Analyzing Dynamic Fault Tree using input/output interactive Markov chain (I/O-IMC)

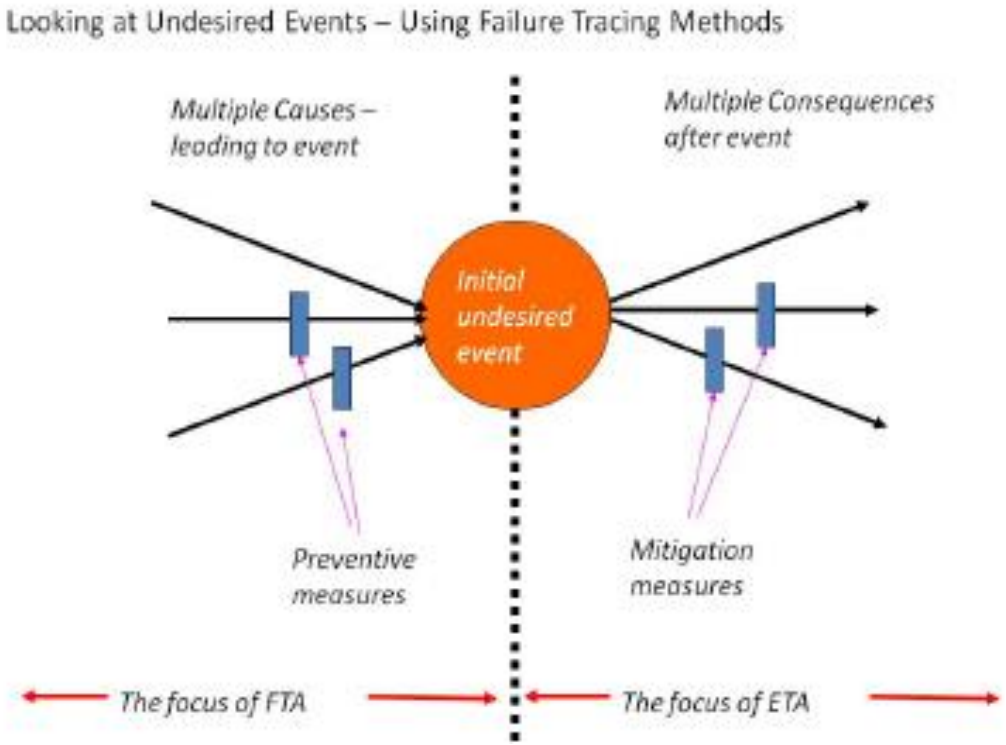
Mohammed Almazaideh

contents

- FTA & ETA
- Static Fault Tree Analysis (SFT)
- Dynamic Fault Tree Analysis (DTE)
- I/O Interactive and Continuous time Markov Chain
- Bisimulation relation
- DFT to I/O-IMC
- Example

FT vs ET

Fault Tree :events cause hazard
Event tree : events caused by hazard



FTA

FTA: A techniques for the dependability analysis used to construct a reliability model combines components, which together can cause system failure.

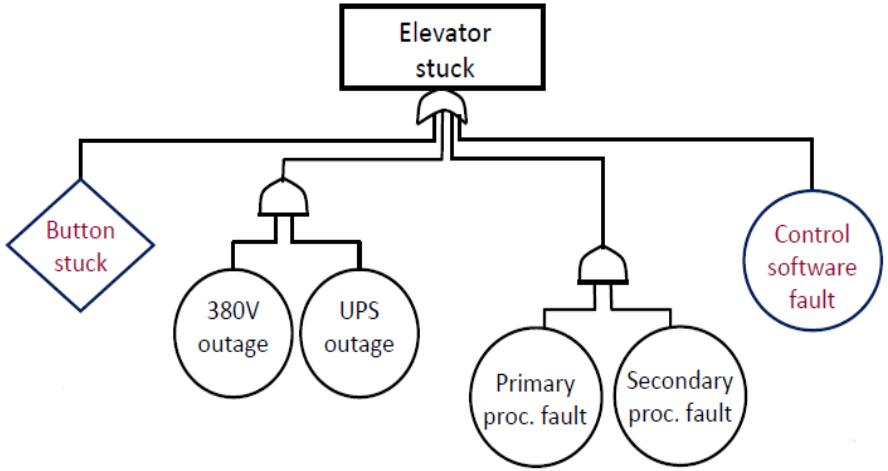
It is executed in two levels:

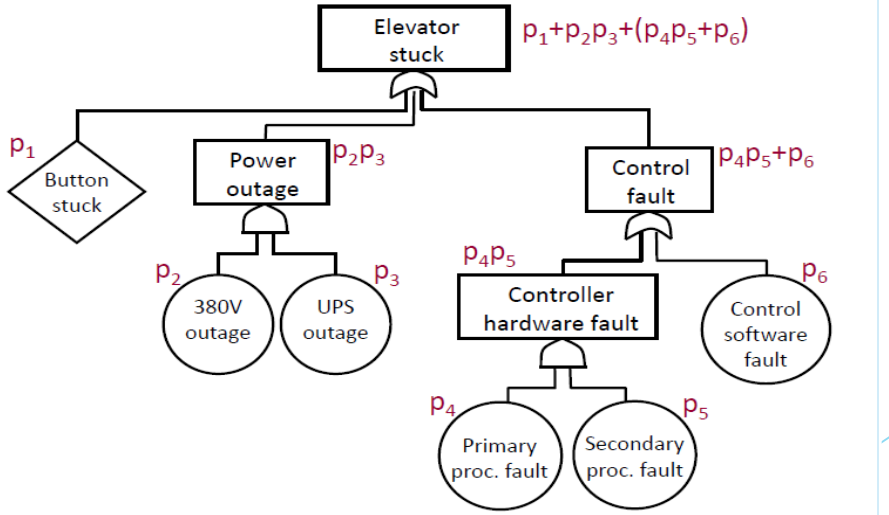
- Qualitative level: Determining the list of all the possible combinations of events that lead to the Top Event (TE)

- Quantitative level in which the probability of TE occurrence and the probability of the other nodes of the tree are calculated.

Static fault tree analysis (SFT):

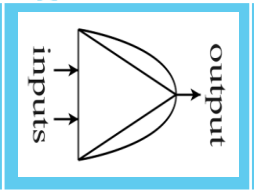
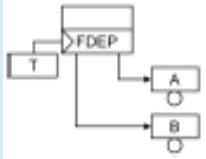
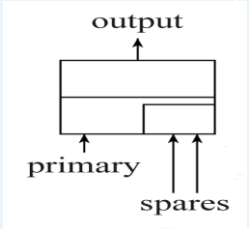
Static fault tree analysis (SFT):basic events must be assumed to be statistically independent, and their interaction is described by means of combination Boolean OR/AND gates *"Independent on time"*





Dynamic fault tree analysis (DFT)

Dynamic fault tree analysis (DFT): It is an extension of SFT, it takes in consideration time requirements and the probability of time dependency among the events. Beside combination gates it uses:

Priority-AND (PAND)		The output event occurs if the all inputs occur in a specific order
Functional Dependency (FDEP)		The inputs occur when trigger input occurs
Cold-Spare (CSP)		Output occurs If all inputs don't occurs, if the primary input doesn't occur, a spare one is promoted.

I/O interactive Markov chain

a? is input

b! is out put

1⟶ 2

Markovian transition

λ : transition rate

Transition takes place after exponential distributed delay

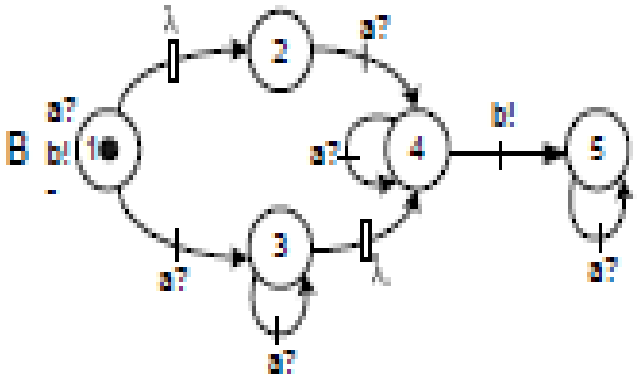
1⟶ 3

Interactive transition

Transition takes place when input a is available

4⟶ 5

Output Interactive transition



Continuous Time Markov Chain (CTMC)

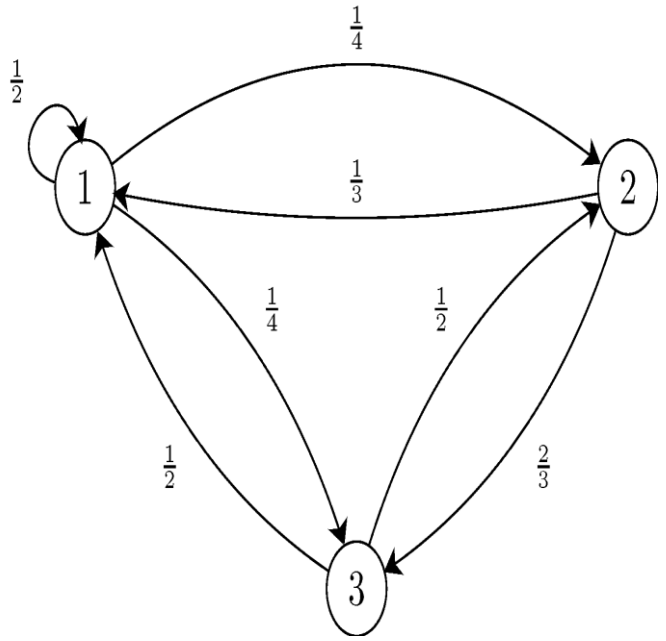
Transition matrix = $\begin{bmatrix} 1/2 & 1/4 & 1/4 \\ 1/3 & 0 & 2/3 \\ 1/2 & 1/2 & 0 \end{bmatrix}$

Probability of staying at node $\pi j = \sum_i \pi i$ Pij

$\pi = \{1/4, 1/4, 1/2\}$

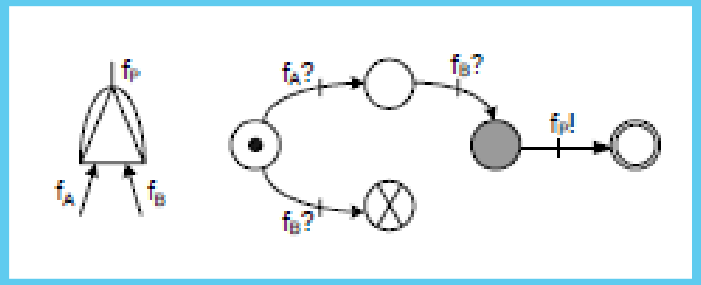
$P\{3 \rightarrow 2 \rightarrow 1\} = \pi 3 * P32 * P21 = 1/12$

Generator matrix: $G_{ij} = \lambda_i * P_{ij}$

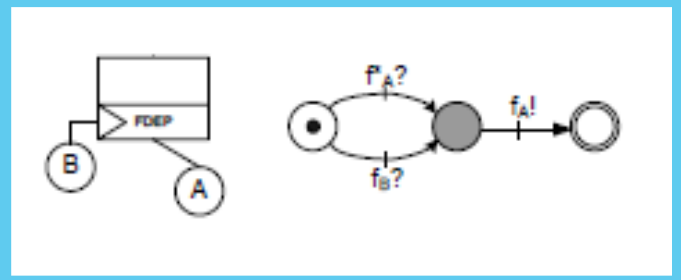


Dynamic gate as I/O-IMC

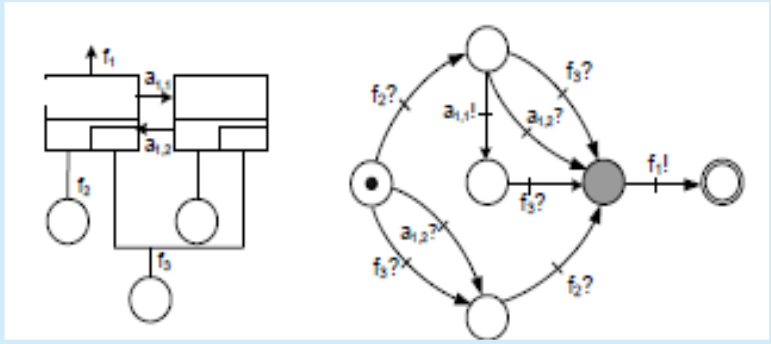
PAND



FDEP



Spare



I/O-IMC State and signals

Instead of converting the DFT to huge CTMC , Basic events and gates are converted to I/O-IMC and then combined together

State	Sym
Initial state	
Active state	
Output a failure signal	
Absorbing a fired state	
Operational absorbing state	

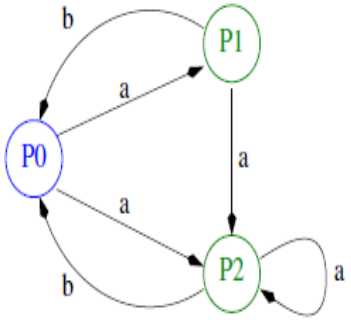
Signals	Discribtion
fA,B,…?	Firing signal
aA,B,…?	Activation signal
fP!	Gate failure output signal
f*A,B,…?	Self failure

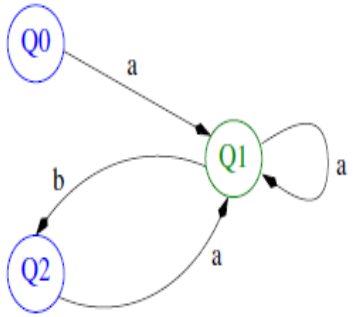
Bisimulation relation

It a technique used to combine two systems

$B \subseteq S \times S$ is a bisimulation, if for all $(s,t) \in B$ and any $a \in Act$, $s',t' \in S$ it holds:

- if $s \xrightarrow{a} s'$ then $\exists t' : t \xrightarrow{a} t'$ and $(s',t') \in B$
- if $t \xrightarrow{a} t'$ then $\exists s' : s \xrightarrow{a} s'$ and $(s',t') \in B$





P0 BiSimulates Q0
P1 BiSimulate Q1
P2 Doesn't Bisimulate Q2

Weak bisimulation

A binary relation $R \subseteq Proc \times Proc$ is a weak bisimulation iff whenever $(s, t) \in R$ then for each $a \in Act$ (including τ):

- if $s \xrightarrow{a} s'$ then $t \stackrel{a}{\Longrightarrow} t'$ for some t' such that $(s', t') \in R$
- if $t \xrightarrow{a} t'$ then $s \stackrel{a}{\Longrightarrow} s'$ for some s' such that $(s', t') \in R$.

Where τ is internal transition which are not visible

Examples:

a+ τ. b ¬≈ τ.a + τ.b

a.(b+ τ.c) ≈ a.(b+ τ.c) +a.c

a+b ¬≈ a+ τ. b

τ.a ≈ a+ τ. b

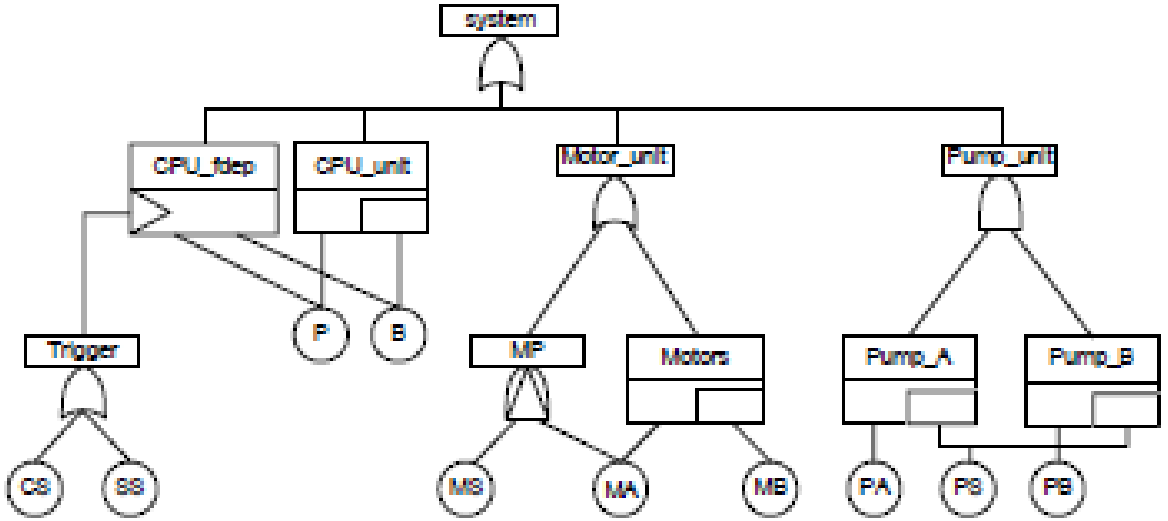
DFT Analysis

1. Map each DFT element to its corresponding I/O-MCT and match all input and output
2. Pick two I/O-MCT and parallel compose them
3. Hide output signals that won’t be subsequently used
4. Aggregate using weak bisimulation I/O-MCT obtained from 2 and 3 (TIPP)
5. Go to step 2 if more than 1 I/O-MCT is left
6. Analysis the aggregated CTMC

Example
The cardiac assist systems

Component	Failure Rate (λ)	Dormancy factor (α)
Primary CPU (P)	0.5	0.5
Spare CPU (B)	0.5	0.5
Cross switch (CS)	0.2	
System supervision (SS)	0.2	
Primary motor (MA)	1	
Spare motor (MB)	1	
Switching device (MS)	0.01	
Primary pump (PA)	1	
Primary paump (PB)	1	
Spare Pump (PS)	1	

The cardiac assist systems DFT



Dynamic Fault Tree analysis using Input/Output Interactive Markov Chains*

Hichem Boudali
hboudali@cs.utwente.nl

Pepijn Crouzen[§,†]
crouzen@alan.cs.uni-sb.de

Mariëlle Stoelinga
marielle@cs.utwente.nl

University of Twente, Department of Computer Science,
P.O. Box 217, 7500 AE Enschede, the Netherlands.

[§]Saarland University, Department of Computer Science,
D-66123 Saarbrücken, Germany.

Thank you