Technical Meeting on Novel Designs and Safety Principles of Nuclear Power Plants

Defence in Depth approach for operational activities of NPPs

Lasse Reiman

3-6 October, 2016
Vienna, Austria
Ch. 3 Implementation of Defence in Depth

3.3 Means of achieving operational safety

- Technical specifications and operating procedures
- The human factor and training of plant personnel
- Maintenance and surveillance
  - Any intervention for maintenance, testing or modification of a safety related system is conducted in accordance with the concept of defence in depth. (71)
  - Degradation of defence in depth is prevented by careful preparation of work, evaluation of the risk, verification of the compatibility between the plant condition and the intended intervention in accordance with the technical specifications related to the system unavailability, use of qualified personnel, strict application and compliance with the prepared documentation, implementation of a requalification process. (71)
3.3 Means of achieving operational safety

- Management and safety culture
  - Safety culture is broadly relevant to all areas related to defence in depth and is particularly important for operational safety. (73)

3.4 Enhancement of safety

- Operating experience
  - Operating experience indicates the significance of events for various levels of defence in depth. (78)
  - It is of particular importance to identify events that indicate hidden deficiencies in defence, such as events with a potential for failures affecting more than one level. (80)
- 3.8 Safety assessment and verification of defence in depth
Ch. 4 Enhancement of defence in depth for plants currently operating

4.3 Human factors

• Human errors bear a potential for jeopardizing defence in depth.

• In some countries, a kind of human redundancy and diversity, with a safety engineer acting during abnormal occurrences in parallel with the operating staff, is stimulated. (113)

• With regard to the potential degradation of defence in depth, one major concern is errors of commission. They bear a considerable potential to trigger common cause failures. (115)

Ch. 5 Development of defence in depth for future nuclear power plants

• “…significant reduction in system complexity with corresponding improvement in operability, including the ability to monitor the plant and to respond to system degradation.” (116)
Human errors related to maintenance and modifications

• Several studies have been performed in Finland to identify examples of human related common cause failure mechanisms which can penetrate the operational defensive barriers and to find out the origin of the error and means to strengthen the defensive barriers, to prevent latent unavailability of the components during power operation.

• Several thousands of failure records were analysed in these studies, good quality of these records and appropriate categorisation of causes of failures is a pre-requisite.

• Most maintenance related errors stem from the outage period, some of the faults remain undetected until the power operation.

• Most important results include
  • Plant modifications seem to be an important contributor to dependent failures.
  • An enhancement of the coverage of the start-up test programs has a significant potential to reduce the consequences of dependent human errors.
  • Installation checks of maintenance actions have also a high potential to enforce the operative barriers.
  • Training of maintenance personnel could reduce the occurrence of specific maintenance related human error cases.
Human and organisational issues may influence implementation of DiD principle

Man-made disasters, Barry A. Turner (1978)

• Tries to gain an understanding of disasters and of the pre-conditions which permit their development
• During an incubation period various hidden, ambiguous or anomalous events accumulate
• The appropriate advance warning information which could be used to prevent large-scale accidents and disasters may be divided into following groups
  ▪ Completely unknown or unsuspected (not supposed to take place, in contradiction to the cultural conceptions about safety)
  ▪ Noted but not fully appreciated
    ⇒ Information not correctly perceived or fully understood
    ⇒ False sense of security or invulnerability
    ⇒ Pressure of work (or other distractions) draw their attention away from the signs of danger
    ⇒ Difficulty to separate it from a mass of irrelevant material
  ▪ Not correctly assembled
    ⇒ Information scattered among several organizations
The defence in depth concept remains valid, but implementation of the concept needs to be strengthened at all levels by adequate independence, redundancy, diversity and protection against internal and external hazards.

- All levels should be strengthened so that they are not simultaneously challenged by an external or internal hazard and are not prone to common cause failures.

- Technical Volume 2 Safety Assessment: The causes of the accident are related to the ability of organizations to detect latent flaws in the sociotechnical system.
  - “…much of this knowledge was not effectively shared among the stakeholders but only known by individual groups of people before the accident.”
IAEA, Safety Fundamentals and Requirements

• **IAEA SF-1** Fundamental Safety Principles (November 2006), Principle 8: “When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects, ..The independent effectiveness of the different levels of defence is a necessary element of the defence in depth.”

• **IAEA SSR-2/1** Safety of Nuclear Power Plants; Design, Rev.1 (March 2016)
  
  • 2.12 “This concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states.”
  
  • **Requirement 7**: “The levels of defence in depth shall be independent as far as is practicable.”
IAEA, Safety Fundamentals and Requirements

- **IAEA SSR-2/2 Safety of Nuclear Power Plants: Commissioning and Operation, Rev.1 (2016)**

- **Requirement 6:** Operational limits and conditions
  - OLCs shall ensure that the plant is operated in accordance with the design assumptions and intent. (4.6)
  - OLCs shall reflect the provisions made in the final design as described in the safety analysis report. (4.7)

- **Requirement 8:** Performance of safety related activities
  - A specific safety review for a non-routine operation or test (4.27)

- **Requirement 9:** Monitoring and review of safety performance
  - The operating organization shall establish a system for continuous monitoring and periodic review of the safety of the plant and of the performance of the operating organization.
  - In quality assurance functions sufficient authority and organizational independence to identify problems relating to quality is required (4.36)
IAEA, Safety Fundamentals and Requirements

- **Requirement 26**: Plant operations
  - Both event based approaches and symptom based approaches shall be used for EOPs, as appropriate.

- **Requirement 31**: Maintenance, testing, surveillance and inspection programmes
  - Para 8.2 The operating organization shall establish surveillance programmes for ensuring compliance with established operational limits and conditions…
  - Para 8.10 The work control system shall ensure that the plant equipment is released from service for maintenance, testing, surveillance or inspection only … in compliance with the operational limits and conditions.
  - Para 8.13 The operating organization shall ensure that maintenance work during power operation is carried out with adequate defence in depth. Probabilistic safety assessment shall be used, as appropriate, to demonstrate that the risks are not significantly increased.
IAEA, Safety Guides for Operation

• **NS-G-2.2** Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants (2000)
  
  • “When it is necessary to remove a component of a safety system from service, confirmation should be obtained that the safety logic continues to be in accordance with design provisions.” (6.6)
  
  • Appendix 1 Selection of limits and conditions for normal operation

• **NS-G-2.4** The Operating Organization for Nuclear Power Plants (2001)
  
  • Performance of safety related activities: Appropriate arrangements should be in place to ensure that safety related activities are adequately controlled. (5.13)
  
  • The operating organization should provide means for independent safety review. (5.18)

• **NS-G-2.6** Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants (2002)
  
  • Work Control: A comprehensive work planning and control system applying the defence in depth principle should be implemented. (5.14)
    
    ▪ Proposals
IAEA, Safety Guides for Operation

• **NS-G-2.14** Conduct of Operations at Nuclear Power Plants (2008)
  
  • Operating Policy: "The defence in depth concept should be generally applied to all safety related activities." (2.6)
  
  • Shift safety engineer or technical adviser: “It is recognized as a good practice that in some States …” (3.9)
  
  • Shift operations: Operating activities involving equipment and systems important to safety should be independently verified, as appropriate (4.10)
    - Equipment line-ups, positioning of components (valves, switches, circuit breakers), removal of jumpers
  
  • Shift operations: In the case of complex and or infrequently performed tasks, the shift supervisor should be involved … (4.12)

• Availability and use of operating procedures (4.21-4.22)
• System alignment (5.5-5.8)
• Control of reactivity related operations (5.21-5.25)
• Work control and authorization (Ch. 7)
Conclusions

• The **Defence in Depth for design** should be maintained during operation
  
  • In addition to maintaining the independency between different levels of DiD, it is necessary to maintain an adequate reliability of each level in all operational activities
    
    ▪ An adequate configuration of the plant should be maintained
    ▪ The OLCs should reflect the DiD principle
    ▪ Preventive maintenance during power operation should be based on risk considerations
    ▪ CCFs should be minimized
      
      ⇒ Human error related failures and their detection mechanisms should be studied
      
      ⇒ Special attention should be devoted to planning of modifications and testing after the implementation
      
      ⇒ Training of maintenance workers concerning the safety significance of their work and their specific tasks important
Conclusions

- To ensure operational safety, **Defence in Depth approach for operational activities** should be enhanced (like DiD for fire safety)
  - Safety assessment, work planning, use of procedures (checking and signing different steps in procedures), use of effective communication, use of qualified equipment, use of trained and when necessary authorized personnel, testing after maintenance and modifications, verification of correct state of equipment, configuration management, independent verifications, shift supervisor, shift safety engineer etc.
  - **A structured approach** for this is proposed
  - The approach should be emphasized and adapted as needed in the revision of IAEA Safety Guides on operational safety of NPPs
- Attention should be paid on organisational factors which may influence all levels of Defence in Depth
  - Warning signs which precede organizational failures should be observed
  - Communication patterns within and between organizations and ways of handling information should be emphasized
  - High level of safety culture shall be ensured
Defence in Depth approach for operation, levels 1-2

Levels 1 and 2

• Function A. High quality of operational activities
  • A.1 Leadership and safety culture
  • A.2 Monitoring of plant status and activities
  • A.3 Conservative decision making
  • A.4 Adequately trained competent staff using unambiguous procedures
  • A.5 Application of human performance tools (4 eye principle, 3-way communication, signing of completion of steps in procedures)
  • A.6 Maintaining the availability of DiD levels
  • A.7 Effective OEF process
  • A.8 Effective methods to assess and develop management system processes
Defence in Depth approach for operation, levels 1-2

- **Function B. Independent assessment of operational activities (inside the plant organization)**
  - B.1 Independent verification of safety status/ component status
  - B.2 Independent safety reviews/audits
  - B.3 Independent inspection/testing

- **Function C. Independent oversight of operational activities (inside the corporate organization)**
  - C.1 Independent assessment of safety status
  - C.2 Independent safety reviews

- **Function D. Independent assessment of operational activities (outside the corporate organization)**
  - D.1 Independent safety reviews
  - D.2 Independent inspection/testing
Defence in Depth approach for operation, levels 3-5

Levels 3-5

- **Function A: High quality of operational activities**
  - A.1 Leadership and safety culture
  - A.2 Monitoring of plant status and activities
  - A.3 Conservative decision making
  - A.4 Adequately trained competent staff using unambiguous procedures
  - A.5 Application of human performance tools (4 eye principle, 3-way communication, signing of completion of steps in procedures)
  - A.6 Maintaining the availability of DiD levels
Defence in Depth approach for operation, levels 3-5

- **Function B**: Independent assessment of operational activities (inside the plant organization)
  - B.1 Independent verification of safety status

- **Function C**: Independent oversight of operational activities (inside the corporate organization)
  - C.1 Independent assessment of safety status

- **Function D**: External support to analyze the plant status and support to manage the event
  - D.1 Support to analyze the plant status and to provide information to minimize the impact
  - D.2 Support with workforce to minimize the burden on plant staff
Thank you