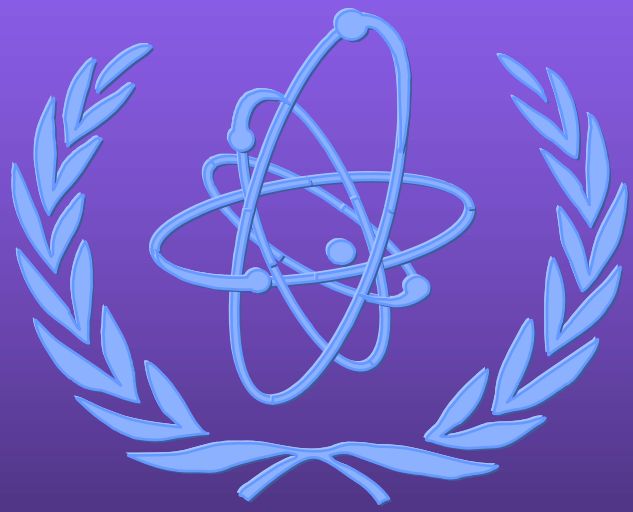
IAEA Training Course on Safety Assessment of NPPs to Assist Decision Making

Accident Sequence Analysis



Lecturer
Lesson IV 3_2.2

Workshop Information

IAEA Workshop

City , Country
XX - XX Month, Year

Accident Sequence Analysis

Contents

- Introduction to Accident Analysis
- Event Tree Development
- Event Trees/Fault Trees Link
- Modelling Techniques
- Plant Response Familiarisation
- Success Criteria
- Event Sequence End States

Introduction to Accident Analysis

- PSA provides a tool for systematic and logical modelling of accident progression including uncertainties estimation
  - Design basis accidents (DBA), BDBA, potential accidents, operating experience (near miss events)
- Starting point is to identify all initiators, i.e. initiating events (IE) of potential accidents leading to the core damage
- Next task is to model realistically how the plant is responding to such initiators
- Various accident potential progression paths are modelled in event sequences using Event Tree (ET) method
  - The selection of IEs and modelling of subsequent plant response is an iterative process

Introduction to Accident Analysis (Cont.)

- The event accident sequences consist of:
  - Initiating event (IE)
  - Safety functions mitigating given IE occurrence
  - Potential human actions to mitigate IE and resulting sequences
- Safety Functions are performed with safety systems (frontline systems, support systems, engineered safety features)
- Safety Functions may result from an automatic or manual actuation of a system, from passive system performance, or from natural feedback
- It is important that the Success Criteria of the safety functions (systems) are relevant to the identified IE and the sequence

Introduction to Accident Analysis (Cont.)

- The typical Safety Functions used in the Accident Sequence Analysis for PWRs are usually well known from the deterministic approach:
  - Reactivity control
  - Maintaining Reactor Coolant System boundary
  - Reactor Coolant System inventory
  - Decay heat removal
  - Containment integrity
- Systems must be identified fulfilling those functions as well as system minimal requirements, so called **success criteria**

Example of Safety Functions. Assignment to Individual Systems

SAFETY FUNCTION	SYSTEM
Reactor Trip	Primary RPS, Diverse RPS, control rods
Subcriticality	Emergency boration system HHI system LHI system Normal charging systems
RCS Integrity	Pressurizer PORV Pressurizer safety valves
RCS Coolant System Inventory	Accumulators HHI system LHI system Normal charging system

Introduction to Accident Analysis (Cont.)

- All identified dependency types should be modelled adequately
  - The dependencies of safety systems with the initiating event
  - Common Cause Failures (CCF)
  - Functional dependency on other systems, components or operator actions
  - Environmental dependencies
- Human actions might recover the operation of a failed safety function and they should be modelled, where applicable, to avoid unnecessary conservatism

Event Tree Development

- Event trees (ET) model the response of the plant to an IE
- The IE is usually defined as an event that creates disturbance in the plant and has potential to lead to the core damage (depending on the operation of mitigating systems)
- IE often lead to a demand for reactor scram (full power), but some IEs may lead directly to core damage (e.g. some external events, reactivity accidents, etc.)
  - In shutdown the IEs are usually defined as events that may lead to loss of fuel cooling, such as loss of RHR, LOCA and draindown events, Loss of SFP cooling, drops of heavy loads, etc.)
- IEs with a similar plant response and success criteria for mitigating safety functions can be grouped together and modelled in the same ET (e.g. LOCAs)

Event Tree Development (Cont.)

- The initiators are grouped together in order to facilitate the use of PSA and to reduce the number of required ETs
- Major IE groups categories:
  - Loss of Coolant Accidents (LOCA)
  - Transients
  - Steam/Feedwater line breaks
  - Loss of Off-Site Power (LOSP)
  - Support systems failures (CCI), e.g.
    - I&C failure events
    - power supply failure events
    - service water failure events
    - loss of ventilation system events
  - CCF events (e.g. multiple equipment actuation due to CCF)

Event Tree Development (Cont.)

- The **Event Trees** are graphic models that order and reflect events according to safety functions and systems success criteria for each initiating event group
- ETs are graphical representations of Boolean algebra equations
- The **Event Tree headings** are normally arranged in chronological or causal order
- These headings (TOPs) represent IE and “events”, which failures or successes define the way of accident sequence progression and may include:
  - safety functions
  - front-line systems, systems trains or specific equipment
  - human errors

Event Tree Development (Cont.)