Probabilistic Model Checking with PRISM
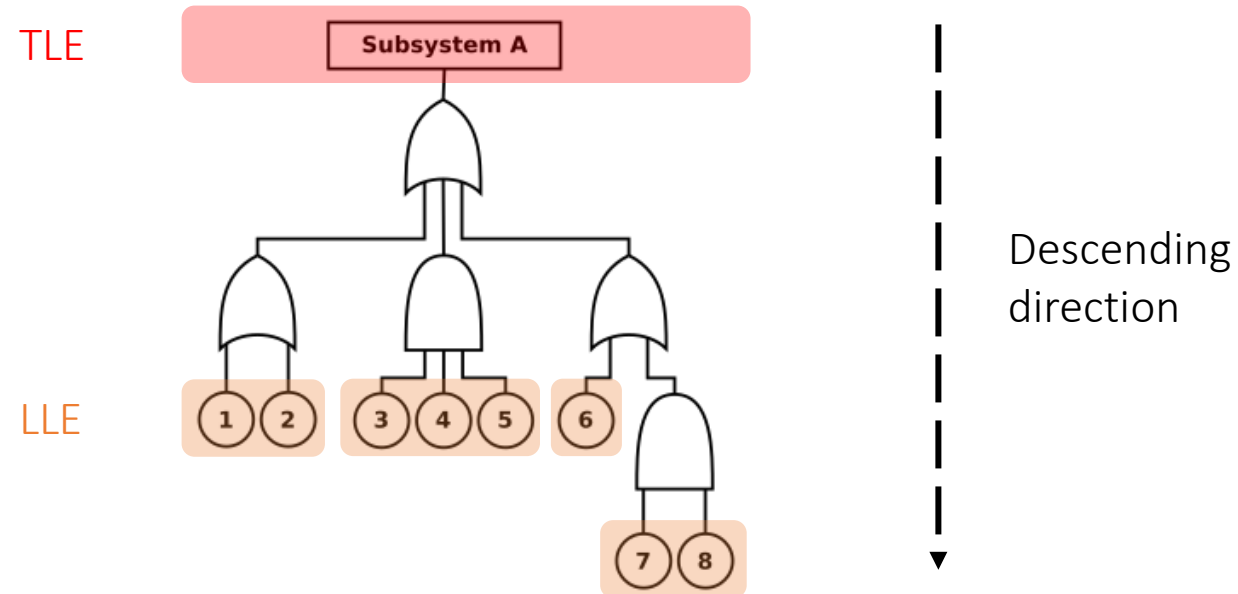
Production Line
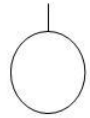
Patrick SARDINHA

Fault Trees

Fault Trees (FT) graphically represent possible combinations of events (Low Levels Events) leading to a predefined undesirable event (Top Level Event)
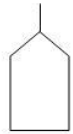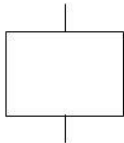
Representation:

TLE

LLE

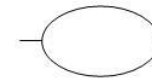Descending direction

Graphic symbols

Events:

Basic event: failure in a system component

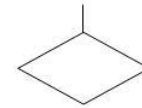**External event**: expected to occur

Intermediate event: events occurring at the exit of a door

Conditioning event: an event with conditions

Undeveloped event: an event with insufficient information

Gates: Describe the relationship between input and output events.

OR gate: the output occurs if any input occurs
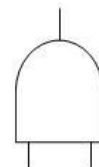
AND gate: the output occurs only if all inputs occur

Fault Tree Analysis (FTA)

Method used to evaluate the risks of a system and allows to:

Understand how a system can fail

Know how to reduce the risks

Visualize the event rates of an accident
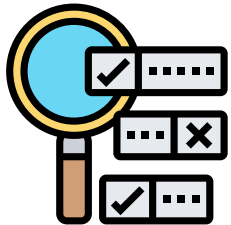
FTA is often performed by transforming the FT into a Boolean function which is used for simulation …

→ … but this methodology has a lot of constraints (time/resources)

A new formal Probabilistic FTA methodology

Efficient Probabilistic Fault Tree Analysis of Safety Critical Systems via Probabilistic Model Checking

Marwan Ammar, Ghaith Bany Hamad, Otmane Ait Mohamed, Yvon Savaria

A new formal Probabilistic FTA methodology

The idea is as follows:

1. Model the system (composed of components) and specify event parameters

2. Synthesize the system fault tree

3. Model the behavior of each FT gate as a probabilistic automaton (PA)

4. Generate a formal MDP(?) model of the fault tree with the parallel composition of the PA (PRISM)

5. Analyze the MDP(?) model to evaluate the maximum probability of Top Level Event (TLE)

System description

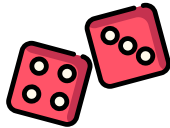We have a **production chain** made up of:

Machines that extract resources

Machines that transform resources

We have different types of **disruptive primary events**:

Technical failures on machines with a certain probability

Non-deterministic quantities of extracted resources

... And others

Resource extraction

We have different kinds of machine:

	Burner mining drill
Inputs	Raw minerals (from a source)
Outputs	Minerals
Basic event	- Can break down - May be affected by an external event - The input quantity may vary

	Offshore pump
Inputs	Water (from a source)
Outputs	Water
Basic event	- Can break down - May be affected by an external event - The input quantity may vary

Resource transformation

We have different kinds of machine:

	Boiler
Inputs	Fuel & water
Outputs	Steam
Basic event	- Can break down - May be affected by an external event - Fuel not supplied - Water not supplied

	Steam engine
Inputs	Steam
Outputs	Electricity
Basic event	- Can break down - May be affected by an external event - Steam not supplied

Resource transformation

	Furnace
Inputs	Fuel & minerals
Outputs	Processed minerals
Basic event	- Can break down - May be affected by an external event - Fuel not supplied - Minerals not supplied

	Assembling machine
Inputs	Electricity & Processed minerals
Outputs	Final product
Basic event	- Can break down - May be affected by an external event - Electricity not supplied - Processed minerals not supplied

Production line: Example

Burner mining drill

Offshore pump

Furnace

Boiler

Steam engine

Assembling machine

End point
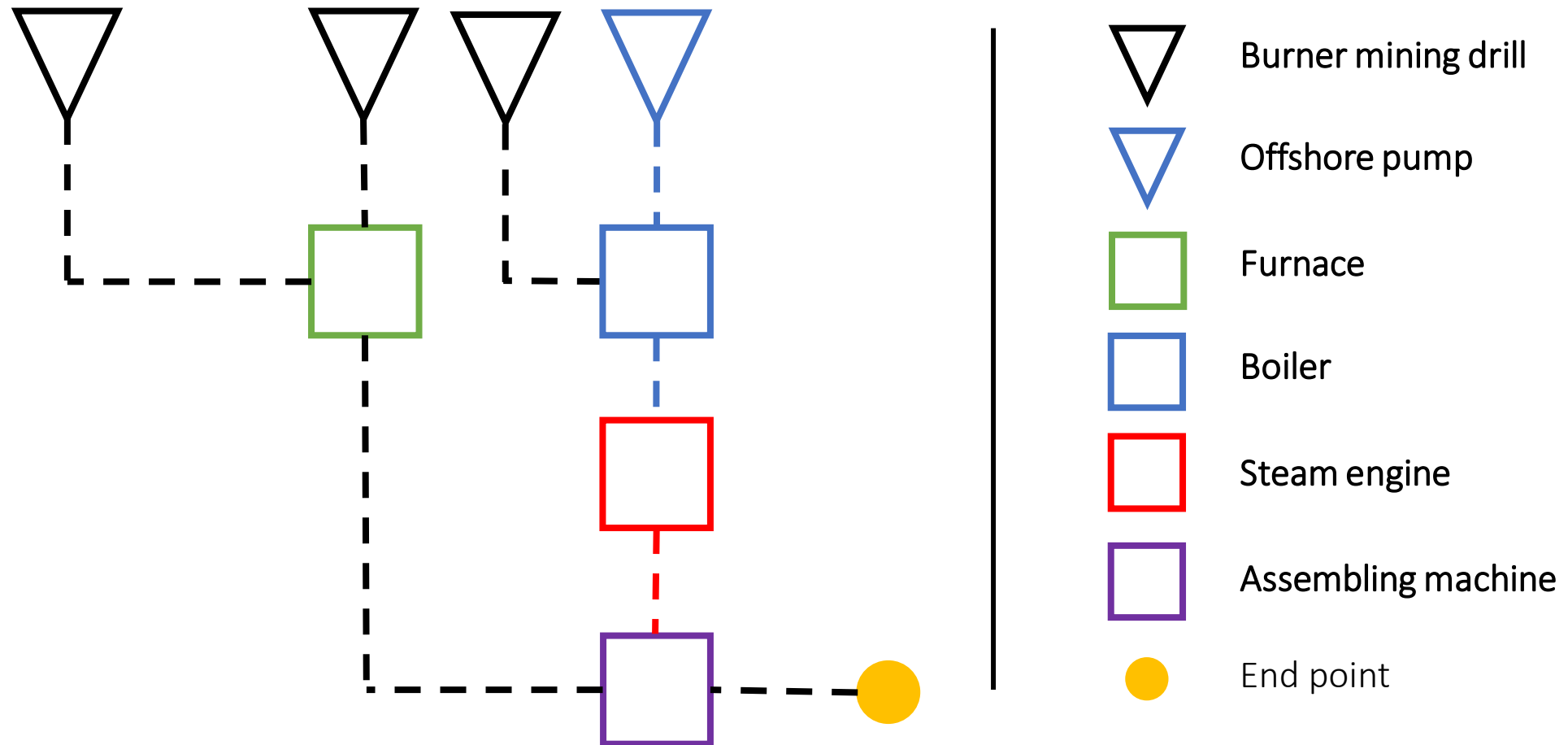
Some tools

VisualParadigm Online

PRISM
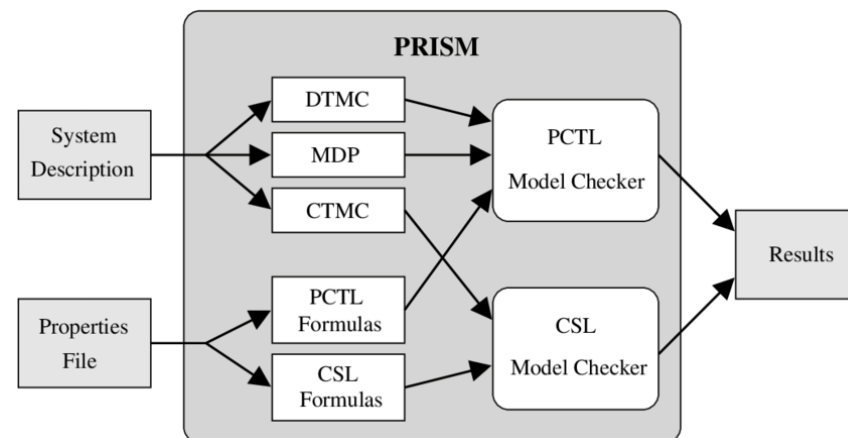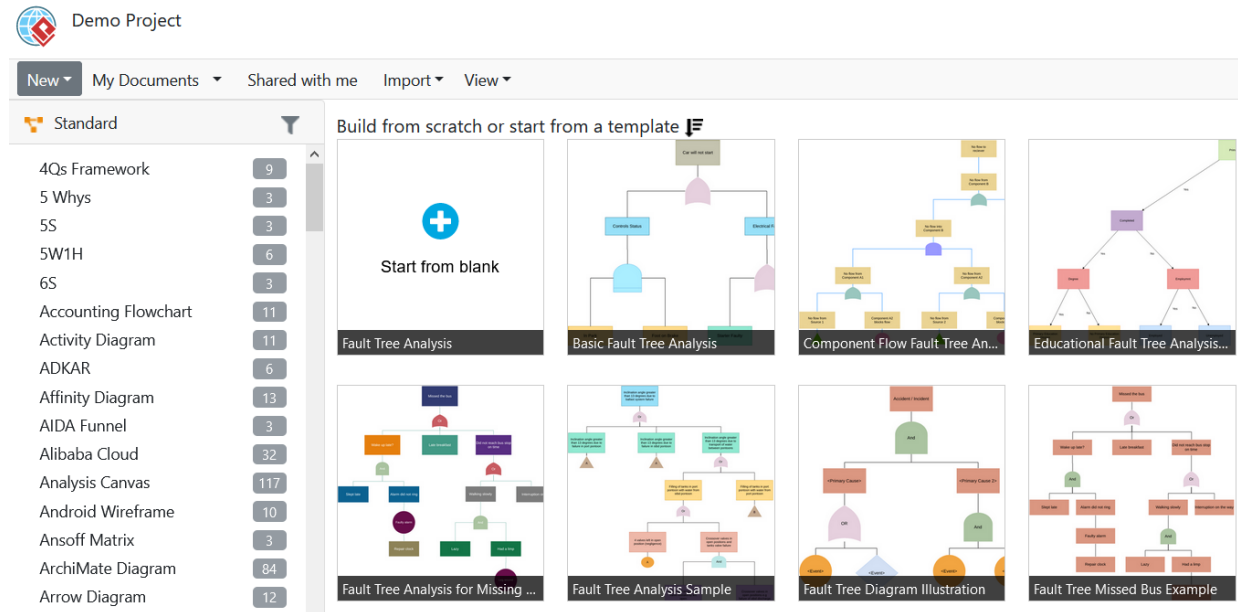
Interesting property to check

Estimate and compare the probability that faults from different low-level events cause a system failure

→ Production of Assembling Machine is zero

System Failure
Undesirable event
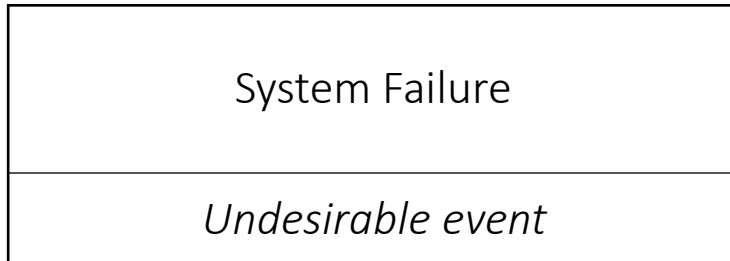
Top Level Event (TLE)

This, allows us to identify the most critical component of the system and we can then apply redundancy (TMR) on this element for example

Some mechanisms

Fault propagation:

An error in a node at a lower level of the tree can propagate to a higher level
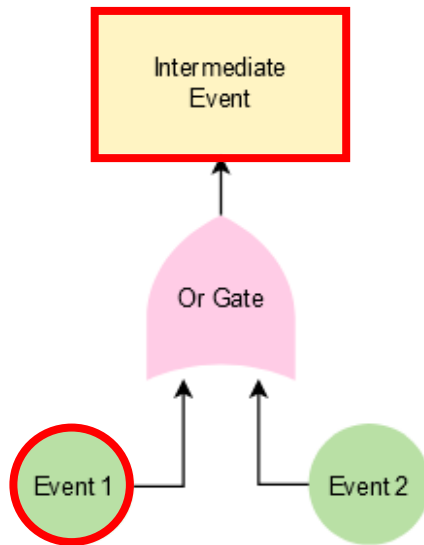
Fault masking:

Adds a probability of fault mitigation inside the gates
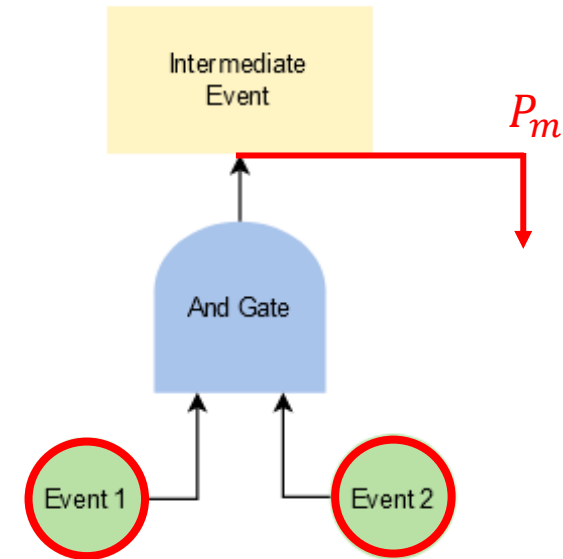
FT gates
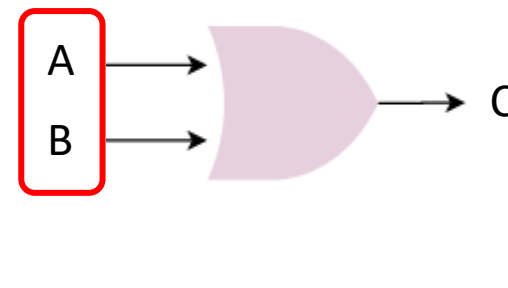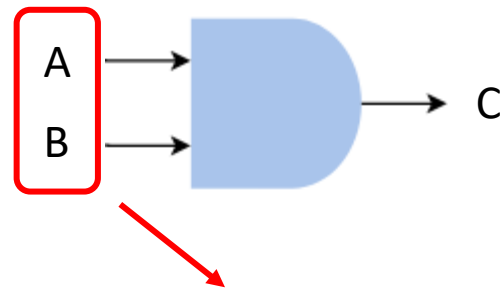
All door entrances reachable with probability and trigger not blockeding triggered

The Only one reachability and trigger is triggered probability and triggerable is masked
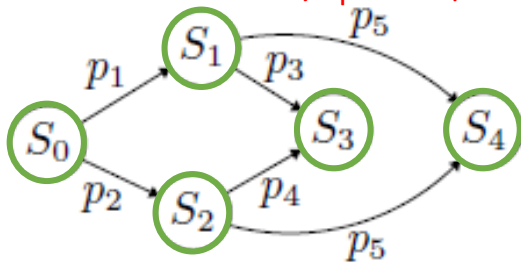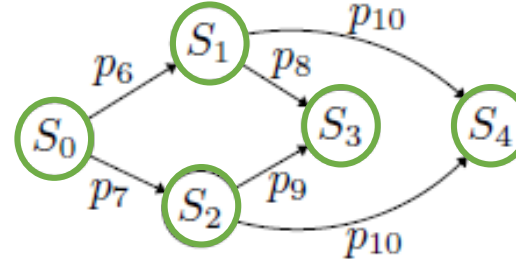
$S_2(A = 0, B = 0, M = 1)$

$S_4(A = 0, B = 0, M = 1)$

Example: Door combination
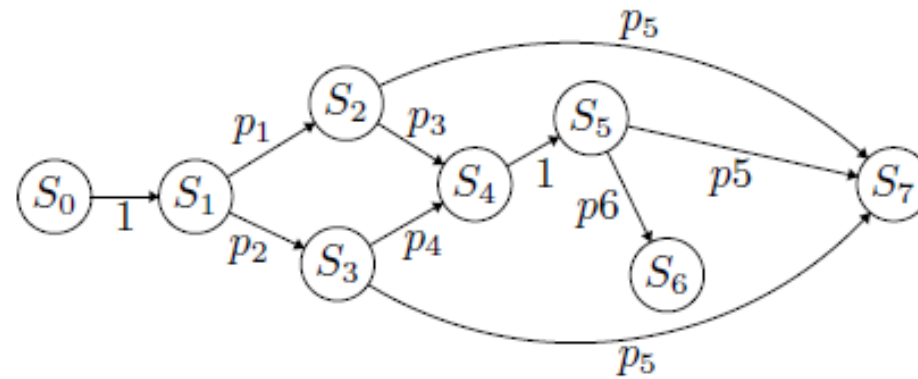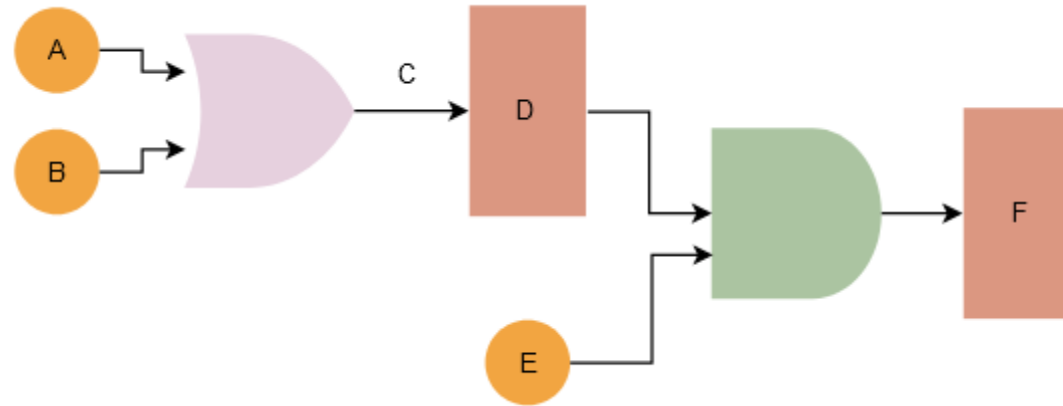
FT gates with PRISM

AND gate

```
module and_gate
[] (and=1)&(X=0)&(Y=0)&(M=0)&(Z=0)->p1:(X'=1)&(and'=2)
                                    +p2:(Y'=1)&(and'=2);
[] (X=1)&(Y=0)&(M=0)->p5:(M'=1)&(X'=0)+p3:(Y'=1)&(Z'=1);
[] (Y=1)&(X=0)&(M=0)->p5:(M'=1)&(Y'=0)+p4:(X'=1)&(Z'=1);
endmodule
```

OR gate

```
module or_gate
[] (or=1)&(A=0)&(B=0)&(M=0)&(C=0)->p1:(A'=1)&(or'=2)
                                    +p2:(B'=1)&(or'=2);
[] (A=1)&(C=0)&(M=0)->p5:(M'=1)&(A'=0)+p3:(A'=0)&(C'=1);
[] (B=1)&(C=0)&(M=0)->p5:(M'=1)&(B'=0)+p4:(B'=0)&(C'=1);
endmodule
```

```
module twogate
[] or=0 -> (or'=1);
[] c=1 -> (c'=0)&(d'=1);
endmodule
module or_gate
[] (or=1)&(a=0)&(b=0)&(m=0)&(c=0)->p1:(a'=1)&(or'=2)
                                    +p2:(b'=1)&(or'=2);
[] (a=1)&(c=0)&(m=0)->p5:(m'=1)&(a'=0)+p3:(a'=0)&(c'=1);
[] (b=1)&(c=0)&(m=0)->p5:(m'=1)&(b'=0)+p4:(b'=0)&(c'=1);
endmodule
module and_gate
[] (and=1)&(d=0)&(e=0)&(m=0)&(f=0)->p6:(d'=1)&(and'=2)
                                    +p7:(e'=1)&(and'=2);
[] (d=1)&(e=0)&(m=0)->p5:(m'=1)&(d'=0)+p8:(e'=1)&(f'=1);
[] (e=1)&(d=0)&(m=0)->p5:(m'=1)&(e'=0)+p9:(d'=1)&(f'=1);
endmodule
```

Combination OR / AND

Application example: Boiler
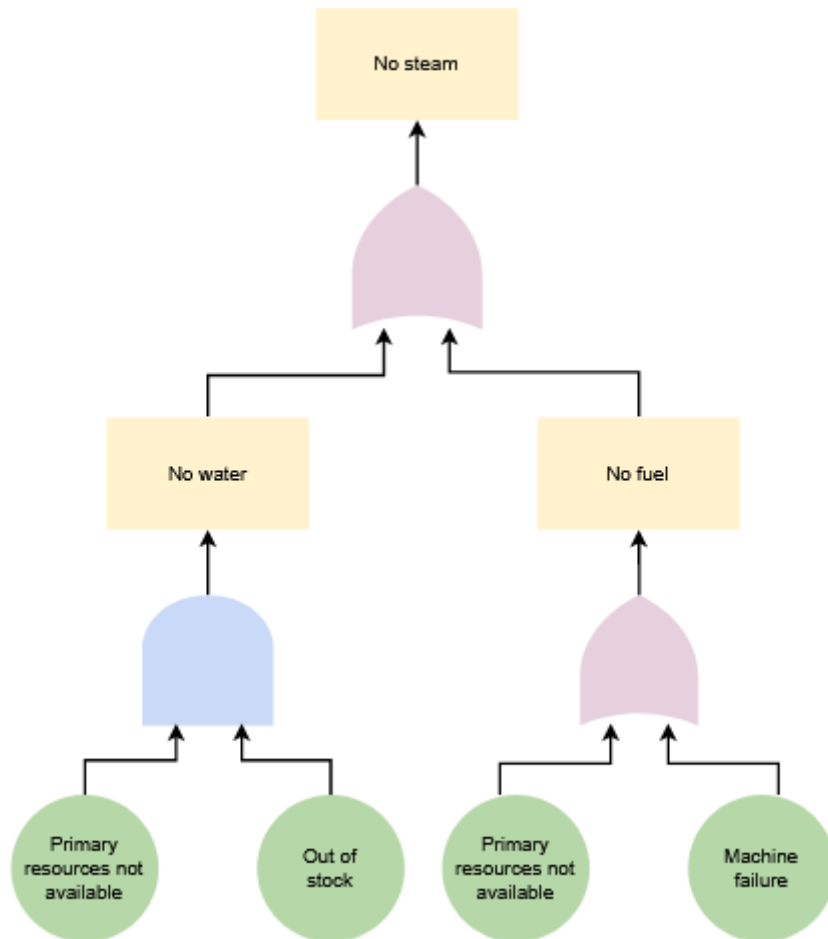
Bottom Event	Probability
Primary resources not available	3%
Out of stock	10%
Primary resources not available	7%
Machine failure	25%

Fault masking prob: 5%

Application example: Boiler
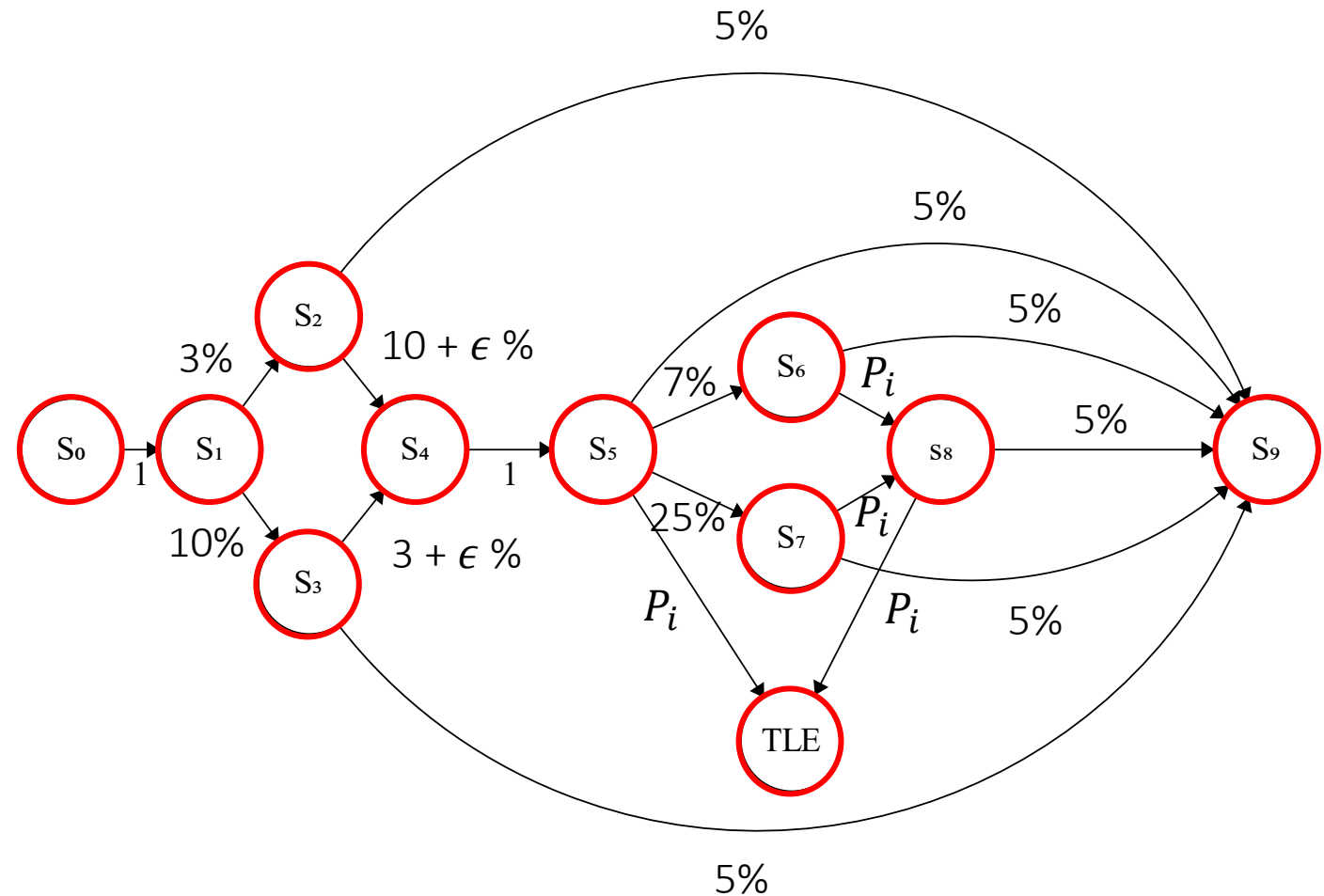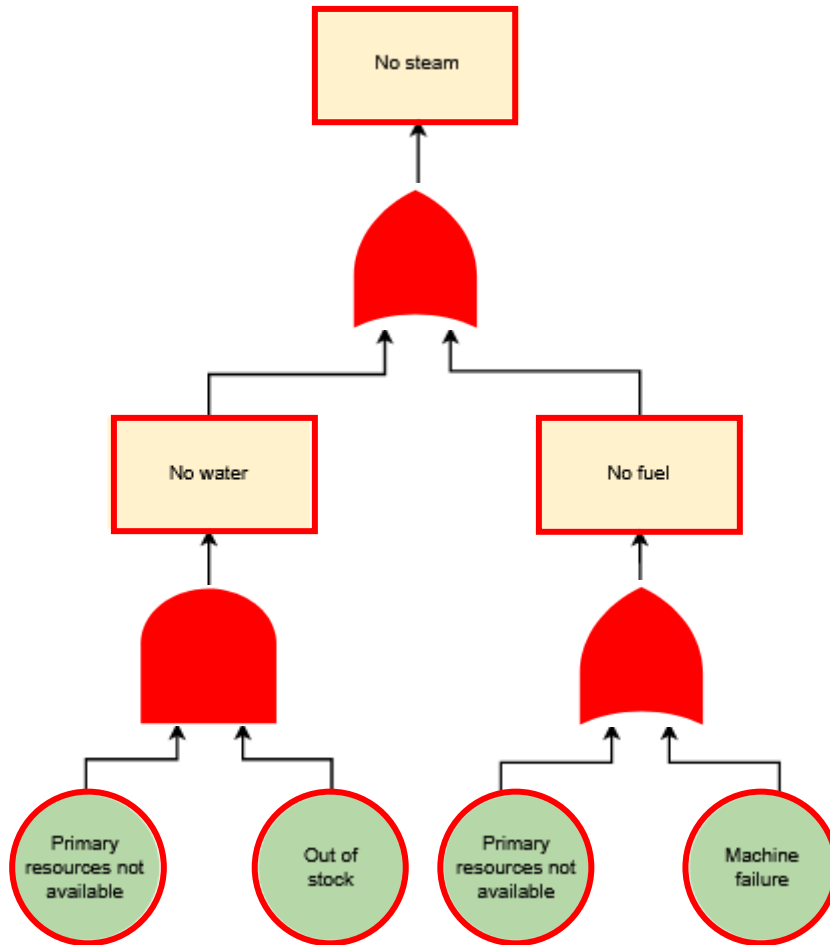
Add redundancy

Example of TMR
(Triple Modular Redundancy)

It's a way to improve a production system

with the use of thresholds …
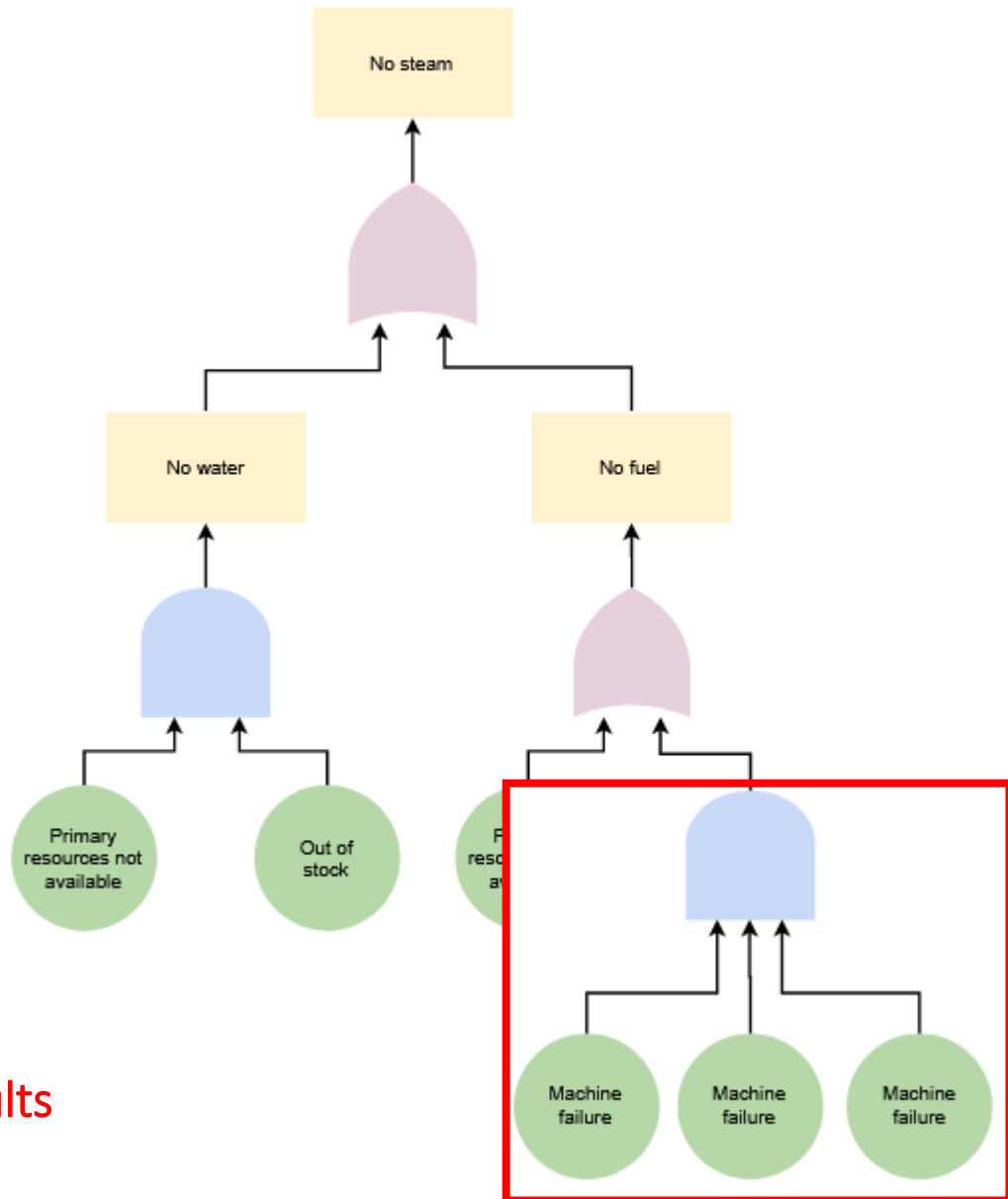
→ We can abstract this method by **masking faults**

Prod. line with VP

Production line fault tree

Diagram of the production line

21
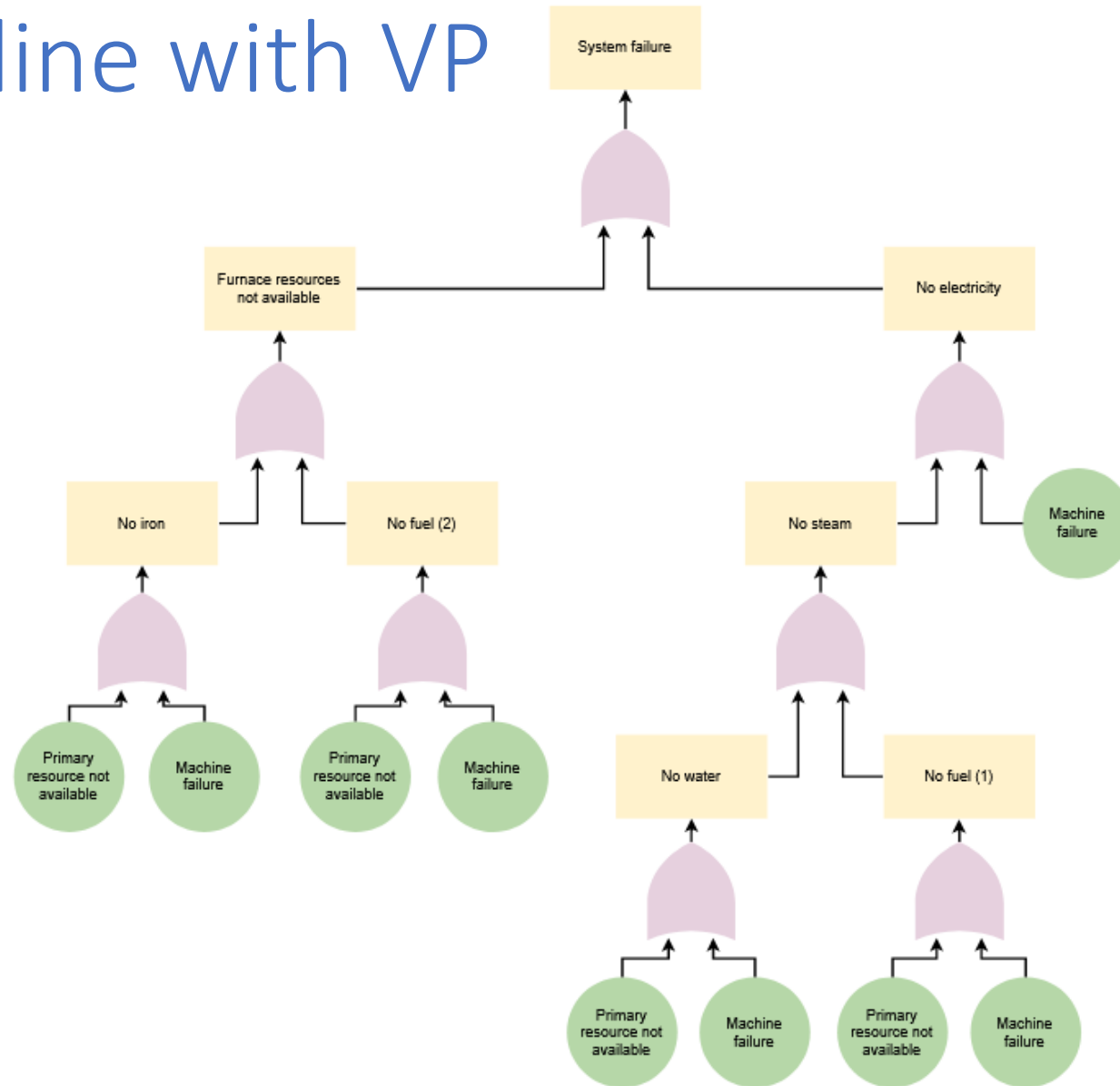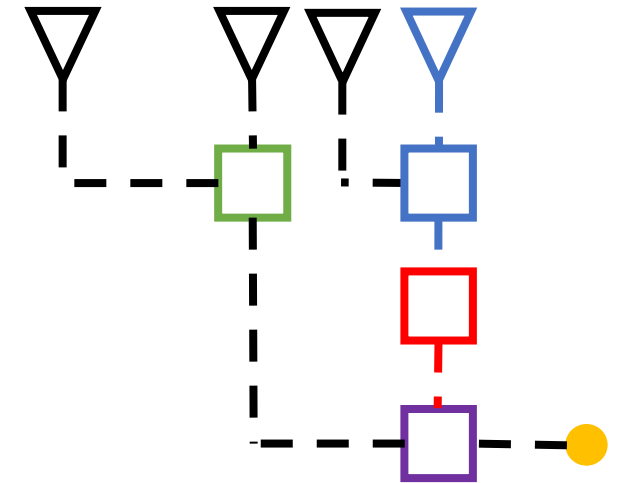
Check property with PRISM

To estimate the probability that a low-level event leads to system failure with PRISM

For a node connected to an **OR gate**:

$$P_{max} = ? \ [\ (F \ X_i = 1) \ \& \ (F \ TLE = 1)]$$

The maximum probability that event X_i will trigger and the fault is propagated to the TLE ?

For a node connected to an **AND gate**:

$$P_{max} = ? \ [\ (F \ X_i = 1) \ \& \ \left(F \ X_j = 1\right) \ \& \ (F \ TLE = 1)]$$

The maximum probability that event X_i will trigger and event X_j will trigger and the fault is propagated to the TLE ?

Gates' order

Depending on the order in which the gates are evaluated, the PA of the TF will be different
but intuitively the probability that a low-level event leads to the system failure will not change
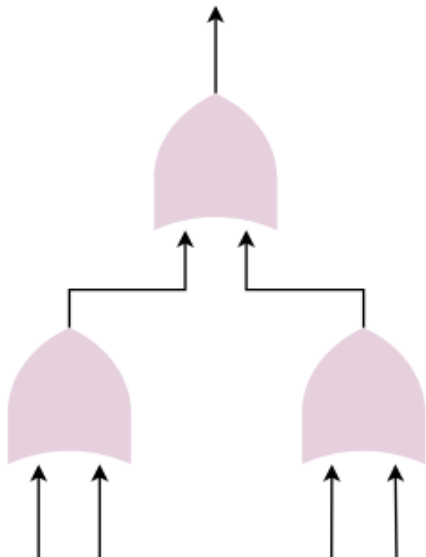
- Events on different gates have no connection

- When evaluating a door, we consider all the inputs

Idea

However, depending on the gate, only one or more inputs are needed

~~Only one entry required :~~

All entries required

: All entries required

Idea

The idea is therefore to first evaluate all the doors of a layer ...

.. and then move to a higher layer
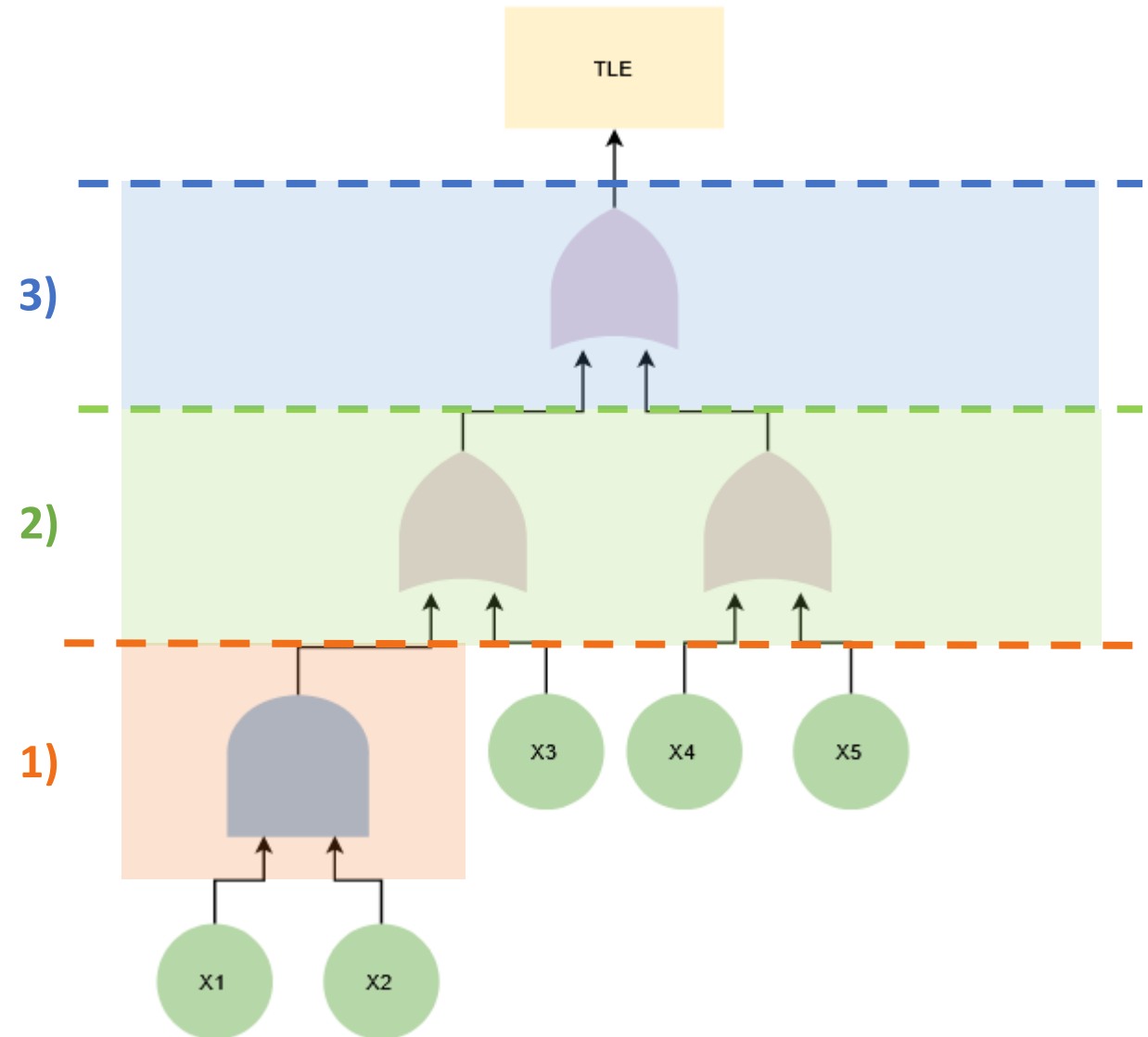
Example
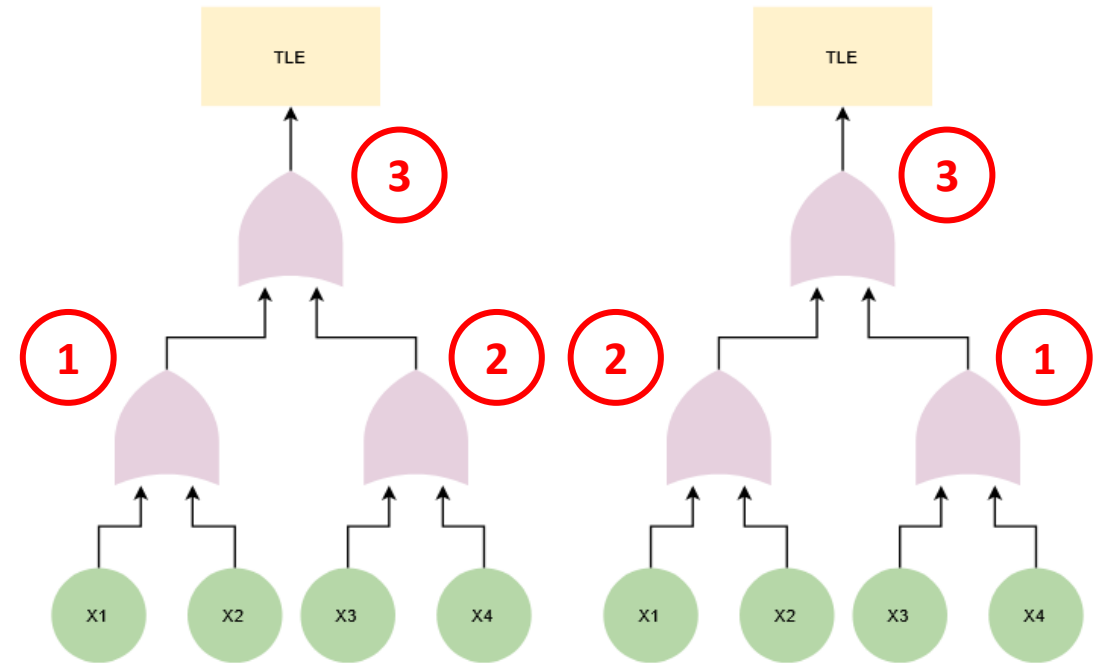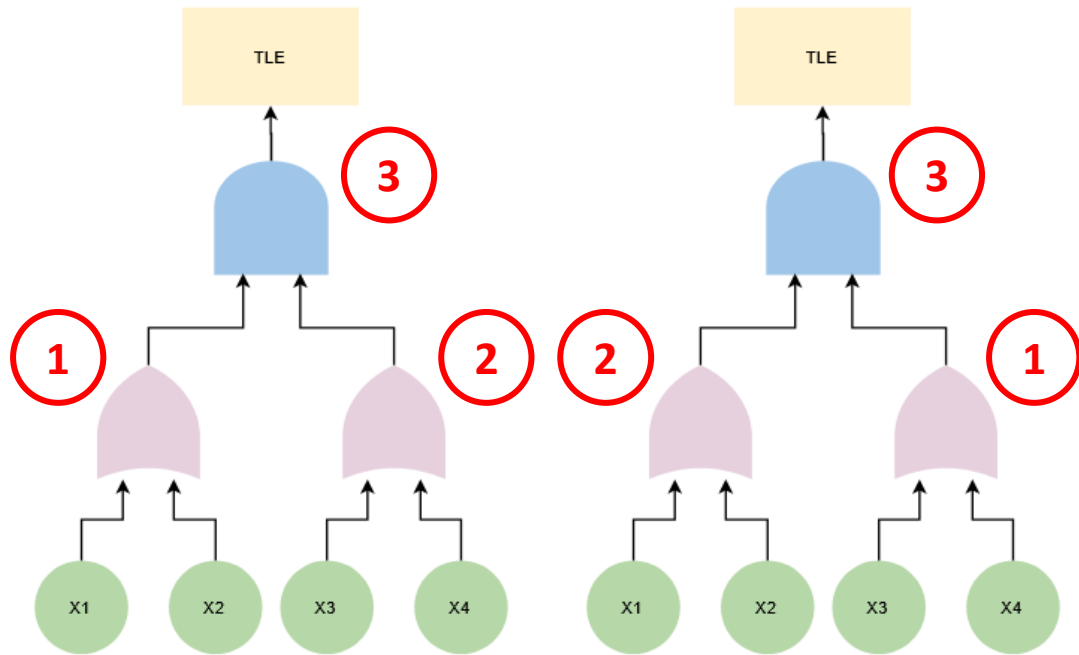
The result of property valuations are equal

Using PRISM
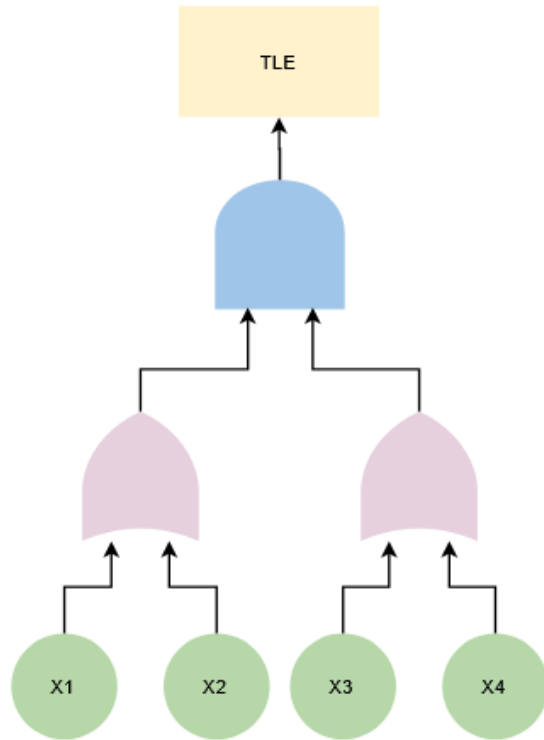
Bottom Event	Probability trigger
X_1	5%
X_2	32%
X_3	15%
X_4	20%

Fault masking prob: 10%

Simulation parameters:

Confidence: 0.01
Number samples: 1000
Max path length: 10000

$P = ? \, [\, (F \, X_1 = 1) \, \& \, (F \, TLE = 1)] = 0.102$

$P = ? \, [\, (F \, X_2 = 1) \, \& \, (F \, TLE = 1)] = 0.623$

$P = ? \, [\, (F \, X_3 = 1) \, \& \, (F \, TLE = 1)] = 0.319$

$P = ? \, [\, (F \, X_4 = 1) \, \& \, (F \, TLE = 1)] = 0.406$

Using PRISM
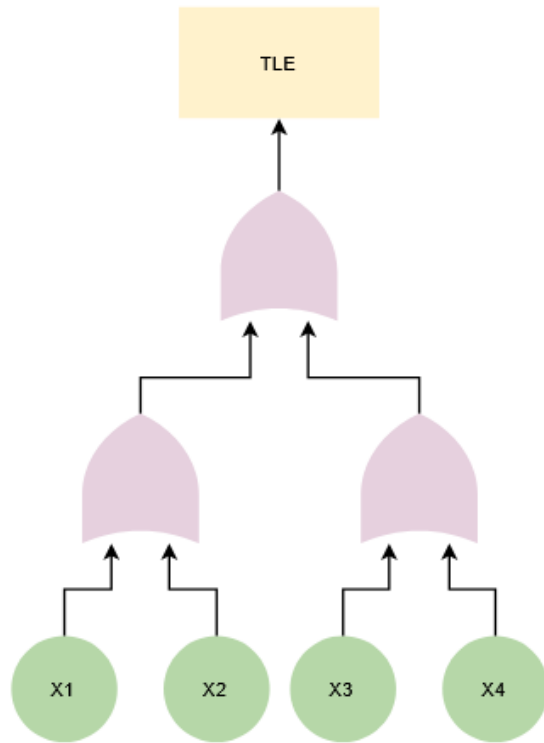
Bottom Event	Probability trigger
X_1	5%
X_2	32%
X_3	15%
X_4	20%

Fault masking prob: 10%

Simulation parameters:

Confidence: 0.01
Number samples: 1000
Max path length: 10000

$P = ?\ [\ (F\ X_1 = 1)\ \&\ (F\ TLE = 1)] = 0.104$

$P = ?\ [\ (F\ X_2 = 1)\ \&\ (F\ TLE = 1)] = 0.709$

$P = ?\ [\ (F\ X_3 = 1)\ \&\ (F\ TLE = 1)] = 0.350$

$P = ?\ [\ (F\ X_4 = 1)\ \&\ (F\ TLE = 1)] = 0.461$

DTMC vs MDP

The main difference between DTMC & MDP:

DTMC   →   In each state, the successor state is determined by
a discrete probability distribution   (Known & predictable environment)

MDP   →   In each state, the successor state is determined by a nondeterministic choice between several discrete probability distributions

(Unknown environment)

We will test both and observe the differences

Recall: Prod. line
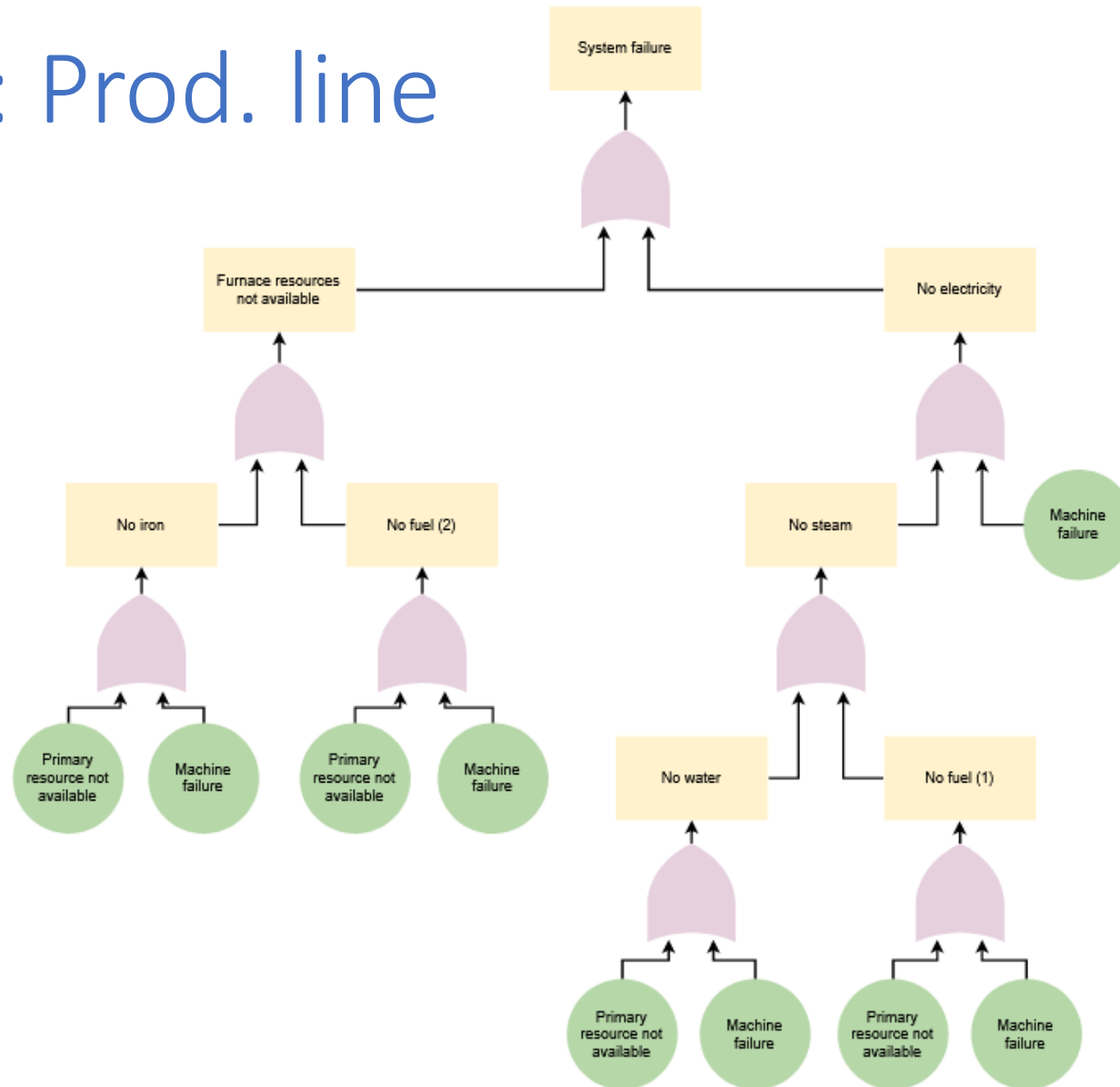
Production line fault tree
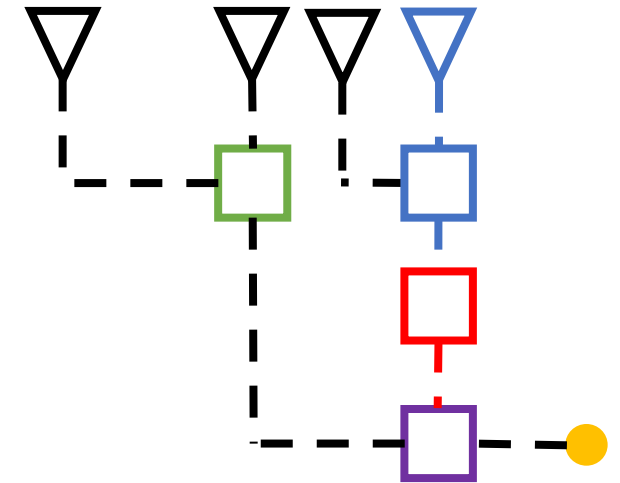
Diagram of the production line

Corresponding PA
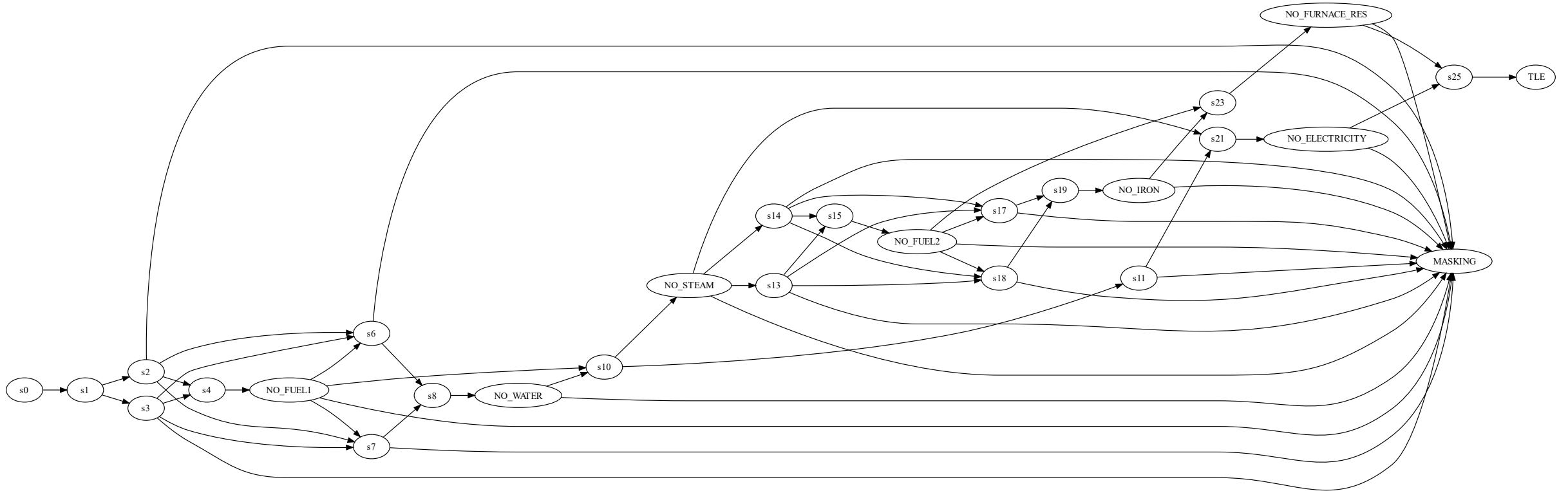
Properties to check with our propagation model

Estimate and compare the probability that a fault in a low-level events cause a system failure **before X_t time units**

$$P_{max} = ? \; [\; (F \; X_i = 1) \; \& \; (F \; TLE = 1) \; \& \; (F \; T < X_t) \;]$$

Add time value to each machine

T += 3

3 UT

T += 3

2 UT

2 UT   2 UT   1 UT

1 UT

1 UT
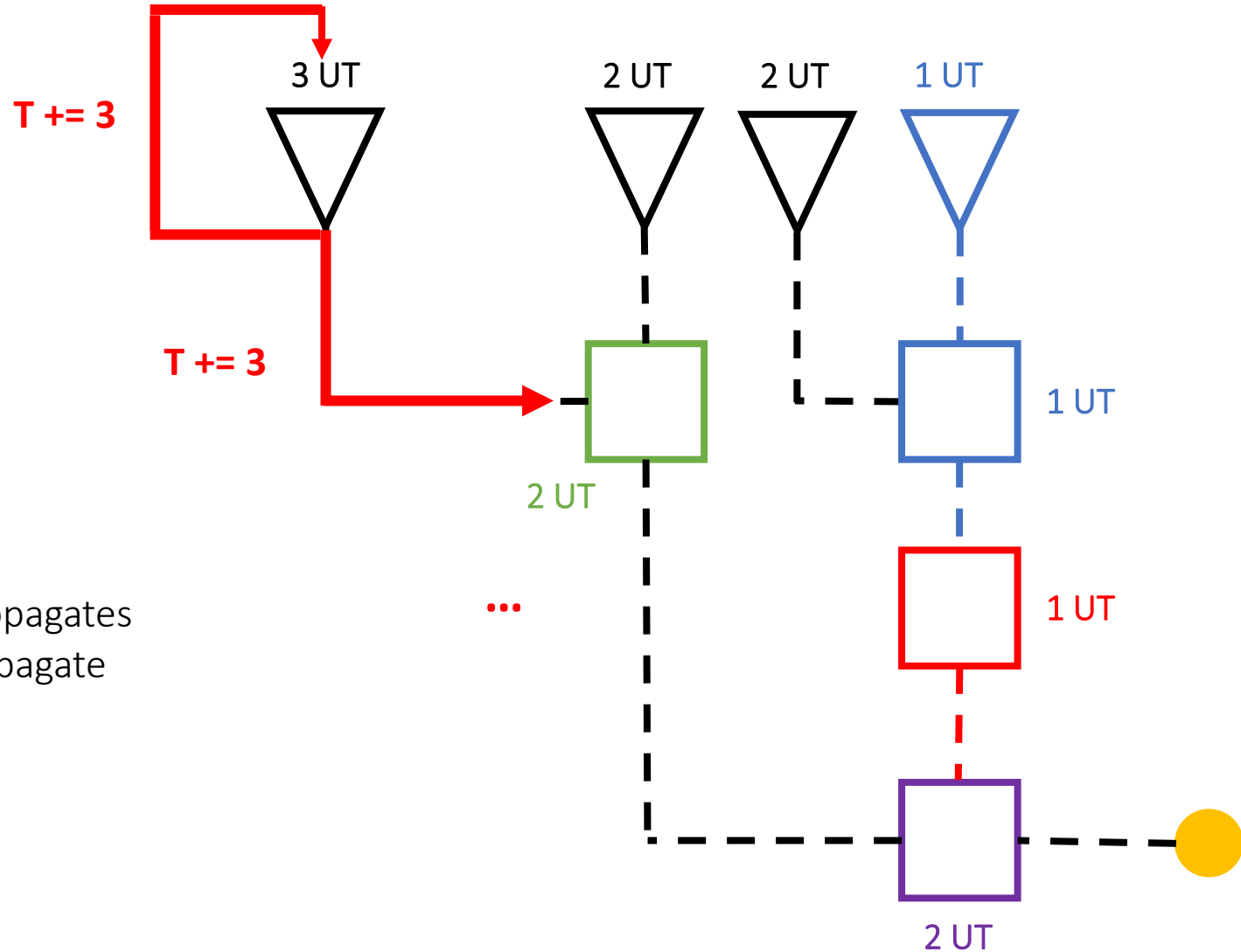
Time increment when a fault propagates
through a gate or does not propagate

•••

2 UT

Using PRISM

Bottom Event	Probability trigger
Primary res. (X_1)	0.32
Machine failure (X_2)	0.05
Primary res. (X_3)	0.15
Machine failure (X_4)	0.20
Primary res. (X_5)	0.32
Machine failure (X_6)	0.05
Primary res. (X_7)	0.10
Machine failure (X_8)	0.05
Machine failure (X_9)	0.25

$P = ? \, [(F \, X_1 = 1) \, \& \, (F \, TLE = 1) \, \& \, (T < 20)] = 0.73147581$

$P = ? \, [(F \, X_2 = 1) \, \& \, (F \, TLE = 1) \, \& \, (T < 20)] = 0.13139391$

$P = ? \, [(F \, X_3 = 1) \, \& \, (F \, TLE = 1) \, \& \, (T < 20)] = 0.34049867$

$P = ? \, [(F \, X_4 = 1) \, \& \, (F \, TLE = 1) \, \& \, (T < 20)] = 0.45398480$

$P = ? \, [(F \, X_5 = 1) \, \& \, (F \, TLE = 1) \, \& \, (T < 20)] = 0.73571484$

$P = ? \, [(F \, X_6 = 1) \, \& \, (F \, TLE = 1) \, \& \, (T < 20)] = 0.14989343$

$P = ? \, [(F \, X_7 = 1) \, \& \, (F \, TLE = 1) \, \& \, (T < 20)] = 0.51207102$

$P = ? \, [(F \, X_8 = 1) \, \& \, (F \, TLE = 1) \, \& \, (T < 20)] = 0.25612831$

$P = ? \, [(F \, X_9 = 1) \, \& \, (F \, TLE = 1) \, \& \, (T < 20)] = 0.06466131$

Fault propagation prob: 90%

Fault masking prob: 10%

Parallelism between machines

We go through the gates of the tree sequentially for the propagation of faults …

… but for the temporal notion we must consider the parallelism of certain machines

Parallelism: How it works

$T_1 = \left\{ \quad T_1 + 2 * v_1 \quad v_1 < \text{max\_}M_1 \right.$

$T_2 = \left\{ \quad T_2 + 1 * v_2 \quad v_2 < \text{max\_}M_2 \right.$

$T_3 = \left\{ \begin{array}{l} \max(T_1, T_2) + 1 \\ T_1, T_2 = \max(T_1, T_2) + 1 \end{array} \right.$

$T_4 = \left\{ \quad T_4 + 3 * v_4 \quad v_4 < \text{max\_}M_4 \right.$

$T_5 = \left\{ \quad T_5 + 2 * v_5 \quad v_5 < \text{max\_}M_5 \right.$

$T_6 = \left\{ \begin{array}{l} \max(T_4, T_5) + 2 \\ T_4, T_5 = \max(T_4, T_5) + 2 \end{array} \right.$

$T_7 = \left\{ \begin{array}{l} T_3 + 1 \\ T_1, T_2 = T_3 + 1 \end{array} \right.$

$T_f = \left\{ \begin{array}{l} \max(T_6, T_7) + 2 \\ T_1, T_2, T_4, T_5 = \max(T_6, T_7) + 2 \end{array} \right.$
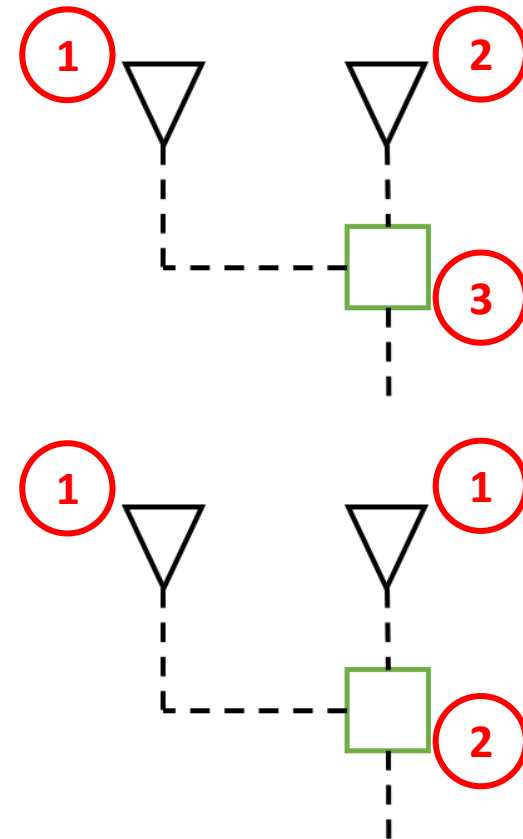
Parallelism: How it works
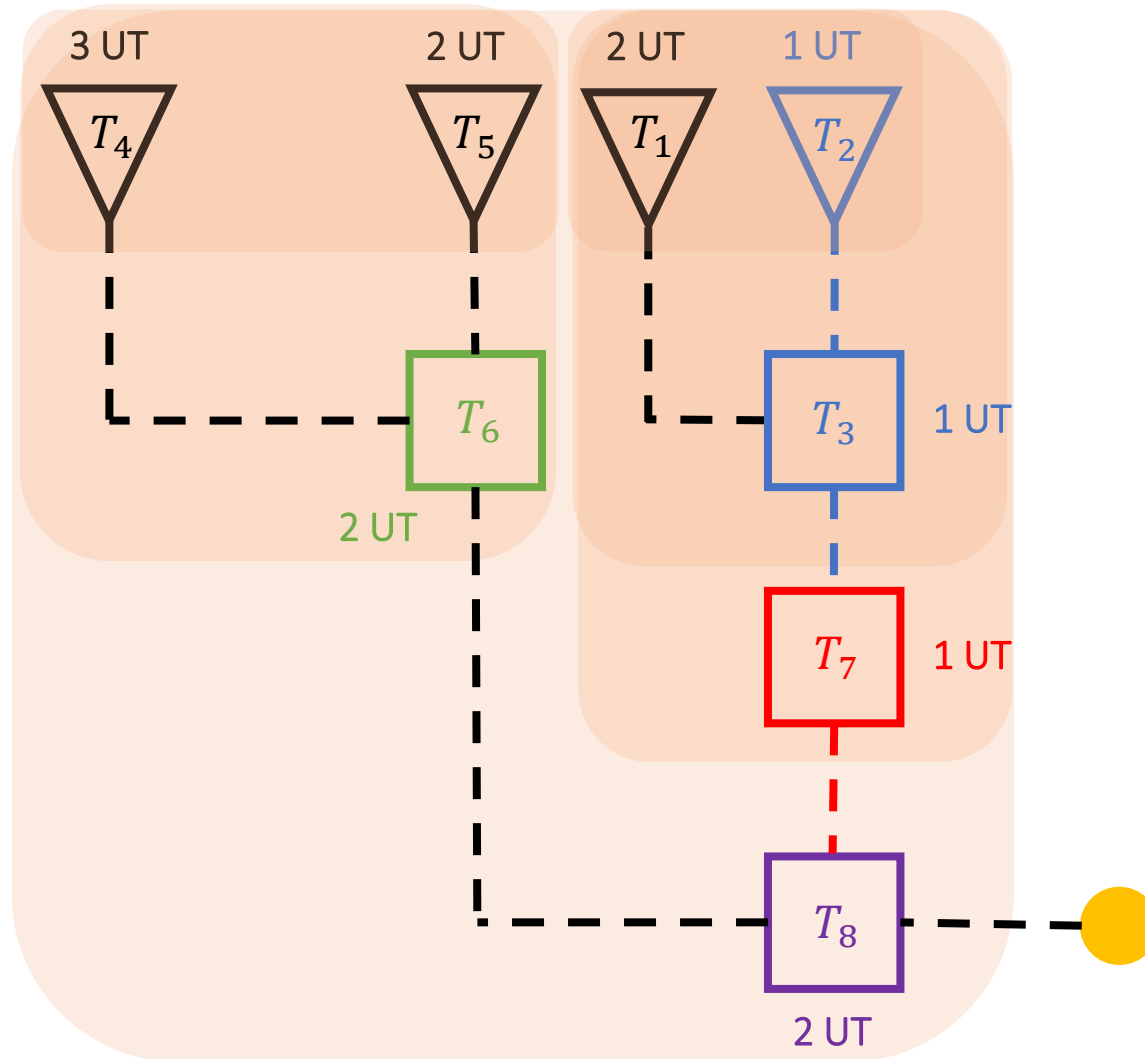
$$T_1 = \begin{cases} T_1 + 2 * v_1 & v_1 < \text{max\_}M_1 \end{cases}$$

$$T_2 = \begin{cases} T_2 + 1 * v_2 & v_2 < \text{max\_}M_2 \end{cases}$$

$$T_3 = \begin{cases} \max(T_1, T_2) + 1 \\ T_1, T_2 = \max(T_1, T_2) + 1 \end{cases}$$

Results: $T_{f1} < 10$

Bottom Event	Probability trigger
Primary res. (X_1)	0.32
Machine failure (X_2)	0.05
Primary res. (X_3)	0.15
Machine failure (X_4)	0.20
Primary res. (X_5)	0.32
Machine failure (X_6)	0.05
Primary res. (X_7)	0.10
Machine failure (X_8)	0.05
Machine failure (X_9)	0.25

Fault propagation prob: 90%

Fault masking prob: 10%

$$P = ?\left[(F\ X_1 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10)\right] = 0.54066383$$

$$P = ?\left[(F\ X_2 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10)\right] = 0.08447872$$

$$P = ?\left[(F\ X_3 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10)\right] = 0.26791824$$

$$P = ?\left[(F\ X_4 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10)\right] = 0.35722432$$

$$P = ?\left[(F\ X_5 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10)\right] = 0.54066383$$

$$P = ?\left[(F\ X_6 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10)\right] = 0.08447872$$

$$P = ?\left[(F\ X_7 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10)\right] = 0.41676170$$

$$P = ?\left[(F\ X_8 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10)\right] = 0.20838085$$

$$P = ?\left[(F\ X_9 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10)\right] = 0.12502851$$

Results: $T_{f1} < 10$

Bottom Event	Probability trigger
Primary res. (X_1)	0.32
Machine failure (X_2)	0.05
Primary res. (X_3)	0.15
Machine failure (X_4)	0.20
Primary res. (X_5)	0.32
Machine failure (X_6)	0.05
Primary res. (X_7)	0.10
Machine failure (X_8)	0.05
Machine failure (X_9)	0.25

Fault propagation prob: 90%

Fault masking prob: 10%

$$P = ? \left[(F\ X_1 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10) \right] = 0.54066383$$

$$P = ? \left[(F\ X_2 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10) \right] = 0.08447872$$

$$P = ? \left[(F\ X_3 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10) \right] = 0.26791824$$

$$P = ? \left[(F\ X_4 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10) \right] = 0.35722432$$

$$P = ? \left[(F\ X_5 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10) \right] = 0.54066383$$

$$P = ? \left[(F\ X_6 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10) \right] = 0.08447872$$

$$P = ? \left[(F\ X_7 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10) \right] = 0.41676170$$

$$P = ? \left[(F\ X_8 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10) \right] = 0.20838085$$

$$P = ? \left[(F\ X_9 = 1)\ \&\ (F\ TLE = 1)\ \&\ (T_{f1} < 10) \right] = 0.12502851$$

Results: $T_{f2} < 20$

Bottom Event	Probability trigger
Primary res. (X_1)	0.32
Machine failure (X_2)	0.05
Primary res. (X_3)	0.15
Machine failure (X_4)	0.20
Primary res. (X_5)	0.32
Machine failure (X_6)	0.05
Primary res. (X_7)	0.10
Machine failure (X_8)	0.05
Machine failure (X_9)	0.25

Fault propagation prob: 90%

Fault masking prob: 10%

$P = ? \left[(F\ X_1 = 1) \ \& \ (F\ TLE = 1) \ \& \ (T_{f2} < 20) \right] = 0.83347989$

$P = ? \left[(F\ X_2 = 1) \ \& \ (F\ TLE = 1) \ \& \ (T_{f2} < 20) \right] = 0.13023123$

$P = ? \left[(F\ X_3 = 1) \ \& \ (F\ TLE = 1) \ \& \ (T_{f2} < 20) \right] = 0.41301905$

$P = ? \left[(F\ X_4 = 1) \ \& \ (F\ TLE = 1) \ \& \ (T_{f2} < 20) \right] = 0.55069207$

$P = ? \left[(F\ X_5 = 1) \ \& \ (F\ TLE = 1) \ \& \ (T_{f2} < 20) \right] = 0.83347989$

$P = ? \left[(F\ X_6 = 1) \ \& \ (F\ TLE = 1) \ \& \ (T_{f2} < 20) \right] = 0.13023123$

$P = ? \left[(F\ X_7 = 1) \ \& \ (F\ TLE = 1) \ \& \ (T_{f2} < 20) \right] = 0.64247408$

$P = ? \left[(F\ X_8 = 1) \ \& \ (F\ TLE = 1) \ \& \ (T_{f2} < 20) \right] = 0.32123704$

$P = ? \left[(F\ X_9 = 1) \ \& \ (F\ TLE = 1) \ \& \ (T_{f2} < 20) \right] = 0.19274222$

Results: $T_{f2} < 20$

Bottom Event	Probability trigger
Primary res. (X_1)	0.32
Machine failure (X_2)	0.05
Primary res. (X_3)	0.15
Machine failure (X_4)	0.20
Primary res. (X_5)	0.32
Machine failure (X_6)	0.05
Primary res. (X_7)	0.10
Machine failure (X_8)	0.05
Machine failure (X_9)	0.25

Fault propagation prob: 90%

Fault masking prob: 10%

$$P = ? \left[(F \, X_1 = 1) \, \& \, (F \, TLE = 1) \, \& \, \left(T_{f2} < 20 \right) \right] = 0.83347989$$

$$P = ? \left[(F \, X_2 = 1) \, \& \, (F \, TLE = 1) \, \& \, \left(T_{f2} < 20 \right) \right] = 0.13023123$$

$$P = ? \left[(F \, X_3 = 1) \, \& \, (F \, TLE = 1) \, \& \, \left(T_{f2} < 20 \right) \right] = 0.41301905$$

$$P = ? \left[(F \, X_4 = 1) \, \& \, (F \, TLE = 1) \, \& \, \left(T_{f2} < 20 \right) \right] = 0.55069207$$

$$P = ? \left[(F \, X_5 = 1) \, \& \, (F \, TLE = 1) \, \& \, \left(T_{f2} < 20 \right) \right] = 0.83347989$$

$$P = ? \left[(F \, X_6 = 1) \, \& \, (F \, TLE = 1) \, \& \, \left(T_{f2} < 20 \right) \right] = 0.13023123$$

$$P = ? \left[(F \, X_7 = 1) \, \& \, (F \, TLE = 1) \, \& \, \left(T_{f2} < 20 \right) \right] = 0.64247408$$

$$P = ? \left[(F \, X_8 = 1) \, \& \, (F \, TLE = 1) \, \& \, \left(T_{f2} < 20 \right) \right] = 0.32123704$$

$$P = ? \left[(F \, X_9 = 1) \, \& \, (F \, TLE = 1) \, \& \, \left(T_{f2} < 20 \right) \right] = 0.19274222$$

Results analysis

We can observe that the probability that a fault propagates and reaches the top of the tree is much higher for $T_2 > T_1$
which implies that the longer the production time, the more likely a technical failure will occur

The same machines with the same properties at the same level (of the FT) **give similar results**

The **number of time units** associated with each machine will influence the results

A particular event will be **more impacted** by events that are **more or less directly linked to it** (same door, sub-part of the tree, etc.)

Disadvantages

Our model is a bit complex and is made up of many states …

Built Model
States: 897646
Initial states: 1
Transitions: 1562080

Built Model
States: 147876427
Initial states: 1
Transitions: 275801627

… that's why we must limit the maximum number of loops concerning fault masking

Work incoming

Try to reduce complexity (code)

See & evaluate other properties

Start writing the report

References - Github

Source code: https://github.com/sardinhapatrick/PMC_PRISM

References

PRISM: https://www.prismmodelchecker.org/

Factorio wiki: https://wiki.factorio.com/Main_Page

Modélisation et simulation de flux de production:

Franck Fontanili, *Intégration d'outils de simulation et d'optimisation pour le pilotage d'une ligne d'assemblage multiproduit à transfert asynchrone,* Partie IV, page 87-133

References

FTA: https://en.wikipedia.org/wiki/Fault_tree_analysis

FTA via PMC: M. Ammar, G. B. Hamad, O. A. Mohamed and Y. Savaria, *"Efficient probabilistic fault tree analysis of safety critical systems via probabilistic model checking "*

https://ieeexplore.ieee.org/abstract/document/7880373/metrics#metrics

SML: https://fr.wikipedia.org/wiki/Systems_Modeling_Language

VP: https://online.visual-paradigm.com/fr/diagrams/features/fault-tree-analysis-software/

MDP: https://en.wikipedia.org/wiki/Markov_decision_process

References

FMTs:

M. Ammar, G. B. Hamad and O. Ait Mohamed, "Probabilistic High-Level Estimation of Vulnerability and Fault Mitigation of Critical Systems Using Fault-Mitigation Trees (FMTs)," *2019 IEEE Latin American Test Symposium (LATS)*, Santiago, Chile, 2019, pp. 1-6

https://ieeexplore.ieee.org/document/8704589

FTA via PMC (case study):

M. Ammar, K. A. Hoque and O. A. Mohamed, "Formal analysis of fault tree using probabilistic model checking: A solar array case study," *2016 Annual IEEE Systems Conference (SysCon)*, Orlando, FL, USA, 2016, pp. 1-6

https://ieeexplore.ieee.org/abstract/document/7490556

Finite State Machine Designer:

https://www.cs.unc.edu/~otternes/comp455/fsm_designer/

Probabilistic Model Checking with PRISM

Production Line

Patrick SARDINHA