PSA Scenario Modeling and Representation - a view based on dynamic PSA research

V.N. Dang

Risk and Human Reliability Group
Laboratory for Energy Systems Analysis

PSA Software Workshop
"Next Generation PSA Software, Declarative Modeling, and Model Representation Standards"

KKG, Switzerland
June 12, 2007

Presentation Outline

- Some issues for PSA
- Dynamic PSA
  - Accident dynamics
  - The dynamic event tree
- Implications for PSA software, model portability and representation

Some issues for PSA

- Uncertainties
  - ☑ aleatory and epistemic
- Human Reliability Analysis
  - ☑ decision-making performance
  - ☑ errors of commission

Also

- Procedure verification in PSA scenarios
- Digital systems (I&C) safety

Aleatory and Epistemic Uncertainties

Definitions:

- Aleatory: random or stochastic effects
  - ☑ e.g. hardware performance (e.g. failure to start, to open, close)
  - ☑ operator interventions
- Epistemic: state-of-knowledge
  - ☑ parameter uncertainty (TH coefficients, etc, **as well as** failure probabilities)
  - ☑ establishment of natural circulation
  - ☑ material behavior
  - ☑ severe accident phenomena
    - – for some events and behaviors (e.g. last examples), the distinction is not clear-cut. Some events involve both types of uncertainties

Human Reliability Analysis

- ➢ Decision-making performance
  - ☑ diagnosis failure probabilities, initially represented by Time Reliability Curves (TRCs, e.g. THERP curves: HEP vs. available time)
    - – this model (and variants) continues to dominate HRAs, mainly due to lack of alternatives
  - ☑ less emphasis on time as the main driving factor
    - – SLIM performance shaping factors (but calibration values required to "complete" the method)
    - – CREAM, INEL's SPAR-H
  - ☑ **ultimately, two questions**
    - – what factors should drive estimates of decision-making failures?
    - – what about other decisions, i.e. errors of commission?

Analyzing Errors of Commission (EOCs)

performance of any inappropriate action that aggravates the situation

Compare *omissions*: failure to perform a required action

Identification

- What are plausible EOC situations?

  How do we search efficiently, given that an aggravating action can potentially take place any time, in connection to any system?

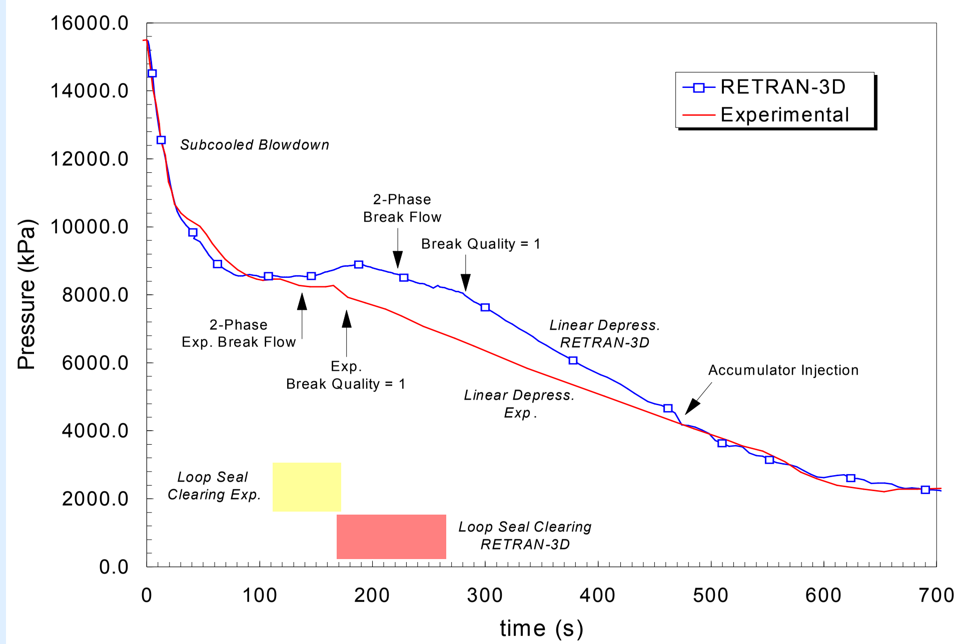
- Number of methods have emerged: MERMOS, ATHEANA, MDTA, CESA

Quantification

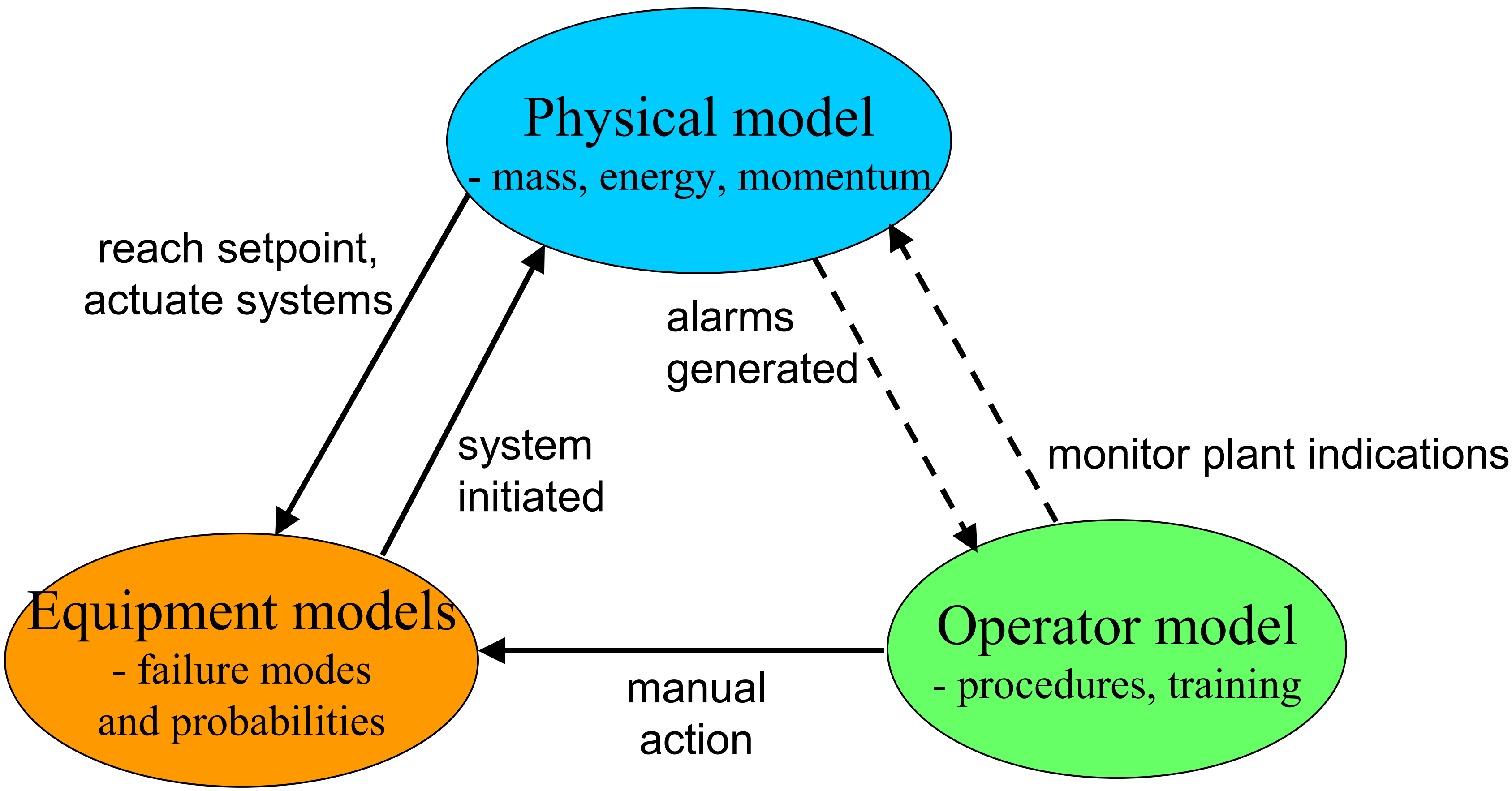
- Contexts where the EOC corresponds to the nominal, expected operator response, also referred to as "error-forcing".
  - Once identified, can be handled
- Situations where the decision is more "uncertain" are more difficult.
  - Time pressure plays a role but a time reliability approach does not seem workable. Need to characterize "attractiveness" of multiple options
- Once EOC is performed, need to assess the probability of correction
  - Function of cues and time window

Accident Scenarios – What dynamics, What interactions?

- **thermal-hydraulics and physics** : P, T, energy balances
  - ☑ heat removed during blowdown
  - ☑ amount of lost coolant
  - ☑ maximum temperatures
- **automatic system actions**
  - ☑ initiation and termination of systems
  - ☑ active and passive
- **operator actions** : procedures and training
  - ☑ initiation, termination, throttling
  - ☑ inhibit, reset, override
- **equipment failures**
  - ☑ to start (and while running)
  - ☑ cycling
  - ☑ support systems



Dynamic interactions in accident scenarios



Accident scenario analysis

➢ For design basis calculations

- ☑ Defined, bounding scenarios
- ☑ Few cases for each initiating event
- ☑ 0-1 operator actions in first 30 minutes, 1-3 subsequently
- ☑ Conservative scenarios

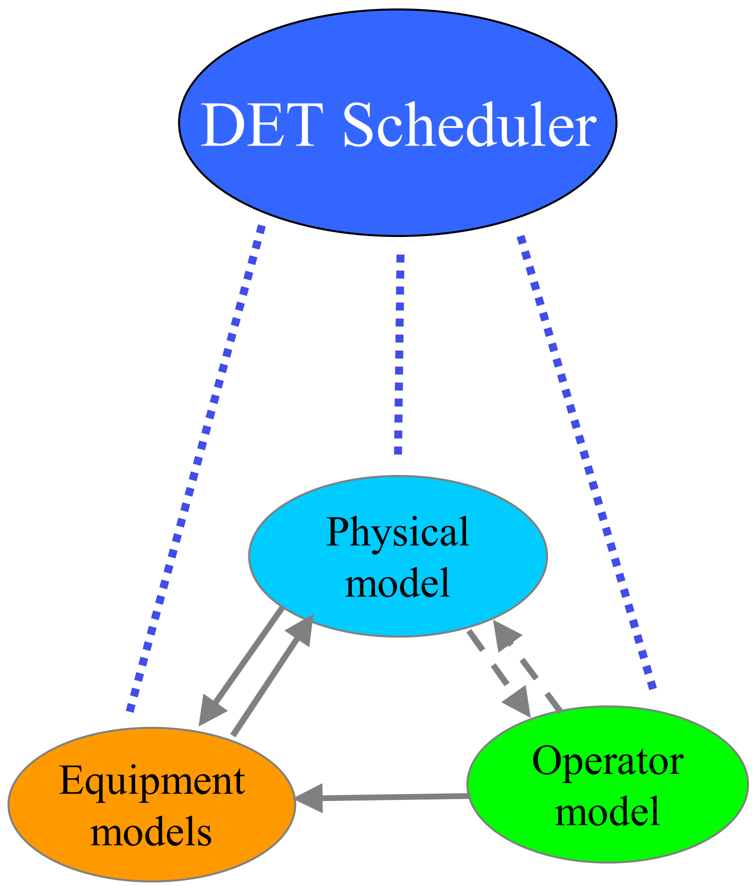
➢ For PSA

- ☑ Consider multiple failures and probabilities of scenarios
- ☑ Calculation of success criteria: minimum number of systems, minimum time of operation, latest time for interventions
- ☑ 2-6 cases per initiating event, supplemented by bounding calculations

➢ Integrated deterministic/probabilistic analysis

- ☑ Integration of deterministic (accident evolutions) and probabilistic perspectives (account for likelihood of failure events and distributions of occurrence times)
- ☑ Especially relevant for advanced and future reactor and plant designs (no artifacts from the “design basis” approach)

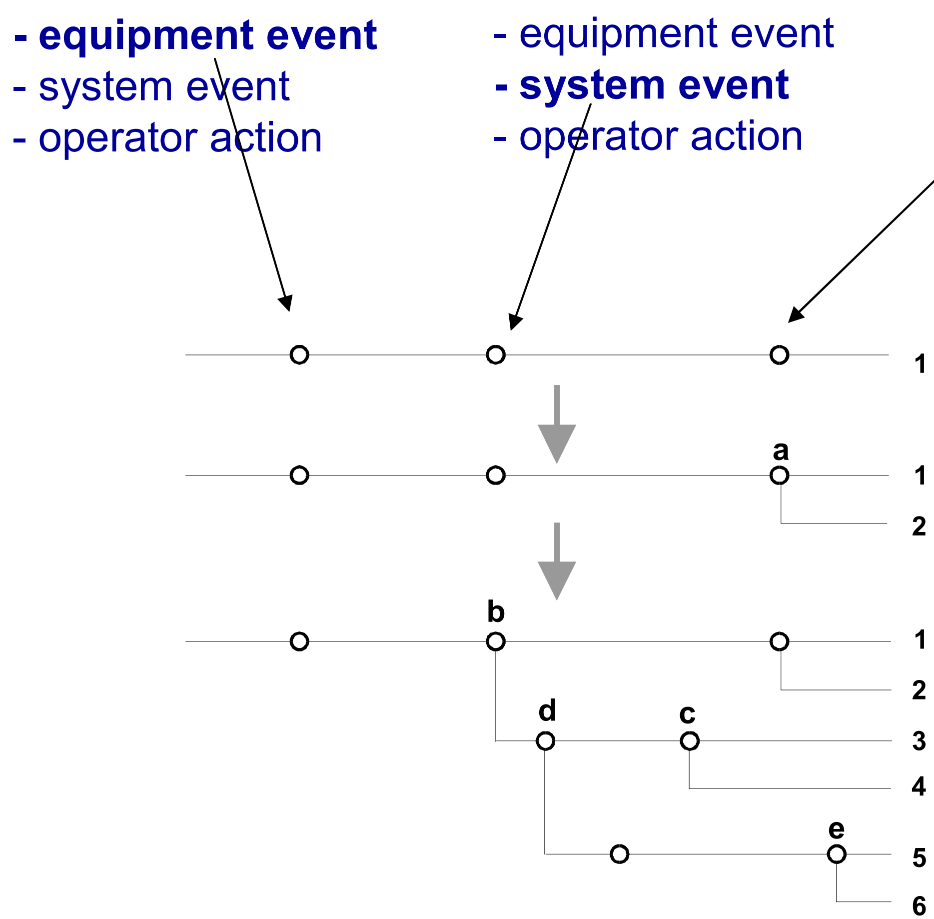
Dynamic event trees – a framework for solving probabilistic dynamics



Functions of the scheduler

- advance physical model solution
- respond to model events
  - ☑ setpoints and alarms
  - ☑ equipment demands
  - ☑ running failures
  - ☑ monitoring and manipulations
- question probabilistic events (equipment failures)
- set physical model boundary conditions
- probability accounting, truncation in background

The Discrete Dynamic Event Tree (DDET)



Coupled models of

- plant dynamics and control
- equipment availability, and
- operator response

determine...

- type of event
- time of event
- probability of event

Application of DET to a PRA level 2 problem (MCDET)

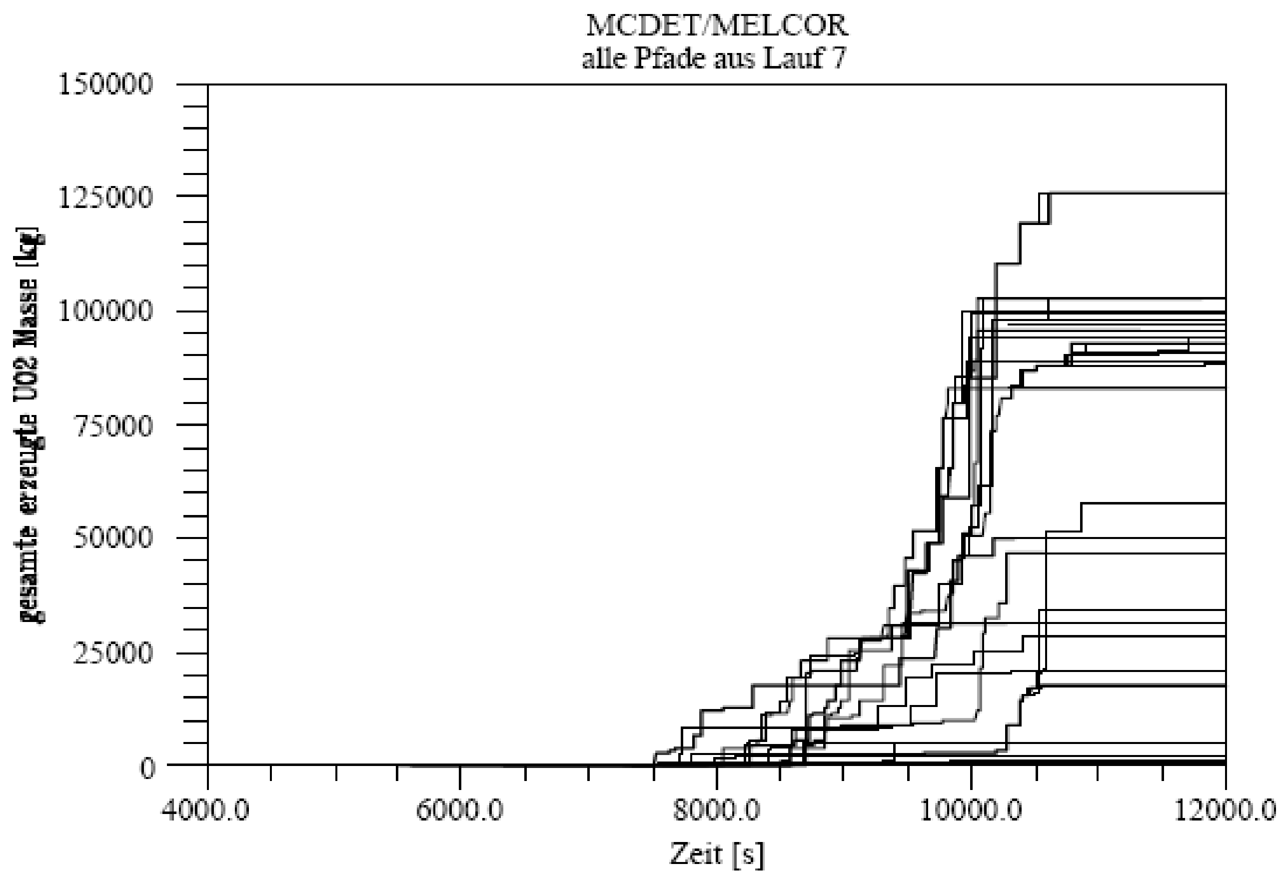
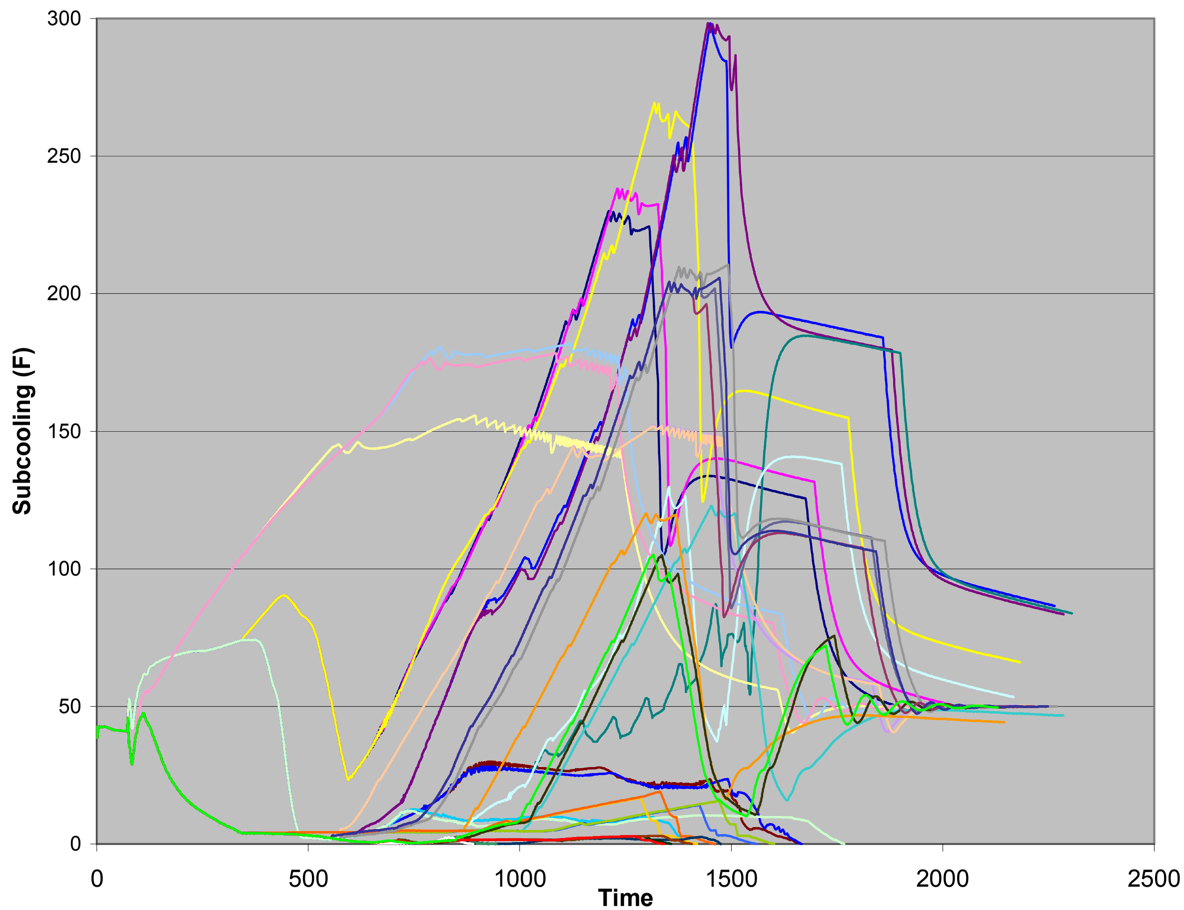


Fig. 4: Dynamic event tree no. 7 of the sample presented in the time/state plane for the state variable "total generated UO_2 melt mass"

Hofer et al, 2002 (Eurosafe)

DET Results

Subcooling Margin in SGTR Sequences



36 Sequences

- ❑ **MSIVs open/closed**
- ❑ **HPI automatic start**
- ❑ **HPI manually started**
  - based on training
  - guided by procedure
- ❑ **variability in timing of operator response**

Conclusions (1 of 2)

- A number of different PSA issues motivate a dynamic PSA approach.
  - accident evolutions
    - in severe accident space (Level 2 PSA, e.g. passive components, creep rupture)
    - effect of partial failures, timing of failures on success criteria (Level 1)
  - analysis of decision-making and EOCs in Human Reliability Analysis
  - verification of procedures in PSA scenario space
- Large parts of the PSA continue to drive system unavailability and are therefore needed
  - support system dependencies
  - component failure data
  - common cause failures
  - latent system failures
  - maintenance and test unavailabilities

Conclusions (2 of 2)

- In extending the safety analysis towards dynamic PSA, there is a motivation to re-use the models from existing PSAs
  - large models, fortunately relatively stable
  - quality-controlled
  - re-use allows comparison with “classical” ET/FT analysis
- Portability and clarity of the models and data compatibility are major issues.
- Besides supporting next generation calculation engines and user interfaces, progress along these lines will be crucial to the development of dynamic PSA
  - as software
  - as an analysis framework