SENIOR REGULATORS' MEETING

Strengthening the Implementation of Defence in Depth
IAEA Perspective

58th IAEA General Conference
25 September 2014

James Lyons

Director of the Division of Nuclear Installation Safety

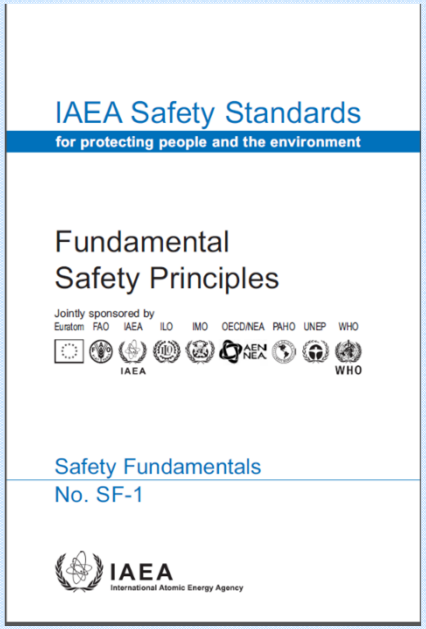
Department of Nuclear Safety and Security
International Atomic Energy Agency

IAEA's Perspective

1. Defence in Depth Approach in IAEA SSs. Application to existing and new Nuclear Power Plants
2. Conclusions from the International Conference on Topical Issues (21 – 24 October 2013) on Defence in Depth
3. Current IAEA Work on considerations for the application of IAEA Safety Requirements for NPP Design, including Defence in Depth.

IAEA
International Atomic Energy Agency

IAEA's Concept of Defence in Depth (SF-1)



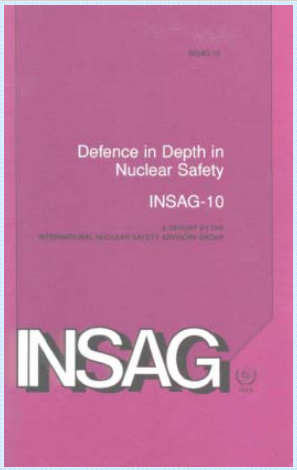
Principle 8:
Prevention of accidents

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

- 'Defence in depth' is the primary means
- Comprises a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused. If one level/barrier fails, another subsequent level or barrier would be available.
- Properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects

IAEA
International Atomic Energy Agency

IAEA's Concept of Defence in Depth



IAEA
International Atomic Energy Agency

- Defence in Depth in Nuclear Safety, INSAG-10, 1996
- Nuclear Safety Requirements NS-R-1, Safety of Nuclear Power Plants: Design, 2000
- Specific Safety Requirements SSR-2/1, Safety of Nuclear Power Plants: Design, 2012
  - Introduced Design Extension Conditions (DEC)

Summary of DiD levels in INSAG 10

Applied in most existing NPPs

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

Summary of DiD levels in IAEA SSR 2/1

Specifications for new NPPs

Level of defence	Objective	Essential design means	Essential operational means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures
Level 2	Control of abnormal operation and detection of failures	Limiting and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures
Level 3	Control of design basis accidents	Engineered safety features (safety systems)	Emergency operating procedures
Level 4	Control of design extension conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Safety features for design extension conditions. Technical Support Centre	Complementary emergency operating procedures/ severe accident management guidelines
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans

IAEA International Atomic Energy Agency

Design Extension Conditions

- Accidents that are either more severe than design basis accidents or that involve additional failures.
- Capable to withstand without unacceptable radiological consequences
- Derived on the basis of:
  - Engineering judgment
  - Deterministic assessments
  - Probabilistic assessments

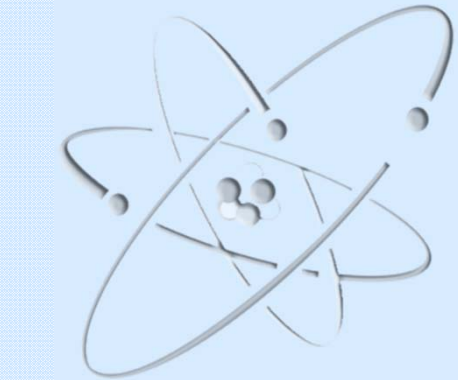
IAEA
International Atomic Energy Agency

Design Extension Conditions

- Identify the additional accident scenarios to be addressed in the design.
- Plan practicable provisions for the prevention of such accidents or,
- Mitigation of their consequences if they do occur.

IAEA
International Atomic Energy Agency

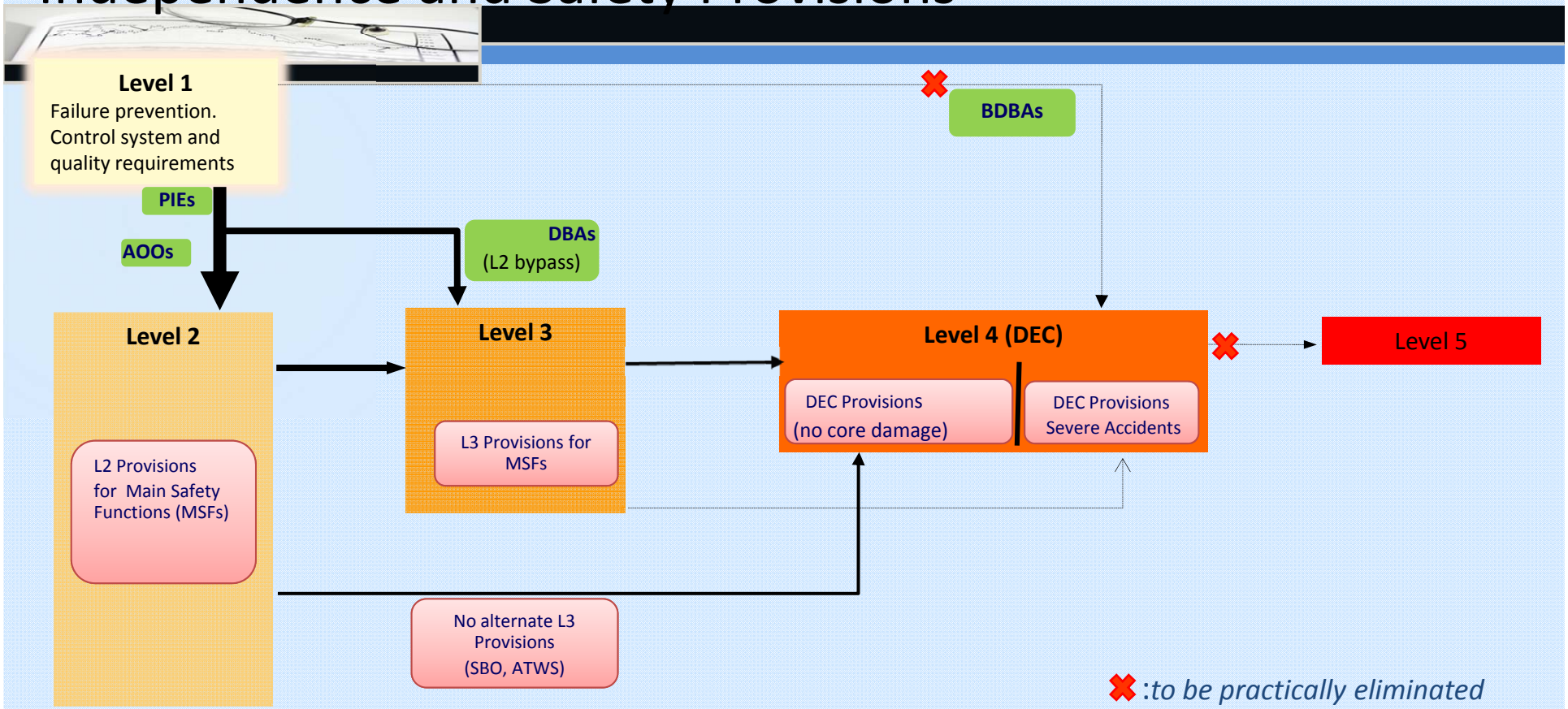
Design Extension Conditions



- Conditions that could lead to significant radioactive releases are practically eliminated.
- If not practically eliminated
  - Only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public
  - Sufficient time shall be made available to implement these measures.

IAEA
International Atomic Energy Agency

DiD Levels
Independence and Safety Provisions



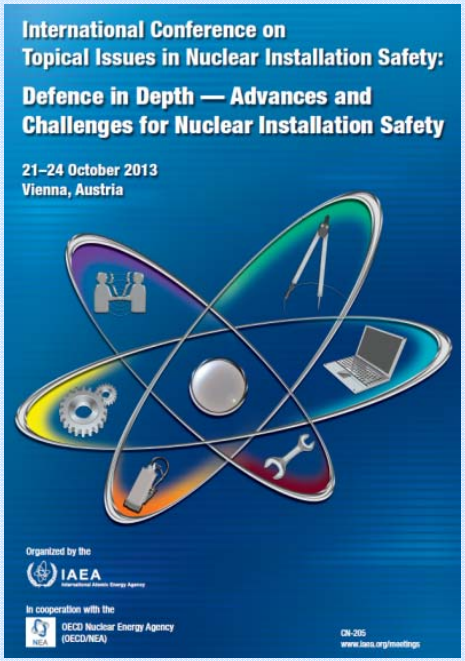
Provisions need to:

- *Be balanced and meet safety goals*
- *Rely on adequate design bases of SSCs, including sufficient margins*
- *Ensure sufficient reliability at each level*
- *Be independent to the extent possible, in particular of level 4 from 2&3.*

IAEA International Atomic Energy Agency

PIE: Postulated Initiating Event, AOO: Anticipated Operational Occurrence, DBA: Design Basis Accident, BDBA: Beyond DBA

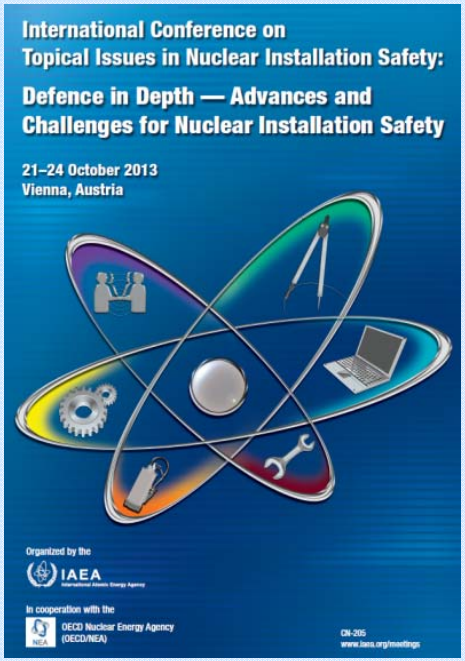
International Conference Conclusions



- Concept remains valid after the Fukushima accident
- Needs to be strengthened and applied to meet recent safety objectives such as those from recent CNS
- New and existing installations

IAEA
International Atomic Energy Agency

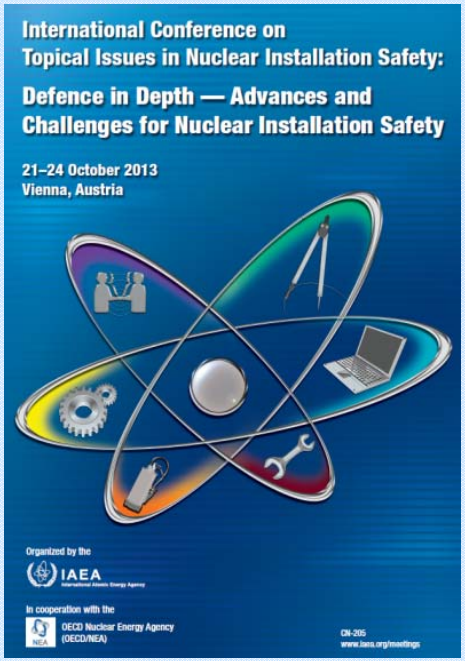
International Conference Conclusions (continued)



- Further development and guidance are required on several subjects
  - Consistent application of design basis definitions at the international level;
  - Postulation of multiple failures;
  - Practical elimination of sequences;
  - Independence and reliability of different levels of DID;
  - Common cause failures due to internal or external hazards;
  - How to deal with very low probability events leading to very large health and society consequences;
  - Tools to be based on already developed methodology.

IAEA
International Atomic Energy Agency

International Conference Conclusions (continued)

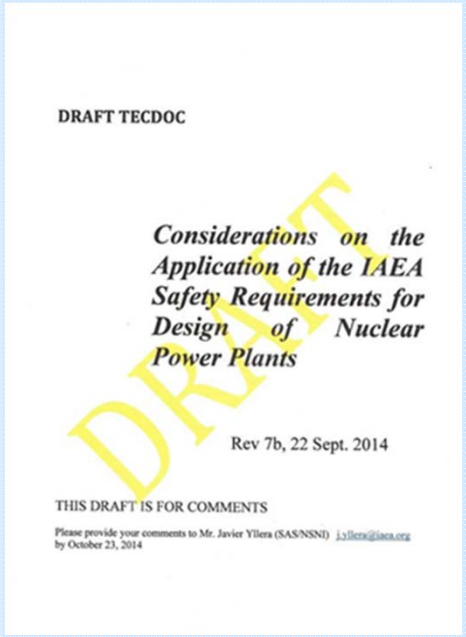


- Wider use of IAEA review services, especially those related to siting, design and emergency preparedness.
- Enhance mitigation levels of DiD in operational safety, while also maintaining prevention
- Technical concept of DiD is necessary but not sufficient to ensure safety…
- *…Effective institutional systems need to be established; applying the same DiD concept and principles, involving all stakeholders (operators, regulators, industry, etc.).*

IAEA
International Atomic Energy Agency

Current IAEA Work - IAEA Technical Document

Interpret and harmonize implementation of selected topics of SSR-2/1


DRAFT TECDOC

Considerations on the Application of the IAEA Safety Requirements for Design of Nuclear Power Plants

DRAFT

Rev 7b, 22 Sept. 2014

THIS DRAFT IS FOR COMMENTS

Please provide your comments to Mr. Javier Yllera (SAS/NSNI) j.yllera@iaea.org by October 23, 2014

IAEA
International Atomic Energy Agency

- Plant states to be considered in the design
- DECs to be included in the design
- Design basis of plant equipment versus beyond design basis
- DiD strategy for new plants - IAEA vs. WENRA
- DiD for the spent fuel pool
- Independence of the levels of DiD
- Prevention of common cause failures
- Reliability of heat transfer to the ultimate heat sink
- Design margins and cliff-edge effects
- Interpretation of the concept of practical elimination
- Design for external hazards
- Use of mobile sources of electrical power and coolant
- Acceptance criteria for different plant states

QUESTIONS?

Working to protect people, society and the environment

thank you

IAEA
International Atomic Energy Agency