Accountability of Dynamic Calculations

Pavel Krcal, Pengbo Wang, Ola Bäckström

27 June 2022

RISK SPECTRUM

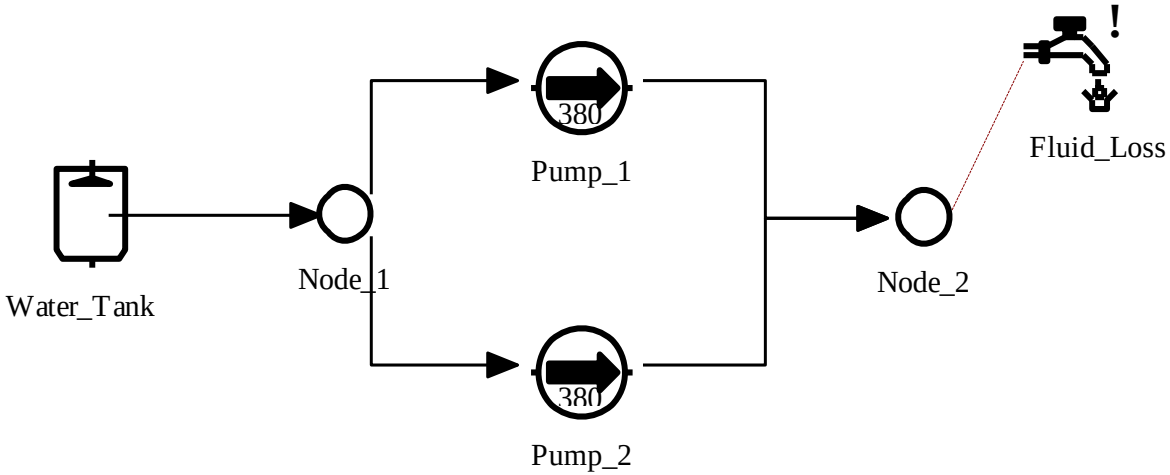
The Meaning of “Dynamic” in this Presentation

- Different from previous talks
- Exhaustive risk assessment
- Dynamic vs static

RISK SPECTRUM

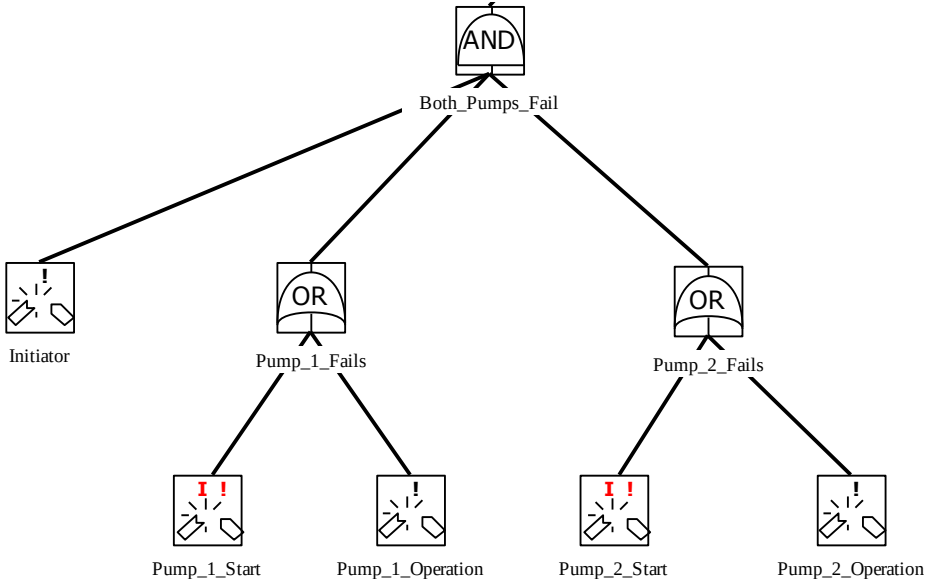
Static Calculations

Example: a simple pumping system



Static Calculations

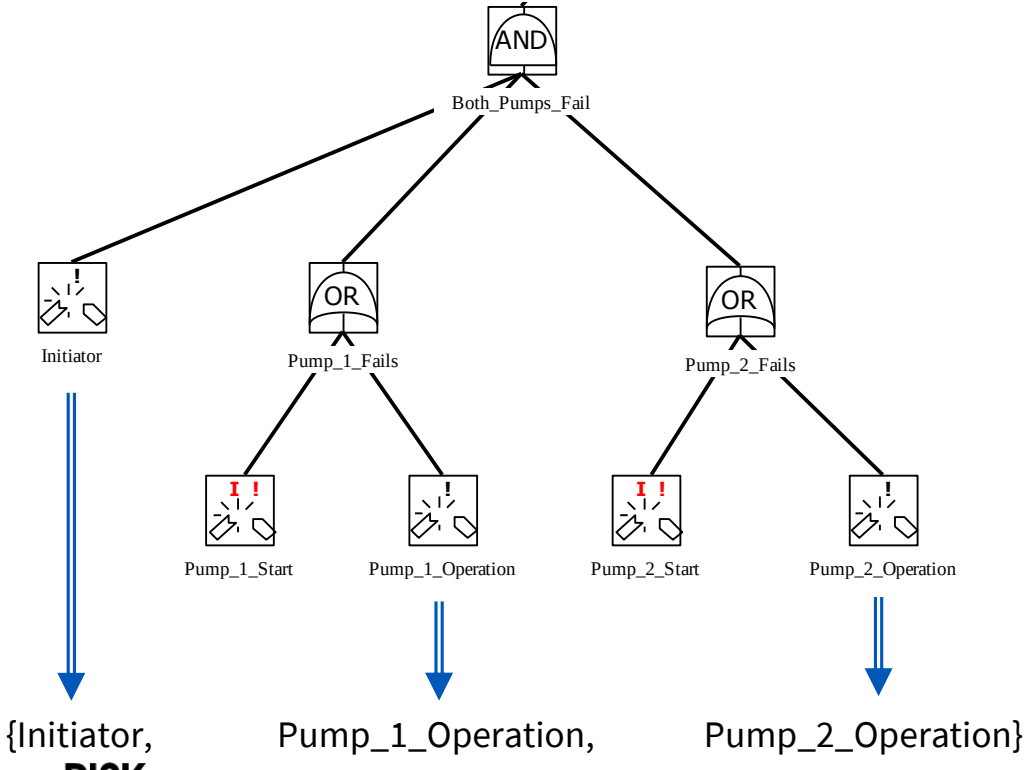
A fault tree capturing failure combinations



RISK SPECTRUM

Static Calculations

A fault tree capturing failure combinations

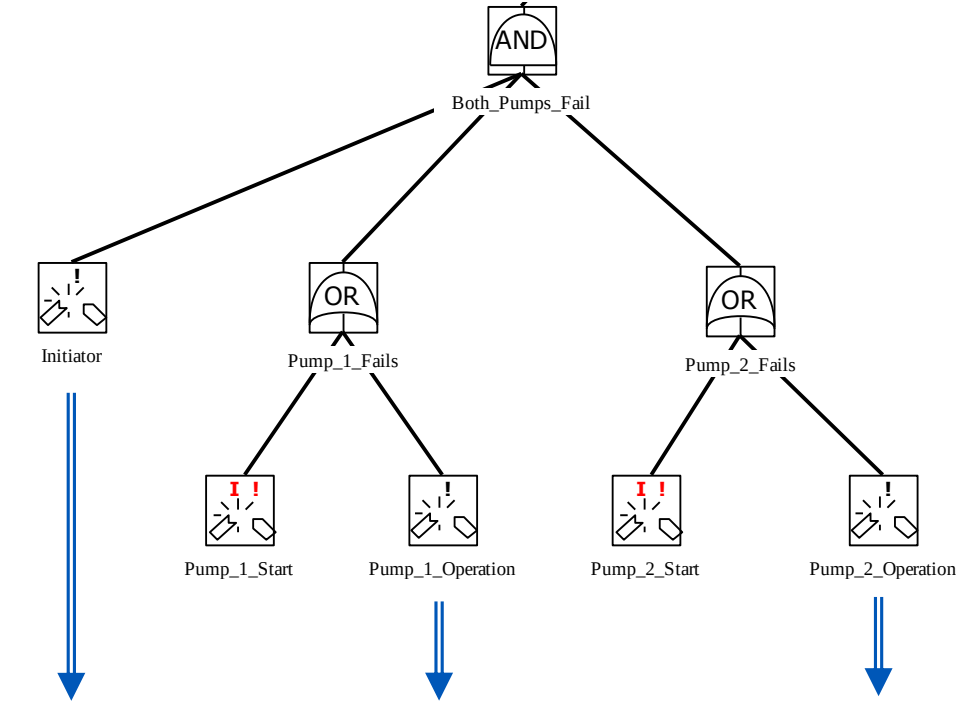


- Freq x $Prob_1$ x $Prob_2$

RISK SPECTRUM

Static Calculations

A fault tree capturing failure combinations



- Freq x $Prob_1$ x $Prob_2$
- Failures in operation:
  - Failure rate
  - Mission time
- Meaning:

RISK SPECTRUM

Result Accountability

Minimal cut set list and the top failure frequency

- Validation, explanation, interpretation of quantitative results
  - Clear meaning of minimal cut sets
  - Simple mathematical connection to minimal cut set frequencies

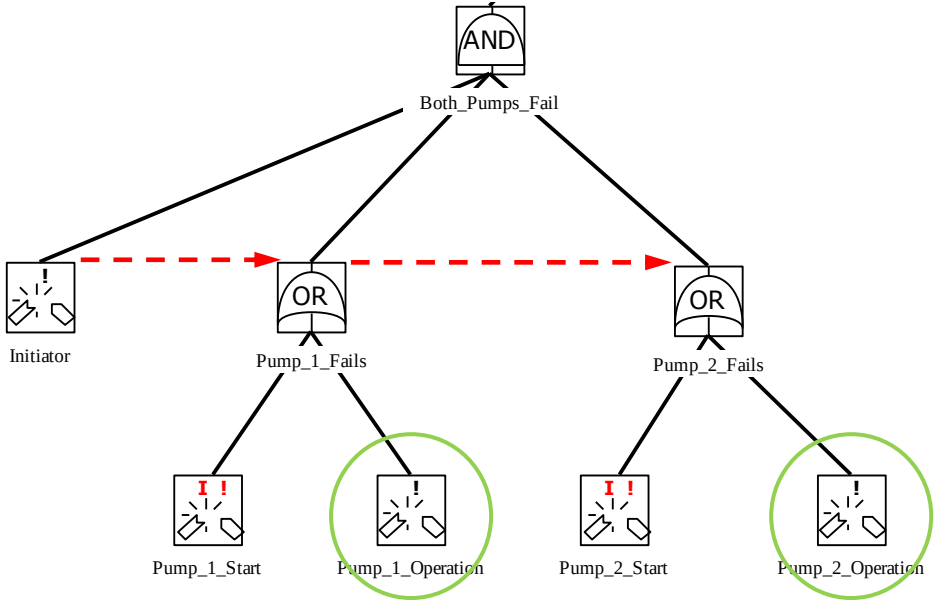
Top Event frequency F = 4,999E-04

No	Probability	%	Event 1	Event 2	Event 3	Event 4
1	1,45E-04	29,01	!IE-S-TRANS	CCF-CCW-PM---A-ALL		
2	1,45E-04	29,01	!IE-S-TRANS	CCF-SWS-PM---A-ALL		
3	6,04E-05	12,09	!IE-LMFW	CCF-SWS-PM---A-ALL		
4	6,04E-05	12,09	!IE-LMFW	CCF-CCW-PM---A-ALL		
5	5,01E-06	01,00	!IE-LMFW	CCF-RHR-PM---D-ALL	FEED&BLEED	
6	4,23E-06	00,85	!IE-LOOP	ACP-GT01-A	CCF-RHR-PM---D-ALL	
7	3,63E-06	00,73	!IE-LOOP	ACP-GT01-A	CCF-ACP-DG---A-ALL	
8	2,87E-06	00,57	!IE-LMFW	CCF-EFW-PM---D-ALL	DPS-MAN--H	
9	2,47E-06	00,49	!IE-S-TRANS	CCF-ACP-DG---A-ALL	OFFSITE-POWER	

RISK SPECTRUM

Dynamic Calculations

Repairs, cold stand-by redundancies

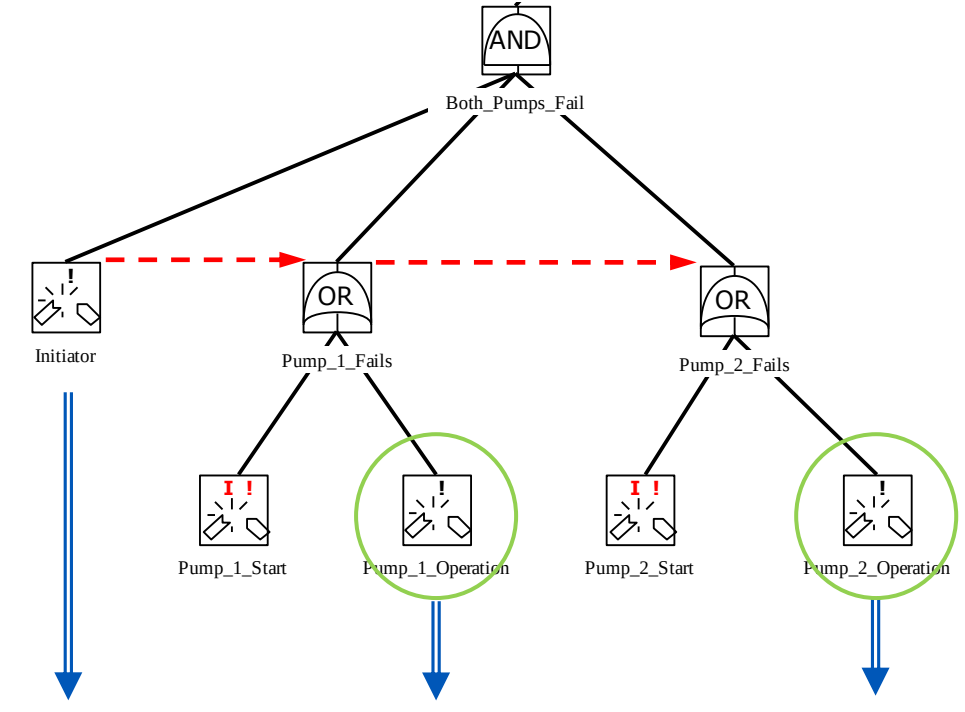


- Pumps can be repaired.
- $Pump_2$ is a cold stand-by for $Pump_1$.
- Event sequences instead of failure combinations
- Formalisms:
  - Dynamic Fault Trees
  - Boolean logic Driven Markov Processes
  - Stochastic Petri Nets
  - Fault Trees with repairs

RISK SPECTRUM

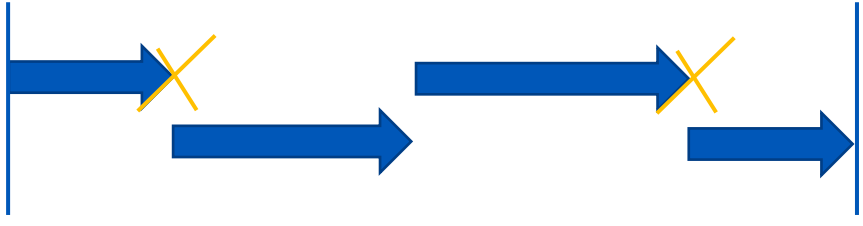
Dynamic Calculations

A stochastic process captures failure sequences



{Initiator, Pump_1_Operation, Pump_2_Operation}

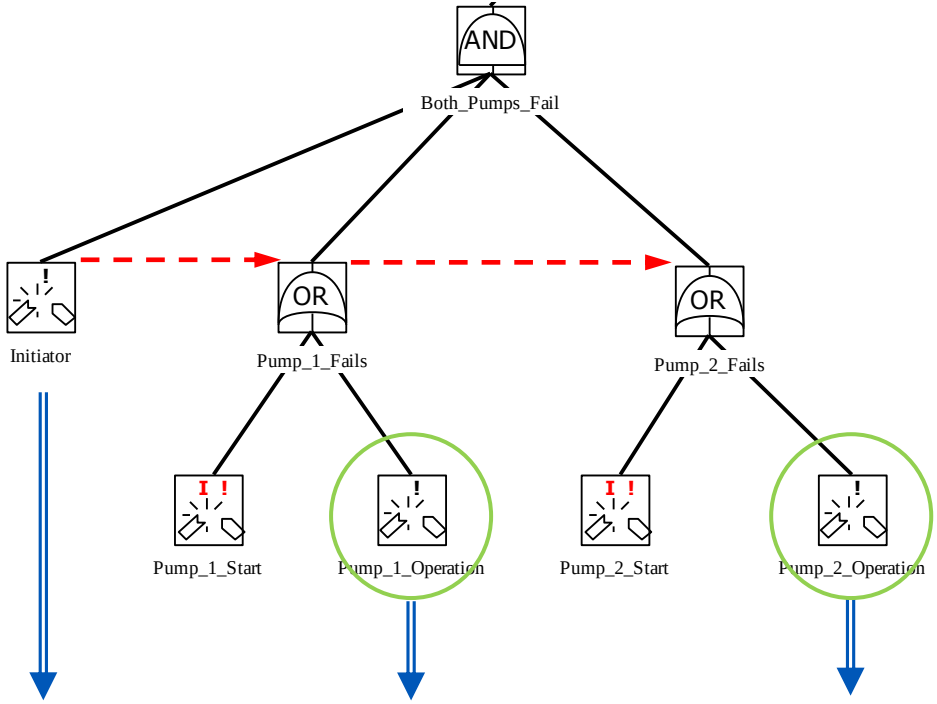
- Failures in operation:
  - Failure rate
  - Safe-end state (E.g., a repair of the initiator)
  - Mean Time To Repair
- Meaning:



RISK SPECTRUM

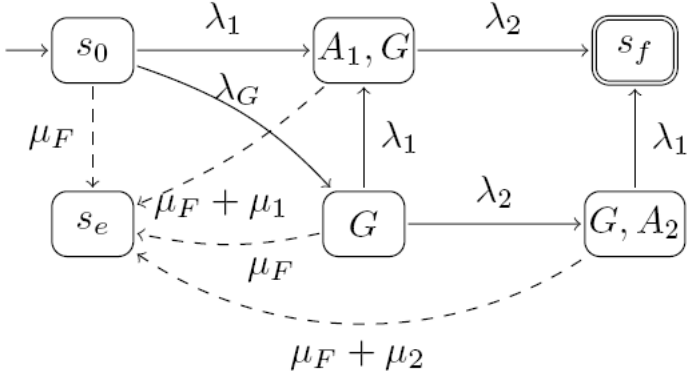
Dynamic Calculations

Analysis possibilities



{Initiator, Pump_1_Operation, Pump_2_Operation}

- A Continuous Time Markov Chain



- Markov analysis
- Simulations
- MCS-based methods

RISK SPECTRUM

Accountability of Dynamic Analysis Results

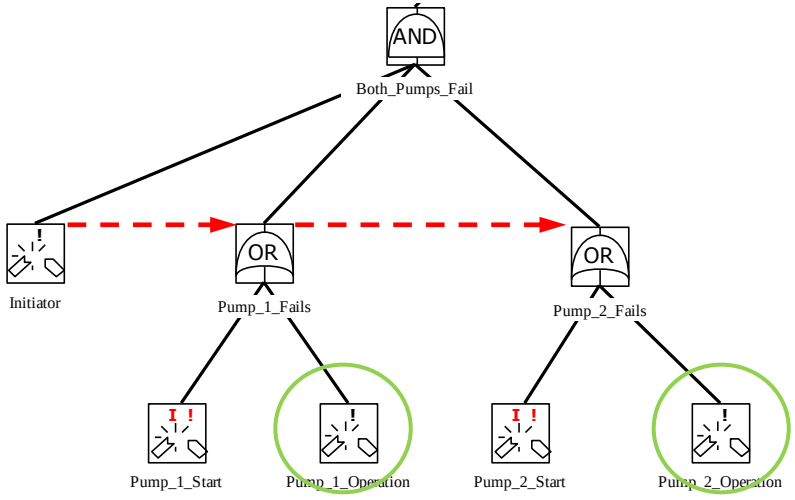
Can we achieve a similar level as for static analyses?

RISK SPECTRUM

Minimal Cut Set Based Methods

I&AB, Bounded Repairs, SDFT

- Decomposition into minimal cut sets



[Initiator, Pump_1_Operation, Pump_2_Operation]

[Initiator, Pump_1_Operation, Pump_2_Start]

[Initiator, Pump_1_Start, Pump_2_Operation]

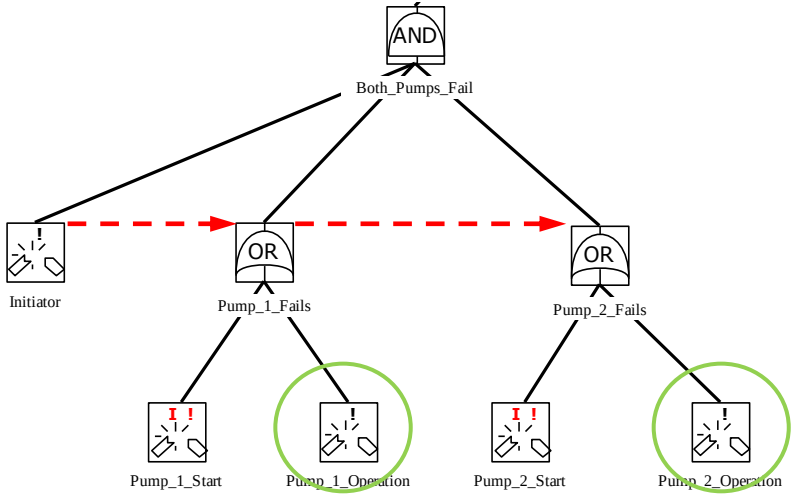
[Initiator, Pump_1_Start, Pump_2_Start]

RISK SPECTRUM

Minimal Cut Set Based Methods

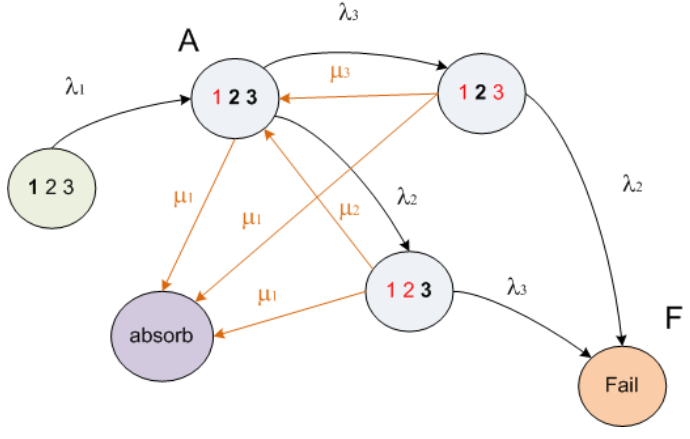
I&AB, Bounded Repairs, SDFT

- Decomposition into minimal cut sets



- Dynamic treatment of cut sets

[Initiator, Pump_1_Operation, Pump_2_Operation]

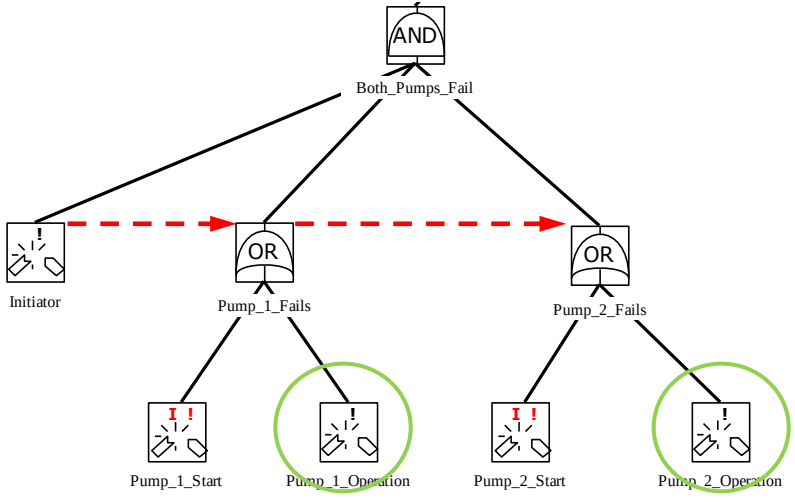


RISK SPECTRUM

Minimal Cut Set Based Methods

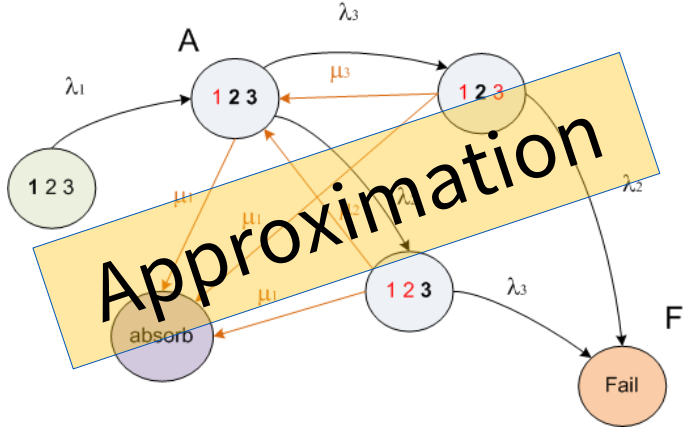
I&AB, Bounded Repairs, SDFT

- Decomposition into minimal cut sets



- Dynamic treatment of cut sets

[Initiator, Pump_1_Operation, Pump_2_Operation]

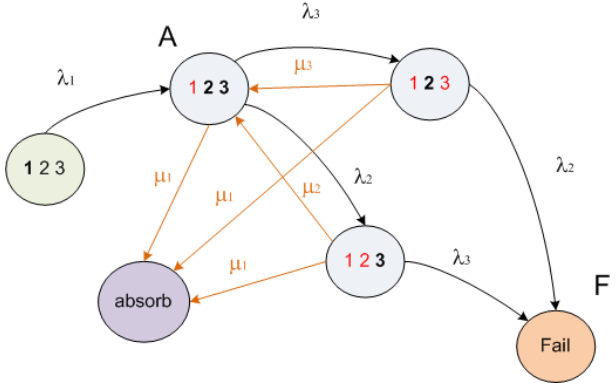


RISK SPECTRUM

Approximation 1: Repairs Only

Initiator and All Barriers (I&AB)

- An (approximate) analytic solution for a CTMC which models repairs
- Applied to minimal cut sets



$$E_c(N(\infty)) = \int_0^\infty \sum_{i=1}^{m+l+1} W_{c,i}(x) \prod_{\substack{j=1 \\ j\neq i}}^{m+l+1} Q_{c,j}(x)dx$$

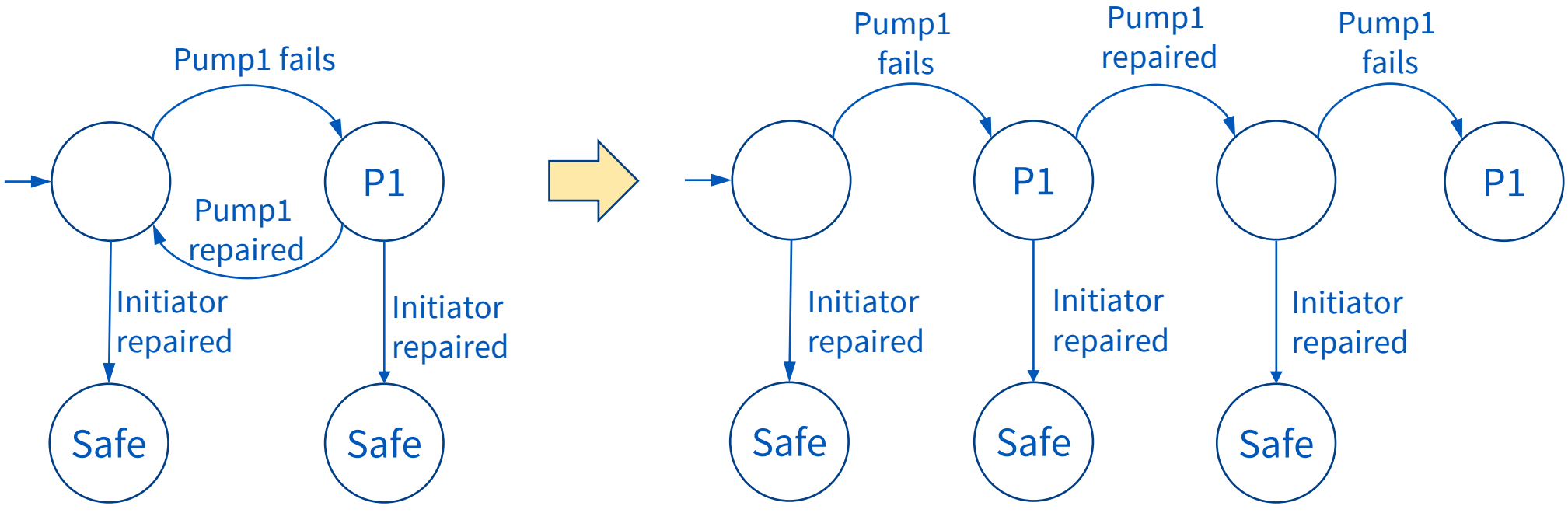
$$= \prod_{i=1}^{l} \gamma_{c,i} \times \int_0^\infty \exp\left[-\left(\mu_{c,ie} + \sum_{j=1}^{l} \mu_{c,j}\right) x\right] \sum_{i=1}^{m} W_{c,i}(x) \prod_{\substack{j=1 \\ j\neq i}}^{m} Q_{c,j}(x)dx$$

RISK SPECTRUM

Approximation 2: Triggers and Repairs

Bounded repairs

- Only **X** repairs considered –> Acyclic Markov Chain



RISK SPECTRUM

Accountability of Dynamic Analysis Results

Can we achieve a similar level as for static analyses?

Top Event frequency I&AB = 1,352E-08

No	Probability	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	2,54E-09	18,77	CCF_GEV_LGR_INIT	DGA_LONG_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF
2	2,54E-09	18,77	CCF_GEV_LGR_INIT	DGA_SHORT_FAILF	DGB_LONG_FAILF	INFNHOUSE_FAILF	TAC_FAILF
3	2,20E-09	16,29	CCF_GEV_LGR_INIT	CCF_DG_FAILF	INFNHOUSE_FAILF	TAC_FAILF	
4	1,63E-09	12,04	CCF_GEV_LGR_INIT	DGA_LONG_FAILF	DGB_LONG_FAILF	INFNHOUSE_FAILF	TAC_FAILF
5	1,44E-09	10,68	CCF_GEV_LGR_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF
6	3,69E-10	02,73	CCF_GEV_LGR_INIT	DGA_SHORT_FAILF	DGB_LONG_FAILF	ONDEMHOUSE_FAILI	TAC_FAILF
7	3,69E-10	02,73	CCF_GEV_LGR_INIT	DGA_LONG_FAILF	DGB_SHORT_FAILF	ONDEMHOUSE_FAILI	TAC_FAILF
8	3,10E-10	02,29	CCF_GEV_LGR_INIT	CCF_DG_FAILF	ONDEMHOUSE_FAILI	TAC_FAILF	
9	2,26E-10	01,67	CCF_GEV_LGR_INIT	DGA_LONG_FAILF	DGB_LONG_FAILF	ONDEMHOUSE_FAILI	TAC_FAILF
10	2,23E-10	01,65	CCF_GEV_LGR_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	ONDEMHOUSE_FAILI	TAC_FAILF
11	8,25E-11	00,61	GRID_INIT	CCF_DG_FAILF	INFNHOUSE_FAILF	TAC_FAILF	
12	5,67E-11	00,42	GRID_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF
13	3,49E-11	00,26	SUBSTATION_INIT	CCF_DG_FAILF	INFNHOUSE_FAILF	TAC_FAILF	

RISK SPECTRUM

Understanding Dynamic Minimal Cut Sets

Local assessments

- Interpreting an effect of repairs
  - Does it matter at all?
  - Importance/sensitivity for repairs of individual events and all events together

IE, DGA_LONG, DGB_SHORT, INFNHOUSE, TAC I&AB: 2.54E-9 Static: 5.68E-9

	No repair	%	Half MTTR	%
DGA_LONG	3.70E-9	145	2.54E-9	0
DGB_SHORT	5.89E-9	232	2.54E-9	0
BOTH	6.18E-9	243	2.54E-9	0

Understanding Dynamic Minimal Cut Sets

Global assessments

- Effect of repairs on the contribution and position in the MCS list
  - Static:

Top Event frequency F = 1,768E-06

No	Probability	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	3,94E-07	22,28	LGR_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF
2	3,94E-07	22,28	GEV_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF

  - I&AB:

Top Event frequency I&AB = 1,352E-08

No	Probability	%	Event 1	Event 2	Event 3	Event 4	Event 5
⋮							
22	1,93E-11	00,14	GEV_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF
23	1,93E-11	00,14	LGR_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF

RISK SPECTRUM

Understanding Dynamic Minimal Cut Sets

Global assessments

- Effect of repairs on the contribution and position in the MCS list
  - I&AB original:

22	1,93E-11	00,14	GEV_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF
23	1,93E-11	00,14	LGR_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF

  - I&AB, MTTR of DGA_SHORT_FAILF and DGB_SHORT_FAILF is 1000 (instead of 5):

48	4,38E-11	00,07	GEV_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF
49	4,38E-11	00,07	LGR_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF

  - I&AB, MTTR of GEV_INIT and LGR_INIT is 50 (instead of 5):

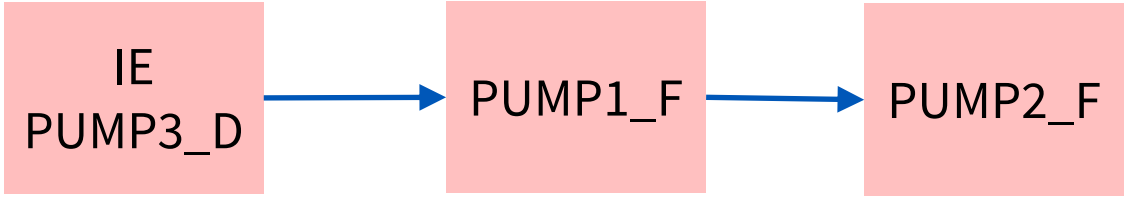
7	3,06E-09	05,95	LGR_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF
8	3,06E-09	05,95	GEV_INIT	DGA_SHORT_FAILF	DGB_SHORT_FAILF	INFNHOUSE_FAILF	TAC_FAILF

Understanding Dynamic Minimal Cut Sets

Trace-based evidence

- Each cut set can be split into event sequences.
- We get an ‘event sequence list’ for a cut set sorted by contribution to the cut set value.

[IE, PUMP1_F, PUMP2_F, PUMP3_D]



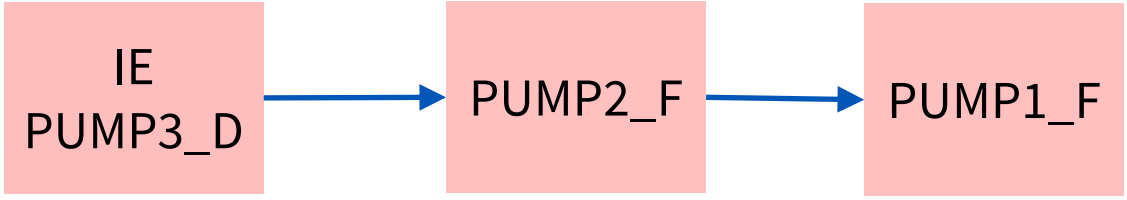
RISK SPECTRUM

Understanding Dynamic Minimal Cut Sets

Trace-based evidence

- Each cut set can be split into event sequences.
- We get an ‘event sequence list’ for a cut set sorted by contribution to the cut set value.

[IE, PUMP1_F, PUMP2_F, PUMP3_D]



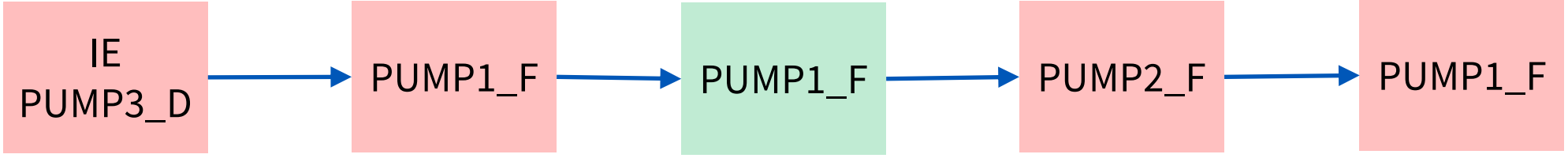
RISK SPECTRUM

Understanding Dynamic Minimal Cut Sets

Trace-based evidence

- Each cut set can be split into event sequences.
- We get an ‘event sequence list’ for a cut set sorted by contribution to the cut set value.

[IE, PUMP1_F, PUMP2_F, PUMP3_D]



RISK SPECTRUM

Conclusions

Dynamic calculations can be as accountable as static ones

- Setup:
  - Fault trees with repairs and cold stand-by redundancies
  - Minimal cut set decomposition
  - Dynamic quantification of minimal cut sets
- Effects of dynamic features on cut set value, contribution and position in the list
- Event sequences
  - Easily understandable sequences of failures/repairs
  - Can be quantified
  - Bounded repairs: a complete list can be presented.

RISK SPECTRUM