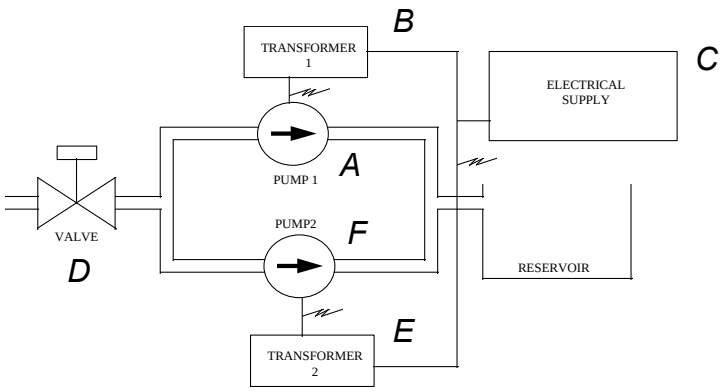
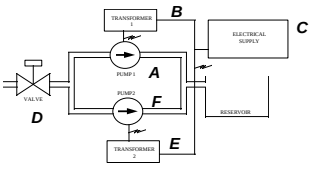
Motivation and issues with current PSA tools

- What is the mean unreliability (P_{top}) of the system's function, based on individual Basic Events probabilities ?

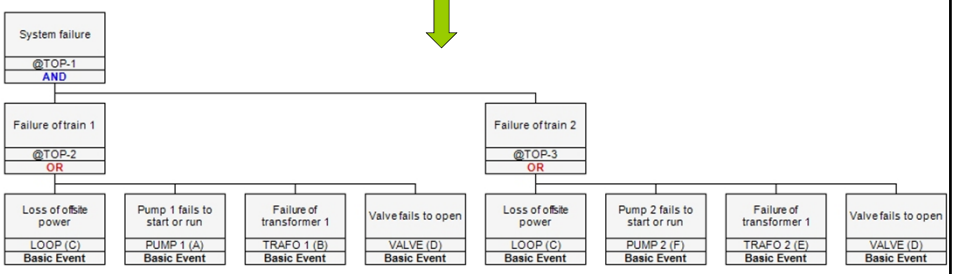


$$P_{top} = D + C + AF + AE + BF + BE$$

Motivation and issues with current PSA tools



$$P_{top} = D + C + AF + AE + BF + BE$$

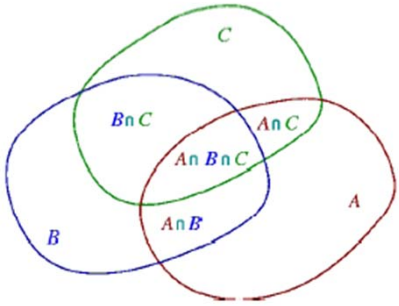


Motivation and issues with current PSA tools

- The rare event approximation (Moivre's equation)

$$|A_1 \cup \ldots \cup A_p| = \sum_{1 \le i \le p} |A_i| - \sum_{1 \le i_1 < i_2 \le p} |A_{i_1} \cap A_{i_2}| + \ldots + (-1)^{p-1} |A_1 \cap \ldots \cap A_p|$$

- Inclusion-exclusion principle



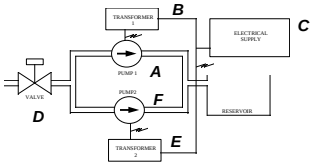
3

Motivation and issues with current PSA tools

- For our system, analytical correct result would yield:

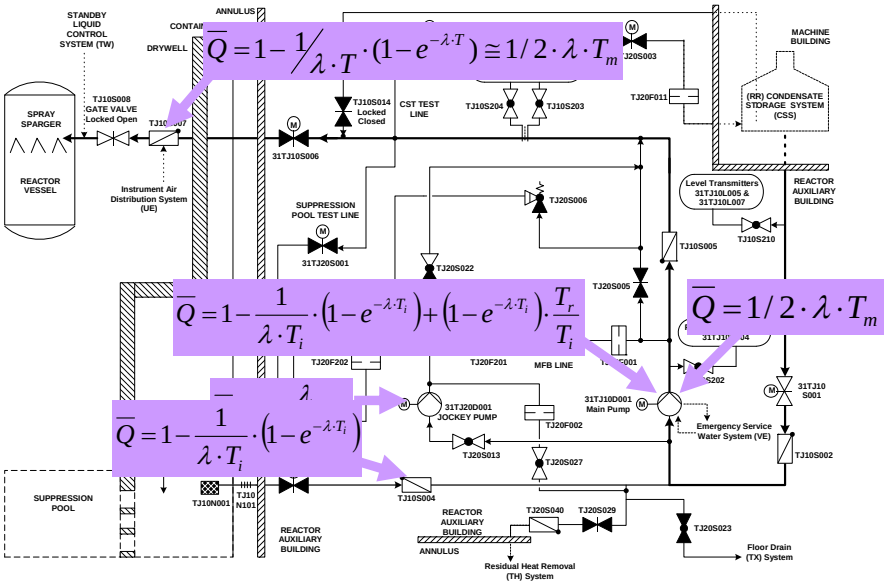
P_{top}= [D + F + E + C - DF - DE - DC - FE - FC - EC + DFE + DFC + DEC + FEC - DFEC]·[A + B + C + D - AB - AC - AD - BC - BD - CD + ABC + ABD + ACD + BCD - ABCD]

= [C - A(-1 + B)(-1 + C) (-1 + D) + B (-1 + C) (-1 + D) + D - C D] · [F - C (-1 + D) (-1 + F) (-1 + E) + D (-1 + F) (-1 + E) + E - FE]



4

Methodologischer Rahmen: Fehlerbäume



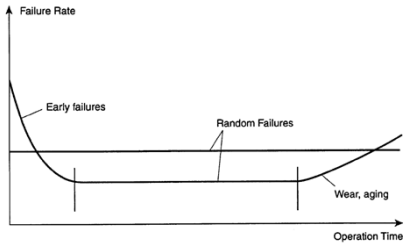
Methodologischer Rahmen: Zuverlässigkeitsdaten

- Reliability Calculation
  - Failure to start: Q=q
  - Failure to run:

$$d(N_0 - N(t)) = -\lambda \cdot N(t) \cdot dt$$

$$N(0) = N_0$$

$$\Rightarrow Q(t) \equiv \frac{N(t)}{N_0} = 1 - e^{-\lambda t}$$ (Probability component is failed at time t)



$$\overline{Q} = 1/T \cdot \int_0^T (1 - e^{-\lambda \cdot t}) \cdot dt = 1 + 1/\lambda \cdot T \cdot (e^{-\lambda \cdot T} - 1) \xrightarrow{Tailor} \sum_{i=2}^{\infty} \frac{(\lambda \cdot T)^{i-1}}{i!} \cong 1/2 \cdot \lambda \cdot T$$

$$MTTF = \int_0^{\infty} \underbrace{\frac{dQ(t)}{dt}}_{\text{density function}} \cdot t \cdot dt = 1/\lambda$$

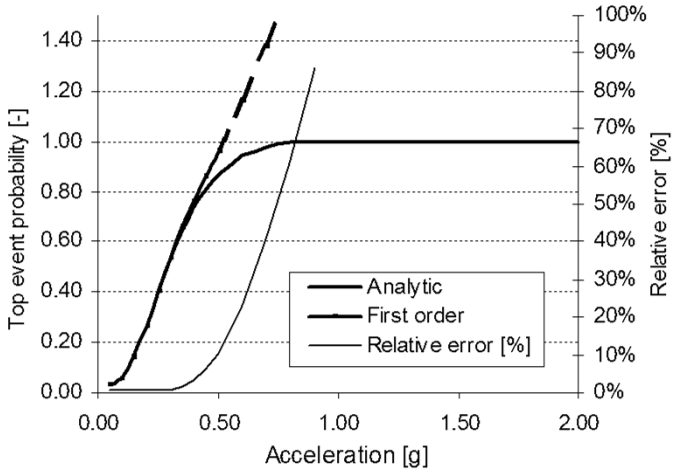
Motivation and issues with current PSA tools

- Rare event is only justified when the probabilities are low
- Existing PSA tools were developed 20 years ago under this assumption
- Modern PSA models include HRA, CCF, seismic and phenomenological events, where failure probabilities approach 1
- None of the existing tools is able to correctly quantify PSA models

7

Motivation and issues with current PSA tools

- Impact of the rare event approximation (In Proc. ESREL Conference, 2005)



8

Motivation and issues with current PSA tools

- Develop a new PSA quantification methodology that
  - Overcomes the deficiencies of the rare approximation, i.e. credit success branches, calculate the rare event up to infinite order
  - Yields correct evaluation of Risk Importance Factors (RIFs)
  - Support the treatment of negative logic
  - Do not apply cutoff when generating the sequences
  - Improve calculation speed and result consistency

9

Binary Decision Diagrams (BDD) as an alternative

- Shannon expansion

$$x \rightarrow y_0, y_1 := (x \wedge y_0) \vee (\overline{x} \wedge y_1) := ite(x, y_0, y_1)$$

- Shannon expansion of *t* with respect to *x*

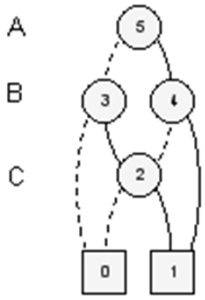
$$t = x \rightarrow t[1/x], t[0/x] \Rightarrow t = (x \wedge t[1/x]) \vee (\overline{x} \wedge t[0/x])$$

- *t[0/x]* and *t[1/x]* both contain one less variable than expression *t*
- One can **recursively** expand a Boolean equation up to the basic elements *0* (*false*) and *1* (*true*)

10

Binary Decision Diagrams (BDD) as an alternative

- Example for a „2 out of 3“ system *t*
- $t = AB + BC + AC$
  - $t = A \rightarrow (t_0, t_1)$
  - $t_0 = B \rightarrow (0, t_{01})$
  - $t_1 = B \rightarrow (1, t_{10})$
  - $t_{01} = C \rightarrow (1, 0)$
  - $t_{10} = C \rightarrow (1, 0)$
- $t = A \rightarrow (B \rightarrow (0, C \rightarrow (1, 0)), B \rightarrow (1, C \rightarrow (1, 0)))$



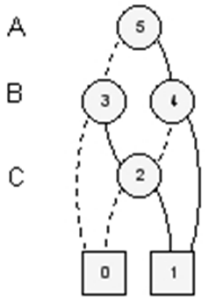
11

Binary Decision Diagrams (BDD) as an alternative

- **Canonical formulation** of Boolean equations !
- For our „2 out of 3“ system *t*

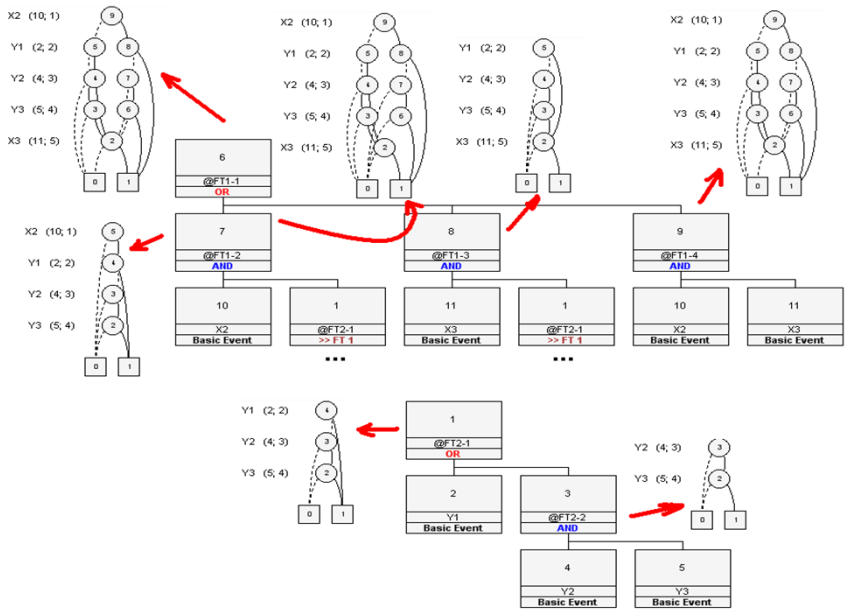
$t = AB + BC + AC$

$P_{top} = AB + A\,(1\text{-}B)\,C + (1\text{-}A)\,B\,C$

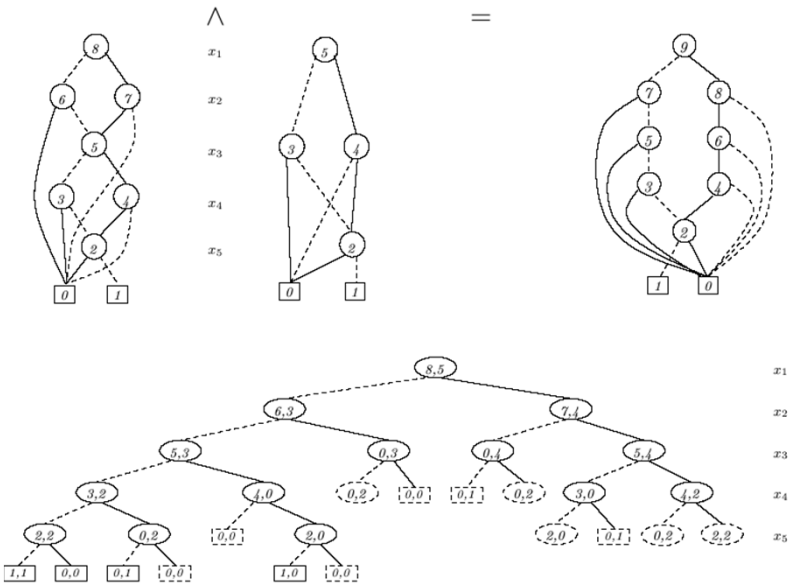


12

Binary Decision Diagrams (BDD) as an alternative



Binary Decision Diagrams (BDD) as an alternative



Binary Decision Diagrams (BDD) as an alternative

Algorithm $Apply[T, H](op, u_1, u_2)$

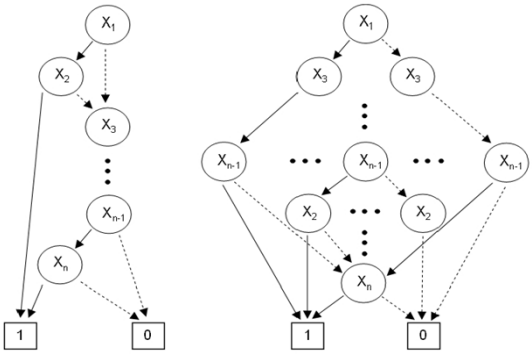
Require: u_1 and u_2 the top nodes of the BDD to assemble.
Ensure: The resulting BDD.

1: **if** $G(u_1, u_2) \neq \emptyset$ **then**
2: **return** $G(u_1, u_2)$
3: **else if** $u_1 \in \{0, 1\}$ and $u_2 \in \{0, 1\}$ **then**
4: $u = op(u_1, u_2)$
5: **else if** $var(u_1) = var(u_2)$ **then**
6: $u = newnode(var(u_1), apply(low(u_1), low(u_2)), apply(high(u_1), high(u_2)))$
7: **else if** $var(u_1) < var(u_2)$ **then**
8: $u = newnode(var(u_1), apply(low(u1), u2), apply(high(u_1), u2))$
9: **else**
10: $u = newnode(var(u_2), apply(u_1, low(u_2)), apply(u_1, high(u_2)))$
11: **end if**
12: $G(u_1, u_2) \leftarrow u$ {Add to computation table}
13: **return** u {Returns node index}

15

Binary Decision Diagrams (BDD) as an alternative

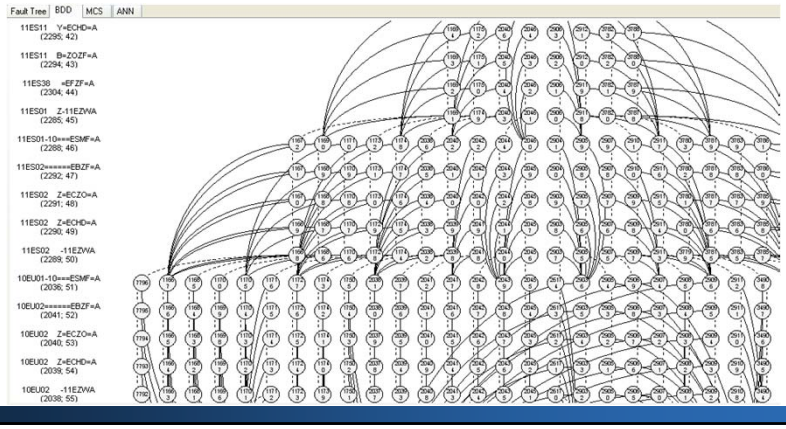
- Impact of variable order on BDD size
  - From linear to exponential
  - Finding the best order is of **NP-Complete complexity** [Bollig / Wegener, 1996]



16

Binary Decision Diagrams (BDD) as an alternative

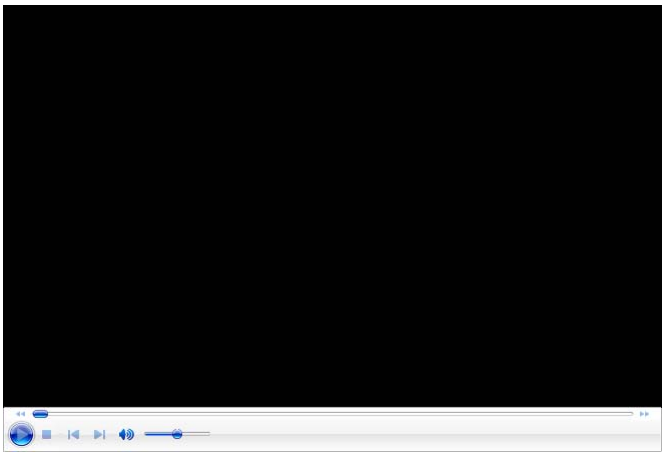
- BDD complexity is not related to the number of prime implicants of the encoded formula
- This small BDD (37620 nodes) encodes a total of 10^9 cutsets !



17

Binary Decision Diagrams (BDD) as an alternative

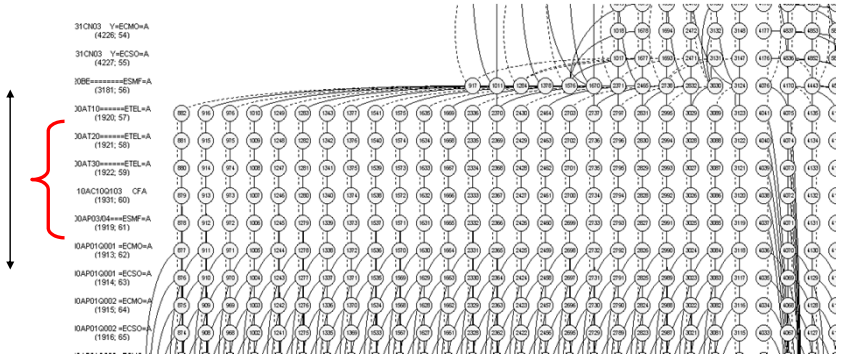
- Let’s have a closer look at…
  - ➢ The BDD of the HPCS System of the Leibstadt NPP



18

Research and development

- Development of Group-Sifting for FTA



	DFLM	Regular Sifting	Group-Sifting
HPCS	6'545	3'204	761
LPCS	206'503	40'656	7'763
RHR A/B	306'339	99'945	11'948

(*) Number of nodes (lower is better)

19