SH2705 Simulation Course

Defense in Depth

Sean Roshan

How do we look at safety?

Basic safety requirements and objectives

- Protecting people, society and the environment from harm by maintaining an effective defense against radiological accidents.
- To LIMIT the harmful effects of ionizing radiation, as far as possible, during normal operation within the power plant, as a result of emissions of radioactivity from the power plant and from formed waste. (ALARA – principle)
- To PREVENT radiological accidents and MITIGATE the consequences of radiation damage in the case of accidents by taking all reasonable practical steps possible.

Defense in Depth Concept

Defense in Depth originated in 1940's when detailed and precise knowledge of design margins were lacking to address the issued brought up by the AEC and its safety Philosophy.

- **Worst case scenario= no power plants**
- **Safegards holding = build power plant everywhere**
- **Plants to get license must have safegard for everything in place**
- **Not all of the accidents will ever be predicted**
- **Accidents are normally caused by a single failure or operational error**

Defense in Depth Concept

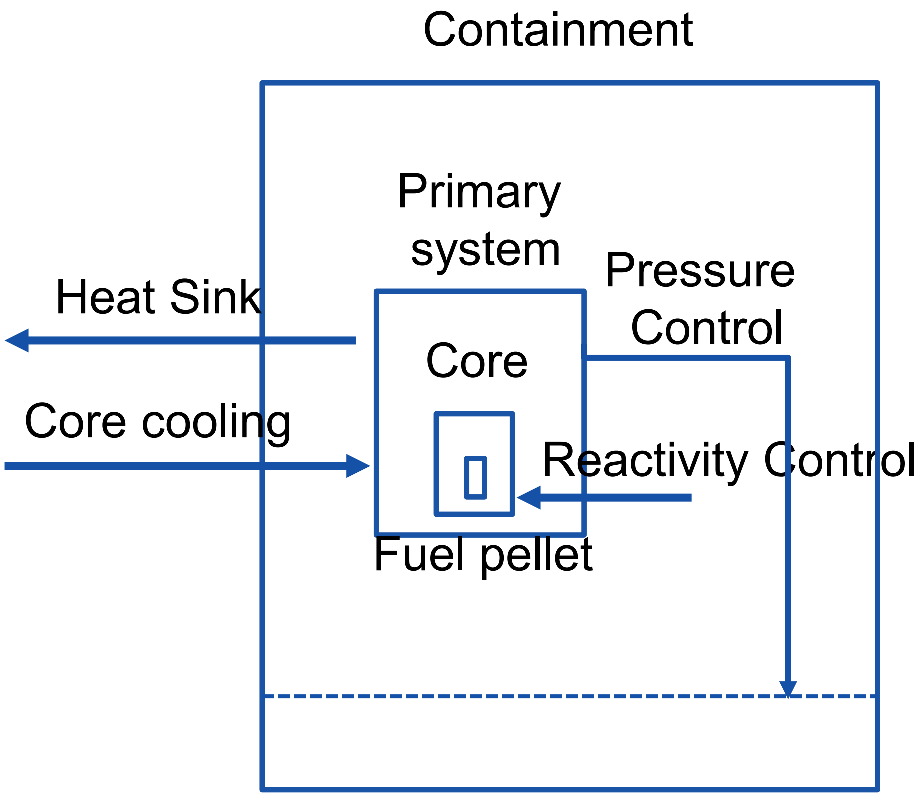
Defense in Depth consists of:

- Multiple functional and/or engineered barriers to preclude Single Failures and prevent release of radioactive materials.
- Incorporation of large Design Margins where possible.
- High Quality in design and manufacture.
- Operation within design limits.
- Testing/inspection to maintain Design Margins.

Defense in depth approach to nuclear power plant safety

- **If we design robust enough there will be less chance for accidents.**
  - Careful design, construction and operation,
- **If something goes wrong, we should have systems to prevent them from getting worst**
  - Systems to prevent such malfunctions as do occur from turning into major accidents, e.g. SCRAM and leak detection systems.
- **If we can't prevent them from getting worst, we should have systems to limit the danger offsite**
  - so that malfunctions which could lead to major accidents will be highly improbable. Systems to limit offsite consequences of postulated, major accidents e.g. emergency core cooling systems.

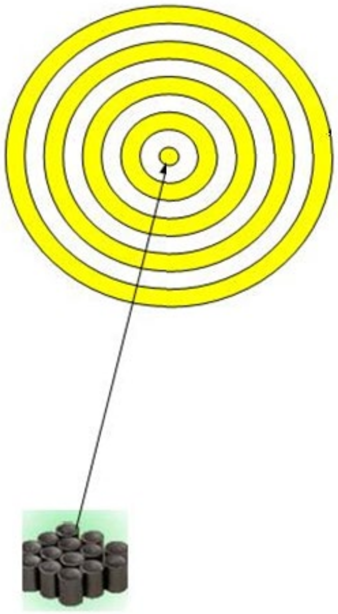
Think Barriers!



DEFENSE – IN DEPTH

THE FIRST ECHELON: PREVENTION

- Provides accident prevention through:
- Sound design (conservative) that can be built and operated with stringent quality standards.
- High degree of freedom from faults and errors.
- High tolerance for malfunctions, should they occur.
- Tested components and materials.
- Redundancy of instrumentation and controls.



1. Fuel Pellet

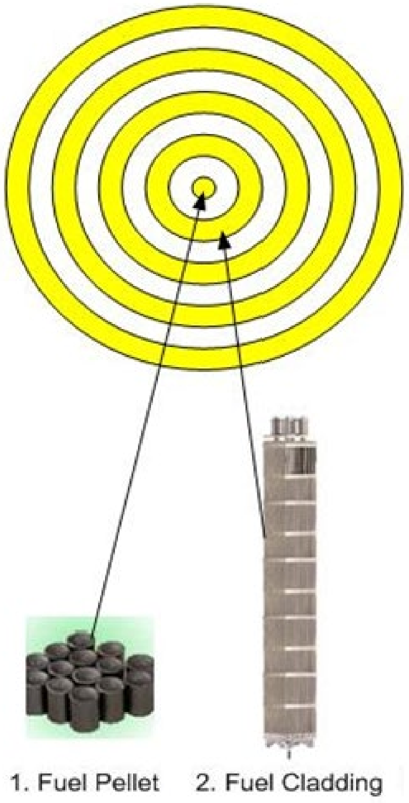
DEFENSE – IN DEPTH

THE SECOND ECHELON: DETECTION AND CONTROL

- Assumes there will be human or equipment failure.
- Provides protection systems to maintain safe operation or shut plant down safely when incidents occur.

Examples.

- Redundant sources of in-plant electricity.
- Sensitive detection systems to warn of incipient failure of fuel cladding or coolant systems
- System for automatic shutdown ("SCRAM") of reactors on signal from monitoring instruments.



DEFENSE – IN DEPTH

THE THIRD ECHELON: PROTECTION (DESIGN-BASE)

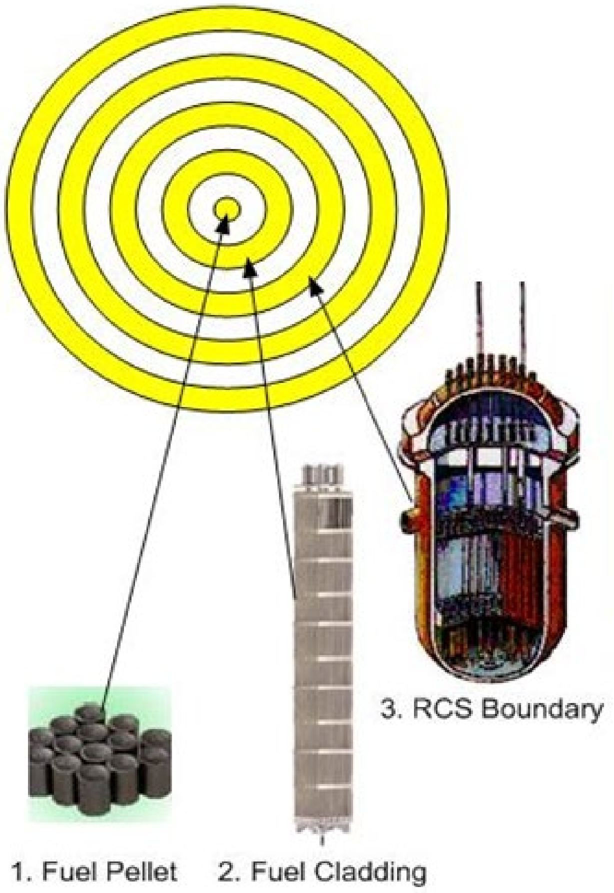
- Assume there will be a human or equipment failure. And we are not able to control it
- Provide Protection (engineered safety) systems to maintain safe operation or shut plan down safely when incidents (design-basis accidents) occur.
- Develop Emergency Operating Procedure (EOP)

DEFENSE – IN DEPTH

THE THIRD ECHELON: *PROTECTION (DESIGN-BASE)*

Examples:

- Redundant sources of in-plant electricity.
- Sensitive detection systems to warn of incipient failure of fuel cladding or coolant systems
- Systems for Automatic Shutdown (“SCRAM”) of Reactors on signal from Monitoring Instruments.
- Emergency Core Cooling System
- Decay Heat Removal System



DEFENSE – IN DEPTH

THE FOURTH ECHELON: SEVERE ACCIDENT MITIGATION

Provides additional margins to protect public should severe failures occur despite first three echelons.

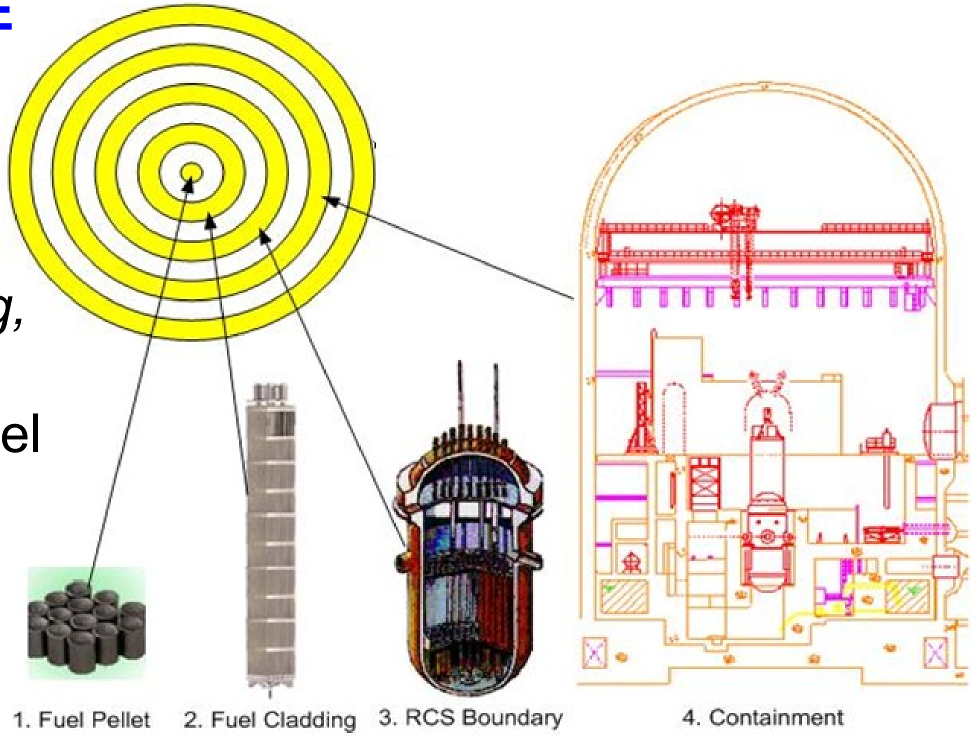
- Control severe plant conditions.
- Prevent further accident progression
- Mitigation of the consequences of beyond-DBAs

DEFENSE – IN DEPTH

THE FOURTH ECHELON: SEVERE ACCIDENT MITIGATION

Example

- *Concrete containment building, typically 1.5m thick and* reinforced with steel and a steel liner.
- Develop Severe Accident Management Strategy and Guidelines

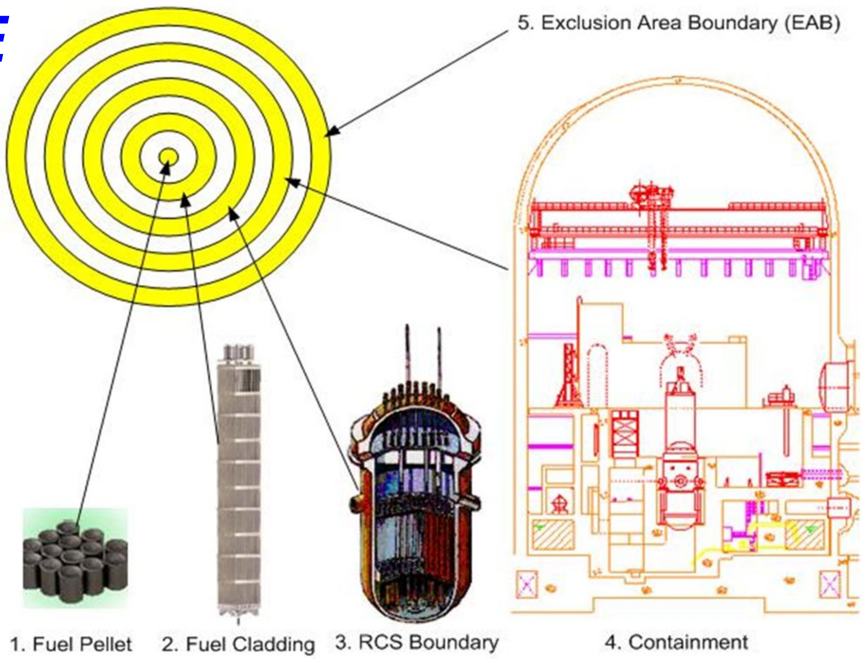


DEFENSE – IN DEPTH

THE FIFTH ECHELON:
DEALING WITH WORSE-CASE

- <u>Mitigate radiological consequences of significant releases of radioactive materials from the plant</u>

- Develop <u>Off-Site Emergency Response</u> Measures

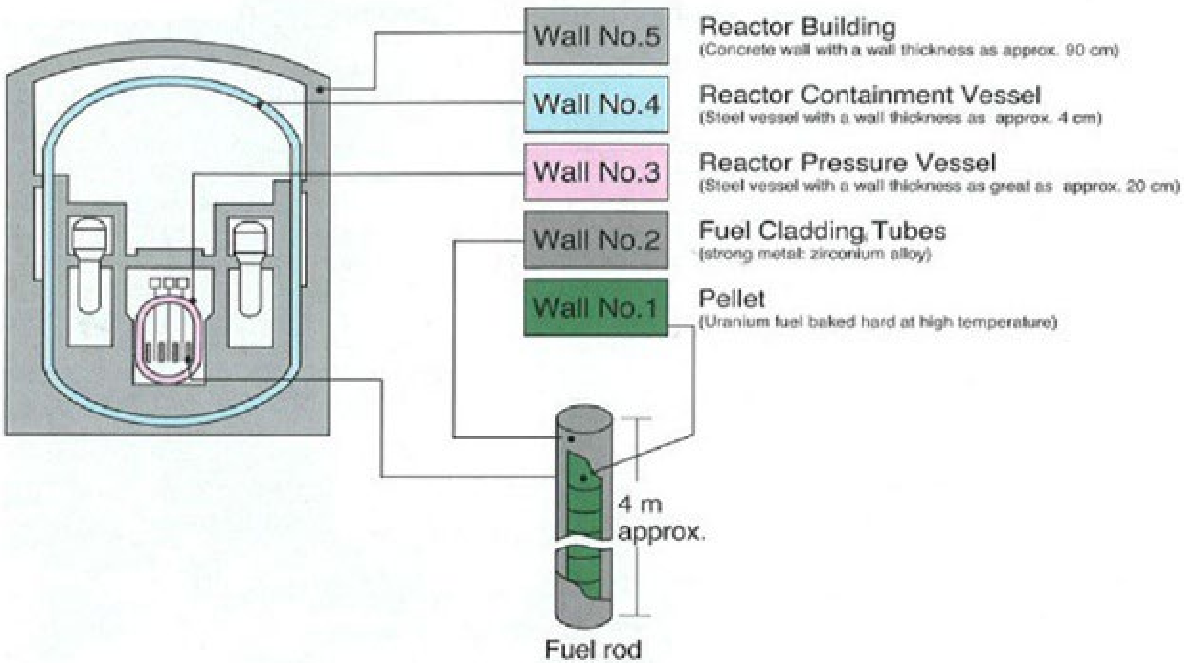


Physical barriers between reactor core and the environment

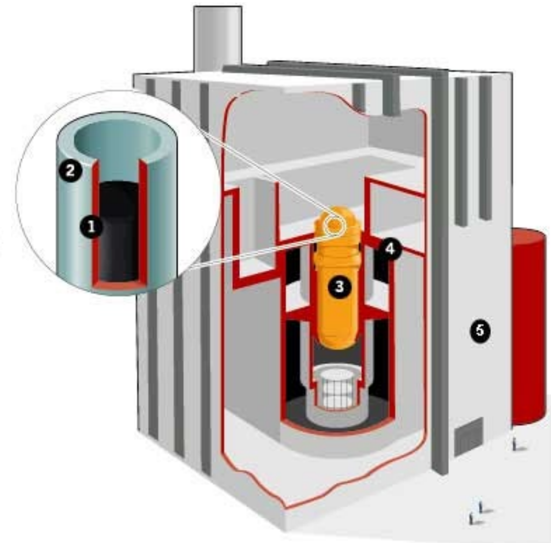
Example of LWR Defense in Depth

- Radioactive fission products in ceramic fuel pellets – operated at relatively low power density.
- Fuel pellets contained in hermetically sealed fuel rods cooled by reactor coolant system.
- Reactor coolant system contained in pressure tested RPV and Primary Coolant System.
- Piping subject to In-Service Inspection & NDT exams.
- Primary Coolant System leaks backed up by ECCS.
- Primary Coolant System contained in hermetically sealed and cooled Containment.
- All activities subject to Quality Assurance verifications.

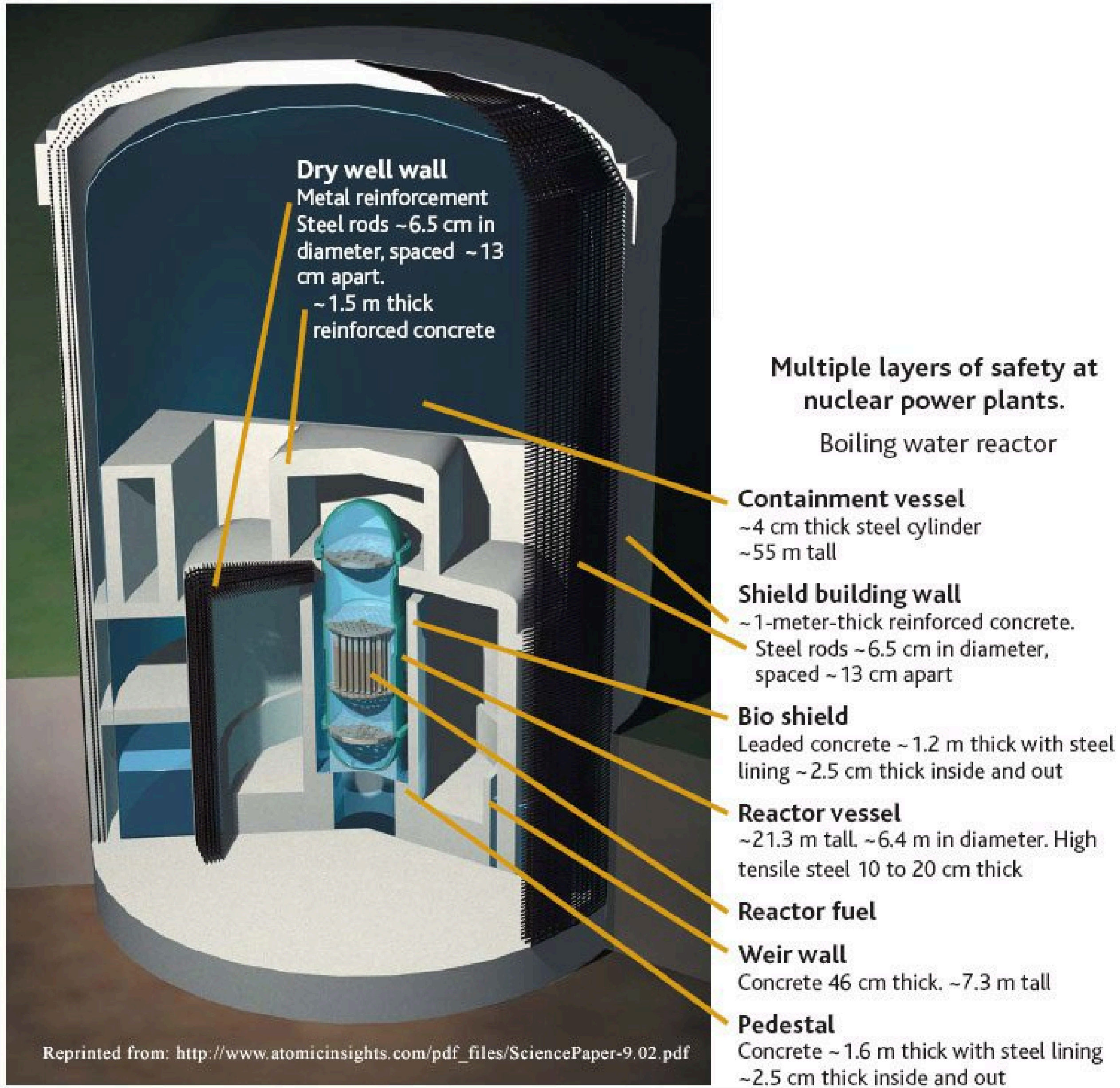
DEFENSE – IN DEPTH WALLS



Five Walls of Protection



DEFENSE – IN DEPTH, LAYER EXAMPLES

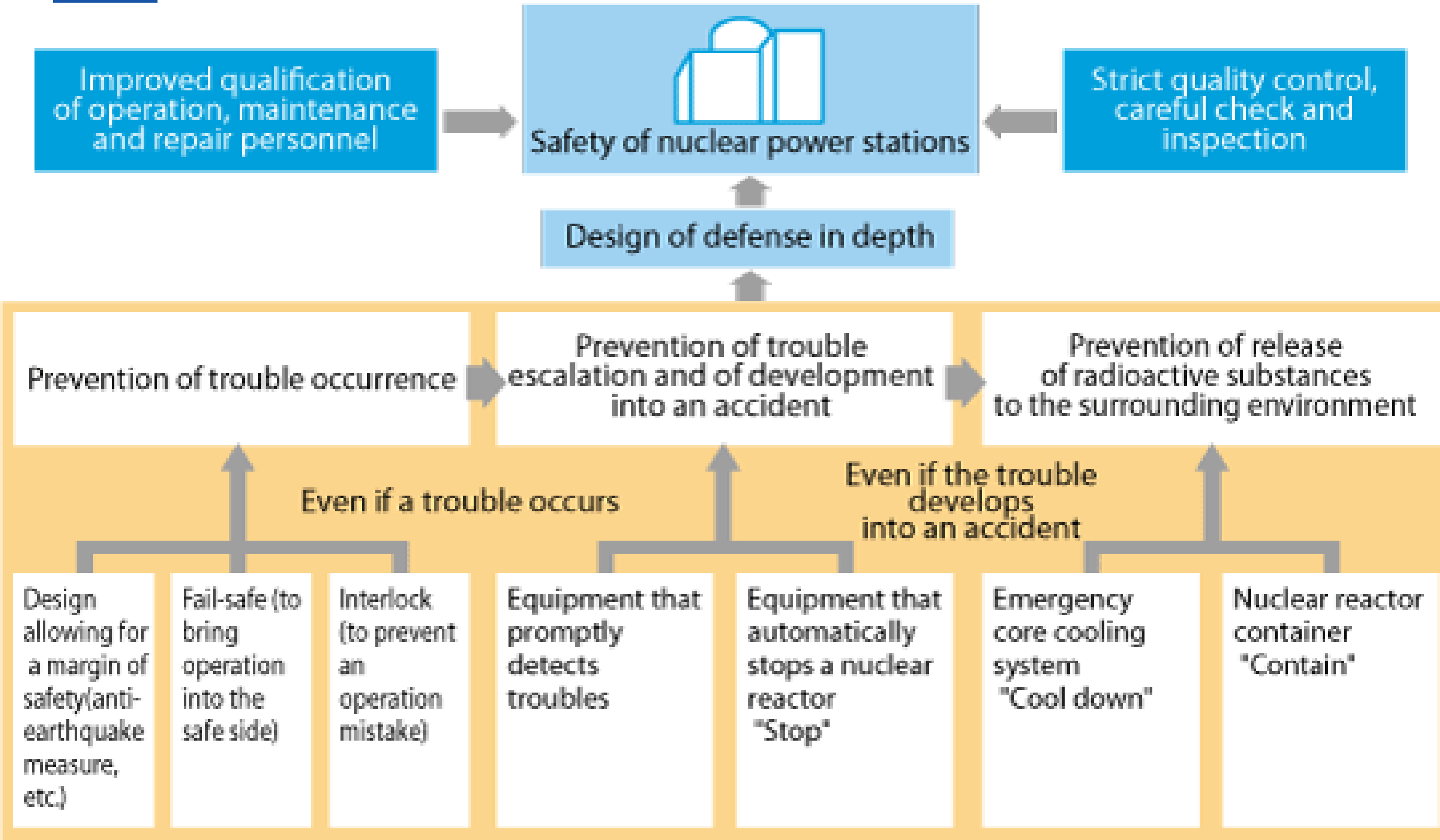


DEFENSE – IN DEPTH

In Short:

- sound design, construction, testing, maintenance, training and guidance,
- control systems,
- protection system,
- safety systems to deal with DBAs,
- measures to deal with Severe Accidents,
- emergency preparedness,
- Distance.

DEFENSE – IN DEPTH



DEFENSE – IN DEPTH SWISS CHEESE FAILURE MODEL