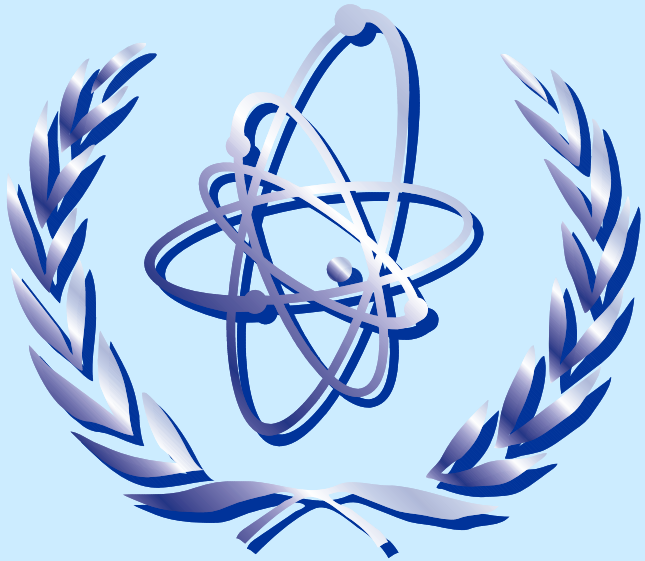
Basic Level 1. PSA course for analysts



Accident Sequence modelling

Content

- Event tree modelling
- Special aspects of scenario development
- Operator actions in the accident sequence
- Treatment of dependencies in the accident sequence
- Experience from reviews

Event Trees

- DISPLAY SEQUENCE PROGRESSION
- DISPLAY SEQUENCE END STATES
- DISPLAY SEQUENCE-SPECIFIC DEPENDENCIES
  - PHYSICAL (SYSTEMS)
  - FUNCTIONAL (SUCCESS CRITERIA)
  - HUMAN
- IMPROVED UNDERSTANDING OF MODELS
  - ANALYSTS / USERS
  - PLANT PERSONNEL
  - REVIEWERS

TRANSIENT-INDUCED IMPACTS

- LOCAs
  - PRIMARY OVERPRESSURE
  - REACTOR COOLANT PUMP SEAL FAILURE
  - MAKEUP / LETDOWN
- OVERCOOLING
  - SECONDARY OVERPRESSURE
  - STUCK-OPEN RELIEF / SAFETY VALVES
- ATWS
- OPERATOR ACTIONS

TRANSIENT-INDUCED LOCAs

- ADD TO LOCA INITIATING EVENT FREQUENCY
  - LOSE ACTUAL INITIATING EVENT INFORMATION
  - LOSE DEPENDENCIES
  - SIMPLIFIED EVENT TREES
  - SIMPLIFIED SYSTEM MODELS

- ADD SEPARATE EVENT TREE TOP EVENT
  - RETAIN DEPENDENCIES
  - EVENT TREES MORE COMPLEX
  - INTERFACE WITH SYSTEMS MORE COMPLEX
  - BETTER UNDERSTANDING OF MODELS / RESULTS

OVERCOOLING SCENARIOS

- PRESSURIZED THERMAL SHOCK (PTS)
  - MAY BE SIGNIFICANT PLANT-SPECIFIC PROBLEM
  - WELD MATERIAL
  - DOCUMENTATION
  - INSPECTIONS
- AUTOMATIC SIGNALS
  - SECONDARY ISOLATION (STEAM AND/OR FEED)
  - SAFEGUARDS ACTUATION
  - AFFECT SEQUENCE PROGRESSION
  - AFFECT AVAILABLE SYSTEMS

ATWS SCENARIOS

- REACTOR SHUTDOWN SUCCESS CRITERIA
- SIGNAL FAILURES (REACTOR PROTECTION SYSTEM)
- MECHANICAL FAILURES (CONTROL RODS)
- ALTERNATE SHUTDOWN OPTIONS
  - TIME WINDOW
  - SUCCESS CRITERIA
  - AVAILABLE SYSTEMS
  - OPERATOR ACTIONS

ATWS MODELS

- CORE NUCLEAR POWER
- PRIMARY / SECONDARY ENERGY BALANCE
- FEEDWATER SUCCESS CRITERIA
- PRIMARY PRESSURE RESPONSE
- ENERGY RELEASE INTO CONTAINMENT

OPERATOR ACTIONS AFTER INITIATING EVENT

- ACTIONS REQUIRED BY EMERGENCY OPERATING PROCEDURES
- USE OF ALTERNATE EQUIPMENT
- REALIGNMENT OF SYSTEMS
- MANUAL BACKUP TO AUTOMATIC SIGNALS
- REPAIR / RECOVERY OF FAILED EQUIPMENT
- NO FUNDAMENTAL DIFFERENCE BETWEEN "PROCEDURE-DIRECTED" ACTIONS AND "RECOVERY" ACTIONS

MODELLING PROCESS

- DEFINE THE ACTION
- ADD THE ACTION TO THE PSA LOGIC MODELS
- EVALUATE THE LIKELIHOOD OF HUMAN ERROR

DEFINE THE ACTION

- SUCCESS CRITERIA
- BOUNDARY CONDITIONS
- TIMING

SUCCESS CRITERIA

- WHAT IS THE OPERATOR REQUIRED TO DO?
- HOW MANY OPERATORS ARE REQUIRED?
- WHAT LEVEL OF OPERATOR SKILL OR TRAINING IS REQUIRED?
- WHERE MUST THE ACTION BE PERFORMED?

BOUNDARY CONDITIONS

- WHAT IS THE INITIATING EVENT?
- WHAT PRECEDING SYSTEM FAILURES (OR SUCCESSES) HAVE OCCURRED?
- WHAT PRECEDING OPERATOR ACTIONS HAVE OCCURRED?

TIMING

- WHEN IS THE ACTION REQUIRED?
- HOW MUCH TIME IS AVAILABLE TO COMPLETE THE ACTION?
- HOW LONG DOES IT TAKE TO COMPLETE THE ACTION?

GENERAL RECOMMENDATIONS

- EVALUATE EACH ACTION IN CONTEXT OF FUNCTIONALLY SIMILAR SCENARIOS
  - INITIATING EVENT
  - TIME WINDOW FOR OPERATOR RESPONSE
  - PRECEDING SYSTEM SUCCESSES AND FAILURES
  - PRECEDING OPERATOR SUCCESSES AND FAILURES
  - PROCEDURAL GUIDANCE AND TRAINING
- BEWARE OF INDEPENDENT COMBINATIONS OF OPERATOR ACTIONS IN EVENT TREES AND/OR FAULT TREES

PROBLEM DEFINITION

- DEFINE SCOPE AND CONTEXT OF OPERATOR ACTIONS DURING EARLY DEVELOPMENT OF PSA MODELS
- INITIATING EVENT GROUPS
- FUNCTION AND SYSTEM SUCCESS CRITERIA
- IDENTIFY WHERE OPERATORS MUST CONTROL FUNCTIONS AND SYSTEMS
- BE AWARE OF PSA SCOPE (LEVEL 1 / LEVEL 2)

PROBLEM DEFINITION

- SPECIFY OPERATOR ACTIONS IN TERMS OF HIGH-LEVEL FUNCTIONAL DESCRIPTIONS
  - START BLEED AND FEED COOLING (PWR)
  - DEPRESSURIZE REACTOR (BWR)
  - ALIGN HIGH PRESSURE RECIRCULATION (PWR/BWR)
  - OPEN CONTAINMENT VENT (LEVEL 2)
- DETAILED ACTIONS DETERMINED BY CONTEXT OF PSA MODELS

BREAKDOWN AND IMPACT ASSESSMENT

- DETERMINE HOW PROCEDURES DIRECT OPERATOR RESPONSE
  - SYMPTOM-BASED VS. EVENT-BASED PROCEDURES
  - OPTIONS DEPEND ON PLANT STATUS
- DETERMINE HOW OPERATOR RESPONSE AFFECTS EVENT PROGRESSION
  - SUCCESSFUL PERFORMANCE OF PROCEDURAL GUIDANCE
  - FAILURE TO PERFORM PROCEDURAL GUIDANCE
  - POSSIBLE ALTERNATE ACTIONS

BREAKDOWN AND IMPACT ASSESSMENT

- IDENTIFY SPECIFIC ACTIONS THAT MAY HAVE A SIGNIFICANT IMPACT ON PLANT STATUS AND EVENT PROGRESSION
- UNDERSTAND HOW MONITORED PARAMETERS AND ALARMS CHANGE WITH PLANT STATUS AND TIME
- IDENTIFY CONDITIONS THAT ARE NOT CONSISTENT WITH NORMAL PROCEDURAL ASSUMPTIONS
  - INITIATING EVENT
  - EQUIPMENT FAILURES
  - PRECEDING ERRORS

PSA MODEL INTEGRATION

- OPERATOR ACTIONS MUST ACCOUNT FOR SCENARIO-SPECIFIC DEPENDENCIES
  - TIME WINDOW FOR RESPONSE
  - HARDWARE AVAILABILITY
  - PRIOR OPERATOR ACTIONS
- IDENTIFY POTENTIAL COGNITIVE DEPENDENCIES BETWEEN MULTIPLE ACTIONS WITHIN A SCENARIO

DEFINITION OF OPERATOR ACTION FOR PSA QUANTIFICATION

- IDENTIFY SPECIFIC APPLICABLE SCENARIOS
  - INITIATING EVENTS
  - FUNCTIONAL SCENARIO PROGRESSION
  - HARDWARE AVAILABILITY
- TIME WINDOW FOR RESPONSE
- CUE-RESPONSE STRUCTURE
- PROCEDURE DIRECTIONS
- DEPENDENCIES WITH OTHER ACTIONS

HUMAN ACTION DEPENDENCIES

- COGNITIVE DEPENDENCIES
  - COMMON AREAS - MULTIPLE ACTIONS INITIATED BY A SINGLE CUE
  - COMMON GOALS - MULTIPLE POSSIBLE ACTIONS TO ACHIEVE THE SAME FUNCTION
  - COMMON TRAINING AND EXPERIENCE
- TIME AVAILABILITY
  - SEQUENTIAL OR COORDINATED ACTIONS LIMITED BY TIME
  - PARALLEL ACTIONS LIMITED BY MANPOWER

EXAMPLE: TWO MANUALLY-INITIATED FUNCTIONS

- CORE DAMAGE OCCURS ONLY IF BOTH FUNCTIONS FAIL
- FUNCTION A: HARDWARE A (HDWA) + OPERATOR ACTION A (OPA)
- FUNCTION B: HARDWARE B (HDWB) + OPERATOR ACTION B (OPB)
- FUNCTION A "PREFERRED", FUNCTION B "ALTERNATE"
- NOMINAL VALUES:

HDWA	=	5.0E-04
HDWB	=	2.0E-03
OPA	=	1.0E-03
OPB	=	1.0E-02

Accident Sequence modelling

EXAMPLE: ASSUMED COMPLETE INDEPENDENCE (GENERALLY INCORRECT)

- **FOUR INDEPENDENT CUTSETS:**

HDWA * HDWB	=	1.0E-06
HDWA * OPB	=	5.0E-06
OPA * HDWB	=	2.0E-06
OPA * OPB	=	1.0E-05

- **CORE DAMAGE FREQUENCY: 1.8E-05**

EXAMPLE:
COMPLETE DEPENDENCE (POSSIBLE FOR SOME SCENARIOS)

- IF OPERATORS FAIL TO PERFORM "PREFERRED" ACTION OPA, THEY WILL ALWAYS FAIL TO PERFORM "ALTERNATE" ACTION OPB
- ONE FUNCTIONAL ACTION: OPA = OPB = OP
- TWO CUTSETS:

HDWA * HDWB	=	1.0E-06
OP	=	1.0E-03

- CORE DAMAGE FREQUENCY: 1.0E-03

EXAMPLE: PARTIAL DEPENDENCE (MOST TYPICAL CASE)

- IF OPERATORS FAIL TO PERFORM "PREFERRED" ACTION OPA, IT IS MORE LIKELY THAT THEY WILL ALSO FAIL TO PERFORM "ALTERNATE" ACTION OPB

- THREE FUNCTIONAL ACTIONS:

OPA (NOMINAL ACTION)	1.0E-03
OPB1 (AFTER SUCCESS OF OPA)	5.0E-03
OPB2 (AFTER FAILURE OF OPA)	1.0E-01

EXAMPLE:
PARTIAL DEPENDENCE (MOST TYPICAL CASE)

- **FOUR CORRELATED CUTSETS:**

HDWA * HDWB	=	1.0E-06
HDWA * OPB1	=	2.5E-05
OPA * HDWB	=	2.0E-06
OPA * OPB2	=	1.0E-04

- **CORE DAMAGE FREQUENCY: 1.1E-04**

Accident Sequence modelling

ADD THE ACTION TO THE PSA LOGIC MODELS

- REVIEW EVENT TREES AND FAULT TREES TO IDENTIFY DIFFERENT RESPONSE SCENARIOS
- GROUP SCENARIOS ACCORDING TO SIMILAR EFFECTS ON OPERATOR RESPONSE
- DEFINE SEPARATE OPERATOR ACTIONS (TOP EVENTS, SPLIT FRACTIONS, BASIC EVENTS) FOR EACH GROUP OF SCENARIOS
- AVOID DIRECT COMBINATION OF OPERATOR ACTIONS WITH SYSTEM HARDWARE FAILURES
- MODELS MUST ACCOUNT FOR DEPENDENCIES IN SCENARIOS THAT INCLUDE MULTIPLE ACTIONS

ACTIONS IN FAULT TREES: EVENT TREE LOGIC

A = OPA + (1-OPA) * (HDWA)

B = OPB + (1-OPB) * (HDWB)

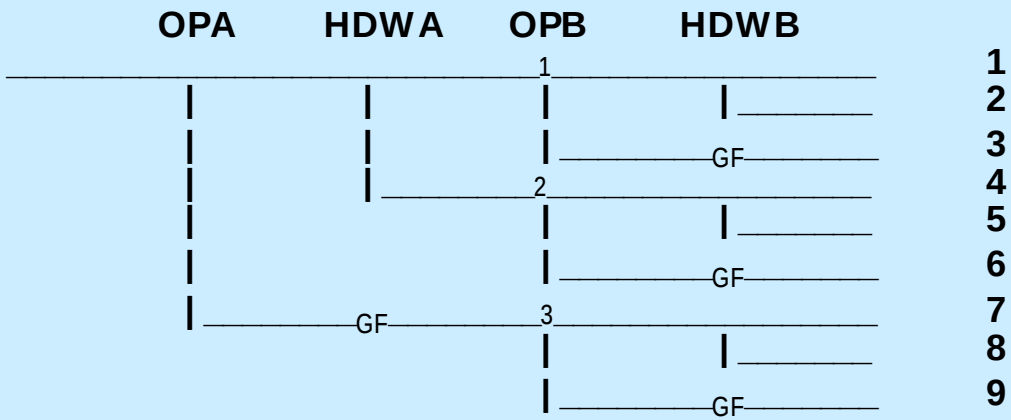
ACTIONS IN FAULT TREES: SEQUENCE RESULTS

SEQUENCE	CUTSET FORM	EXPANDED FORM
1	1 - (OPA + HDWA + OPB + HDWB)	1 - OPA - (1-OPA)*(HDWA) - OPB - (1-OPB)*(HDWB) + (OPA)*(OPB) + (OPA)*(1-OPB)*(HDWB) + (1-OPA)*(HDWA)*(OPB) + (1-OPA)*(HDWA)*(1-OPB)*(HDWB)
2	OPB + HDWB	OPB + (1-OPB)*(HDWB) - (OPA)*(OPB) - (1-OPA)*(HDWA)*(OPB) - (OPA)*(1-OPB)*(HDWB) - (1-OPA)*(HDWA)*(1-OPB)*(HDWB)
3	OPA + HDWA	OPA + (1-OPA)*(HDWA) - (OPA)*(OPB) - (1-OPA)*(HDWA)*(OPB) - (OPA)*(1-OPB)*(HDWB) - (1-OPA)*(HDWA)*(1-OPB)*(HDWB)
4	(OPA)*(OPB) + (HDWA)*(OPB) + (OPA)*(HDWB) + (HDWA)*(HDWB)	(OPA)*(OPB) + (1-OPA)*(HDWA)*(OPB) + (OPA)*(1-OPB)*(HDWB) + (1-OPA)*(HDWA)*(1-OPB)*(HDWB)

ACTIONS IN FAULT TREES

- ADVANTAGES
  - SIMPLER EVENT TREES
- DISADVANTAGES
  - MORE COMPLEX FAULT TREES
  - MORE DIFFICULT FOR ANALYSTS TO IDENTIFY SCENARIO-SPECIFIC DEPENDENCIES
  - HOUSE EVENTS OR SPECIAL LOGIC TO DEFINE CONDITIONS FOR CORRECT ACTIONS
- GENERAL EXPERIENCE FROM REVIEWS
  - POOR TREATMENT OF OPERATOR ACTIONS
  - OPTIMISTIC QUANTIFICATION OF COMBINED ERRORS

ACTIONS IN EVENT TREES: EVENT TREE LOGIC



"GF" DENOTES SYSTEM FAILURE IF OPERATOR ACTION FAILS

ACTIONS IN EVENT TREES: SEQUENCE RESULTS

SEQUENCE	CUTSET FORM	EXPANDED FORM
1	1 - (OPA + HDWA + OPB1 + HDWB)	(1 - OPA)*(1 - HDWA)*(1 - OPB1)*(1 - HDWB)
2	HDWB	(1 - OPA)*(1 - HDWA)*(1 - OPB1)*(HDWB)
3	OPB1	(1 - OPA)*(1 - HDWA)*(OPB1)
4	HDWA	(1 - OPA)*(HDWA)*(1 - OPB2)*(1 - HDWB)
5	HDWA * HDWB	(1 - OPA)*(HDWA)*(1 - OPB2)*(HDWB)
6	HDWA * OPB2	(1 - OPA)*(HDWA)*(OPB2)
7	OPA	(OPA)*(1 - OPB3)*(1 - HDWB)
8	OPA * HDWB	(OPA)*(1 - OPB3)*(HDWB)
9	OPA * OPB3	(OPA)*(OPB3)

ACTIONS IN EVENT TREES

- ADVANTAGES
  - SIMPLER FAULT TREES
  - EASIER FOR ANALYSTS TO IDENTIFY SCENARIO-SPECIFIC DEPENDENCIES
- DISADVANTAGES
  - MORE COMPLEX EVENT TREES
  - BRANCH POINT CONDITIONS TO DEFINE CORRECT ACTIONS
- GENERAL EXPERIENCE FROM REVIEWS
  - IMPROVED TREATMENT OF OPERATOR ACTIONS
  - REALISTIC QUANTIFICATION OF COMBINED ERRORS

EXPERIENCE FROM REVIEWS

- POOR TREATMENT OF OPERATOR ACTION DEPENDENCIES IS THE MOST IMPORTANT SOURCE OF PROBLEMS IN HRA RESULTS
- "CONSERVATIVE SCREENING ERROR RATES" DO NOT NECESSARILY SOLVE THE PROBLEM
- CUTSET EDITING AND POST-QUANTIFICATION "FIXES" ARE OFTEN INCOMPLETE
- CANNOT EXAMINE CUTSETS THAT ARE OPTIMISTICALLY ELIMINATED BY NUMERICAL CUTOFF VALUES

EXPERIENCE FROM REVIEWS

- EXTREMELY DIFFICULT TO IDENTIFY DEPENDENCIES BY EXAMINATION OF FAULT TREES
  - ACTIONS DISTRIBUTED AMONG SEVERAL TREES
  - NO INFORMATION ABOUT SEQUENCE PROGRESSION
- DIFFICULT TO IDENTIFY DEPENDENCIES BY EXAMINATION OF CUTSETS
  - FUNCTIONAL IMPACTS FROM SEQUENCE
  - TIME LIMITATIONS FROM SEQUENCE PROGRESSION
  - HUMAN COGNITIVE DEPENDENCIES
- ANALYSTS RECOGNIZE AND CORRECTLY ACCOUNT FOR DEPENDENCIES IF THEY ARE CLEARLY DISPLAYED