

Probabilistic Model Checking with PRISM

Production Line

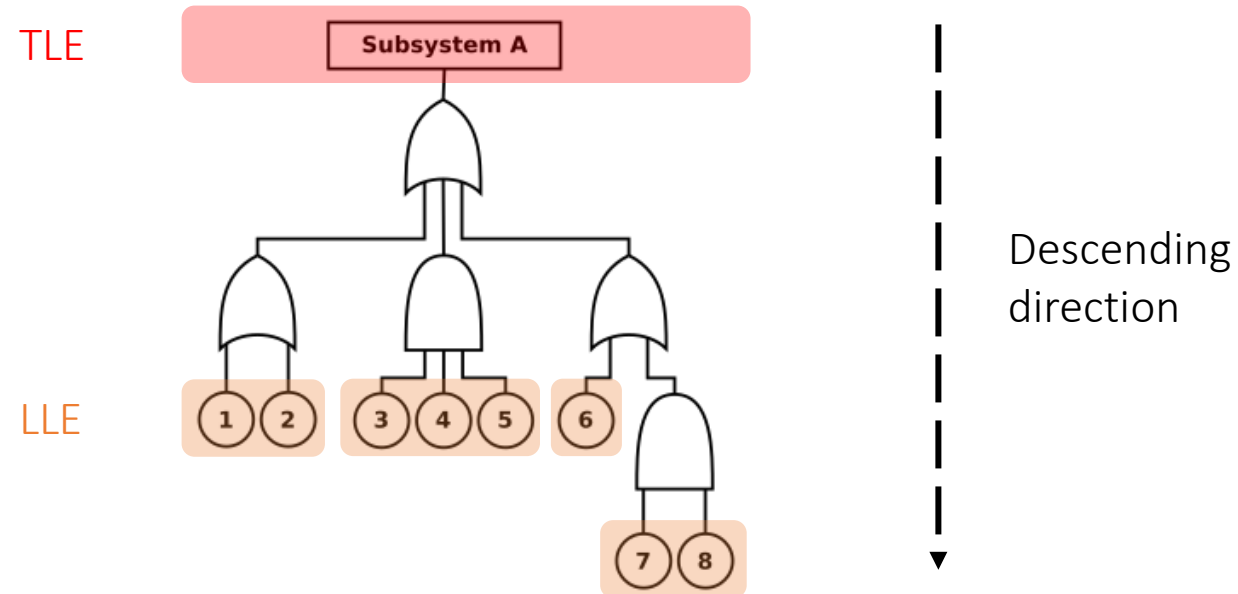
Patrick SARDINHA

Fault Trees



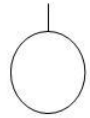
Fault Trees (FT) graphically represent possible combinations of events (Low Levels Events) leading to a predefined undesirable event (Top Level Event)

Representation:

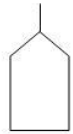


Graphic symbols

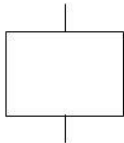
Events:



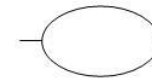
Basic event: failure in a system component



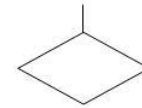
External event: expected to occur



Intermediate event: events occurring at the exit of a door



Conditioning event: an event with conditions



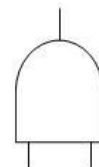
Undeveloped event: an event with insufficient information

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)

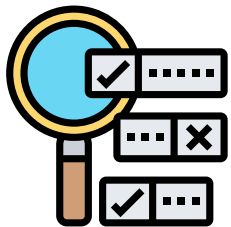


Method used to evaluate the risks of a system and allows to:

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

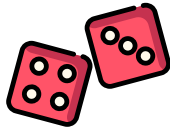


Machines that transform resources

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	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- Can break down- May be affected by an external event- Fuel not supplied- Water not supplied

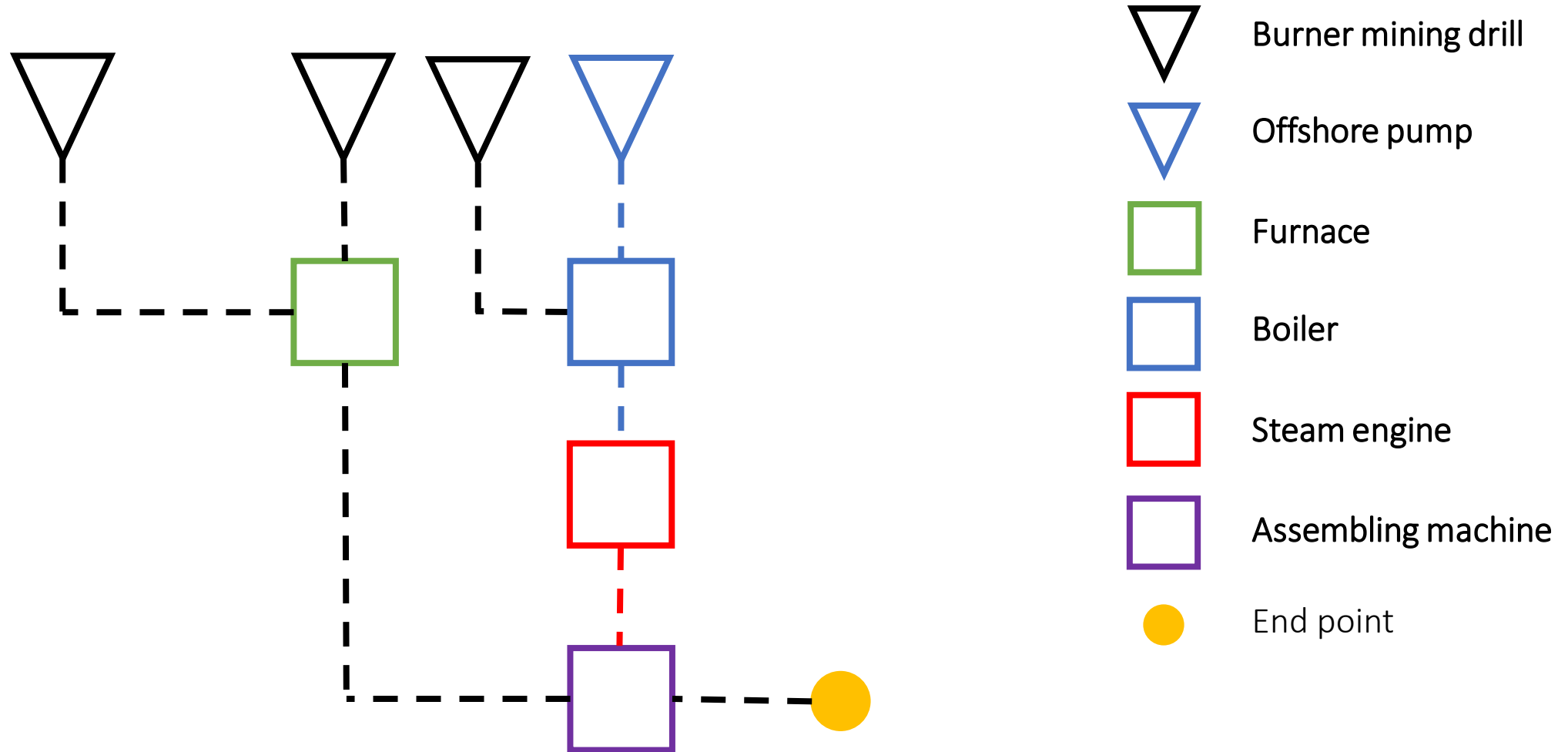
	Steam engine
Inputs	Steam
Outputs	Electricity
Basic event	<ul style="list-style-type: none">- Can break down- May be affected by an external event- Steam not supplied

Resource transformation

	Furnace
Inputs	Fuel & minerals
Outputs	Processed minerals
Basic event	<ul style="list-style-type: none">- 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	<ul style="list-style-type: none">- Can break down- May be affected by an external event- Electricity not supplied- Processed minerals not supplied

Production line: Example



Interesting property to check



Estimate the probability that the production of the assembling machine is zero

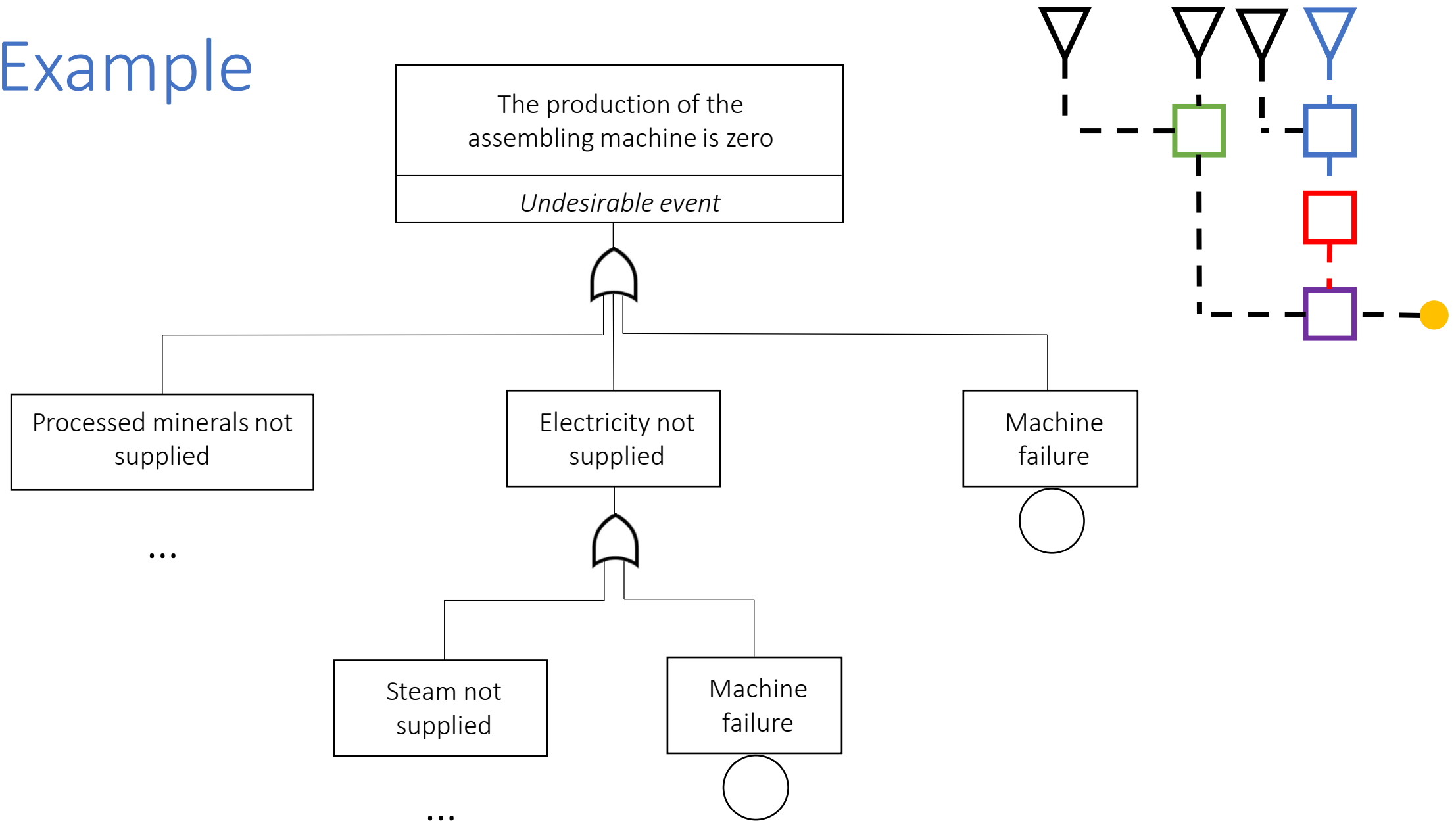
The production of the assembling machine is zero
<i>Undesirable event</i>



Top Level Event (TLE)

This can be obtained with PRISM by checking the property: $P_{max} = ? [F \ TLE = 1]$

Example



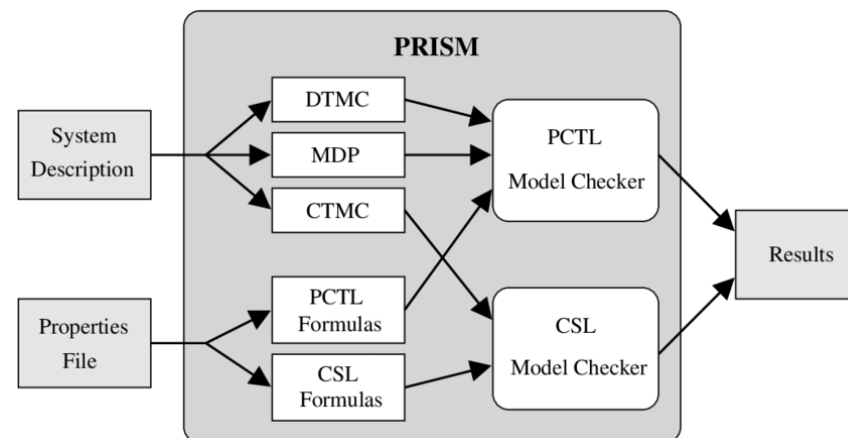
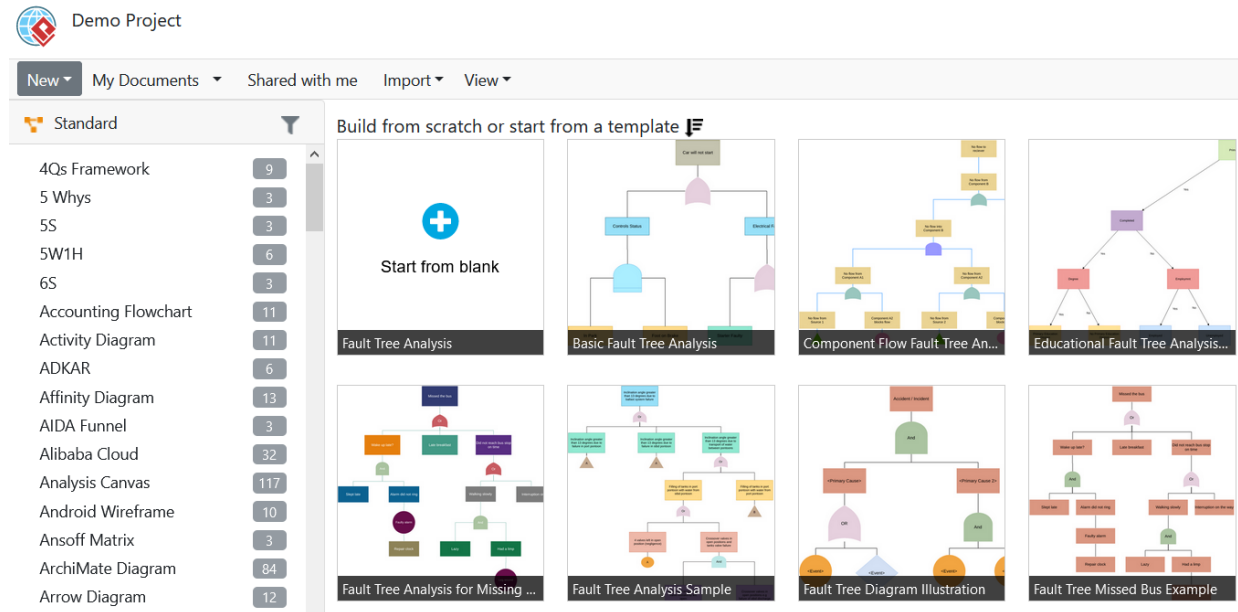
Some tools



VisualParadigm Online



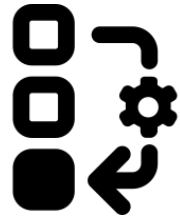
PRISM



Work incoming



Build the FT of our system with VisualParadigm



See how to model the behavior of FT gate as PA



See how to use PRISM with our system

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

Probabilistic Model Checking with PRISM

Production Line

Patrick SARDINHA