Discrete Dynamic Event Trees for Probabilistic Safety Assessment of Nuclear Power Plants

Davide Mercurio

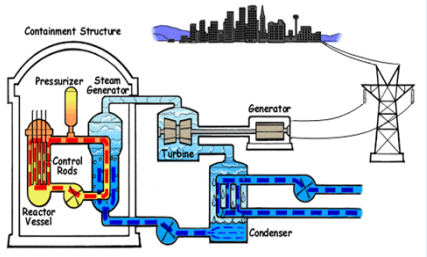
ETH Zürich, May 3rd, 2011

Outline

- Overview of Nuclear Power Plants (NPPs)
- Risk Analysis & Probabilistic Safety Assessment (PSA) Level 1, 2, & 3
  - Fault Tree and Event Tree Approach
    - Use and limitation
- Discrete Dynamic Event Trees (DDETs)
  - Description
  - Applications to PSA
- DDET to support PSA, HRA, & other applications
- Take home messages

NPP overview

NPP (PWR)

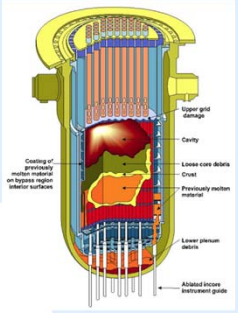


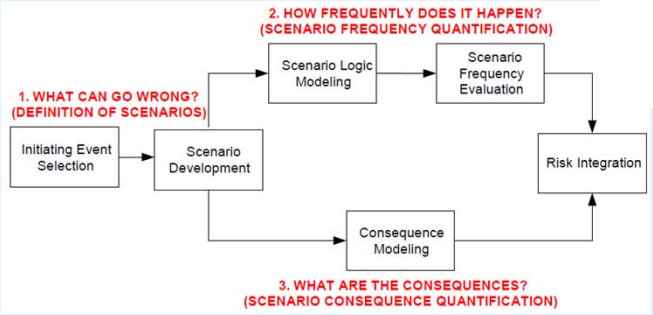
Control Room

- Based of concept of **defense-in-depth**
  - multiple, redundant, and independent layers of safety systems
- If **accident**, goal is to lead system in safe conditions
  - automatic systems & control room operators

Risk Analysis

- **Risk**
  - What can go wrong?
  - How likely is it?
  - What are the consequences?





Probabilistic Risk Assessment Procedures Guide for NASA managers and Practitioners, Office of Safety and Mission Assurance NASA Headquarters Washington, DC 20546

Probabilistic Safety Assessment

- Approach to risk analysis: Probabilistic Risk/Safety Assessment
  - identify the possible accident sequences
  - quantify their probabilities and consequences

- PSA is a multilevel analysis technique in respect of the multiple-barrier principle

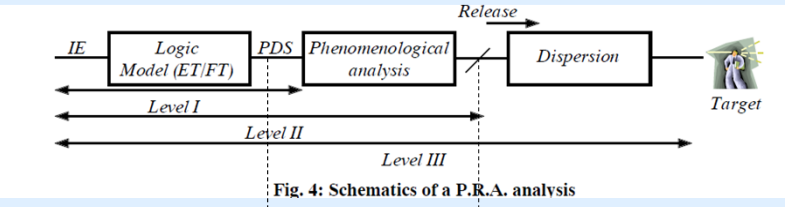


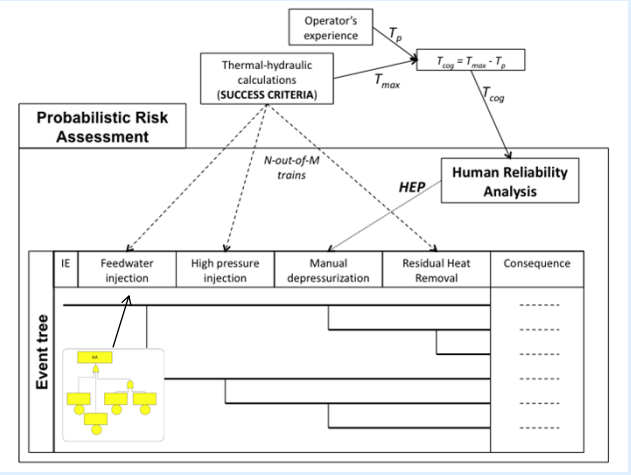
Fig. 4: Schematics of a P.R.A. analysis

Core damage

Containemnt failure

Event Trees and Fault Trees

- PSA Level 1 framework

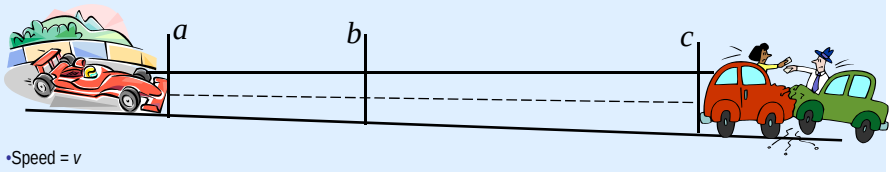


Classical PSA

- Classical PSA is a quasi-static approach
  - Analysis is based on a few thermal-hydraulic calculations
    - Chosen for the most conservative/limiting case by expert
  - Limited evaluation of the effects of the variability of system and operator responses
- In a quasi-static approach is difficult to address:
  - Variability of time & variability of strategies → alternative ways of succeeding
  - Variability of system response
  - Plant effect on crew performance and the vice versa
  - Interactions between them

Dynamic approach!

Example: car accident



•Speed = *v*

•Classical approach:

- Minimum distance (*b*) to avoid accident & available time (t_{ab})?
  - Success: at *b* at *v* and 100% braking
  - Failure: too late or <100% braking or no action → no action

•Dynamic approach:

- What does the pilot do? What does he see? What is his decision?
- What is the distribution of responses? If response, what braking force is selected?

Model calculates the speed at *c* → *evaluate the consequences*

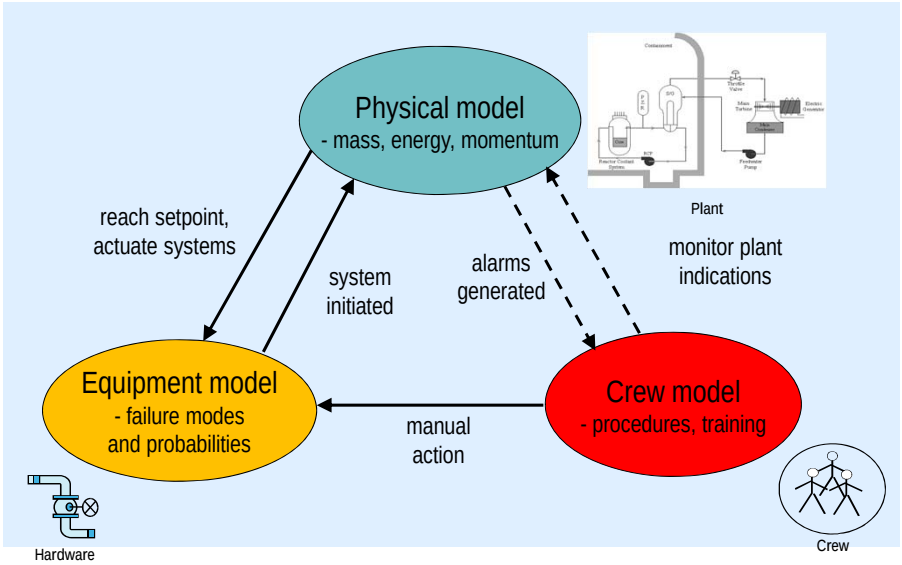
Road conditions
Tire conditions
Vehicle type …

Dynamic Approach

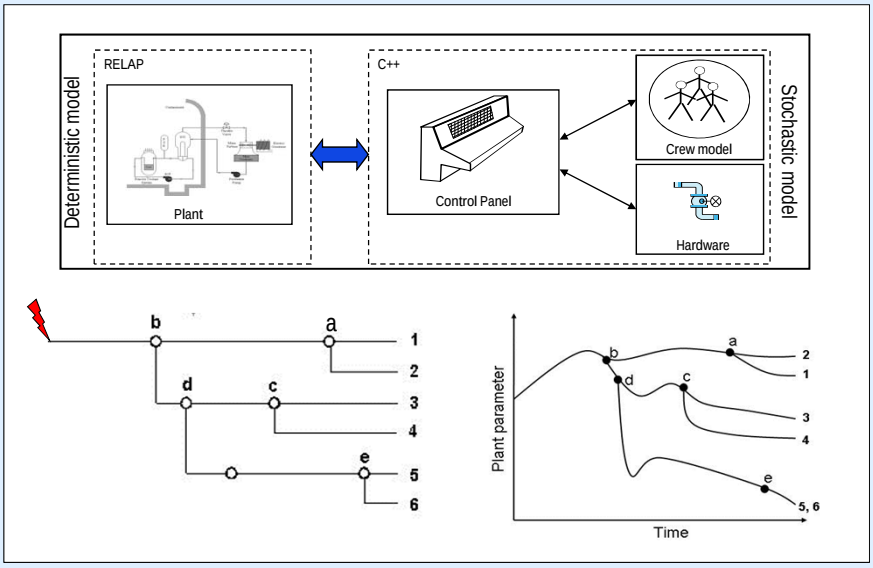
- Attempt to integrate **deterministic** and **stochastic processes**
- Explicitly model the **plant-crew interactions**
- Give **variability** to these interactions
- Model the evolution of the **operator understanding**

DDET as a mean for dynamic approach!

Dynamic Event Tree – the interacting models

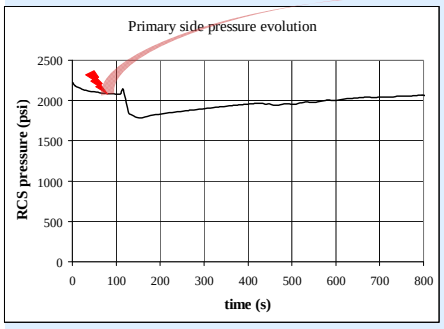


DDET framework



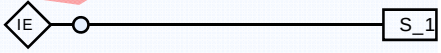
Dynamic Event Tree evolution

- Parameter evolution



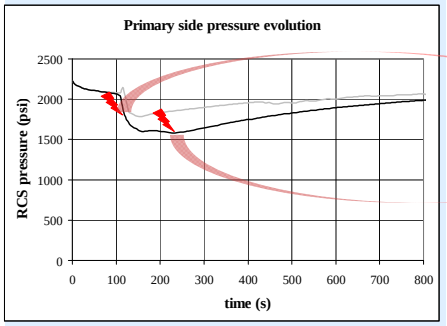
- At each branching point all the parameters are saved in memory

- DET

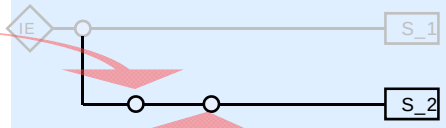


Dynamic Event Tree evolution

•Parameter evolution

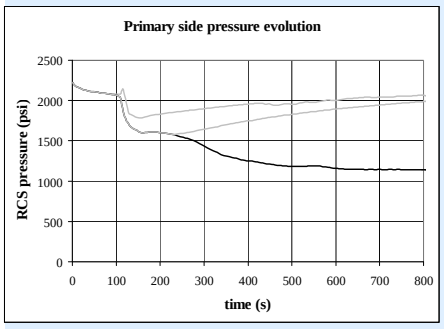


•DET

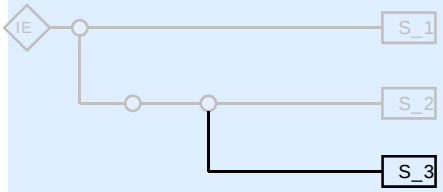


Dynamic Event Tree evolution

•Parameter evolution

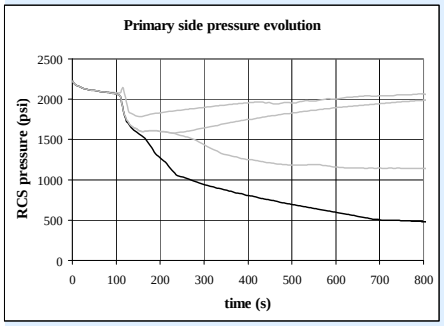


•DET

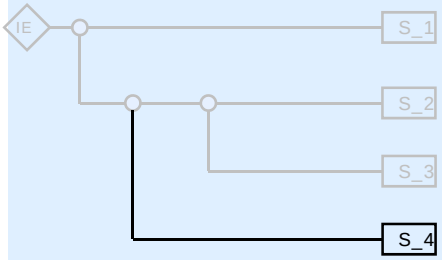


Dynamic Event Tree evolution

•Parameter evolution

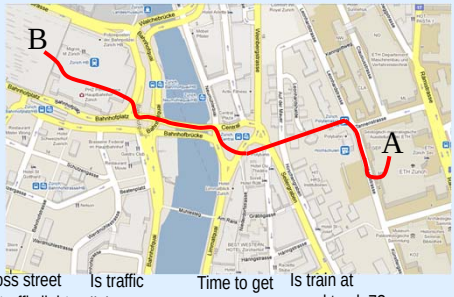


•DET

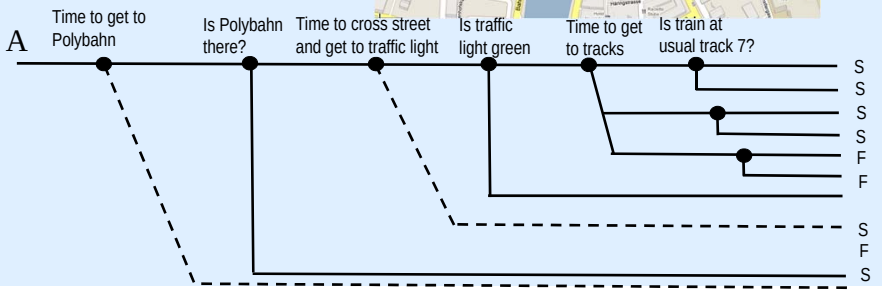


Example DDET construction

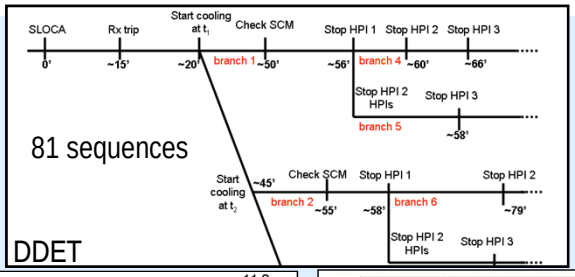
Goal: Go to the train station

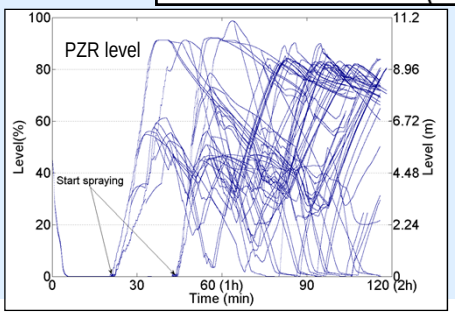


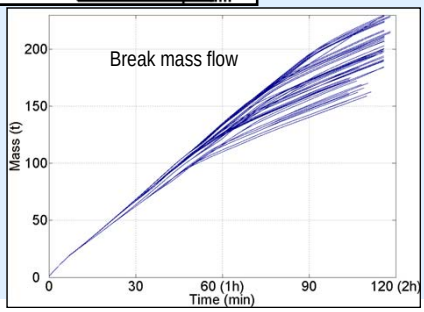
•Many factors will influence the performance:



Example DDET output



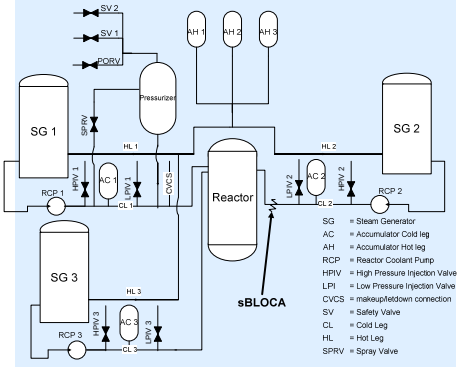




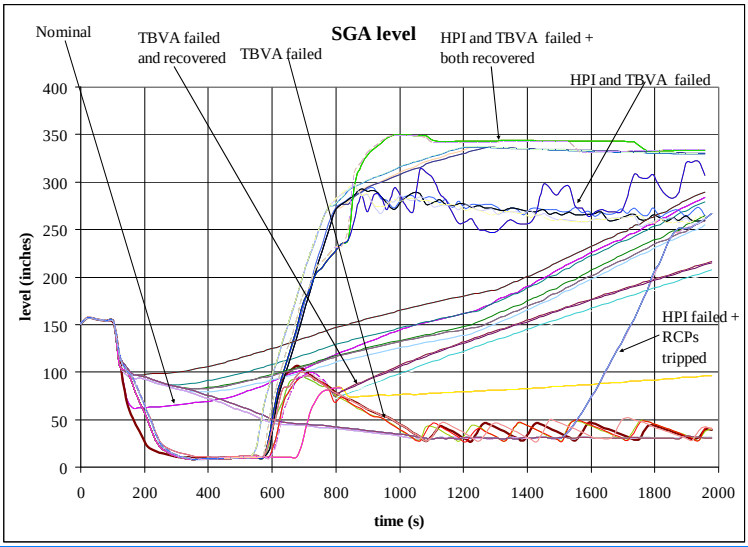
Example of case study - SLOCA

- Initiating event
  - Leak with diameter of 1 inch in one of the primary side cold legs of a three-loop PWR
    - the break is not sufficient to depressurize and cooldown the primary side
- Main operators' actions after reactor and turbine trips
  - **Cooldown** at 100 K/h through the turbine bypass valves
  - **Depressurize** the system to low pressure conditions
  - **Maintain** the SG levels with the feedwater pumps
  - **Start** the PZR sprays to increase PZR level
  - **Stop** HPI pumps if enough subcooling margin

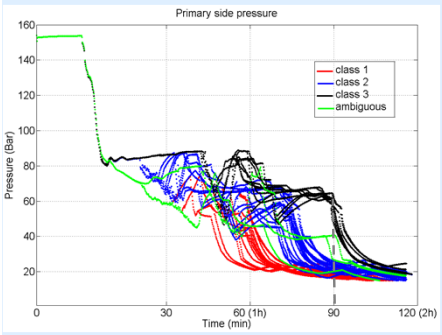
Primary side

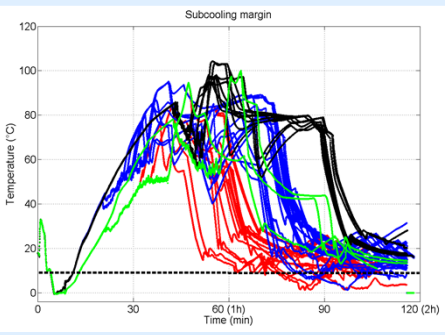


Steam Generator level (all sequences)



Scenario Analysis

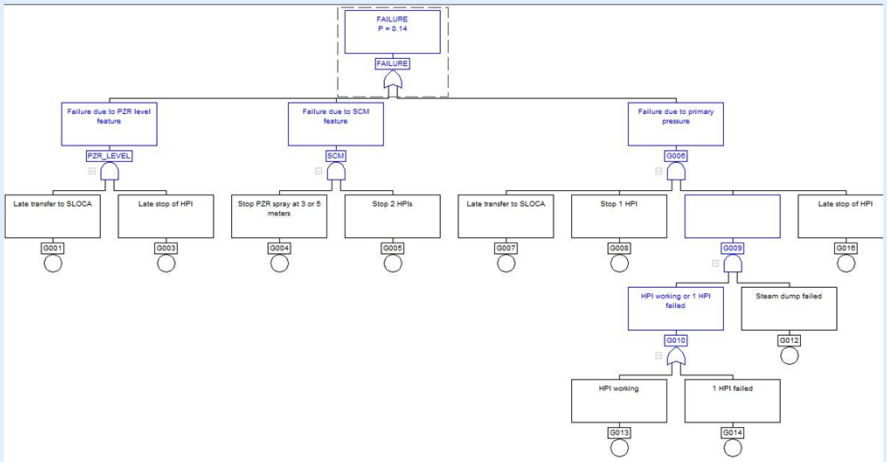




- Post-simulation tools → identification of failure/success scenarios
- Frequency of failure based on frequencies of each sequence

Failure probability estimation

- Tool extracts information about the contributors to failure



Human Reliability Analysis

- HRA model
  - study the interactions between humans and systems (NPPs)
  - attempt to predict the impact of such interactions on the system reliability
  - HRA analyst models and quantifies these interactions (HEPs)

- HRA Example: rush to the train station (A to B)

Diagnosis:
Should I stay or should I go?

Executions:
1.Pack your stuff
2.Rush to the Polybahn
3.Cross the street to get to Bahnhofbrüche
4.Cross the street to get to Bahnhof
5.Go to the right track

→ Performance Shaping Factors will influence the response!

DDET to support HRA (SPAR-H)

A. Evaluate PSFs for the Diagnosis Portion of the Task, If Any.

PSFs	PSF Levels	Multiplier for Diagnosis	Ple PS col
Available Time	Inadequate time	P(failure) = 1.0	
	Barely adequate time (≈2/3 x nominal)	10	
	Nominal time	1	
	Extra time (between 1 and 2 x nominal and > than 30 min)	0.1	
	Expansive time (> 2 x nominal and > 30 min)	0.01	
	Insufficient information	1	
Stress/ Stressors	Extreme	5	
	High	2	
	Nominal	1	
	Insufficient Information	1	
Complexity	Highly complex	5	
	Moderately complex	2	
	Nominal	1	
	Obvious diagnosis	0.1	
	Insufficient Information	1	
Experience/ Training	Low	10	
	Nominal	1	
	High	0.5	
	Insufficient Information	1	
Procedures	Not available	50	
	Incomplete	20	
	Available, but poor	5	
	Nominal	1	
	Diagnostic/symptom oriented	0.5	
	Insufficient Information	1	
Ergonomics/ HMI	Missing/Misleading	50	
	Poor	10	
	Nominal	1	
	Good	0.5	
	Insufficient Information	1	
Fitness for Duty	Unfit	P(failure) = 1.0	
	Degraded Fitness	5	
	Nominal	1	
	Insufficient Information	1	
Work Processes	Poor	2	
	Nominal	1	
	Good	0.8	
	Insufficient Information	1	

- Influence human performance in complex systems → Performance Shaping Factors (PSFs)
  - Positive way → low multiplier
  - Negative way → high multiplier

$$HEP = f(PSFs)_{Diag} + f(PSFs)_{Exec}$$

Issues from Scenario Analysis

- Not only the variability of time generates different scenarios but also:
  - Dynamic constraints
    - Operators cannot shut down 2 pumps because SCM is low → slow crews
  - Different strategies
    - Depressurization (fast crews) Vs. maintaining SCM (slow crews)
  - Competing goals
    - Quick depressurization vs. high SCM vs. high PZR level
      - Shut 2 HPI pumps → loss of SCM
      - Slowly stop 1 HPI per time → slow depressurization & too high break flow
      - Spray long → loss of SCM

Support HRA

- SLOCA with HPI systems available
  - PRA → 80' to cooldown & 10' for decision

	SPAR-H	Dynamic
DIAG.	2.5E-2	2.5E-2
EXE.	1.0E-2	5.0E-2
TOT.	3.5E-2	7.5E-2

•Dynamic insights to support PSF evaluation:
- •Competing goals
- •Dynamic context
- •Strategies

PSF complexity increases!!!

- Classical HRA → diagnosis most important
- Dynamic → **execution** most important!!!

Other applications...

- <u>Success criteria identification</u>
  - A success criterion is a condition that must be verify in order to have the success of the top event in the event tree
    - Based on a few thermal-hydraulic calculations
    - Complete spectrum of potential plant response is not addressed
  - DDETs can support a wide spectrum of plant response due to different system and operator interactions and the edge between success and failure scenarios can be identified
- <u>Uncertainty analysis</u>
  - Probability distributions can be propagated into the DDET to assess the uncertainty boundaries
  - Help Level 2 analysis

Laboratorium für Sicherheitsanalytik
INSTITUT FÜR ENERGIETECHNIK

Take home messages

- Dynamic approach is a **new research branch** to model and analyze **dynamic interactions** between **plant**, **automatic systems**, and **operators**
- DDET is a (not "the") dynamic approach and it is already applied to **accident scenarios analysis** and **support** HRA
- DDET approach could be used in PSA for **success criteria identification** and **uncertainty analysis**