The Abdus Salam
International Centre
for Theoretical Physics

2473-14

Joint ICTP-IAEA School on Nuclear Energy Management

15 July - 3 August, 2013

Lecture Notes

M.lipar
IAEA, Vienna, Austria

Strada Costiera, 11 - 34151 - Trieste - Italy • Tel. +39 0402240111 • Fax. +39 040224163 • sci_info@ictp.it • www.ictp.it
ICTP is governed by UNESCO, IAEA, and Italy, and it is a UNESCO Category 1 Institute

The ICTP/IAEA School of Nuclear Energy Management School, Trieste, 18 July 2013

MAIN PRINCIPLES OF NUCLEAR INSTALLATIONS SAFETY

Miroslav Lipár

Head, Operational Safety Section

M.Lipar@iaea.org +43 1 2600 22691

IAEA

International Atomic Energy Agency

Outline

- Introduction
- Specificity of nuclear power
- Defence in depth
- Safety systems
- Management for safety and safety culture
- Operational safety
- Conclusions

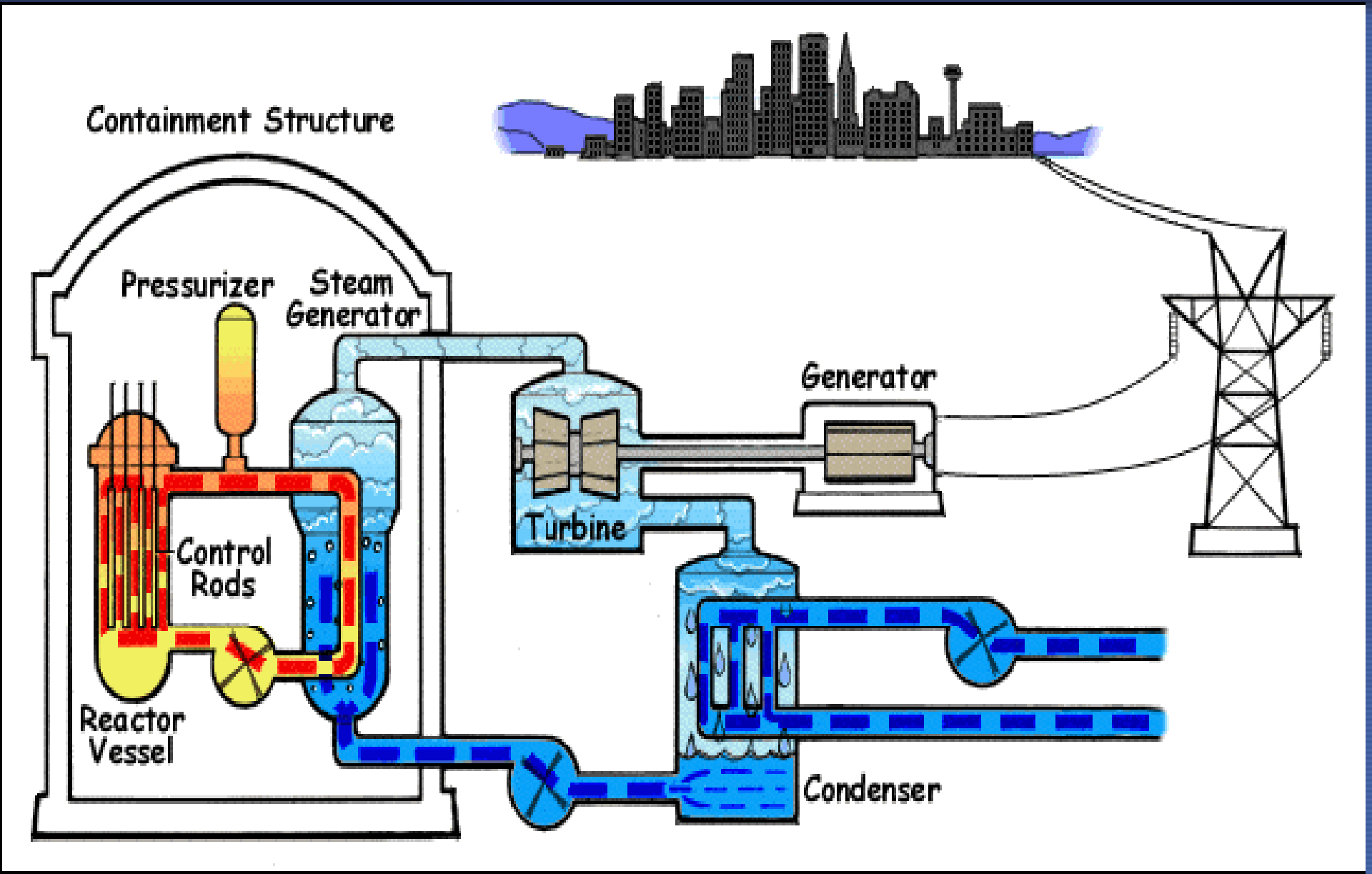
IAEA

Major Nuclear Safety Lessons

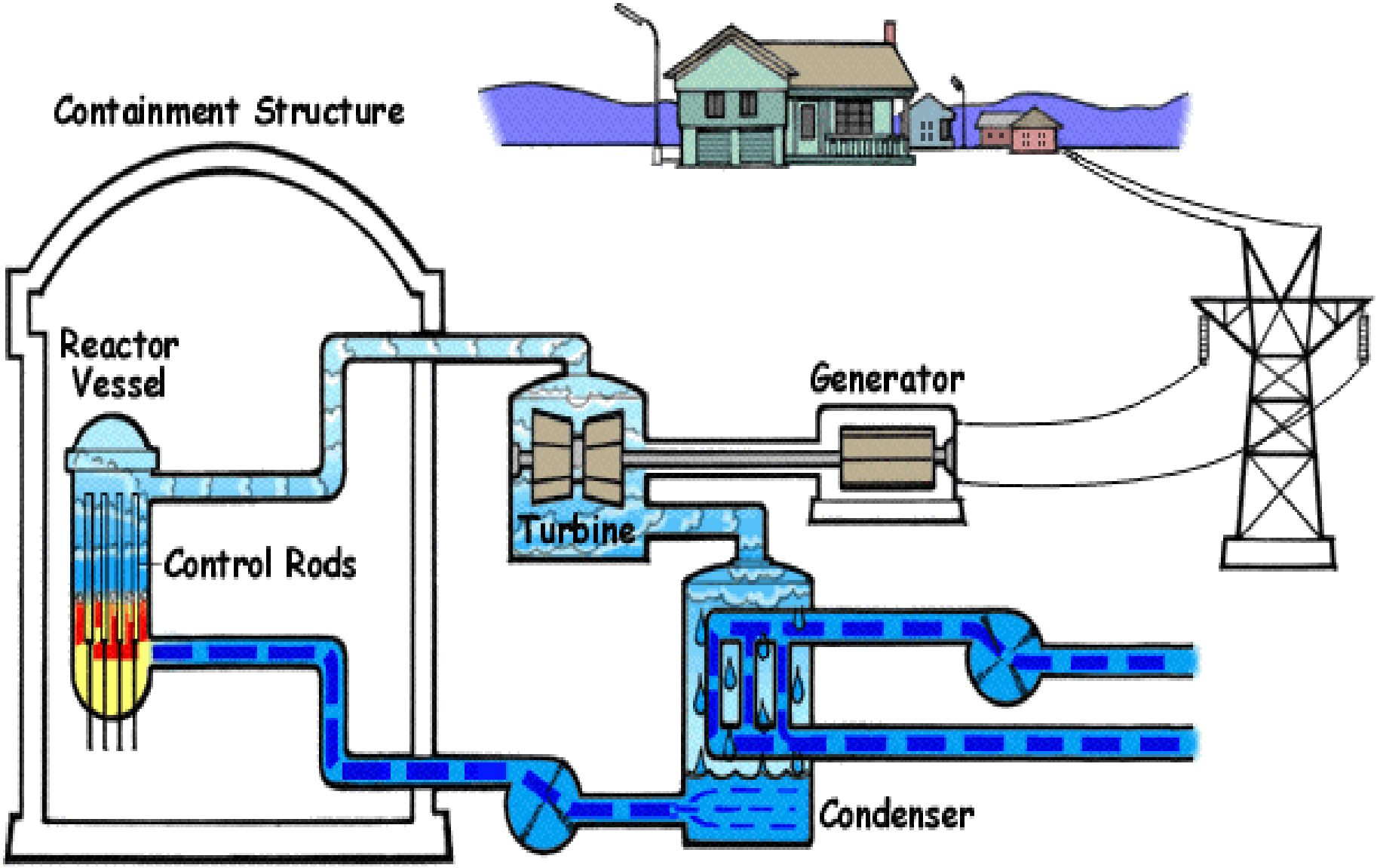
Fukushima Dai-ichi
Units 1 - 4

IAEA

Pressurized water reactor PWR



Boiling water reactor BWR



Safety and safety objectives (SF-1)

- **Safety:** means the protection of people and the environment against radiation risks
- The **fundamental safety objective** is to protect people and the environment from harmful effects of ionizing radiation

IAEA

Safety and safety objectives (SF-1)

- **Measures to achieve the highest standard of safety**:
  - (a) To control the radiation exposure of people and the release of radioactive material to the environment;
  - (b) To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;
  - (c) To mitigate the consequences of such events if they were to occur

IAEA

Specificity of Nuclear Power

Security

Proliferation

Production of radioactive materials

Power control

Heat removal

Radiation hazards to workers, public and the environment

Nuclear Safety

- Technical aspects
- Management aspects

IAEA

Nuclear Safety Concept

Adequate site and 3 essential factors must be in a complex interaction

IAEA

Fundamental Safety Functions:

1) controlling the reactivity,

2) cooling the fuel,

3) confining the radioactive material and control of operational discharges, as well as limitation of accidental releases

IAEA

Defence in depth

- **Defence in depth (INSAG-10)** – hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers, placed between radioactive material and workers, the public or the environment, in normal operation, anticipated operational occurrences and, for some barriers, in accident at the plant

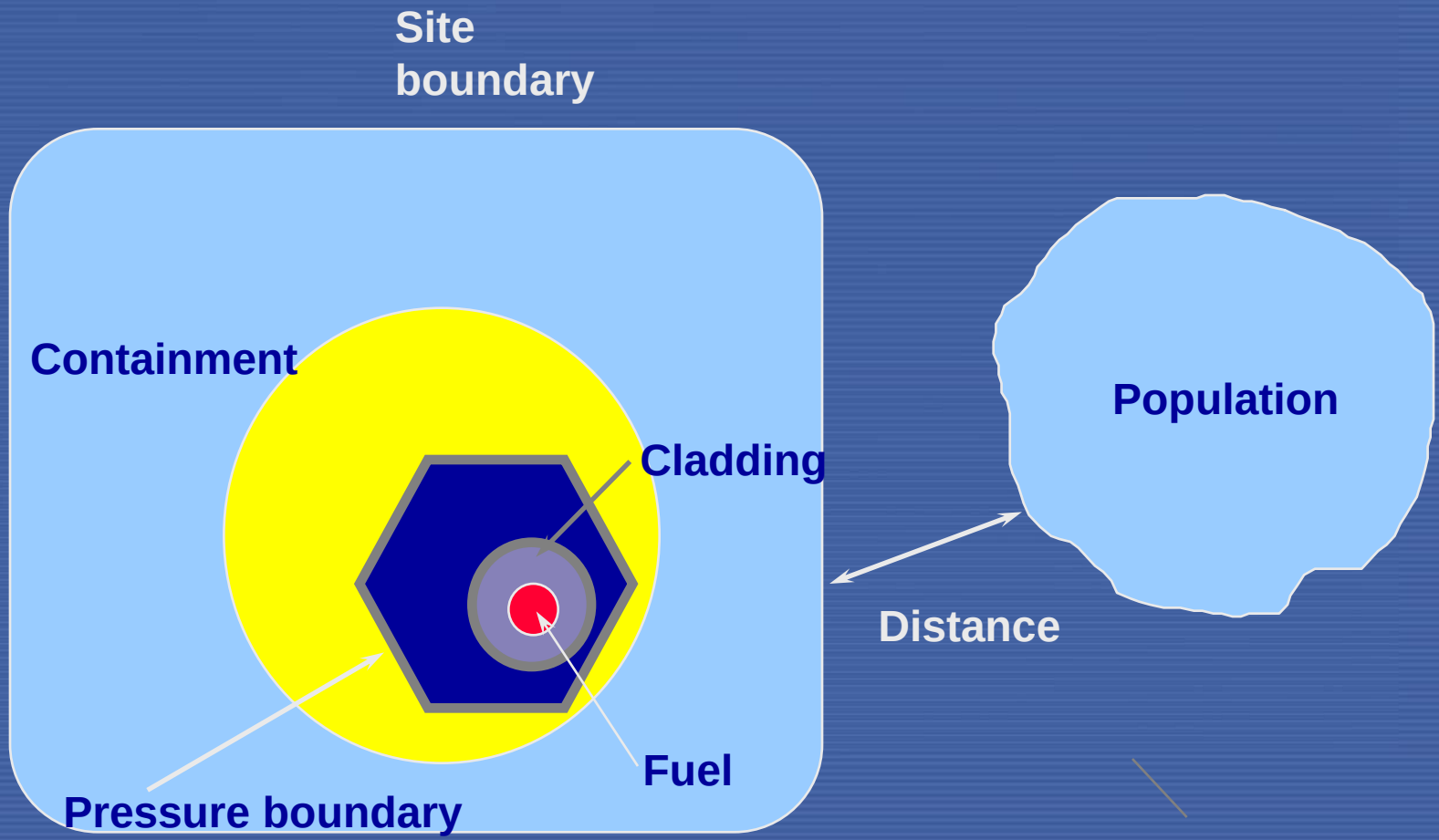
IAEA

Defence in depth

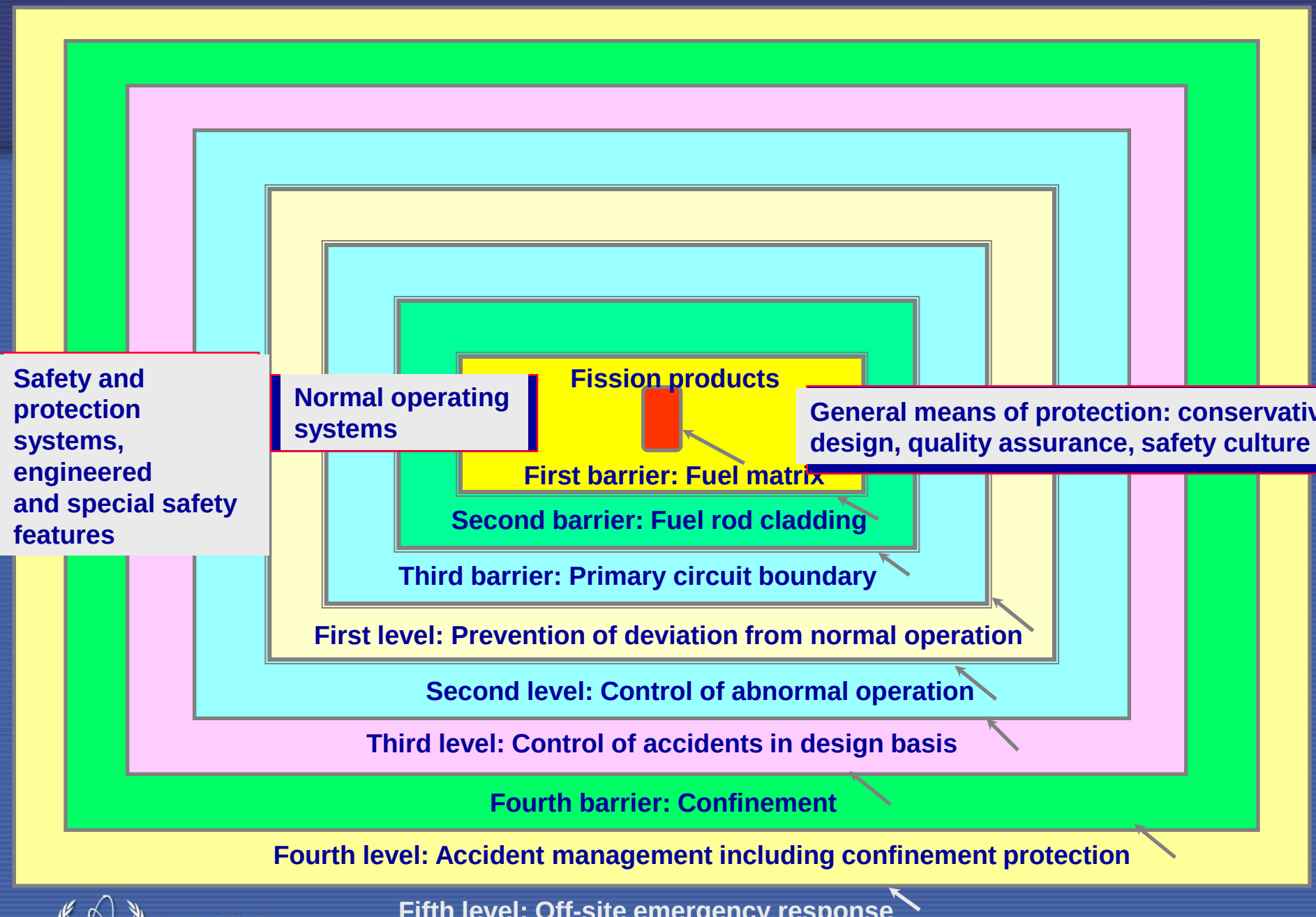
- Defence in depth – ensures that the fundamental safety functions are reliably achieved and with sufficient margins to compensate for equipment failure and human errors
- To the extent possible, provisions at different levels of defence should be independent

IAEA

Barriers against releases of radioactivity



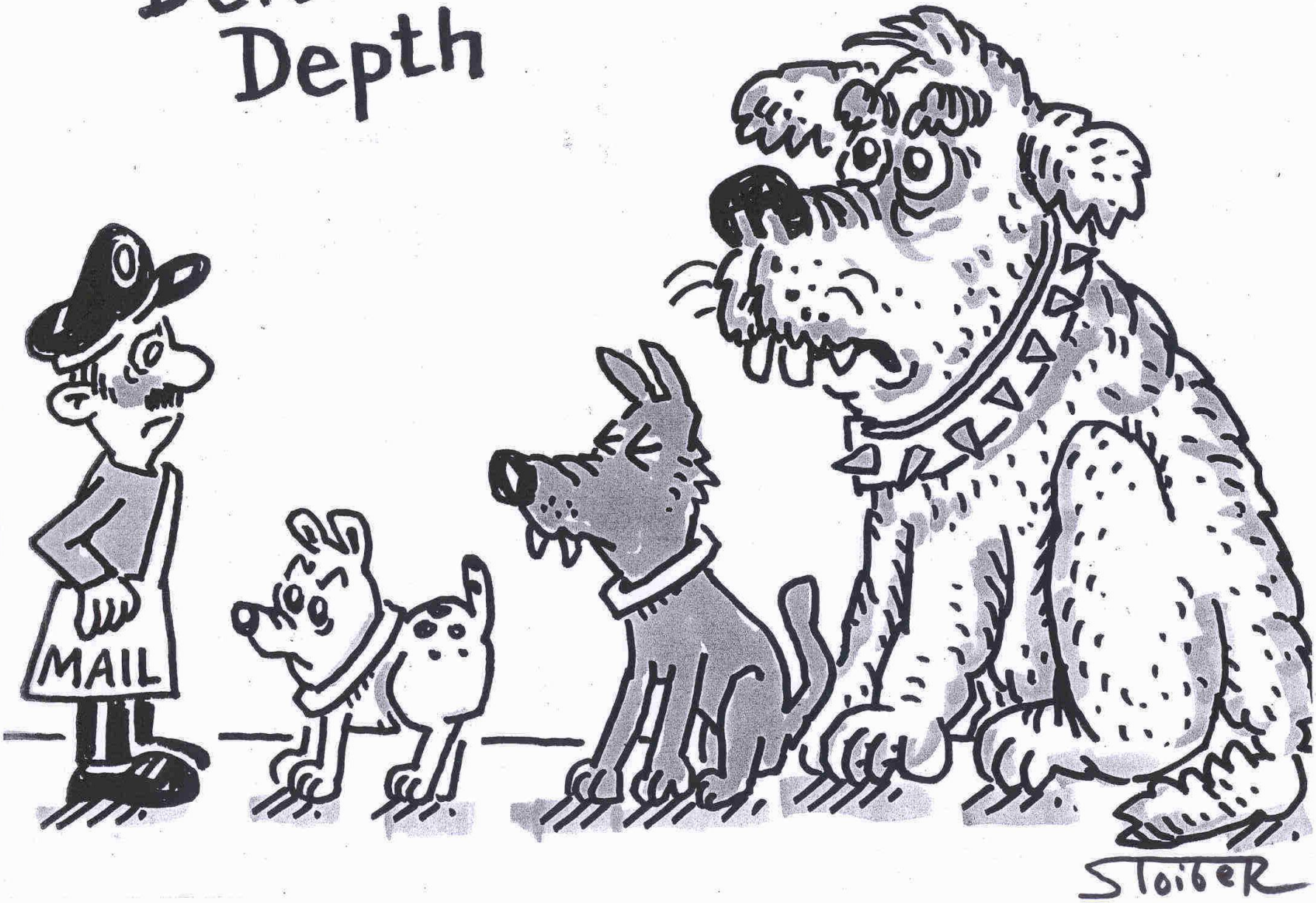
IAEA



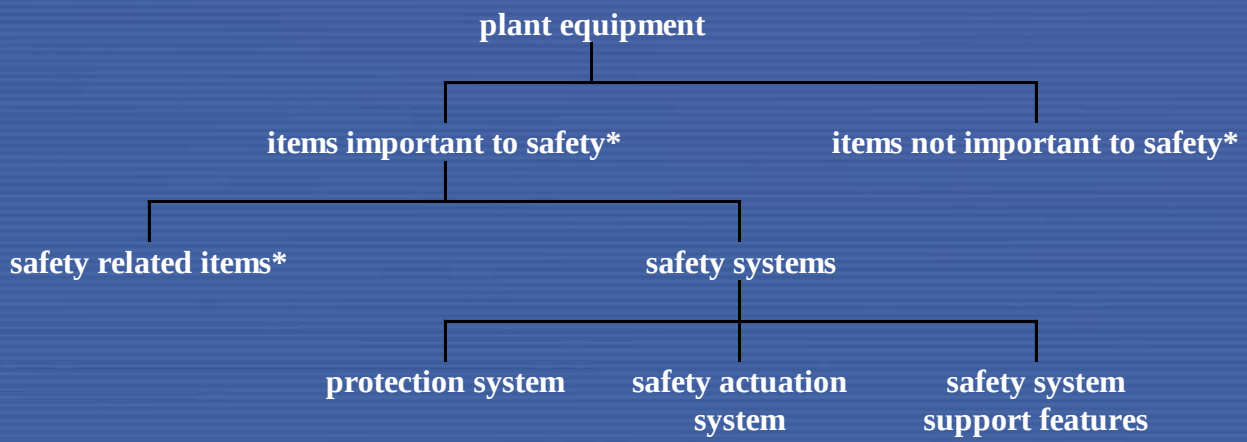
IAEA

Defence in depth - relation between barriers and levels

Defense in Depth



Safety Systems



* In this context, an 'item' is a *structure, system or component*.

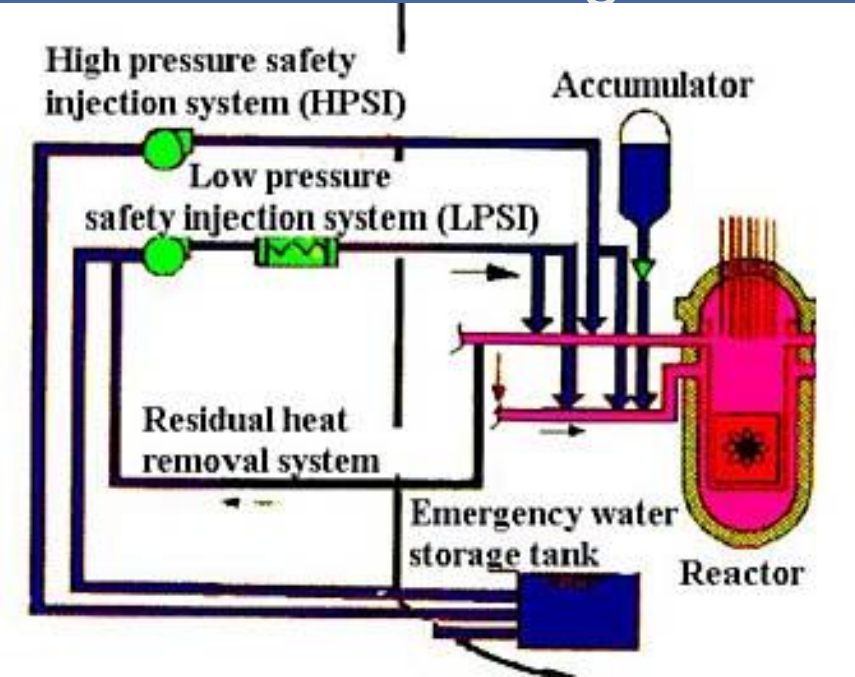
WHY do we need safety systems?

- To fulfill an important role in defense in depth concept.
- To perform their design safety function in case that normal operating systems fail, to avoid that anticipated operating occurrences evolve to accident conditions, or
- To cope with postulated initiating events

IAEA

Safety systems - main features

- Active
  - need external energy supply (el. power, compressed air, steam etc.)
  - need actuation signal



- Passive
  - do not need external energy supply – it is accumulated (gas pressure, hydrostatic liquid pressure etc.)
  - do not need actuation signal – they actuate when conditions are met (change of Δp or ΔT)

Main requirements for design of NPPs

- Management of safety in design
- Application of defence in depth
- Radiation protection and acceptance criteria
- Design basis of SS&C important to safety
- Safety classification
- Provisions for ISI, surveillance, maintenance
- Ageing
- Human factors

IAEA

Main requirements for design of NPPs

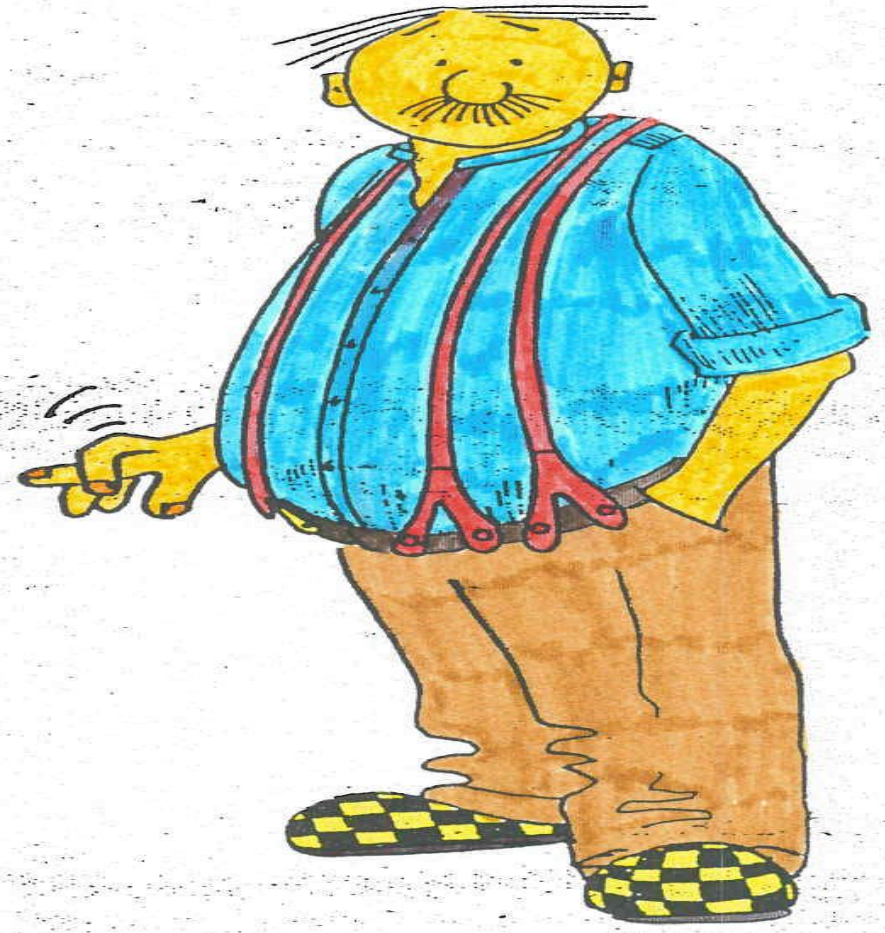
- Reliability of SS&C
  - Common cause failures
    - Failure of two or more SS&C due to a single specific event or cause
  - Single failure criterion
    - Requirement applied to a system such that it must be capable of performing its task in the presence of any single failure
  - Fail safe design
    - when an element of the considered system fails, the system is able to meet its design function – esp. I&C sytems

IAEA

Main requirements for design of NPPs

- **Redundancy** (2x100%, 3x100%, 4x50%,4x 100%)
- **Independence** – physical, electrical, I&C, to assure single failure criterion
- **Diversity** – based on different methods, physical or at least different suppliers
- Safety assessment
  - Deterministic
  - Probabilistic

IAEA



Redundancy
The use of more than one item to carry out a particular task.

Common Mode Failure
Coincidental failure of the same component in two or more items or systems.

Diversity
The use of different
means to carry out a task

Equipment qualification

- Safety systems must be able to meet their safety function under environmental conditions during accidents and also in case of following occurrences:
  - **external** – earthquake, flooding, aircraft hits, industrial explosions;
  - **internal** – pipe whips, flying objects, environmental parameters (temperature, pressure, humidity, radiation...)

IAEA

Safety Management Systems - Definition

- “Those arrangements made by the organisation for the management of safety in order to promote a strong safety culture and achieve good safety performance” (INSAG-13)

IAEA

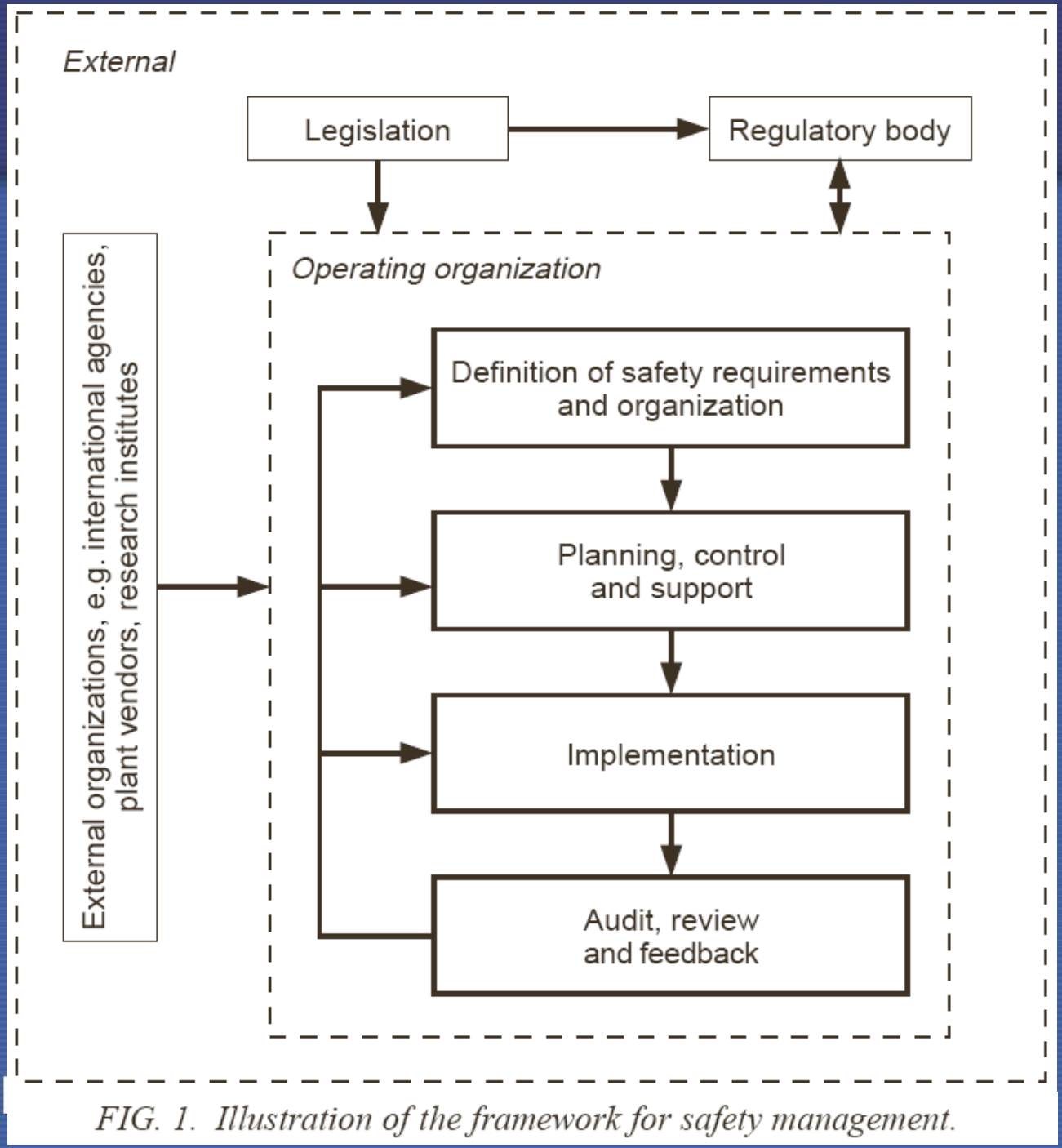
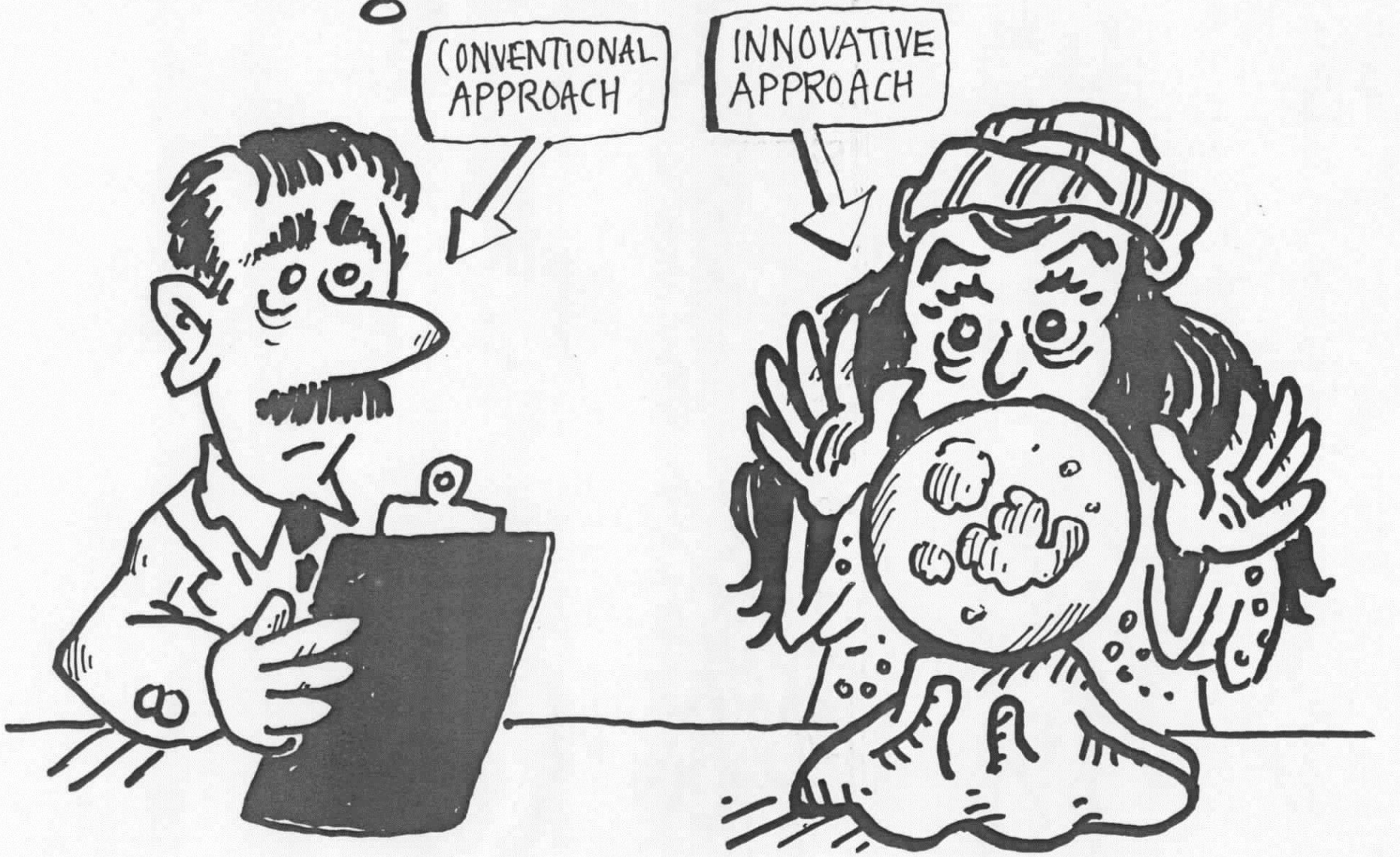


FIG. 1. Illustration of the framework for safety management.

Different Approaches to Management Assessment



Operational safety

Direct obligation of the operating organization:

- To ensure physical barriers against radiological hazards are maintained
- To ensure robust levels of protection are in place to prevent accidents
- To mitigate consequence of accidents, should they occur

IAEA

Operational Safety - definition

Operational safety of NPP -
protection of employees, the public and the environment from potential hazards during NPP operation assured by means of maintaining proper operating conditions, prevention of accidents or mitigation of accident consequences.

IAEA

Operational Safety

Safe plant operation is characterized by:

- conservative, safety-oriented decision making
- operating the plant within the design safety envelope at all times
- ensuring all plant and procedure modifications are carefully considered for safety consequences
- maintaining defense-in-depth against unplanned events and their consequences through high levels of equipment reliability and human performance

IAEA

Operational safety levels

- well trained, competent personnel,
- high quality processes, tools and facilities,
- strong application of programs in the field,
- reliable process systems,
- available safety systems,
- detection and correction of problems - OE
- strong presence of Safety Culture.

IAEA


THANKS FOR YOUR FAILURE... WE LEARNED A LOT FROM YOU!

ROOT CAUSE IS SELDOM VISIBLE FROM THE SURFACE

IT TAKES SOME DIGGING

Operational Safety

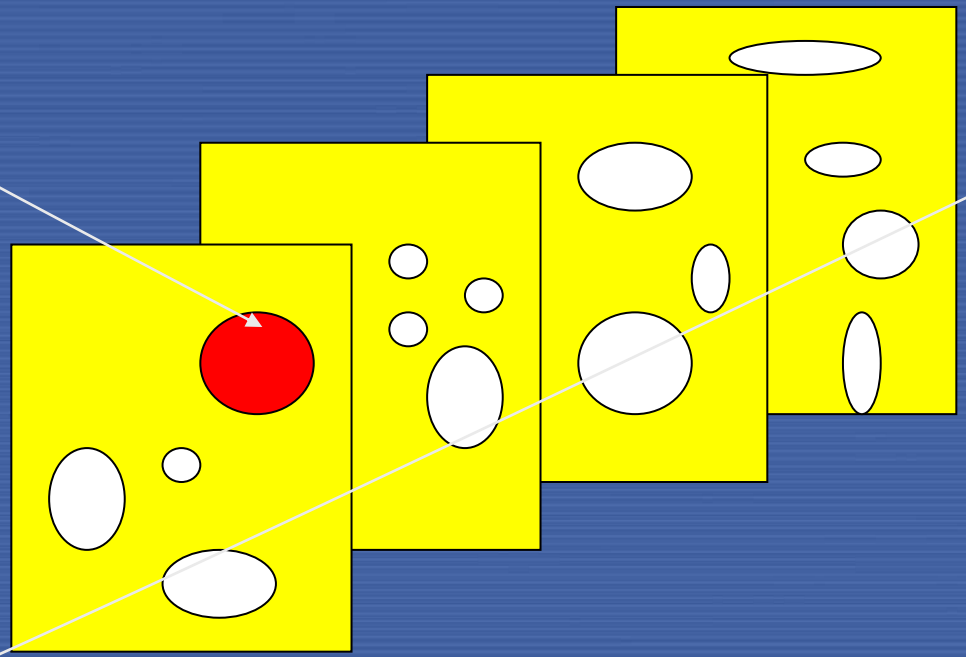
INCIDENTS

- Series of weaknesses leading to major consequences
- Incident could have been avoided if any one of the weaknesses was detected beforehand
- Many of the weaknesses causing errors were in existence before the incident (latent weaknesses). Some were well known and tolerated by management.

IAEA

Why Do Events Happen? (Swiss Cheese Model)

Past Errors Result in Latent Weakness in "Defence in Depth" of Organisations, Processes and Equipment



Significant Events

(Consequences)

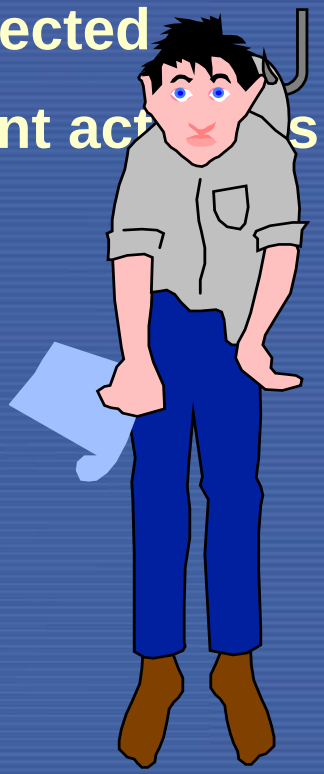
Active Errors by Individuals Result in Initiating Action (s)

Dr. James Reason, *Managing the Risks of Organisational Accidents, 1997.*

IAEA

TYPICAL PRECURSORS OF INCIDENTS

- Acceptance of low standards of performance
- Line management and workers not held accountable
- Performance weaknesses not recognized or corrected
- Insufficient direction provided for conduct of plant activities
- Deficient control room activities
- Inadequate procedures
- Ineffective training
- Insufficient use of operating experience
- Root causes of abnormal events not determined
- Design configuration not controlled
- Increasing trend of human errors



IAEA


And after two weeks, "abnormal" operating conditions automatically become "normal"!

Attributes of excellent plants

- Personal involvement of management in *directing* improvements
- Effective communication in all levels of the organization
- High standards set and visible throughout the whole organization and shown in the plant
- Strong focus of line management on *goals*
- Clear and visible processes
- Leadership *development* programme for supervisors

IAEA


LOOKING FOR SOLUTIONS TO THE AGING PERSONNEL PROBLEM
BUT YOU'LL LOVE BEING A REACTOR OPERATOR!

IAEA

Attributes of excellent plants

- **Willingness and ability to learn from experience**
- **Cultivation of *teamwork***
- **Effective corporate *support***
- **Long- range outlook in developing *plans***
- **Effective plant configuration control programme**
- **Delegation of *responsibility* to the lowest level**
- ***Enthusiastic,* stable staff**
- **Strong *training* programmes**

IAEA

Attributes of excellent plants

- ***Effective*** **and** ***efficient*** **use of manpower**
- **Workers** ***motivated*** **to assume responsibility**
- **Managers accepting constructive criticism from lower levels**
- **Managers attentive to workers problems**
- **Pro-active behaviour of staff**
- **Information flow between management and workers**

IAEA

Key Common Operational Issues

- Maintaining competence
- Application of acceptable standards
- Questioning attitude
- Organisational “complacency”/Loss of focus/Organisational drift
- Poor communication
- Loss of “oversight”
- Management of change (often involving contractorisation)
- External pressures

IAEA

METHODS OF SELF-ASSESSMENT

Conclusions

- Safety is a paramount requirement for future of nuclear power
- Safety objective require that NPPs are designed/operated so as to keep all sources of radiation exposure under strict control
- Several successive physical barriers for the confinement of radioactive material are put in place; the safety objective can be achieved by maintaining integrity of the barriers, which in turn is ensured by fulfilment of 3 fundamental safety functions

IAEA

Conclusions

- Implementation of the **defence in depth** ensures that the **safety functions are reliably achieved with sufficient margins** to compensate for equipment failures and human errors
- **Defence in depth is a deterministic approach**, which is however closely related and normally complemented by probabilistic approach; but, **defence in depth can not be replaced by PSAs**

IAEA

Conclusions

- Possible **challenges to the safety functions** are dealt with by the **provisions (measures) established at a given level of defence** which include inherent safety characteristics, safety margins, active and passive systems, procedures, operator actions, organizational measures, safety culture aspects

IAEA

SENIOR MANAGEMENT COMMITTMENT IS A CRUCIAL POINT OF IMPLEMENTATION OF SAFETY MANAGEMENT!

Main relevant documents

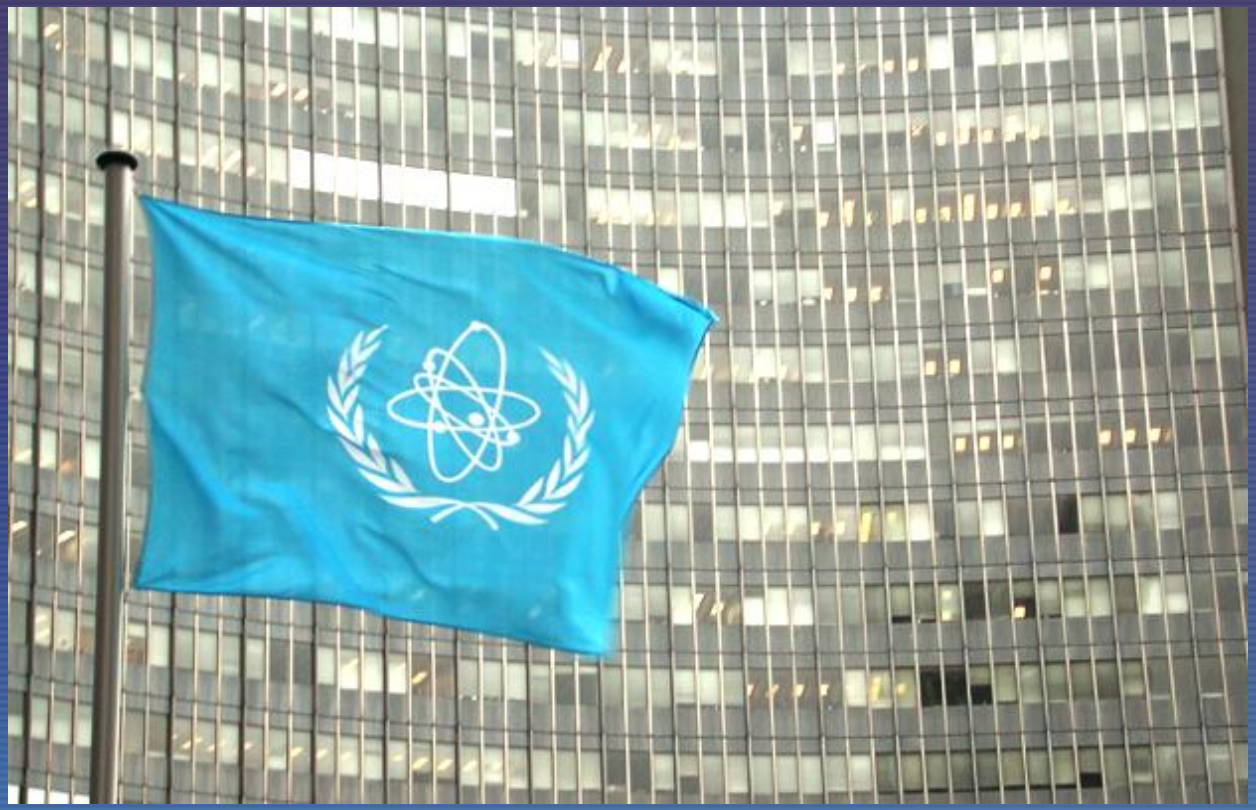
- **Fundamental Safety Principles,** Safety Standards Series No. SF-1, IAEA, Vienna (2006)
- **Basic Safety Principles for Nuclear Power Plants,** 75-INSAG-3 Rev.1, INSAG-12, A report by the International Nuclear Safety Advisory Group, IAEA, Vienna (1999)

IAEA

Main relevant documents

- **Defence in Depth in Nuclear Safety,** INSAG-10, International Nuclear Safety Advisory Group, IAEA, Vienna (1996)
- **Assessment of defence in depth for nuclear power plants,** Safety Report Series No. 46, IAEA , Vienna (2005)
- **Safety of Nuclear Power Plants: Design,** Safety Standards Series No. NS-R-1, IAEA, Vienna (2000)
- **Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements** Series No. SSR-2/2, IAEA, Vienna (2011).

IAEA



…Thank you for your attention

http://www.iaea.org

IAEA

International Atomic Energy Agency