application of Defense-in-Depth in Reactor Design (Cont'd)

- **Level 4 Application (Beyond DBA)**
  - **First Three Levels:**
    - **Provide maintenance of the structural integrity of the core and limit potential radiation hazard for the public and environment.**
  - **Additional Efforts to Further Reduce the Risk:**
    - **Considering multiple failures;**
    - **Equipment and procedures or guidelines to cope with beyond DBA.**
  - **Accident management:**
    - **To control the course of severe accidents and mitigate their consequences.**

Application of Defense-in-Depth in Reactor Design (Cont'd)

- **Level 5 Application (Large Release)**
  - **On-Site & Off-Site Emergency Plan:**
    - **Collecting and assessing information about level of exposures;**
    - **Short and long term protective actions that constitute intervention;**
    - **Prepared in consultation with the operating organization and the responsible authorities;**
    - **Exercised periodically.**

Basic Prerequisites of Effective Defense-in-Depth

- **Conservatism**
  - **Broadly applied at the first three levels of defense with appropriate conservative assumptions and safety margin.**
- **Quality Assurance**
  - **A major element making each level of defense effective.**
- **Safety Culture**
  - **An impact at each level of defense through commitment to safety, accountability, a questioning attitude and lack of complacency.**