



SAFEST

Probabilistic Risk Assessment
Dynamic Fault Trees & Reward Event Trees

Static/Dynamic Fault Trees & Reward Event Trees Analysis Tool

www.safest.dgbtek.com

User Manual

Version 2.0.0

Dr. Falak Sher,
Asst. Prof. Matthias Volk,
Prof. Joost-Pieter Katoen,
Prof. Mariëlle Stoelinga

Prepared by
DGB Technologies LLC
Wyckoff, NJ 07481, USA

DGB Technologies is a multimission company specializing in formal verification tools and technologies for stochastic analysis of mission and life-critical systems.



DGB Technologies LLC
Risk & Reliability Analysis
Wyckoff, NJ 07481, USA

Static/Dynamic Fault Trees & Reward Event Trees Analysis Tool
www.safest.dgbtek.com

Dr. Falak Sher,
[DGB Technologies LLC](#)
Asst. Prof. Matthias Volk,
[Eindhoven University](#)
Prof. Joost-Pieter Katoen,
[RWTH Aachen University](#)
Prof. Mariëlle Stoelinga,
[Twente University](#)

Abstract

SAFEST is a powerful tool for modeling and analyzing both static and dynamic fault trees as well as reward event trees. Dynamic fault trees (DFTs) extend standard fault trees by providing support for faithfully modeling spare management, functional dependencies, and order-dependent failures. Reward event trees (RETs) extend traditional event trees with state rewards as well as non-deterministic decision-making at states, thus providing upper and lower bounds on the analysis results.

In addition to BDD-based analysis, the SAFEST tool provides an efficient and powerful analysis of DFTs/RETs via probabilistic model checking – a rigorous, automated analysis technique for probabilistic systems. The backbone of the analysis is based on efficient state space generation. Several optimization techniques are incorporated, such as exploiting irrelevant failures, symmetries, and independent modules. Probabilistic model checking allows us to analyze the resulting state space concerning a wide range of measures of interest. In addition, an approximation approach is provided that builds only parts of the state space and allows to refine the computations up to the desired accuracy iteratively.

The SAFEST tool allows embedding DFTs within RETs thus providing probabilities of transition branches of RETs. It provides a graphical user interface for creating, generating, simulating, simplifying, and visualizing the results of fault trees/event trees.

SAFEST is a state-of-the-art analysis tool, as demonstrated by an experimental evaluation and comparison with existing tools. A variety of case studies, including vehicle guidance systems, train operations in railway station areas, and energy systems such as (nuclear) power plants have been done. This document explains how to use the SAFEST.

Contents

[Contents](#)

- [Introduction](#)

- [Dynamic Fault Trees \(DFTs\)](#)

- [Reward Event Trees \(RETs\)](#)

- [Probabilistic Model-checking](#)

- [SAFEST Project](#)

- [Creation](#)

- [Preferences](#)

- [Open](#)

- [Export](#)

- [Features](#)

- [Help](#)

- [Status](#)

- [Fault Tree Analysis Module](#)

- [Fault Trees](#)

- [Add Fault Tree](#)

- [Import Fault Trees](#)

- [Import Fault Trees from SysML v2 Models:](#)

- [Get the SysML model from a file](#)

- [Get the SysML model/project via API](#)

- [Fault Tree Pages](#)

- [Add Fault Tree Page](#)

- [Update Fault Tree Page](#)

- [Labelled Events](#)

- [CCF Groups](#)

- [Probabilistic Dependencies](#)

- [Initial Conditions](#)

Configurations

Parameter Sets

View

Creation

Import

Duplicate

Export

Update

Constants

Constant Expressions

Failure event distributions

Empirical failure distributions

Attribute Sets

Metrics

Basic

Complex

Importance

Custom

Computing

(Exact) Analysis

Bounded analysis

Graphs

Interactive simulation

Minimal cut set (for static fault trees)

• Event Tree Analysis

Configurations

Parameter Sets

View

Creation

Import

Duplicate

Export

Update

Constants

Constant Expressions

Loss Sets

Consequence Sets

Event Trees

View

Creation

Export

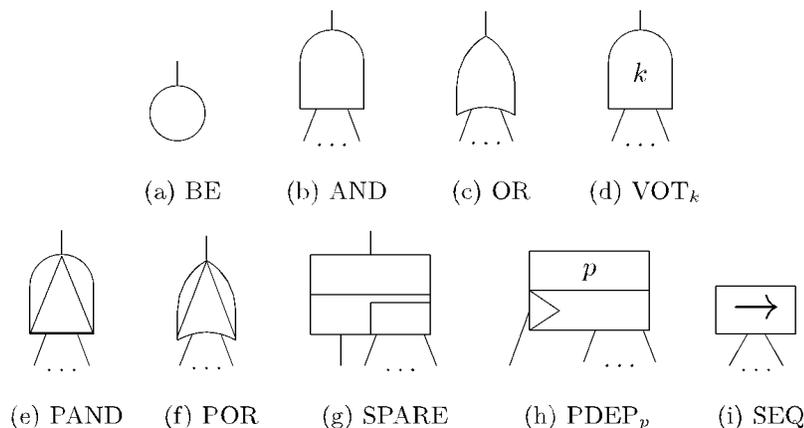
- [Import](#)
- [Update](#)
- [Computing](#)
- [\(Exact\) Analysis](#)
- [Graphs](#)
- [Interfaces](#)
 - [Constants](#)
 - [Constant Expressions](#)
 - [FT event](#)
 - [FT event expression](#)
- [Annotation of SysML Models with Safety Information](#)
- [Grammars](#)
 - [Regular Expressions of Identifiers and Numeric Constants](#)
 - [Context Free Grammar \(CFG\) of Real Expressions](#)
 - [Context Free Grammar \(CFG\) of Boolean Expressions](#)
 - [Context Free Grammar \(CFG\) of Continuous Stochastic Logic \(CSL\)](#)

Introduction

Probabilistic risk assessment (PRA) is of critical importance to ensure the safe and reliable operation of today's systems in areas such as transportation, infrastructure, power generation, space exploration, etc. Fault trees and event trees are popular models in PRA and are recommended by many standards and regulatory bodies.

Dynamic Fault Trees (DFTs)

While standard (or static) fault trees (SFT) are widely used and well supported by PRA tools, their modeling capabilities are limited. Several extensions to fault trees have been proposed



over the years to overcome these limitations. Dynamic fault trees (DFT) were introduced by Dugan and are one of the most prominent extensions. DFTs introduce new gate types that allow for more faithful modeling by providing explicit support for spare management, functional dependencies, and order-dependent failures. DFT models have been successfully applied for, e.g., aerospace systems, autonomous driving, railway engineering, and analysis of spacecraft via the COMPASS toolset.

Reward Event Trees (RETs)

Reward event trees extend standard event trees with reward models for states as well as non-deterministic decision-making at states. Unlike standard event trees, the analysis of RETs not only provides the probabilities/frequencies of different outcomes/consequences (for an initiating/accidental event) but also provides upper and lower bounds on the results in the case of decision-making. Furthermore, it allows the evaluation of expected values of different quantities of interest e.g. radionuclide emission, etc. Details about event trees can be read at the [link](#).

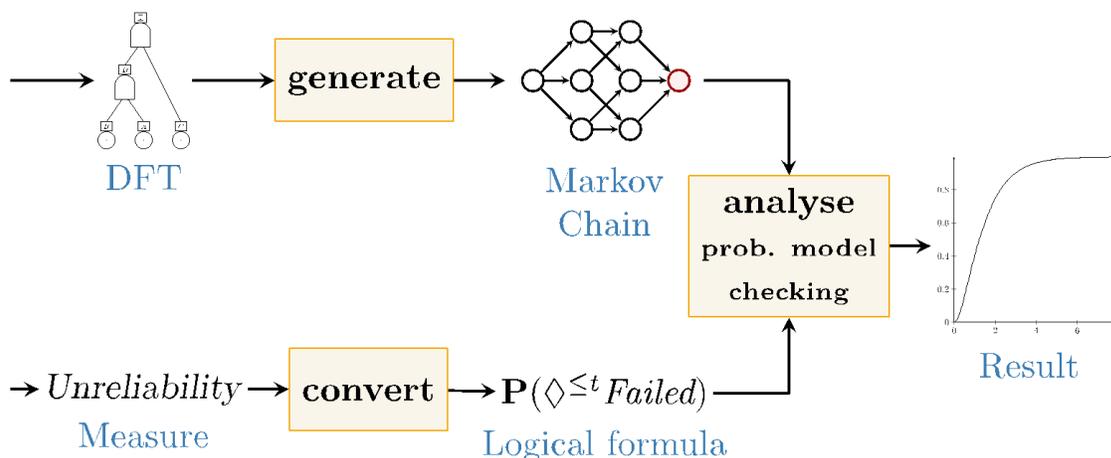
SAFEST is a modern, state-of-the-art tool that allows for modeling and analyzing both standard (static) and dynamic fault trees as well as event trees. SAFEST comes with a web-based graphical interface that allows efficient modeling, visualization, simplification, and interactive simulation of fault trees using a graphical editor. Moreover, it allows embedding DFTs

within RETs thus providing probabilities of transition branches of RETs. The analysis of dynamic fault trees/event trees is enabled via an efficient translation to Markov models and the use of state-of-the-art techniques from probabilistic model checking.

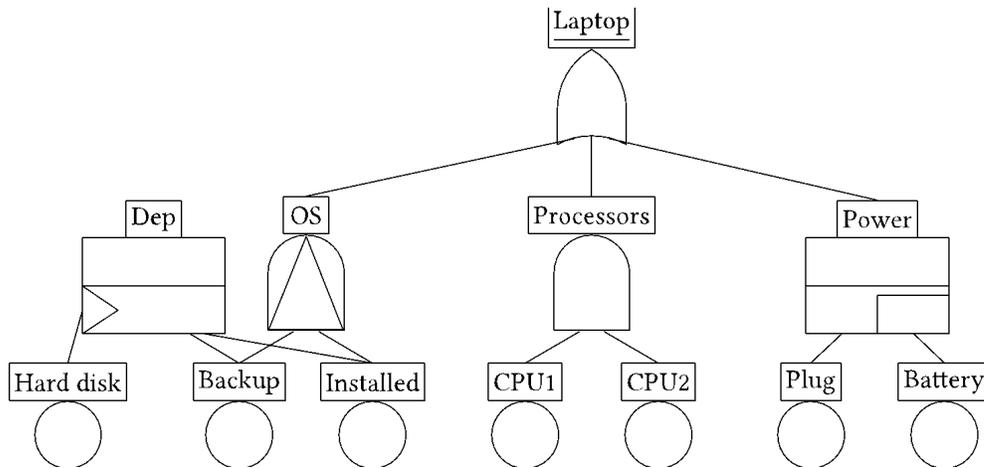
Probabilistic Model-checking

Model checking is a rigorous technique for checking whether a given model satisfies a specification given as a logical formula. Model checking uses highly optimized techniques to efficiently analyze the state space. Probabilistic model checking considers probabilistic systems that capture random behavior, such as Markov models. The approach uses tailored numerical algorithms and answers queries such as “What is the probability of a system failure within a year?” or “What is the expected time to failure when the system has entered a degraded state?”.

We apply probabilistic model checking to DFT/DET analysis. The input is a DFT/DET and a measure of interest, for instance, the unreliability or the mean-time-to-failure (MTTF). From the DFT/DET, a Markov chain is generated. The measure is converted to a logical formula. Both the Markov chain and the logical formula are fed into a probabilistic model checker which computes the results.



The use of probabilistic model checking has several advantages for the DFT/DET analysis. First, model checking supports a wide range of complex logical formulas that can be checked out of the box. Thus, we use a one-for-all analysis approach instead of having to develop algorithms tailored to each type of measure. Second, our approach uses model checking as a black box. This means we can easily change the underlying analysis tools and directly incorporate and benefit from recent advances in model-checking algorithms without changing the overall approach. Third, unlike approaches based on Monte Carlo simulation, probabilistic model checking yields exact results and, in particular, is agnostic to rare events.



The key innovation of our approach is an efficient generation of the state space to combat possible state space explosion. To this end, we developed several optimizations that exploit irrelevant failures of events, symmetric structures, and independent modules in the DFT. Furthermore, we incorporated efficient analysis techniques for static fault trees based on binary decision diagrams (BDD). Finally, we developed an approximation approach based on only building the most relevant parts of the state space. All of these techniques allow for efficient analysis of DFTs.

Our experimental evaluation shows that our tool significantly outperforms existing DFT analysis tools and can handle DFTs with several hundred elements. We have demonstrated the performance of our tool and the modeling capabilities of DFTs in several industrial case studies. Examples include DFT models for vehicle guidance systems and analyzing the impact of infrastructure failures on train operations in railway station areas.

There are two main modules of the SAFEST tool:

Fault Tree Analysis: It allows the building of models of different failure scenarios of systems that may arise during their life cycles.

Event Tree Analysis: This allows the building of event tree models that allow for analysis of the probabilities/frequencies of different outcomes/consequences based on an initiating/accidental event.

SAFEST Project

In the SAFEST tool, multiple fault tree and event tree models can be created under Fault Tree Analysis and Event Tree Analysis modules.

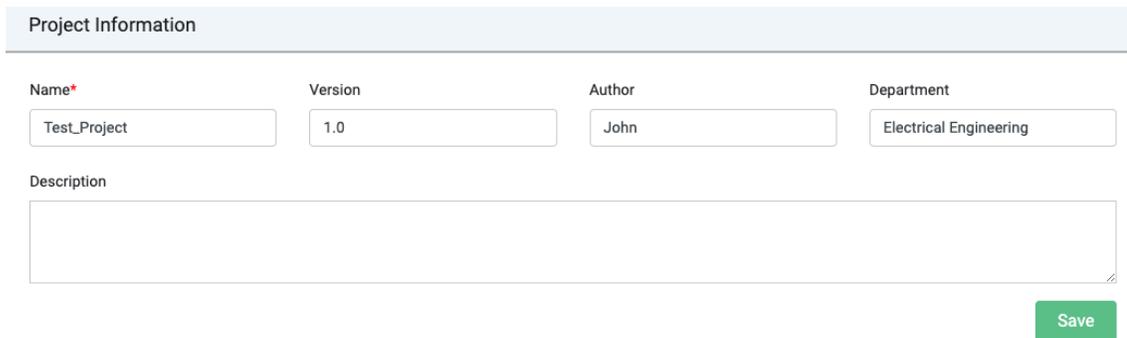
Creation

Click on “New Project” in the File menu of the toolbar. The following window will appear.



The screenshot shows a dialog box titled "New Project". It contains several input fields: "Name*" (with a red asterisk), "Version", "Author", "Department", "Features" (a dropdown menu currently showing "Basic"), and "Description" (a text area). At the bottom right, there are two buttons: "Cancel" (blue) and "Save" (green).

Fill up mandatory fields, and click the “Save” button. The following page will appear, where users can make any changes if required.



The screenshot shows a form titled "Project Information". It has four input fields for "Name*", "Version", "Author", and "Department", and a text area for "Description". The "Name*" field contains "Test_Project", "Version" contains "1.0", "Author" contains "John", and "Department" contains "Electrical Engineering". A green "Save" button is located at the bottom right.

Preferences

Click the “Preferences” in the File menu of the toolbar to set the preferences for your project.



Preferences

Canvas Analysis

Edge Type

Line

Enable Node Tags ⓘ

False

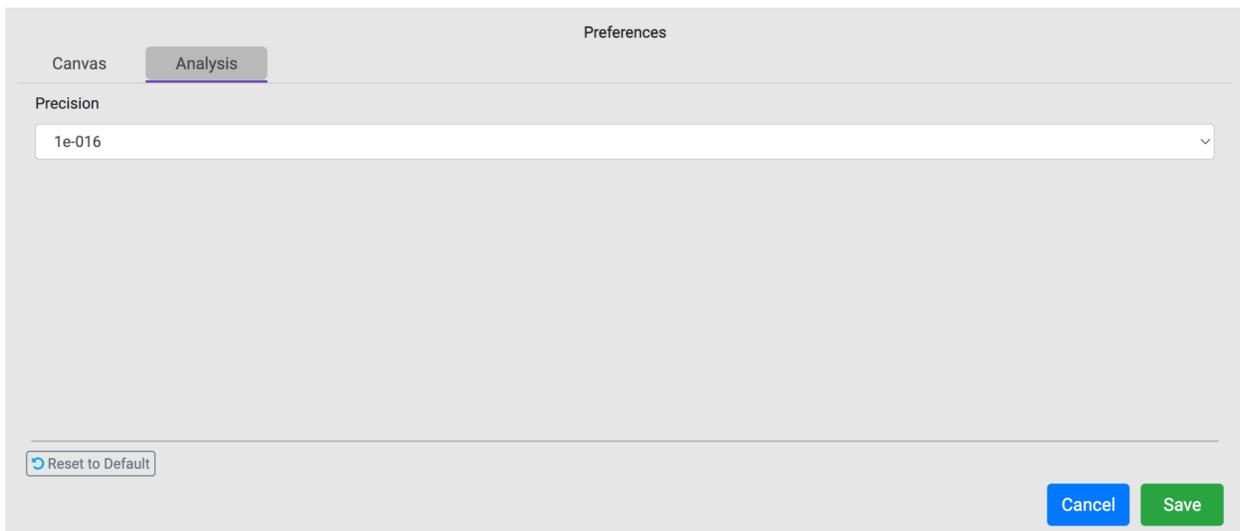
Enable Grid Lines

False

Reset to Default

Cancel Save

Preferences related to Canvas can be set.



Preferences

Canvas Analysis

Precision

1e-016

Reset to Default

Cancel Save

The precision level is set to get the computational results up to the desired level.

Open

Click the “Open Project” in the File menu of the toolbar to open an already existing SAFEST project from your drive.

Export

Click the “Export Project” in the File menu of the toolbar to export the current SAFEST project on your drive.

Features

There are two levels of features that can be enabled for a Project from the Features menu of the toolbar.

- Basic. It is for simple users. Reliability metrics can only be computed for top-level events (TLE or system_failed). Moreover, only basic reliability measures like *reliability/unreliability*, *mean time to failure*, and *average failure probability per hour* can be computed for the TLE.
- Advance. It is for advanced users or researchers. This view gives the full functionality of the SAFEST tool.

Help

In the Help menu of the toolbar, we have:

- Documentation: It contains a link to the user manual of the SAFEST tool, as well as the grammar for expressions used in the models as parameters.
- Activation key: Here you can add a license key and activate the SAFEST tool functionality.

Status

In the status bar, the information about the view of the currently selected project is shown along with the status of the Analysis engine, which is either Running or Stopped.

Fault Tree Analysis Module

It contains three sub-sections:

Fault Trees: It contains all fault trees in the project.

Configurations: It contains parameter sets and attribute sets that are used in the fault tree. It also contains metrics that are analyzed on fault trees in the computing section/

Computing: It contains all methods that are used to analyze fault trees: Analysis, Bounded Analysis, Graphs, Interactive Simulation, and Minimal Cut Sets.

Fault Trees

This section contains a list of all fault trees in a project. Each fault tree has sub-sections: Fault Tree Pages, Labelled Events, CCF Groups, Probabilistic Dependencies, and Initial Conditions.

Click on the “Fault Trees” under “Fault Tree Analysis” in the left panel to display all fault trees in a table.

Default: A fault tree that is worked upon the most can be selected as a default model by selecting the corresponding radio button.

Load: One can load/unload fault trees from the list to improve the performance. Note only fault trees that are loaded can be worked upon.

Copy: Click on the plus button in the Actions table to create a copy of the corresponding fault tree.

Download: Click on the download icon to download the corresponding fault tree.

Fault Trees							
Fault tree	Fault tree type	Reference manuals	Time-bound (Life cycle)	Description	Loaded ⁱ	Default ⁱ	Actions
BipolarHVDC	Dynamic	asdfd	365 days		<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	
ICS_Dynamic	Dynamic		1 years	Isolation Condenser System	<input checked="" type="checkbox"/>	<input type="radio"/>	
SCR_Dynamic	Dynamic		1 years	Boron Injection System	<input checked="" type="checkbox"/>	<input type="radio"/>	
RIS_Dynamic	Dynamic		1 years	Reactor Isolation Systems	<input checked="" type="checkbox"/>	<input type="radio"/>	
NPP_RPS	Dynamic		20000 hours	Reactor Protection System	<input checked="" type="checkbox"/>	<input type="radio"/>	
NPP_PIS	Dynamic		20000 hours	Pool Isolation System	<input checked="" type="checkbox"/>	<input type="radio"/>	
NPP_ECCS	Dynamic		20000 hours	Emergency Core Cooling System	<input checked="" type="checkbox"/>	<input type="radio"/>	
NPP_CIS	Dynamic		20000 hours	Containment System	<input checked="" type="checkbox"/>	<input type="radio"/>	
NPP_RRS	Dynamic		20000 hours	Reactor Regulation System	<input checked="" type="checkbox"/>	<input type="radio"/>	
NPP_EVS	Dynamic		20000 hours	Emergency Ventilation System	<input type="checkbox"/>	<input type="radio"/>	
NPP_NCHRS	Dynamic		20000 hours	Natural Circulation Heat Removal Failure	<input type="checkbox"/>	<input type="radio"/>	
NPP_PowerSupply_EDF	Dynamic		100 hours		<input type="checkbox"/>	<input type="radio"/>	
CentCompSys_5	Dynamic		12 months		<input type="checkbox"/>	<input type="radio"/>	
AFDS	Dynamic		100 hours		<input checked="" type="checkbox"/>	<input type="radio"/>	
LOCA	Dynamic		1 years		<input checked="" type="checkbox"/>	<input type="radio"/>	
AFDS_2	Dynamic		100 hours		<input checked="" type="checkbox"/>	<input type="radio"/>	
BipolarHVDC1	Dynamic		365 days		<input checked="" type="checkbox"/>	<input type="radio"/>	
BipolarHVDC2	Dynamic		365 days		<input checked="" type="checkbox"/>	<input type="radio"/>	

Click on the fault tree name in the left panel/table to see details about the model.

Model Information

Name* Version Author

Fault tree Static Dynamic

Time-bound (Life cycle)* ⁱ Parameter set ⁱ

Attribute set ⁱ Reference manuals

Description

Change fields and click the “Save” button.

Add Fault Tree

Click on the “Add fault tree” button on the “Fault Trees” page to create a new fault tree.

Fault Tree

Name*

Version

Author

Time-bound (Life cycle)* ⓘ

Parameter set ⓘ

HVDC_800KV_day
▼

Attribute set ⓘ

AttributeSet
▼

Reference manuals

▼

Description

Fault tree type Dynamic Static

- A time bound for which the model is to be analyzed may be inserted. This value can be changed at the time of analysis as well.
- A parameter set in which parameters to be used in the model are defined may be selected. It can also be changed at the time of analysis.
- An attribute set can be attached to a fault tree. It allows the annotation of additional information about the elements of fault trees. For example, all motors in a system can be attached “Motor” attribute.
- A list of reference manuals can also be attached with a fault tree.
- The type of fault tree can be selected as “Static” or “Dynamic”.

Fill up the mandatory fields and click the “Save” button.

Import Fault Trees

Click on the “Import failure model” button on the “Fault Trees” page to import an already created fault tree.

Import Fault Tree

Name*

File format

Import models
 parameters attributes

No file chosen

Select the format of the model and a file from the drive. Click the “Save” button. We support “JSON” “Galileo” and “Fault Tree” formats. Note that Fault Tree (.fm) is the format of the SAFEST tool. If the selected model has parameters/attributes, one can decide whether they are to be imported or not.

Import Fault Trees from SysML v2 Models:

Users have the option to extract failure models from SysML 2.0 models. The SysML model has to be annotated with safety information in order to generate DFTs automatically out of it. Click the “Import failure model from SysML” button on the “Failure Models” page.

Fault Trees Extraction From SysML

Get SysML models/projects via API

API base path

↻

<http://sysml2.intercax.com:9000>

Models/Projects

Commits

Get SysML model form a file

No file chosen

The user has two options to extract DFTs out of SysML models

Get the SysML model from a file

Compile a SysML model, which is annotated with safety information – please read the **Annotate SysML Models with Safety Information section** below for further details on how to annotate SysML models with safety information to prepare them for automatic extraction of DFTs out of them, in a Jupyter notebook. And run the following command to export the model in JSON format. **Currently, we support the latest version – v0.45.0 – of SysML 2.0: [SysML-v2-Release](#)**

```
%export <package_name>
```

After downloading, DFTs can be extracted from it. Select the radio button “Get SysML model from a file”, select the downloaded file (in JSON format), and click the “Extract” button.

The following popup will appear that contains fault trees of all failure scenarios that have been mentioned in the SysML model. It also contains parameters that have been given in the SysML mode e.g. failure rates of components inside the SysML.

Extracted Fault Trees from SysML

Fault Trees			
Name	Override	Load	
LaptopPackage_Laptop_laptop	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
LaptopPackage_Laptop_power	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Parameter Set			
Name	Override	Load	
LaptopPackage (8)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

The user can select the failure models as well as parameters to be included in the project.

Get the SysML model/project via API

SysML projects are normally uploaded to some central repository. One has the option to connect to that repository using its API and upload the model from there. Select the “Get SysML models/projects via API” radio button, enter a path in the “API base path” and click the circular arrow.

Fault Trees Extraction From SysML

Get SysML models/projects via API

API base path

<http://sysml2.intercax.com:9000>

Models/Projects

- ABC Sat May 27 08:08:31 CEST 2023 (379e3cca-b7df-4874-93ab-4c8627aa9539)**
- ActionTest Thu May 11 13:29:19 CDT 2023 (2c4e1b30-1f61-4f6e-8bf3-253c45fe88ec)
- ActuatorSystem_LogicalArchitecture Thu Mar 23 11:27:50 UTC 2023 (10b9f602-2f37-4808-afdd-7e4cb2db4d2f)
- AircraftFuelDistributionSystem Tue Aug 29 16:25:35 PKT 2023 (2f70107f-c98d-487c-bb08-48dcd0850f24)
- AnalysisAnnotation Fri Oct 13 12:48:03 CEST 2023 (36140cb4-fa5d-4321-91d0-feb606180c39)
- AnalysisAnnotation Fri Oct 13 15:06:54 CEST 2023 (05d7e586-7044-4b6f-a7e0-9c2c7da2c92a)
- AvionicsDataLibrary Wed Mar 29 08:46:59 MDT 2023 (27a0dac1-120d-4c2f-af52-ff0c299f1a8b)

Commits

- 2023-05-27T02:08:34.62199-04:00 (d3657db0-371d-4273-a074-b2fd79cc37d3)**

Get SysML model form a file

No file chosen

Select a project and its commit, and then click the “Extract” button to upload the SysML model. The rest of the steps are the same as above. For testing purposes, we have uploaded our “LaptopPackage” project to the above repository.

The algorithm will automatically generate fault trees and show them on the “Failure Models” page. Please read [Annotate SysML Models with Safety Information section](#) below for further details.

Fault Tree Pages

A fault tree may consist of multiple pages. Click on the “Fault Tree Pages” to view a list of pages for the corresponding fault tree.

Fault Tree Pages		
Name	Description	Actions
MainPage		 
Pole1		 
Pole2		 

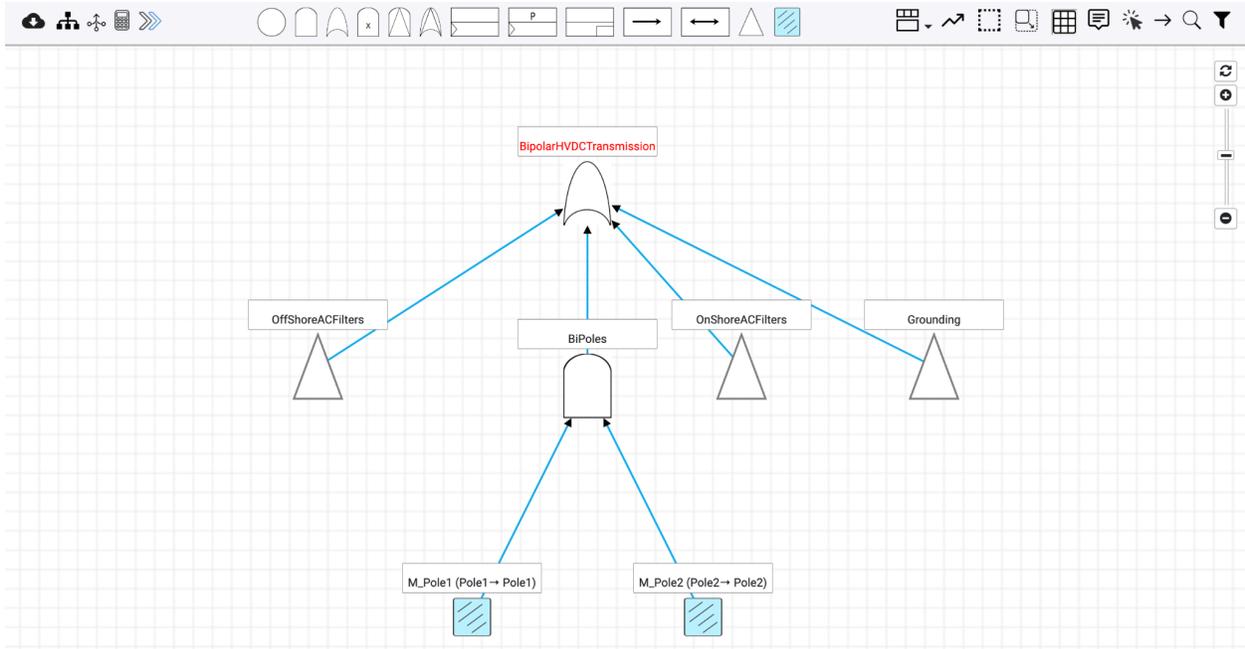
[Add page](#)

Add Fault Tree Page

Click on the “Add page” to generate a new fault tree page.

Update Fault Tree Page

Click on a fault tree page to open a drag-and-drop canvas.



- Draw your tree by dragging different elements from the toolbar.
- Click on an element to update its information in the corresponding popup window

Module Form

Title

Name* 

Create a fault tree Import a fault tree from a file

Select file format

*If there are any fault tree parameters, they will be added to the fault tree's parameter set.
A new parameter set will be created if the existing one is absent.*

No file chosen

Import parameters of the model

Tag

Tag datetime

Attributes

Reference manuals

Description

- A module can be created from scratch or uploaded from the drive. To upload, select the file (in JSON or Galileo format) and click the save button.

MUTEX Gate

Type
MUTEX

Title

Name* 
I1

Children

1	I2	
2	I3	

Only one of the children can fail at a time. MUTEX gate does not propagate failure.

Tag
None

Tag datetime
dd/mm/yyyy, --:--

Attributes

Reference manuals

Description

SEQ Gate

Type
SEQ

Title

Name* ⓘ
I1

Children

1	I2	
2	I3	

The children can only fail one-by-one from top to bottom. SEQ gate does not propagate failure.

Tag
None

Tag datetime
dd/mm/yyyy, --:--

Attributes

Reference manuals

Description

OR Gate

Type
OR

Title

Name* 
I1

Children
I2
I3
OR gate propagates failure if any of its children will fail.

Tag
None

Tag datetime
dd/mm/yyyy, --:--

Attributes

Reference manuals

Description

The element will be marked as a root of the fault tree. Generate label for the failure event 

AND Gate

Type
AND

Title

Name* 
I1

Children
I2
I3
AND gate propagates failure if all of its children will fail.

Tag
None

Tag datetime
dd/mm/yyyy, --:--

Attributes

Reference manuals

Description

The element will be marked as a root of the fault tree. Generate label for the failure event 

VOT Gate

Type
VOT

Title

Name* ⓘ
I1

Threshold(θ) * ⓘ
1

Children
I2
I3

VOT gate propagates failure only if number of children that fail is greater than the threshold value.

Tag
None

Tag datetime
dd/mm/yyyy, -:- -

Attributes

Reference manuals

Description

The element will be marked as a root of the fault tree. Generate label for the failure event ⓘ

POR Gate

Type
POR

Title

Name* 
I1

Children

1	I2	
2	I3	

POR gate fails only if the top child will fail first. Otherwise, it will enter into fail-safe state.

Tag
None

Tag datetime
dd/mm/yyyy, --:--

Attributes

Reference manuals

Description

The element will be marked as a root of the fault tree. Generate label for the failure event 

PAND Gate

Type
PAND

Title

Name* 
I1

Children

1	I2	
2	I3	

PAND gate fails only if the children will fail one-by-one from top to bottom. Otherwise, it will enter into fail-safe state.

Tag
None

Tag datetime
dd/mm/yyyy, --:-- --

Attributes

Reference manuals

Description

The element will be marked as a root of the fault tree. Generate label for the failure event 

FDEP Gate

Type
FDEP

Title

Name* 
I1

Children

1	I2	
2	I3	

The failure of first child renders all other children failed.

Tag
None

Tag datetime
dd/mm/yyyy, --:--

Attributes

Reference manuals

Description

PDEP Gate

Type
PDEP

Title

Name* 
I1

Probability (p)* 
1

Children

1	I2	
2	I3	

The failure of first child renders all other children failed with the above probability.

Tag
None

Tag datetime
dd/mm/yyyy, --:-- --

Attributes

Reference manuals

Description

SPARE Gate

Type
SPARE

Title

Name* 
I1

Children

1	I2	
2	I3	

The children are activated from top to bottom. SPARE gate propagates failure on the failure of all children.

Tag
None

Tag datetime
dd/mm/yyyy, --:-- --

Attributes

Reference manuals

Description

The element will be marked as a root of the fault tree. Generate label for the failure event 

BE

Type
BE

Title

Name* ⓘ
I2

BE models failure of a system component that cannot be decomposed further into subcomponents.

Enter failure distribution ⓘ Select failure event distribution ⓘ

Exponential

Rate (λ)* ⓘ
1 per day

Enter dormancy (ζ) when BE is used as a spare component* ⓘ
0

Parents
I1

Tag
Red

Tag datetime
19/10/2024, 10:05 AM

Attributes

Reference manuals

Description

The element will be marked as a root of the fault tree. Generate label for the failure event ⓘ

Mirror/Referring Element

Title

Name* ⓘ
M_Pole1

Referred element*
(Pole1) Pole1 – OR, Labelled Event

Description

- Elements of a fault tree can be on different pages.

- A fault tree can be split on multiple pages, by generating mirrors of elements on different pages. This helps to improve the readability of fault trees.
- Only one element can be selected as a top-level element in a tree among all pages.
- The values of some of the fields e.g. failure rates, probabilities, etc can be given as parameters (defined later) instead of constant values.
- The “Generate label for the failure event” checkbox is only visible in the advance view.
- The “Generate label for the failure event” checkbox is available only for those elements that propagate failure to their parents. If this checkbox is selected for an element, it is added to the sub-section “Labelled Events” of the fault tree (in the left panel) as a basic event.
- Elements can be connected by drawing edges between them.
- A module can be annotated with attributes, reference manuals, and/or color tags.
- Click on the download icon  , a popup comes up to download the tree in JSON, Latex, and Galileo formats.

Export

Select file format

Galileo

A fault tree with a root element representing the root of the main page will be created and stored in a Galileo file.

Parameter set

HVDC_800KV_day

Before creating the fault tree, the model's parameters, if any, will be substituted with their values from the parameter set.

Galileo format will lose layout, reference manual, and attribute data.

Export

Select file format

Latex

A fault tree with a root element representing the root of the main page will be created and stored in a Latex file.

Parameter set

HVDC_800KV_day

Before creating the fault tree, the model's parameters, if any, will be substituted with their values from the parameter set.

Export

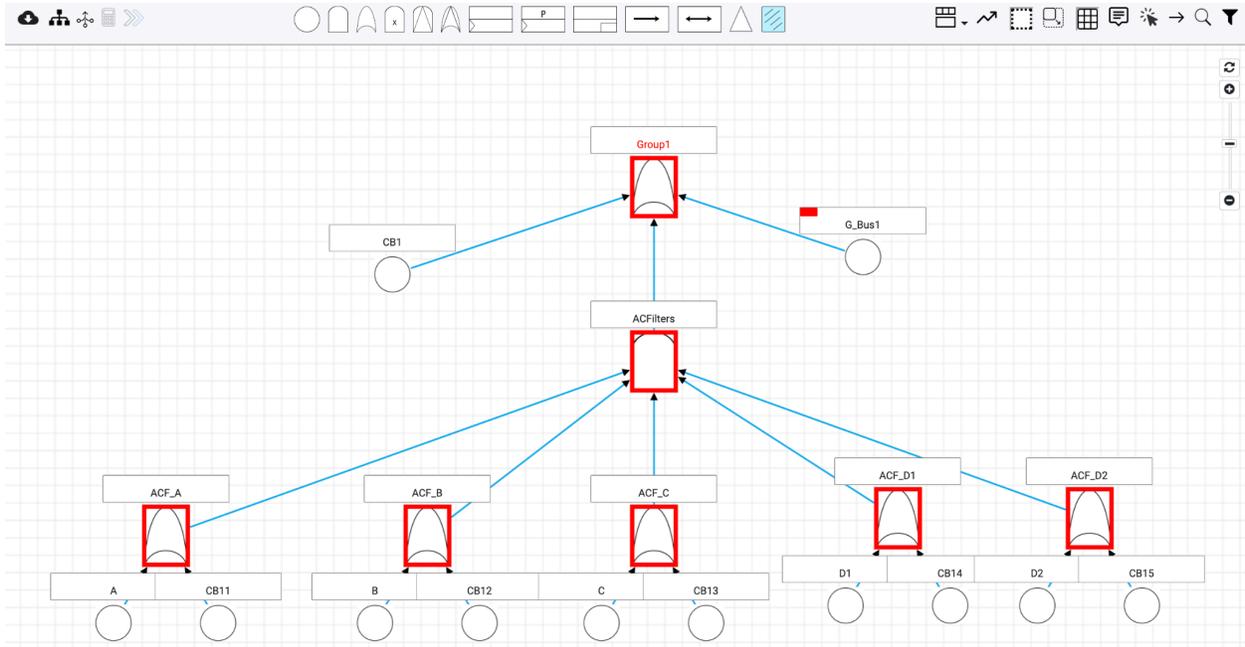
Select file format

JSON

All data given on the current page will be downloaded recursively.

The list of parameters, if any, used by the model will be created and saved in the JSON file together with the fault tree. Note that JSON format retains layout data whereas reference manual and attribute data might get lost. Moreover, it does not require a valid tree in order to export the data.

- Click on the icon  to highlight the elements that, along with their children, can be converted into modules (independent sub-trees). To convert an element and its children into a module, right-click on it and then click “Make Module”.



- To simplify a fault tree click on the down arrow along the icon .

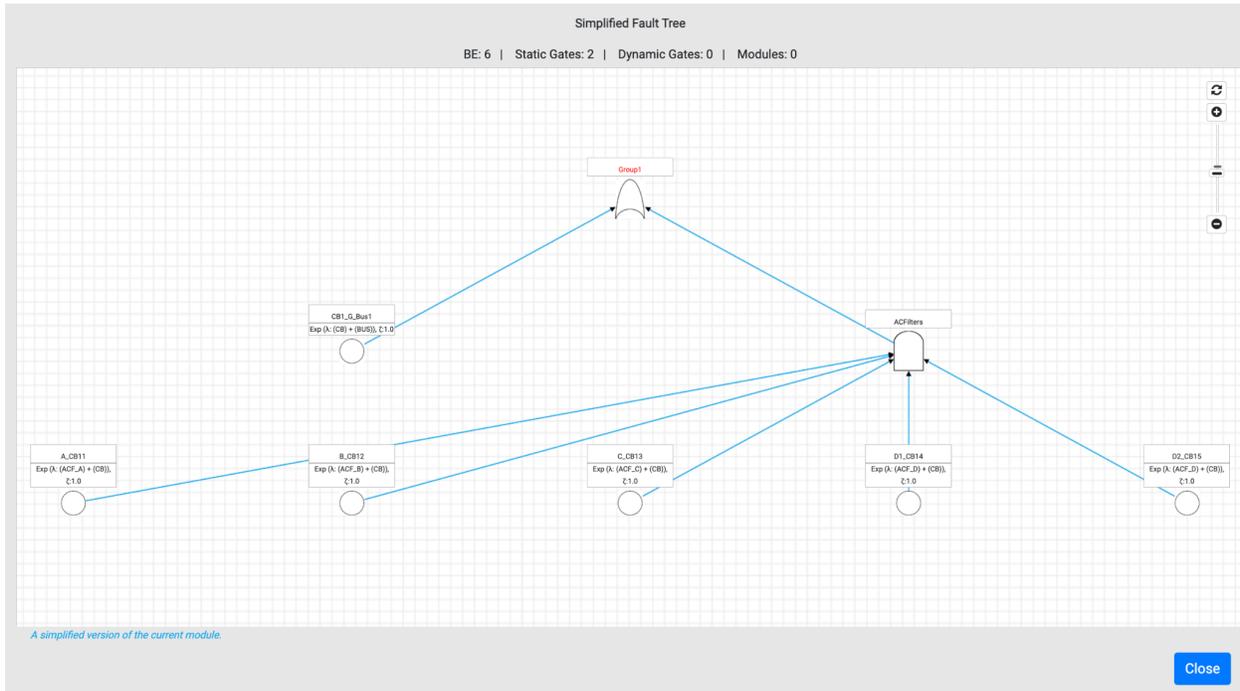
Simplification

<input type="checkbox"/> Apply	Rule	Abbreviation
<input checked="" type="checkbox"/>	Split FDEPs with two or more children into single FDEPs with only one child.	SPLIT_FDEPS
<input checked="" type="checkbox"/>	Try to merge BEs under an OR-gate into one BE.	MERGE_BES
<input checked="" type="checkbox"/>	Trim parts of the DFT in place which do not contribute to the top level element.	TRIM
<input type="checkbox"/>	Try to remove superfluous dependencies. These dependencies have a trigger which already leads to failure of the top level element.	REMOVE_DEPENDENCIES_TLE
<input type="checkbox"/>	Try to merge gates with the same type and identical successors. These gates surely fail simultaneously and thus, one gate can be removed.	MERGE_IDENTICAL_GATES
<input checked="" type="checkbox"/>	Remove gates with just one successor. These gates will fail together with this child, so they can directly be eliminated.	REMOVE_SINGLE_SUCCESSOR
<input checked="" type="checkbox"/>	Flattening of AND-/OR-/PAND-gates.	FLATTEN_GATE
<input type="checkbox"/>	Subsumption of OR-gate by AND-gate or of AND-gate by OR-gate.	SUBSUME_GATE
<input type="checkbox"/>	Eliminate FDEPs by introducing an OR-gate. Let A be the trigger and B be the dependent element. Both must be connected to the top level element. B must have only one predecessor and no SPARE or PAND/POR in its predecessor closure.	REPLACE_FDEP_BY_OR
<input type="checkbox"/>	Eliminate superfluous FDEP from AND or OR. This FDEP is triggered after the failure of the dependent element and thus, it does not influence anything else.	REMOVE_SUPERFLUOUS_FDEP
<input type="checkbox"/>	Eliminate FDEP between two successors of an OR or PAND. Only supports FDEPs with one common predecessor.	REMOVE_SUPERFLUOUS_FDEP_SU...

Replace modules with their corresponding sub-trees before simplifying the fault tree.

Simplification will only be applied to the fault tree given in the current module.

- Select rules that you want to apply for the simplification. The most important rules are selected by default.
- Check the radio button if you want to replace modules with their corresponding sub-trees before simplifying the fault tree.
- One can simplify a module or the whole fault tree spread across multiple pages.
- On clicking “Simplify”, a popup will appear with the simplified fault tree



- Click on the icon  (not visible when modules are in focus) to do a basic analysis that includes reliability, mean-time-to-failure, and average-failure-probability per hour. It will take the user to the “Analysis” window under “Computing” in the left panel.

Basic Analysis

Metric(s) *

All Metrics

Fault tree*

BipolarHVDC2

Fault tree root element i

Root Element (Default)

Initial condition

None

Metric parameters

Name	Value i
time_bound	365

Assign labelled events (of the model) to metric labels

Metric label	Model labelled event
system_failed	system_failed
event	system_failed ▼

Model parameter set i

HVDC_800KV_day

Simplify fault tree before analysis
 Analysis type: Markov Hybrid (Markov and/or BDD)

Result tab: Existing New
 Results ▼

Cancel
Start

- Click on the icon  to start the interactive simulation. It will take the user to the “Interactive Simulation” window under “Computing” in the left panel. A popup will appear to select/change the model, a parameter set, and an Initial Condition. On clicking the “Start” button the simulation window appears.

Simulation

Fault tree

BipolarHVDC2 ▼

Before the simulation, data from all pages will be collected to create a uniform fault tree with its root element given on the main page.

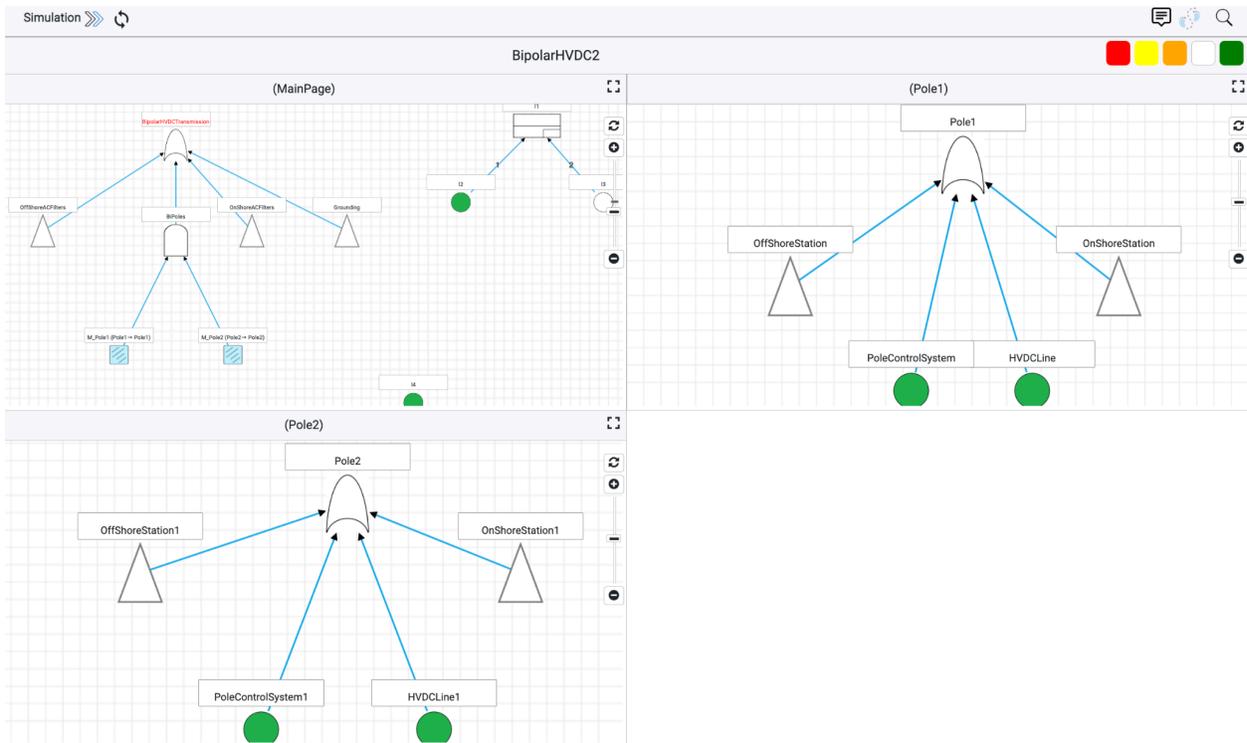
Parameter set* ⓘ

HVDC_800KV_day ▼

Initial condition*

None ▼

Cancel
Start



In case “Initial Condition” is applied, one fault tree is generated by collected data from all pages for simulation purposes. Otherwise, a simulation is run by keeping elements of each page separate from others.

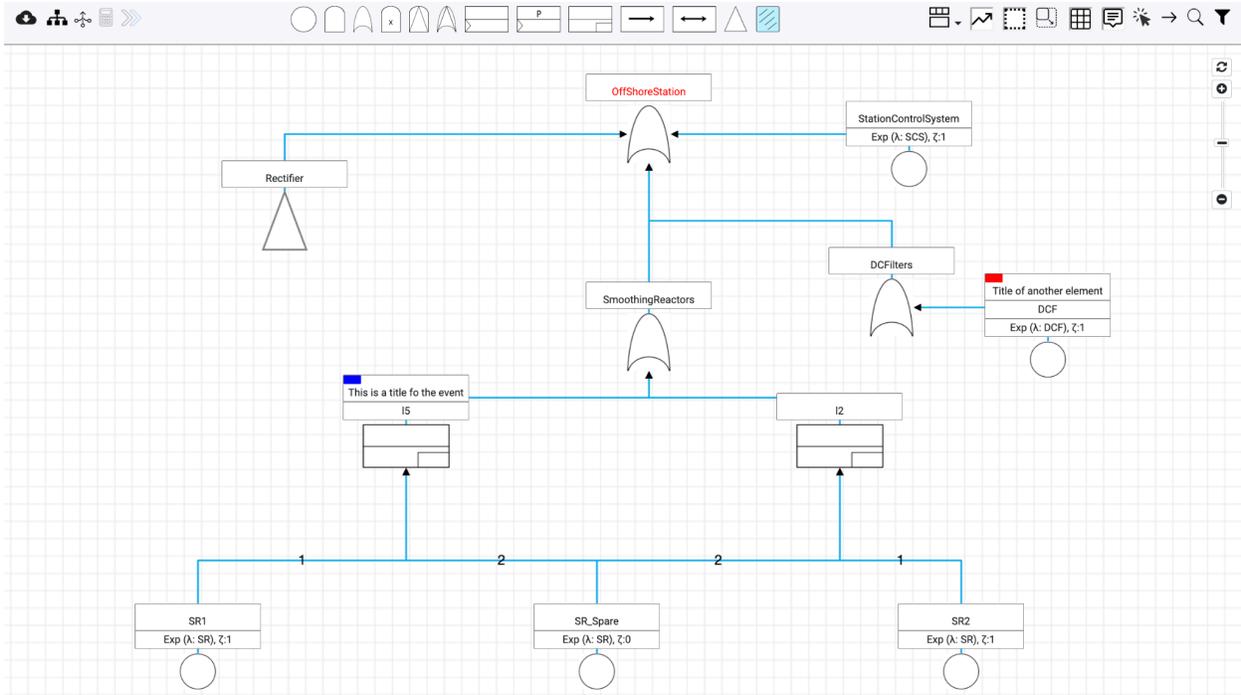
- Click on the down arrow new the icon  , it will give four options to display a tree:
 - Canvas view. It shows the tree in the grid.
 - Tabular view. It will show the tree in a tabular form
 - Galileo view. It shows the tree in Galileo format.
 - Parametric Galileo view: It shows the tree in Galileo format along with the parameters of the model.

Tabular View

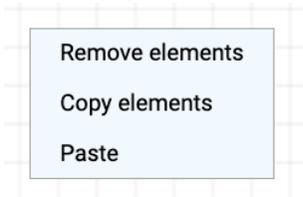
Fault Tree (MainPage)

Expand ALL Collapse All BE: 336 | Static Gates: 214 | Dynamic Gates: 0 | Modules: 43

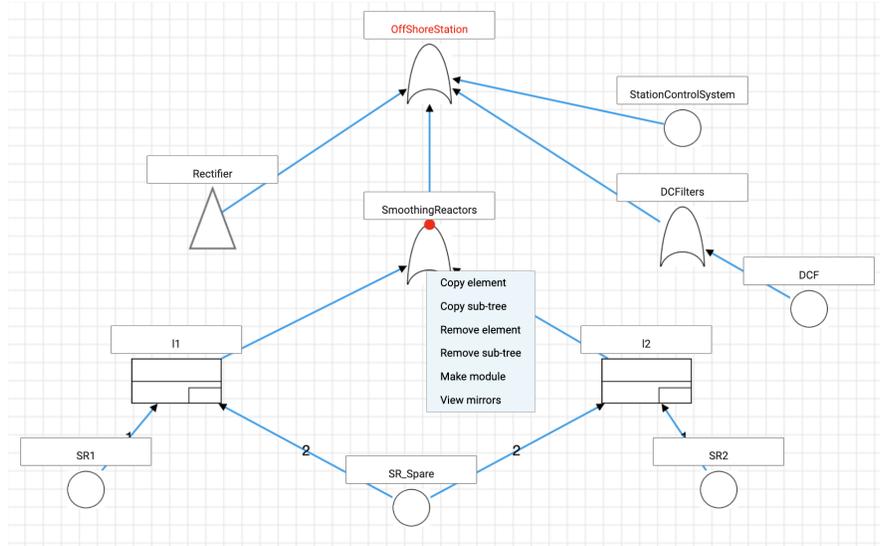
Element Name	Title	Type	Information	Attributes	Tag
1 BipolarHVDCTransmission		OR	Root Element		
2 M_Pole2		MIRROR	Pole2 → Pole2 : Labelled Event		
3 M_Pole1		MIRROR	Pole1 → Pole1 : Labelled Event		
4 BiPoles		AND	Labelled Event		
5 OffShoreACFilters	<small>Collapse Module</small>	MODULE			
6 OffShoreACFilters -> OffShoreACFilters		OR	Labelled Event , Module Root Element		
7 OffShoreACFilters -> M_Bus		BE	Exp (A: BUS), ζ: 1		
8 OffShoreACFilters -> ACFilterGroups	<small>Collapse Module</small>	MODULE			
9 ACFilterGroups -> ACFilterGroups		AND	Module Root Element		
10 ACFilterGroups -> Group1	<small>Collapse Module</small>	MODULE			
11 Group1 -> Group1		OR	Module Root Element		
12 Group1 -> ACFilters		AND			
13 Group1 -> CB15		BE	Exp (A: CB), ζ: 1		
14 Group1 -> D2		BE	Exp (A: ACF_D), ζ: 1		
15 Group1 -> ACF_D2		OR			
16 Group1 -> CB14		BE	Exp (A: CB), ζ: 1		
17 Group1 -> D1		BE	Exp (A: ACF_D), ζ: 1		
18 Group1 -> ACF_D1		OR			
19 Group1 -> CB13		BE	Exp (A: CB), ζ: 1		
20 Group1 -> C		BE	Exp (A: ACF_C), ζ: 1		
21 Group1 -> ACF_C		OR			
22 Group1 -> CB12		BE	Exp (A: CB), ζ: 1		
23 Group1 -> B		BE	Exp (A: ACF_B), ζ: 1		
24 Group1 -> ACF_B		OR			
25 Group1 -> CB11		BE	Exp (A: CB), ζ: 1		
26 Group1 -> A		BE	Exp (A: ACF_A), ζ: 1		
27 Group1 -> ACF_A		OR			
28 Group1 -> G_Bus1		BE	Exp (A: BUS), ζ: 1		
29 Group1 -> CB1		BE	Exp (A: CB), ζ: 1		
30 ACFilterGroups -> Group2	<small>Collapse Module</small>	MODULE			
31 Group2 -> Group2		OR	Module Root Element		
32 Group2 -> ACFilters		AND			



- Click on the icon  to enable the selection of multiple elements in the grid view. This can be done by clicking on a screen and then drawing the mouse. All elements with a rectangle will be selected, which can then be moved together.
- Right-click on the canvas and the following popup will appear:



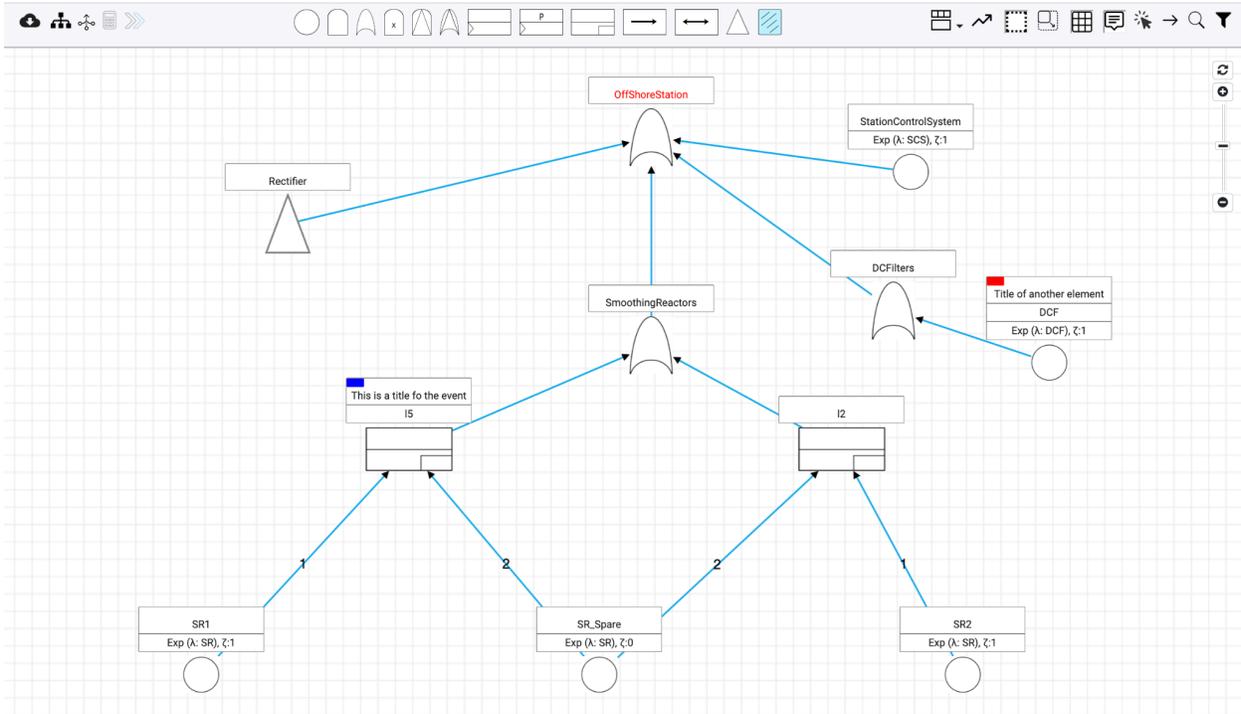
- By clicking “Remove Elements” all selected elements will be removed.
 - By clicking “Copy elements” all selected elements will be copied.
 - By clicking “Paste” previously copied elements will be pasted.
- On right-clicking on an element, a popup comes up that allows you to copy the element, copy the sub-tree under it, delete the element, delete the sub-tree under it, or convert the sub-tree under it into a module (if possible), and view mirrors of the selected element.



- Right-click an element and then select “View Mirrors”, a popup window will come up showing all mirrors of the selected element.



- Click  icon to enable the navigator at the bottom of the screen.
- Click  icon to show the grid on the screen.
- Click  icon to show the summary information about each element on the screen.



- Click  icon to display summary information about an element on hovering.
- Click  icon to draw edges between two elements of a fault tree. Both elements must be on the same page/module.

Add Edge

Source

OffShoreStation ▼

Target

DCFilters ▼

Cancel

Add

- Click  icon to search for any element on the screen.
- Click  icon to search elements based on filters. A popup will appear to apply filters.
 - All fields that are filled up, their data is AND together to find the nodes. Within a field, the data is OR-together unless it is mentioned otherwise.
 - If any field is not filled up, it is not considered to be a part of the filtering process, and thus ignored.

- On clicking the “Search” button, the result will be displayed in the “Search results” table.

Advance Search

Filters

Pages: & Element name: & Attributes: All selected must be present & Tag: &

Element type:

Search results

BE: 254 | Static Gates: 157 | Dynamic Gates: 64 | Modules: 23

Index	Name	Type	Information	Attributes	Tag	Tag datetime	
0	(MainPage) Pole2	MODULE					<input type="checkbox"/>
1	(MainPage) OffShoreACFilters	MODULE					<input type="checkbox"/>
2	(MainPage) OnShoreACFilters	MODULE				2024-10-18T18:25	<input type="checkbox"/>
3	(MainPage) BipolarHVDCTransmission	OR					<input type="checkbox"/>
4	(MainPage) Pole1	MODULE					<input type="checkbox"/>
5	(MainPage) BiPoles	AND	Labelled Event				<input type="checkbox"/>
6	(MainPage) Grounding	MODULE					<input type="checkbox"/>
7	(MainPage) Pole2 → Pole2	OR	Labelled Event				<input type="checkbox"/>
8	(MainPage) Pole2 → HVDCLine	BE	Exp (λ: HVDC.LINE)				<input type="checkbox"/>
9	(MainPage) Pole2 → OffShoreStation	MODULE					<input type="checkbox"/>
10	(MainPage) Pole2 → OnShoreStation	MODULE					<input type="checkbox"/>

| |

- An element can be updated by clicking its name and opening the corresponding popup.
- By selecting elements of the same type in the “Search results” table, operations can be performed on them at once. For example, in the case of BEs, the following operations can be performed:
 - Update attributes

Update Attributes

Selected elements

Name	Type	Information	Attributes	Tag	Tag datetime
(MainPage) I13_CPPFailed	BE	Exp (λ: (SCP)/(1))	MotorA		

Update attributes

Attribute	Actions
SystemA	No change
ComponentA	Add
MotorA	Remove

- Update tags

Update Tag

Selected elements

Name	Type	Information	Attributes	Tag	Tag datetime
(MainPage) OffShoreACFilters → M_Bus	BE	Exp (λ: BUS)			2024-10-18T18:...
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: CB)			
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: BUS)			2024-10-18T18:...
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: ACF_A)			
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: CB)			
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: ACF_B)			
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: CB)			
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: ACF_C)			
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: CB)			
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: ACF_D)			

New tag

Red

Cancel
Update

- Delete elements
- Update rates

Update Rate

Selected elements

Name	Type	Information	Attributes	Tag	Tag datetime
(MainPage) OffShoreACFilters → M_Bus	BE		Exp (λ: BUS)		2024-10-18T18:...
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: CB)		
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: BUS)		2024-10-18T18:...
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: ACF_A)		
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: CB)		
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: ACF_B)		
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: CB)		
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: ACF_C)		
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: CB)		
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: ACF_D)		

Update rate

4

Cancel
Update

- Update distribution

Update Distribution

Selected elements

Name	Type	Information	Attributes	Tag	Tag datetime
(MainPage) OffShoreACFilters → M_Bus	BE		Exp (λ: BUS)		2024-10-18T18:...
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: CB)		
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: BUS)		2024-10-18T18:...
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: ACF_A)		
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE		Exp (λ: CB)		

Update distribution

Enter distribution

Distribution

Exponential

Rate (λ) ⓘ

1

Cancel
Update

- Update label

Update Label

Selected elements

Name	Type	Information	Attributes	Tag	Tag datetime
(MainPage) OffShoreACFilters → M_Bus	BE	Exp (λ: BUS)		 	2024-10-18T18:...
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: CB)		 	
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: BUS)		 	2024-10-18T18:...
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: ACF_A)		 	
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	BE	Exp (λ: CB)		 	

Update label

Generate label Remove label

Cancel
Update

- The threshold values of multiple VOT gates can be changed at once.

Update Threshold

Selected elements

Name	Type	Information	Attributes	Tag	Tag datetime
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	VOT			<input type="text"/>	
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	VOT			<input type="text"/>	

Update threshold

Cancel
Update

- The probability field of multiple PDEP gates can be changed at once.

Update Probability

Selected elements

Name	Type	Information	Attributes	Tag	Tag datetime
(MainPage) OffShoreACFilters → ACFilterGroups → Group1 ...	PDEP			<input type="text"/>	

Update probability

Cancel
Update

Labelled Events

All fault propagating elements whose checkbox “Generate label for the failure event” is selected, appear as basic labelled events on the Labelled Events page. Compound events can be defined by boolean equations on (basic and compound) labelled events. Advanced measures can be computed on basic as well as compound labelled events.

In the advanced view, each fault tree has a section “Labelled Events” separated into Basic and Compound events.

Labelled Events ?

Event label	Boolean expression on events that characterize the compound event	Description	
ALLPOLES	Pole2_Pole2_failed & Pole1_Pole1_failed		 
OnFilters	OnShoreACFilters_OnShoreACFilters_failed		 
OffFilters	OffShoreACFilters_OffShoreACFilters_failed		 
ACFilters	OnFilters & OffFilters		 
AllPolesNotOpr	Pole2_Pole2_failed Pole1_Pole1_failed		 
Pole2_Rectifier_SmoothingReactor	Pole2_OffShoreStation_SmoothingReactors_failed & Pole2_OffShoreStation_Rectifier_Rectifier_failed		 

[Add labelled event](#)

Labelled Events ?

Event label	Fault tree element whose failure causes the event	Description
system_failed	Root Element (Default)	Root element of the fault tree.
BiPoles_failed	(MainPage) BiPoles	
Pole2_Pole2_failed	(MainPage) Pole2 → Pole2	
Pole2_OffShoreStation_OffShoreStation_failed	(MainPage) Pole2 → OffShoreStation → OffShoreStation	
Pole2_OffShoreStation_SmoothingReactors_failed	(MainPage) Pole2 → OffShoreStation → SmoothingReactors	
Pole2_OffShoreStation_SR_Spare_failed	(MainPage) Pole2 → OffShoreStation → SR_Spare	
Pole2_OffShoreStation_Rectifier_RectifierSet1_failed	(MainPage) Pole2 → OffShoreStation → Rectifier → RectifierSet1	
Pole2_OffShoreStation_Rectifier_Rectifier_failed	(MainPage) Pole2 → OffShoreStation → Rectifier → Rectifier	
Pole2_OffShoreStation_Rectifier_RectifierSet2_failed	(MainPage) Pole2 → OffShoreStation → Rectifier → RectifierSet2	
Pole2_OnShoreStation_OnShoreStation_failed	(MainPage) Pole2 → OnShoreStation → OnShoreStation	
Pole2_OnShoreStation_SmoothingReactors_failed	(MainPage) Pole2 → OnShoreStation → SmoothingReactors	
Pole2_OnShoreStation_Inverter_Inverter_failed	(MainPage) Pole2 → OnShoreStation → Inverter → Inverter	
OffShoreACFilters_OffShoreACFilters_failed	(MainPage) OffShoreACFilters → OffShoreACFilters	
OnShoreACFilters_OnShoreACFilters_failed	(MainPage) OnShoreACFilters → OnShoreACFilters	
Pole1_Pole1_failed	(MainPage) Pole1 → Pole1	
Pole1_OffShoreStation_OffShoreStation_failed	(MainPage) Pole1 → OffShoreStation → OffShoreStation	
Pole1_OffShoreStation_SmoothingReactors_failed	(MainPage) Pole1 → OffShoreStation → SmoothingReactors	
Pole1_OffShoreStation_Rectifier_Rectifier_failed	(MainPage) Pole1 → OffShoreStation → Rectifier → Rectifier	

Click on the “Add labelled event” to create a new compound event.

Labelled Event

Event label* i

Boolean expression * i

The above expression can use the following event labels.

system_failed
BiPoles_failed
Pole2_Pole2_failed

Pole2_OffShoreStation_OffShoreStation_failed

Pole2_OffShoreStation_OffShoreStation_failed

Description

Cancel
Add

Enter the event label and boolean expression on existing events shown below in the field “The above expression can use the following Event labels”. On filling in mandatory fields, click the “Add” button.

CCF Groups

Common cause failures (CCF): a sub-category of dependent failures, representing events where multiple failures occur due to a shared cause. They are important to consider because they can violate the effects of redundancy. CCFs may violate the performance of an individual safety barrier, or result in the simultaneous failure of several safety barriers. Semi-automatic common cause failure (CCF) modeling can be performed by placing basic elements into CCF groups. This approach to modeling CCFs is more practical than the typical modeling method, which involves adding CCF events by hand to the fault trees. When modeling systems with high levels of redundancy, in particular, such CCF modeling in the fault trees can occasionally greatly increase the overall size and complexity of the fault trees.

CCF Elements & CCF Events: CCF elements are a set of basic elements of a fault tree that (may) fail due to certain common causes. Whereas CCF events are the causes of failures of CCF elements. CCF groupings are groups made up of these CCF elements.

A fault tree structure (CCF Tree), which is an OR-gate that takes in CCF events (causes of failures of CCF elements) as inputs, is automatically generated for each element in a CCF group to illustrate the propagation of failure due to common causes. Each CCF element in a CCF group is substituted with its matching CCF tree in the original fault tree before analysis. Assume that a fault tree has four redundant components represented by the basic elements A, B, C, and D, placed in a CCF group. The following CCF events are automatically created by the SAFEST for this group: AB, AC, AD, BC, BD, CD, ABC, ABD, ACD, BCD, and ABCD; for example, AB denotes a failure event involving components A and B jointly. Subsequently, the software generates CCF trees for CCF elements. Before analysis, these CCF trees will replace the CCF elements in CCF groups in the fault tree. For instance, the program generates a CCF tree for the basic element A, with an OR-gate acting as the top gate and events A (individual failure), AB, AC, AD, ABC, ABD, ACD, and ABCD as inputs.

Analysis Models: There are two types of CCF modeling: explicit and implicit. Explicit CCF modeling is used once each distinct cause of CCF (CCF event) is identified, along with its reliability data e.g. probability of failure. Human error, shared equipment, utility problems (such as power, cooling, heating failure, or loss of hydraulic power), and natural events (such as lightning, flooding, or storms) are some of the specific causes.

Implicit modeling may be used when the reliability data of CCF events are unknown. Their failure probabilities are quantified using various analysis models. These models aid in determining the proportion of component failures attributable to common causes. There are several implicit models, e.g. Beta-factor model, the Alpha-factor model, the Multiple Greek Letter model, the Binomial failure rate model, etc. Each model has its own set of parameters required to quantify probabilities of CCF events. In the case of the Custom Model, reliability data for each CCF event is defined manually.

For a fault tree, we can create common cause failures (CCF) groups, which are displayed on the “Common Cause Failure Groups” page under a fault tree. These CCF groups may be incorporated into a fault tree before analysis.

Common Cause Failure Groups ⓘ

Name	Analysis model ⓘ	Reference manuals	Description	Actions
V5ABC_CCF	Custom			 
V6ABC_CCF	Custom			 
HEXs_CCF	Custom			 

[Add CCF group](#)

- Click the “Add CCF group” button to create a new group.

V5ABC_CCF

Elements in a CCF group ⓘ

CCF element ⓘ	Abbreviation*	Actions
(MainPage) Loop_A → V56 → V5_CCF	▼ A	
(MainPage) Loop_B → V56 → V5_CCF	▼ B	
(MainPage) Loop_C → V56 → V5_CCF	▼ C	

[Add element](#)

CCF analysis model* ⓘ

Custom

CCF events ⓘ

CCF event	Failure distribution	Graph
AB	Select distribution ▼ ICS_V501_F [Exp (k: ICS_V501_CCF)]	▼ 
AC	Select distribution ▼ ICS_V502_F [Exp (k: ICS_V502_CCF)]	▼ 
BC	Select distribution ▼ ICS_V503_F [Exp (k: ICS_V503_CCF)]	▼ 
ABC	Select distribution ▼ ICS_V504_F [Exp (k: ICS_V504_CCF)]	▼ 

[Save](#)

- Add fault tree elements (CCF elements) to the group. Only BEs can be added to CCF elements in a group.
- Select “CCF analysis model”. For each model, there is a set of parameters that need to be defined. Currently, the following analysis models are supported by SAFEST.
 - Beta Factor Model

VSABC_CCF

Elements in a CCF group ⓘ

CCF element ⓘ	Abbreviation*	ⓘ
(MainPage) Loop_A → V56 → V5_CCF	A	⊗
(MainPage) Loop_B → V56 → V5_CCF	B	⊗
(MainPage) Loop_C → V56 → V5_CCF	C	⊗

[Add element](#)

CCF analysis model* ⓘ

Beta Factor Model

Model parameters ⓘ

Parameter	Value*	ⓘ
β ⓘ		✎

Save

○ Multiple Greek Letter Model

VSABC_CCF

Elements in a CCF group ⓘ

CCF element ⓘ	Abbreviation*	ⓘ
(MainPage) Loop_A → V56 → V5_CCF	A	⊗
(MainPage) Loop_B → V56 → V5_CCF	B	⊗
(MainPage) Loop_C → V56 → V5_CCF	C	⊗

[Add element](#)

CCF analysis model* ⓘ

Multiple Greek Letter Model

Model parameters ⓘ

Parameter	Value*	ⓘ
β ⓘ		✎
γ ⓘ		✎
δ ⓘ		✎

Save

○ Alpha factor Model

VSABC_CCF

Elements in a CCF group ⓘ

CCF element ⓘ	Abbreviation*	ⓘ
(MainPage) Loop_A → V56 → VS_CCF	A	⊗
(MainPage) Loop_B → V56 → VS_CCF	B	⊗
(MainPage) Loop_C → V56 → VS_CCF	C	⊗

[Add element](#)

CCF analysis model* ⓘ

Alpha Factor Model

Model parameters ⓘ

Parameter	Value*	ⓘ
$\alpha 1$ ⓘ		✎
$\alpha 2$ ⓘ		✎
$\alpha 3$ ⓘ		✎

[Save](#)

○ Binomial Model

VSABC_CCF

Elements in a CCF group ⓘ

CCF element ⓘ	Abbreviation*	ⓘ
(MainPage) Loop_A → V56 → VS_CCF	A	⊗
(MainPage) Loop_B → V56 → VS_CCF	B	⊗
(MainPage) Loop_C → V56 → VS_CCF	C	⊗

[Add element](#)

CCF analysis model* ⓘ

Binomial Failure Rate Model

Model parameters ⓘ

Parameter	Value*	ⓘ
μ ⓘ		✎
ω ⓘ		✎
ρ ⓘ		✎

[Save](#)

○ Custom Model

- In the case of the custom model, the failure distribution of each CCF event has to be defined.

VSABC_CCF

Elements in a CCF group

CCF element	Abbreviation	
(MainPage) Loop_A → V56 → V5_CCF	A	
(MainPage) Loop_B → V56 → V5_CCF	B	
(MainPage) Loop_C → V56 → V5_CCF	C	

[Add element](#)

CCF analysis model

Custom

CCF events

CCF event	Failure distribution			Graph
AB	Enter distribution	Exponential	Rate (λ) 1	
AC	Enter distribution	Exponential	Rate (λ) 1	
BC	Enter distribution	Exponential	Rate (λ) 1	
ABC	Enter distribution	Exponential	Rate (λ) 1	

[Save](#)

Probabilistic Dependencies

Probabilistic functional dependencies may exist in a system, e.g., failure-on-demand, failure-rate-increment, or addition of a new failure-mode in case an element services the impact of an (accidental) event, etc. Instead of modeling them explicitly in fault trees, SAFEST allows for specifying them separately in a tabular form. These dependencies are applied to a fault tree before analysis. This helps simplify the modeling process enormously.

For a fault tree, we can create probabilistic dependencies groups, which are displayed on the “Probabilistic Dependencies” page under a fault tree. All elements in a probabilistic CCF group may fail with a given probability when a common cause (CC) of failure occurs. As CCF elements in a group may not fail with a positive probability, their failure rates might be increased or/and a new failure mode can be active for them, thus a new fault tree emerges in a post-CCF event scenario.

Before analysis, for each CCF group, say G, a dynamic fault tree structure is constructed. For each element, say A, in group G, a new OR-gate is created that accepts two inputs, the element A and a new basic element, say B, that models e.g. an incremented failure rate for the element A. The element B is made the second child of a new SEQ gate, and element A is made the dependent child of a new PDEP gate that models the failure probability of group G on the occurrence of common causes. Both PDEP and SEQ gates have their first child another OR-gate that has all CCF (trigger) events as its children.

Probabilistic Dependencies			
Name	Reference manuals	Description	Actions
V56A_FOD			 
V56B_FOD			 
V56C_FOD			 
LINE_BREAK_FRI			 
HEX_FRI			 
VALVES_RUPTURE_FMD			 

[Add probabilistic dependency](#)

- Click the “Add probabilistic dependency” button to create a new prob. Dependency.

V56A_FOD

Probabilistic dependencies groups

Group failure probability*	Name*	Elements in a group*	Failure dist. of additional failure mode if element survives *	Actions
ICS_V502_X + (1-ICS_V502_X)*ICS_V501_X	(MainPage) Loop_A → V56 → V5		None	 
ICS_V602_X + (1-ICS_V602_X)*ICS_V601_X	(MainPage) Loop_A → V56 → V6		None	 

[Add group](#)

CCF (trigger) events

Event name	Failure distribution/fault tree element		Rate (λ)*	Actions
E1	Select FT element	(MainPage) LOCA		 
E2	Enter distribution	Exponential	1	 

[Add event](#)

[Save](#)

- Each CCF group in the “Probabilistic Dependencies Groups” table is affected if any event mentioned in the “CCF (trigger) events” table occurs.
- On the occurrence of a CCF (trigger) event, elements in a CCF group fail with a probability given in “Group failure probability”.
 - In case the group failure probability is less than one, the CCF elements can survive. In this case, one can specify the failure distribution of additional failure mode in the “Failure dist. Of additional failure mode if element services” column.

- Click the “Add event” button to create a new CCF event in the “CCF (trigger) events” table. Failure distribution of the new CCF event can be
 - Specified manually, or
 - Derived from an element of the fault tree

Initial Conditions

Initial conditions/boundary conditions consist of:

- CCF groups,
- Probabilistic dependencies, and
- Evidence

that we apply before analyzing a fault tree.

Evidence is a group of modules that are assumed to have already failed. A module is a subtree with a root node, say v , if all failures within the subtree have to propagate through the root node v . Thus, the state of the entire module is represented by the state of its root node. We call a module a dynamic module if it contains at least one dynamic gate; otherwise, it is a static module. During analysis, all possible failure orderings (traces) of the modules in the evidence are examined. Note that the elements within a module cannot be selected as evidence because their failure ordering might impact the failure behavior of its corresponding module.

For a fault tree, we can create Initial Conditions, which are displayed on the “Initial Conditions” page under a fault tree. One can apply any initial condition for analyzing the fault tree.

Initial Conditions				
Name	Reference manuals	Description	Default	Actions
None			<input type="radio"/>	 
InitCond			<input checked="" type="radio"/>	 
InitCond2			<input type="radio"/>	 

[Add initial condition](#)

- Click the “Add initial condition” button to create a new condition.

InitCond2

CCF groups

CCF group	Apply
V5ABC_CCF	<input checked="" type="checkbox"/>
V6ABC_CCF	<input checked="" type="checkbox"/>
HEXs_CCF	<input checked="" type="checkbox"/>
Test	<input checked="" type="checkbox"/>

Probabilistic dependencies

Probabilistic dependency	Apply
V56A_FOD	<input checked="" type="checkbox"/>
V56B_FOD	<input checked="" type="checkbox"/>
V56C_FOD	<input checked="" type="checkbox"/>
LINE_BREAK_FRI	<input checked="" type="checkbox"/>
HEX_FRI	<input checked="" type="checkbox"/>
VALVES_RUPTURE_FMD	<input checked="" type="checkbox"/>

Evidence

Elements	Apply	
(MainPage) ICS_ABC	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(MainPage) Loop_C → V1234 → V12	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[Add element](#)

[Save](#)

- The page contains all CCF groups and probabilistic dependencies that we have already created for the fault tree.
- Select “Apply” checkboxes for the CCF groups and prob. Dependencies that we want to apply to the fault tree before analysis.
- Click the “Add element” button in the “Evidence” table to add elements of the fault trees that we assume have already failed at the start of the analysis as evidence of failure.
- Select “Apply” checkboxes for the elements in the “Evidence” table that we assume failed at the start of the analysis.

Configurations

Parameter Sets

Each parameter set contains a list of parameters that are key-value pairs. They are used to specify values of e.g. probabilities, failure rates, etc. in fault tree models. By changing their values several variants of fault trees can be generated, which can then be compared with each other based on the results of metrics of interest. Each parameter set comprises:

- Constants
- Constant expressions
- Failure event distributions (Exponential, Erlang, Weibull, Log-normal)
- Failure event empirical distributions – failure distributions generated from data sets.

View

Click the “Parameter Sets” under “Configurations” in the left panel to view all existing parameter sets.

Parameter Sets			
Name	Reference manuals	Description	Actions
HVDC_800KV_day			   
SMRs_Rates			   
NPP_LOCA_Rates			   
NPP_RRS_Rates			   
ElectricPowerSupplyRates			   
CentCompMFR2			   
AircraftFuelDistributionSystem (2)			   
HVDC_800KV_day1			   

[Add parameter set](#) [Import parameter set](#)

Creation

Click the “Add parameter set” button to create a new parameter.

Import

Click the “Import parameter set” to import the parameter set in .ps format (a format in which parameter sets are imported/exported in SAFEST).

Duplicate

Click the icon  to duplicate a parameter set.

Export

Click the  icon to export a parameter set in .ps format.

Update

Click a parameter set to update its details

Constants

SMRs_Rates			
Constant			
Name*	Numeric value*	Description	
MIN_PER_YEAR	1	525600 Minutes, 8760 Hours in a year	  
HTP_TPOINT	0.02	In 0.02h, Temp & pressure are at the peak	  
ILPER_INC	0.3		  
BLPER_INC	0.3		  
MINPINT	1		  

[Add constant](#)
[Export](#)
[Import](#)
[Find & replace](#)

[Evaluate](#)
[Save](#)

Constants can only be numeric e.g. 4, 2.3, 4e-6 etc. Their value can be changed at the time of analysis. For example, graphs can be plotted for matrix results against ranges of values of constants.

- Click the “Add constant” button to enter a new row in the table.
- Click the “Export” button to export constants in a CSV format.
- Click the “Import” button to import constants from a CSV file.
- Click the “Find & replace” button to search sub-strings among Constants and replace them with a new string.

Find & Replace

Filter type

Search substring

Replace substring

[Replace](#)
[Cancel](#)

- Click the  icon in the last column of any row to add a new row above it.
- Click the  icon to duplicate the row.
- Click the “Evaluate” button to evaluate expressions in all tabs. The result will be displayed in a popup.

Evaluation

Constant			
Name	Value	Description	
MIN_PER_YEAR	1	525600 Minutes, 8760 Hours in a year	
HTP_TPOINT	0.02	In 0.02h, Temp & pressure are at the peak	
ILPER_INC	0.3		
BLPER_INC	0.3		
MINPINT	1		

Constant expression			
Name	Value	Description	
ICS_V602_X	1e-9	Failure to open, Signal failure (3 source), No flow path	
ICS_LUV0_X	0.00305	N/A, All, Loop Unavailable, Isolation for test or maintenance, No flo...	
ICS_NC01_X	1e-7	Natural circulation, All, Loss of natural circulation, Thermal-hydrauli...	
ICS_V501_CCF	0.000037	CCF of EH Valves ICV_5A & 5B	
ICS_V502_CCF	0.000037	CCF of EH Valve ICV_5A & 5C	
ICS_V503_CCF	0.000037	CCF of EH Valve ICV_5B & 5C	

Failure event dist.			
Name	Value	Description	
ICS_V501_F	Exp (λ : 3.7e-05)	CCF of EH Valves ICV_5AB	
ICS_V502_F	Exp (λ : 3.7e-05)	CCF of EH Valve ICV_5AC	
ICS_V503_F	Exp (λ : 3.7e-05)	CCF of EH Valve ICV_5BC	
ICS_V504_F	Exp (λ : 3.7e-06)	CCF of EH Valve ICV_5ABC	
ICS_V601_F	Exp (λ : 1.85e-06)	CCF of EH Valves ICV_6AB	
ICS_V602_F	Exp (λ : 1.85e-06)	CCF of EH Valve ICV_6AC	
ICS_V603_F	Exp (λ : 1.85e-06)	CCF of EH Valve ICV_6BC	

CCF of EH Valve ICV_5B & 5C

Close
Download

- Click the “Save” button to save the data. This action will save data in all the tabs.

Constant Expressions

SMRs_Rates

Constant Constant expression Failure event dist. Failure event empirical dist.

Name*	Value (Expression)*	Description
A	557.234652248256	
B	10.29543322700475	
T0	0.02015544529662807	
C	0.04652294275902187	
T	$A + B / (1 + 4^{\text{pow}}((\text{HTP_TPOINT}-T0)/C,2))$	Temperature equation
D	7.117778574626758	
E	0.8107229626814564	
T1	0.023891687618278354	
F	0.01980042408933875	
P	$D + E / (1 + 4^{\text{pow}}((\text{HTP_TPOINT}-T1)/E,2))$	Pressure equation
ICS_LINE_BRK	7.66E-04/MIN_PER_YEAR	
RVL_V101_X	2E-03	Electro-hydraulic valve, FAI, ICS Line Break, Failure to shut (Mechanical)
RVL_V102_X	1E-09	Electro-hydraulic valve, FAI, ICS Line Break, Failure to shut (Signal)
RVL_V201_X	1E-04	Electro-hydraulic valve, FAI, ICS Line Break, Failure to shut (Mechanical)
RVL_V202_X	1E-09	Electro-hydraulic valve, FAI, ICS Line Break, Failure to shut (Signal)
RVL_V301_X	1E-04	Electro-hydraulic valve, FAI, ICS Line Break, Failure to shut (Mechanical)
RVL_V302_X	1E-09	Electro-hydraulic valve, FAI, ICS Line Break, Failure to shut (Signal)
RVL_V401_X	2E-03	Electro-hydraulic valve, FAI, ICS Line Break, Failure to shut (Mechanical)
RVL_V402_X	1E-09	Electro-hydraulic valve, FAI, ICS Line Break, Failure to shut (Signal)

Add expression
Export
Import
Find & replace

Evaluate
Save

These are non-negative, real-value expressions, that can use constants (defined in the Constants tab) e.g. $x + 2$ where x is a constant. The grammar of the expression is given [here](#).

- Click “Add expression” to enter a new row in the table.
- Click “Export” to export expressions in a CSV format.

- Click the “Import” button to import expressions from a CSV file.
- Click the “Find & replace” button to search sub-strings among Constant Expressions and replace them with a new string.

Find & Replace

Filter type
Name, Value

Search substring

Replace substring

Replace
Cancel

- Click the  icon to duplicate the row.
- Click the  icon in the last column of any row to add a new row above it.
- Click the “Save” button to save the data. This action will save data in all the tabs.

Failure event distributions

SMRs_Rates							
Constant		Constant expression		Failure event dist.		Failure event empirical dist.	
Name*		Rate (λ)	Failure distribution	Description			
ICS_V501_F	Exponential	Rate (λ)	ICS_V501_CCF	CCF of EH Valves ICV_5AB			
ICS_V502_F	Exponential	Rate (λ)	ICS_V502_CCF	CCF of EH Valve ICV_5AC			
ICS_V503_F	Exponential	Rate (λ)	ICS_V503_CCF	CCF of EH Valve ICV_5BC			
ICS_V504_F	Exponential	Rate (λ)	ICS_V504_CCF	CCF of EH Valve ICV_5ABC			
ICS_V601_F	Exponential	Rate (λ)	ICS_V601_CCF	CCF of EH Valves ICV_6AB			
ICS_V602_F	Exponential	Rate (λ)	ICS_V602_CCF	CCF of EH Valve ICV_6AC			
ICS_V603_F	Exponential	Rate (λ)	ICS_V603_CCF	CCF of EH Valve ICV_6BC			
ICS_V604_F	Exponential	Rate (λ)	ICS_V604_CCF	CCF of EH Valve ICV_6ABC			
ICS_HX00_F	Exponential	Rate (λ)	ICS_HX00_CCF	CCF of All Heat Exchangers			
ICS_HX01_F	Exponential	Rate (λ)	ICS_HX01_CCF	CCF ICHX 1A/2A			
ICS_HX02_F	Exponential	Rate (λ)	ICS_HX02_CCF	CCF ICHX 1A/1B			
ICS_HX03_F	Exponential	Rate (λ)	ICS_HX03_CCF	CCF ICHX 1A/2B			
ICS_HX04_F	Exponential	Rate (λ)	ICS_HX04_CCF	CCF ICHX 1A/1C			
ICS_HX05_F	Exponential	Rate (λ)	ICS_HX05_CCF	CCF ICHX 1A/2C			
ICS_HX06_F	Exponential	Rate (λ)	ICS_HX06_CCF	CCF ICHX 2A/1B			
ICS_HX07_F	Exponential	Rate (λ)	ICS_HX07_CCF	CCF ICHX 2A/2B			
ICS_HX08_F	Exponential	Rate (λ)	ICS_HX08_CCF	CCF ICHX 2A/1C			
ICS_HX09_F	Exponential	Rate (λ)	ICS_HX09_CCF	CCF ICHX 2A/2C			
ICS_HX10_F	Exponential	Rate (λ)	ICS_HX10_CCF	CCF ICHX 1B/2B			

Evaluate
Save

Failure event distributions can be exponential, erlang, Weibull, log-normal, and constant probability.

- Click the “Add event distribution” button to enter a new row in the table.
- Click the “Export” button to export failure distributions in a CSV format.
- Click the “Import” button to import failure distributions from a CSV file.
- Click the “Find & replace” button to search sub-strings among Constant Expressions and replace them with a new string.

Find & Replace

Filter type
Name, Value

Search substring

Replace substring

Replace Cancel

- Click the  icon to duplicate the row.
- Click the  icon in the last column of any row to add a new row above it.
- Click the  icon to view the graph of the corresponding distribution.
- Click the “Save” button to save the data. This action will save data in all the tabs.

Empirical failure distributions

HVDC_800KV_day					
Constant		Constant expression		Failure event dist.	Failure event empirical dist.
Name	Goodness-to-fit	Failure Distributions		Description	
dataset1	<input checked="" type="radio"/> 67%	Erlang (λ : 10.845734, κ : 1)			 
	<input type="radio"/> 61%	Weibull (θ : 9.179215, η : 0.927731)			
	<input type="radio"/> 26%	Exp (λ : 9.492259)			
	<input type="radio"/> 9%	LogN (μ : 1.580169, σ : 1.388204)			
dataset2	<input checked="" type="radio"/> 55%	LogN (μ : 0.614971, σ : 1.25686)			 
	<input type="radio"/> 36%	Weibull (θ : 3.312209, η : 0.985072)			
	<input type="radio"/> 34%	Erlang (λ : 3.395478, κ : 1)			
	<input type="radio"/> 29%	Exp (λ : 3.333851)			
frg	<input checked="" type="radio"/> 63%	Exp (λ : 859.848794)			 
	<input type="radio"/> 62%	Erlang (λ : 804.786359, κ : 1)			
	<input type="radio"/> 61%	Weibull (θ : 866.064271, η : 1.016585)			
	<input type="radio"/> 19%	LogN (μ : 6.220604, σ : 1.169132)			
sdvf	<input checked="" type="radio"/> 90%	Erlang (λ : 853.683944, κ : 1)			 
	<input type="radio"/> 86%	Weibull (θ : 868.107867, η : 1.007255)			
	<input type="radio"/> 44%	Exp (λ : 865.473321)			
	<input type="radio"/> 0%	LogN (μ : 6.194835, σ : 1.273222)			
afaadf	<input checked="" type="radio"/> 95%	Weibull (θ : 857.266038, η : 0.983812)			 
	<input type="radio"/> 86%	Erlang (λ : 886.282224, κ : 1)			
	<input type="radio"/> 40%	Exp (λ : 863.316789)			
	<input type="radio"/> 0%	LogN (μ : 6.16637, σ : 1.317336)			

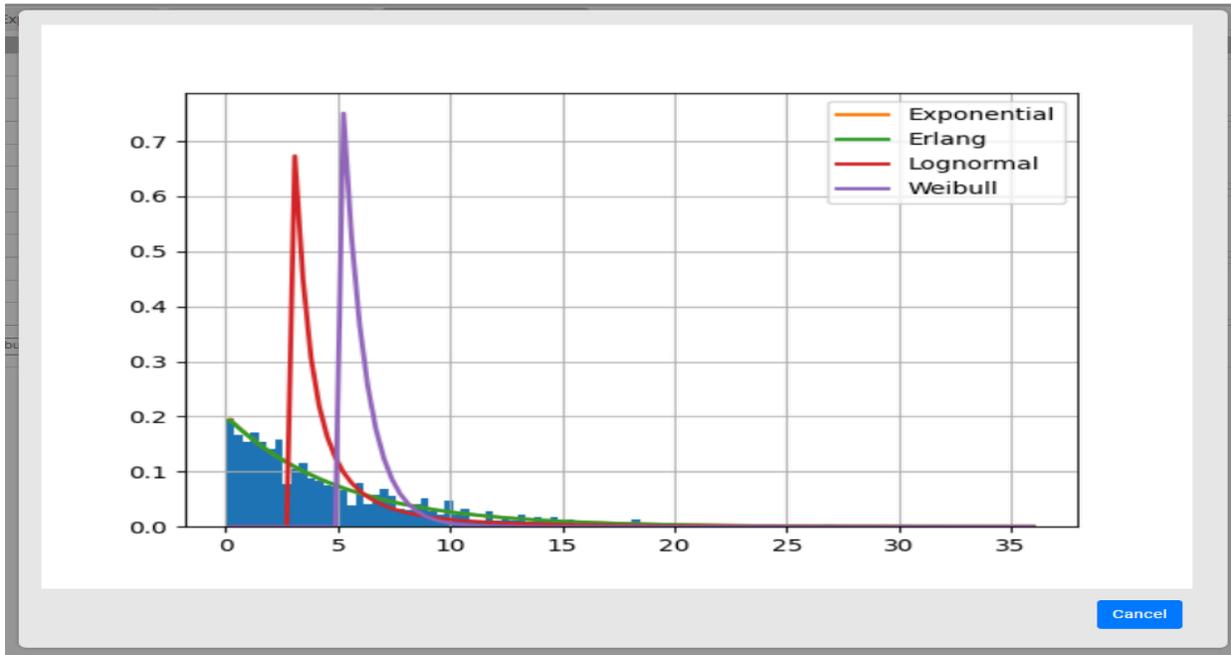
Evaluate Save

Empirical distributions are calculated from a data set using statistical methods. For that, historical failure data of a component is used to estimate the tentative failure probability distributions, which might have generated it, sorted according to their goodness-to-fit (GTF) values -- GTF value indicates the chance the data was generated by the corresponding distribution.

You can see how these distributions fit the data by clicking on the graph icon in the last column of their corresponding rows. Using Empirical distribution:

Each data may fit on multiple distributions, which are sorted according to their goodness-to-fit values, therefore we provide a radio button to select any distribution that we want to use.

Moreover, you can import and export empirical distributions (CSV format) and use them in other projects.



- **Generating empirical distribution.** An empirical distribution can be added by clicking the “Add event distribution” button. It will display all empirical distributions that have been generated previously and stored on the server side. One can compute a new distribution by specifying the file that contains data on which the distribution is to be approximated.

Events with empirical failure distributions

Event Name	Empirical distributions with goodness-to-fit values	Status	Action
Test	63 % Exp ($\lambda: 859.848794$), 62 % Erlang ($\lambda: 804.786359, \kappa: 1$), 61 % Weibull ($\theta: 866.064271, \eta: 1.016585$), 19 % LogN ($\mu: 6.220604, \sigma: 1.169132$)	completed	 

[Refresh](#)

Event name 

Load (comma separated) data to compute possible failure distributions for the event

No file chosen

[Sample data](#)

- In the “Events with empirical failure distributions” table, Click the  icon in a row to add the distribution in the “Empirical Distributions” table in the main tab.
 - To generate a new distribution from data, enter the name of the distribution in the “Distribution Name” field, choose the data file from your drive, and click the “Compute” button. A new row will appear in the “Computed Distributions” table with a “running” status.
 - Click the “Refresh” button to check whether the distributions with “running” status have been computed.
- **Generating mixture distribution:** a mixture distribution can also be generated by clicking the “Mix distributions” button. It will show a popup where distributions along with their weights can be added. For example, $d3 = 0.3*d1 + 0.7*d2$ is a mixture distribution, where $d1$ and $d2$ are existing (empirical) failure distributions in the “Failure distributions” and “Empirical failure distributions” tabs. Click the “Add row” button if you want to add more distributions to the mixture.

Mix Event Distributions

Event name*

Event with failure distribution*	Weight*	
dataset1 [Erlang (λ : 10.845734, κ : 1)]	0.1	
dataset2 [LogN (μ : 0.614971, σ : 1.25686)]	0.1	

+ Add event

Cancel
Add

- Click the “Export” button to export empirical distributions in a JSON format (that includes the image data as well).
- Click the “Import” button to import empirical distributions in a JSON format (that includes the image data as well).
- Click the “Import via API” button to get empirical distributions that have been generated externally at a given API. The same data format can be accessed by clicking “Sample data in JSON format” on the popup.

API

Path *

host:8000/utills/computed-empirical-distributions/empirical/data

Sample data in JSON format

Cancel
Import

Attribute Sets

It contains sets of attributes that can be attached to fault tree elements. Click the “Attribute Sets” link in the left panel to open a page with all attribute sets that have been defined.

Attribute Sets		
Name	Description	Actions
AttributeSet		   
AttributeSet1		   

[Add attribute set](#) [Import attribute set](#)

- Click the  icon to export an attribute set.
- Click the “Import attribute set” button to import an attribute set.
- Click the icon  to duplicate an attribute set.
- Click the “Add attribute set” button to create a new attribute set.

AttributeSet		
Title 	Description	Actions
SystemA		   
ComponentA		   
MotorA		   

[Add attribute](#) [Export](#) [Import](#)

Save

Click “Add attribute” to create a new attribute row in the table. Attributes can be imported/exported and duplicated by clicking the “Import”, and “Export” buttons, and the  icon respectively.

Metrics

Metrics help us formally specify properties of interest we want to verify in fault trees. There is a list of predefined metrics (classified into basic, complex, and Importance metrics). For advanced users, it is possible to define custom metrics using continuous stochastic logic (CSL).

In advance view “Metrics” link is visible in the left panel. Click on it, and a screen with four tabs: Basic, Complex, Importance, and Custom will be visible.

Basic

Metrics				
Basic				
Name	Formula	Parameters	Labels	
Unreliability	$P=? [F<=time_bound\ system_failed]$	time_bound	system_failed	
Reliability	$1 - P=? [F<=time_bound\ system_failed]$	time_bound	system_failed	
Average failure probability per unit time (AFH)	$1/time_bound * P=? [F<=time_bound\ system_failed]$	time_bound	system_failed	
Mean time to failure (MTTF)	$T=? [F\ system_failed]$	No parameters	system_failed	
Event probability within a time-bound	$P=? [F<=time_bound\ event]$	time_bound	event	
Event probability	$P=? [F\ event]$	No parameters	event	
Instantaneous probability	$P=? [true\ U\ [time_bound,time_bound]\ event]$	time_bound	event	

It contains four important metrics that are verified in most of the reliability analysis cases:

- Reliability: Probability of failure in a given time bound.
- Unreliability: The complement of reliability (1- Reliability).
- Average failure probability per hour.
- Mean-time-to-failure. Expected time to system failure or scenario occurrence.
- Event probability within a time-bound: Probability that an event occurs within a given time.
- Event probability: Probability that an event occurs.
- Instantaneous probability: Probability that an event occurs at a given time.

Complex

Metrics				
Complex				
Name	Formula	Parameters	Labels	
Full function availability (FFA)	$1 - P=? [F<=time_bound\ system_failed degraded]$	time_bound	system_failed, degraded	
Failure without degradation (FWD)	$P=? [(degraded) U<=time_bound\ (system_failed \& \text{!}degraded)]$	time_bound	system_failed, degraded	
Mean time from degradation to failure (MTDF)	$\Sigma_e, e \text{ degraded } (P=? [(degraded\ U\ s)] * T=? [F\ system_failed])$	No parameters	system_failed, degraded	
Minimal degraded reliability (MDR)	$argmin_e, e \text{ degraded } (1 - P=? [F<=time_bound\ system_failed])$	time_bound	system_failed, degraded	
Failure under limited operation in degradation (FLOD_1)	$\Sigma_e, e \text{ degraded } (P=? [(degraded) U<=time_bound\ s] * P=? [F<=drive_cycle\ system_failed])$	time_bound, drive_cycle	system_failed, degraded	
Failure under limited operation in degradation (FLOD_2)	$\Sigma_e, e \text{ degraded } (P=? [(system_failed \& \text{!}degraded) U<=time_bound\ (system_failed \& \text{!}s)] * P=? [F<=drive_cycle\ system_failed])$	time_bound, drive_cycle	system_failed, degraded	
System integrity under limited fail-operation (SILFO)	$1 - (FWD * FLOD_1)$	time_bound, drive_cycle	system_failed, degraded	
Reach-avoid probability	$P *? [event_1\ U\ event_2]$	No parameters	event_1, event_2	
Time-bounded reach-avoid probability	$P *? [event_1\ U<=time_bound\ event_2]$	time_bound	event_1, event_2	

Some of these metrics cannot be verified directly by the Storm model-checker. They need some additional computations for their verification.

- Full Function Availability (FFA) describes the time-bounded probability that the system provides full functionality, i.e., it has neither failed nor degraded. It is described as the complement of the time-bounded reachability of a failed or degraded state.
- Failure Without Degradation (FWD) describes the time-bounded probability that the system fails without being degraded first. It is the time-bounded reach-avoid probability of reaching a failed state without reaching a degraded state.

- Mean Time from Degradation to Failure (MTDF) describes the expected time from the moment of degradation to system failure. It is obtained by taking the expected time of failure for each degraded state and scaling it with the probability of reaching this state while not being degraded before.
- Minimal Degraded Reliability (MDR) describes the criticality of degraded states by giving the worst-case failure probability when using the system in a degraded state. For all degraded states, the time-bounded reachability of a TLE failure is computed. The MDR is the minimum over the complement of this result for all degraded states.
- Failure under Limited Operation in Degradation (FLOD_1) describes the probability of failure when imposing a time limit for using a degraded system. For all degraded states, the time-bounded reachability probability of a failed state is computed within the restricted time-bound given by a drive cycle. This value is scaled by the time-bounded reach-avoid probability of reaching a degraded state without degradation before.
- Failure under Limited Operation in Degradation (FLOD_2) describes the probability of failure when imposing a time limit for using a degraded system. For all degraded states, the time-bounded reachability probability of a failed state is computed within the restricted time-bound given by a drive cycle. This value is scaled by the time-bounded reach-avoid probability of reaching a degraded state without degradation or system failure before.
- System Integrity under Limited Fail-Operation (SILFO) considers the system-wide impact of limiting the degraded operation time. SILFO is split into two parts considering failures without degradation (FWD) and failures with degradation (FLOD_1).
- Reach-avoid probability: Probability to occur an event, say e1, without occurring another event, say e2, before.
- Time-bounded reach-avoid probability: Probability to occur an event, say e1, within a time_bound without occurring another event, say e2, before.

Importance

Metrics			
Basic	Complex	Importance ⓘ	Custom
Name	Formula	Parameters	Labels
Birnbaum Index (BI) ⓘ	$\partial \text{Unr}(\text{system_failed}, \text{time_bound}) / \partial \text{Unr}(\text{component_failed}, \text{time_bound})$	time_bound	system_failed, component_failed
Criticality Importance (CI) ⓘ	$\text{BI} * \text{Unr}(\text{component_failed}, \text{time_bound}) / \text{Unr}(\text{system_failed}, \text{time_bound})$	time_bound	system_failed, component_failed
Risk Achievement Worth (RAW) ⓘ	$\text{Unr}(\text{system_failed} [p(\text{component_failed}) = 1], \text{time_bound}) / \text{Unr}(\text{system_failed}, \text{time_bound})$	time_bound	system_failed, component_failed
Risk Reduction Worth (RRW) ⓘ	$\text{Unr}(\text{system_failed}, \text{time_bound}) / \text{Unr}(\text{system_failed} [p(\text{component_failed}) = 0], \text{time_bound})$	time_bound	system_failed, component_failed
Diagnostics Importance Factor (DIF) ⓘ	$\text{Unr}(\text{system_failed} \& \text{component_failed}, \text{time_bound}) / \text{Unr}(\text{system_failed}, \text{time_bound})$	time_bound	system_failed, component_failed
BAGT+ ⓘ	$ \text{MTTF}(\text{system_failed}) - \text{MTTF}(\text{system_failed} [p(\text{component_failed}) = 1]) $	No parameters	system_failed, component_failed
BAGT- ⓘ	$ \text{MTTF}(\text{system_failed}) - \text{MTTF}(\text{system_failed} [p(\text{component_failed}) = 0]) $	No parameters	system_failed, component_failed

These metrics cannot be verified directly by the Storm model-checker. They need some additional computations for verification. Note that different importance measures often give different results. In general, this does not mean that one of them gives a wrong result; rather, they measure different aspects of importance. Therefore, it is recommended to consider multiple importance measures and combine their results to have a stronger understanding of the importance of each component.

- Birnbaum Index (BI): How much the unreliability of the system depends on the unreliability of a specific component.

- Criticality Importance (CI): How much the unreliability of the system depends on the unreliability of a specific component scaled by the ratio of component and system unreliability.
- Risk Achievement Worth (RAW): The impact of a component's total degradation on system unreliability.
- Risk Reduction Worth (RRW): The impact of making the component fully reliable on the system's unreliability.
- Diagnostics Importance Factor (DIF): How often a component fails in states where the system has failed.
- BAGT+: Change in MTTF if the component fully degrades.
- BAGT-: Change in MTTF if the component is fully reliable.

Custom

Metrics					
Basic		Complex	Importance ⓘ	Custom	
Name	Formula	Parameters	Labels ⓘ	Reference manuals	Action
DegradedButFunctional	$P=? [(degraded \& !sys_failed) U<=time_bound (sys_failed \& degraded)]$	time_bound	sys_failed, degraded		  
DegButOperational	$P=? [true U<=time_bound (!sys_failed \& degraded)]$	time_bound	sys_failed, degraded		  
NotDegButFailed	$P=? [true U<=time_bound (sys_failed \& !degraded)]$	time_bound	sys_failed, degraded		  
RIS_LOCA	$P=? [true U<time_bound event]$	time_bound	event		  
ReachAvoid	$P=? [(degraded sys_failed) U<=time_bound (sys_failed \& degraded)]$	time_bound	degraded, sys_failed		  
AAA	$P=? [F<=a b]$	a	b		  

[Add metric](#) [Export metrics](#) [Import metrics](#)

One can create custom metrics on the “Custom” tab. It allows specifying metrics using continuous stochastic logic (CSL).

Custom Metric ?

Name* ?

Enter parameter and label names (comma separated) to be used in the below formula.

Parameters ?

Labels ?

Formula* ?

Complement ?

Reference manuals

Description

Cancel
Save

- Click the “Add metric” button to add a new metric.
 - Parameters and labels used inside metrics formulae must have unique names among themselves, starting with a letter or underscore (_) followed by underscores, letters, and/or numbers. They must not be from the list of keywords - - true, false, Pin, Pmax, Smin, Smax, Tmin, Tmax, LAmin, LRAmax, P, R, T, S, LRA, min, max, G, U, F, W, C, I, failed.
 - The formula can be defined using probabilistic computation tree logic (PCTL)/continuous stochastic logic (CSL). For example, $P = ? [\text{true} \cup \leq 10000 (\text{failed} \ \& \ ! \ \text{mode1})]$, where failed and mode1 represent quantifiable states. The grammar of expressions is given [here](#).
 - The “Complement” checkbox can be selected to calculate the complement of a property mentioned in the formula field. It only makes sense for properties that calculate probabilities of events.
 - Reference manuals can be attached with a metric.
 - Note that metric parameters which are entered on the above screen are exclusively dedicated to metrics. Their values are not taken from the parameter set that is attached to a failure model. However, their values can be changed at the time of analysis, and ranges for their values can be provided to draw plots.
 - Click the “Export metrics”/”Import metrics” to export/import metrics in the .metrics format (a format supported by our SAFEST tool).

Computing

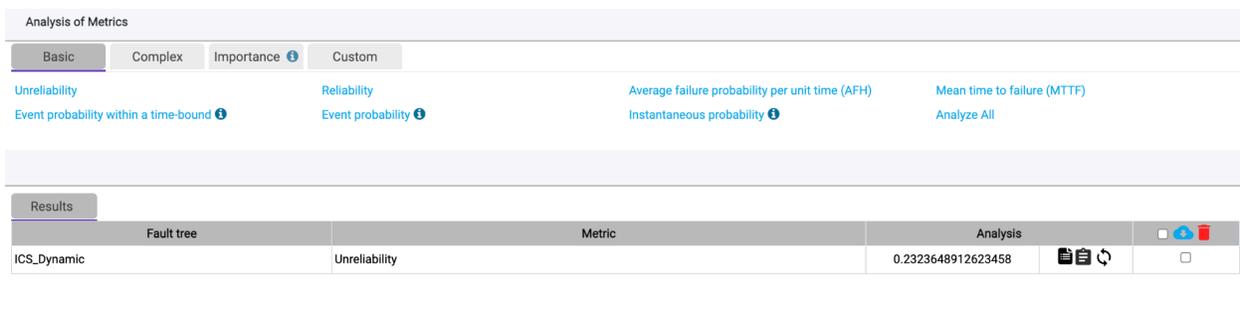
Failure models can be analyzed in different ways:

- Analysis – the exact results of different metrics can be computed.
- Bounded Analysis – the exact values of metrics can be bounded from above and below graphically.
- Graphs – the exact results of different metrics can be graphed against e.g. time.
- Interactive Simulation – failure propagation in fault trees can be shown interactively on multiple pages at the same time.
- Minimal Cut Sets – for static fault trees MCS can be computed and displayed graphically.

(Exact) Analysis

Complex systems usually have dynamic behavior because of e.g. spare components, failure sequence among components, functional dependencies, etc. The analysis of such systems is quite complex which is usually based on simulation or generalization techniques. Unlike others, we implement formal verification techniques e.g. probabilistic model-checking, and thus provide exact results on measures of interest.

Click on the “Analysis” link under “Computing” in the left panel. The following window will appear with four tabs for different classes of metrics.



Analysis of Metrics			
Basic	Complex	Importance ⓘ	Custom
Unreliability Event probability within a time-bound ⓘ	Reliability Event probability ⓘ	Average failure probability per unit time (AFH) Instantaneous probability ⓘ	Mean time to failure (MTTF) Analyze All
Results			
Fault tree	Metric	Analysis	
ICS_Dynamic	Unreliability	0.2323648912623458	  

- One can verify a metric on each tab, the mechanism is more or less the same. For example, click on the “Minimal degraded reliability (MDR)” link on the complex tab. The following window will appear:

Complex Analysis

Metric(s) *

Minimal degraded reliability (MDR): $\text{argmin}_s \in \text{degraded} (1 - P^s = ? [F \leq \text{time_bound system_failed}])$

Fault tree*

ICS_Dynamic

Fault tree root element ⓘ Root Element (Default)

Initial condition

InitCond

Metric parameters

Name	Value ⓘ
time_bound	1

Assign labelled events (of the model) to metric labels

Metric label	Model labelled event
system_failed	system_failed
degraded	system_failed

Model parameter set ⓘ

SMRs_Rates

Constants

Name	Value ⓘ
MIN_PER_YEAR	1
HTP_TPOINT	0.02
ILPER_INC	0.3
BLPER_INC	0.3

Simplify fault tree before analysis Analysis type: Markov Hybrid (Markov and/or BDD)

Result tab: Existing New Results

Cancel
Start

- “Fault tree” dropdown: a fault tree that is selected as a default model in the “Fault trees” window is automatically selected.
- “Fault tree root element”: the root element of the above-selected fault tree is selected by default. One can change the root element by selecting any other element in the dropdown. Note that the dropdown contains only those elements of the fault tree whose “Generate label for the failure event” checkbox is selected in the fault tree.
- Select the initial condition that you want to apply to the fault tree.
- “Metric parameters”: Note that metric parameters cannot take values defined in the parameter set attached to the above-selected fault tree. Each metric parameter has to be assigned a value. For the “time-bound” metric parameter, a

default value is assigned to it that is associated with the above-selected fault tree.

- “Assign labelled events (of the model) to metric labels”: Assign failure events of the fault tree to metric labels.
 - A parameter set that is attached to the selected fault tree (above) is automatically selected. It can be changed at this point to generate another variant of the fault tree.
 - Optionally, change the values of “Constants” defined in the selected parameter set. Note that values of other elements of the parameter set (real-value expressions, (empirical) failure distributions) cannot be changed at the time of analysis.
 - The analysis method is selected automatically based on the selected metric. However, for some metrics both Markov and Hybrid (BDD and/or Markov) analysis are possible. One can decide the analysis type by selecting the corresponding radio button.
 - “Simplify fault tree before analysis”: select this checkbox if the fault tree has to be simplified by applying simplification rules before analysis.
 - Finally, select a tab on which the result of the analysis has to be displayed. It can be an existing tab or a new tab.
- Click the  icon to view configuration of the analysis.

Details

Fault Tree
ICS_Dynamic

Fault Tree Root
Root Element (Default)

Initial Condition
InitCond

Probabilistic Dependencies
V56A_FOD **Applied**
V56B_FOD **Applied**
V56C_FOD **Applied**
LINE_BREAK_FRI **Applied**
HEX_FRI **Applied**
VALVES_RUPTURE_FMD **Applied**

CCF Groups
V5ABC_CCF **Applied**
V6ABC_CCF **Applied**
HEXs_CCF **Applied**
Test **Not Applied**

Parameter Set
SMRs_Rates

Constants
MIN_PER_YEAR: 1
HTP_TPOINT: 0.02
ILPER_INC: 0.3
BLPER_INC: 0.3
MINPINT: 1

[Close](#)

- Click the  icon to view the analysis log.

Logs

Hybrid Analysis
 Fault Tree Simplification : true

Applying V5ABC_CCF CCF Group

Applying V6ABC_CCF CCF Group

Applying HEXs_CCF CCF Group

Applying V56A_FOD Prob. Dependencies

Applying V56B_FOD Prob. Dependencies

Applying V56C_FOD Prob. Dependencies

Applying LINE_BREAK_FRI Prob. Dependencies

Applying HEX_FRI Prob. Dependencies

Applying VALVES_RUPTURE_FMD Prob. Dependencies

***** Replacing CCF Groups, Prob Dependencies and Inital Failed Data *****

Fault Tree:
 DFT (Galileo): [Download](#) [Open in new tab](#)
 JSON: [Download](#) [Open in new tab](#) [Load in fault tree](#)

***** Analysis Start *****

Fault Tree:
 DFT (Galileo): [Download](#) [Open in new tab](#)
 JSON: [Download](#) [Open in new tab](#) [Load in fault tree](#)

Close

- Click the “Download” link to download the generated artifact (DFT/DRN).
- Click the “Open in new tab” link to open the generated artifact in a new browser tab.
- Click the “Load in fault tree” link to load the generated fault tree in the current project.
- Click the  icon to rerun the analysis with selected configurations.
- Click  icon to download the results in the selected rows in a CSV format.

Bounded analysis

To compute exact results for measures using Markov analysis, first of all, the full state space is constructed and then analyzed. However, many states in the state space only marginally contribute to the result. If one is interested in an approximation of the MTTF (or the reliability), these states are of minor interest. We implemented the algorithms, proposed by Dr. Matthias Volk et. al., that generate state space on-the-fly, and then compute an upper and a lower bound to the exact results on a partially unfolded system, which might be much smaller as compared to

the fully unfolded system. The approximation is sound ensuring the exact result lies between these two bounds.

Click on the “Bounded Analysis” link under “Computing” in the left panel and then click e.g. “Mean-time-to-failure” link. The following window will appear:

Bounded Analysis

Metric

Mean time to failure (MTTF) : T=? [F system_failed]

Fault tree

ICS_Dynamic

Fault tree root element i Root Element (Default)

Initial condition*

InitCond

Assign labelled events (of the model) to metric labels

Metric label	Labelled event
system_failed	system_failed

Model parameter set* i

SMRs_Rates

Constants

Name	Value
MIN_PER_YEAR	1
HTP_TPOINT	0.02
ILPER_INC	0.3
BLPER_INC	0.3

Error margin between upper and lower bound of the actual value

0 %

Simplify fault tree before analysis

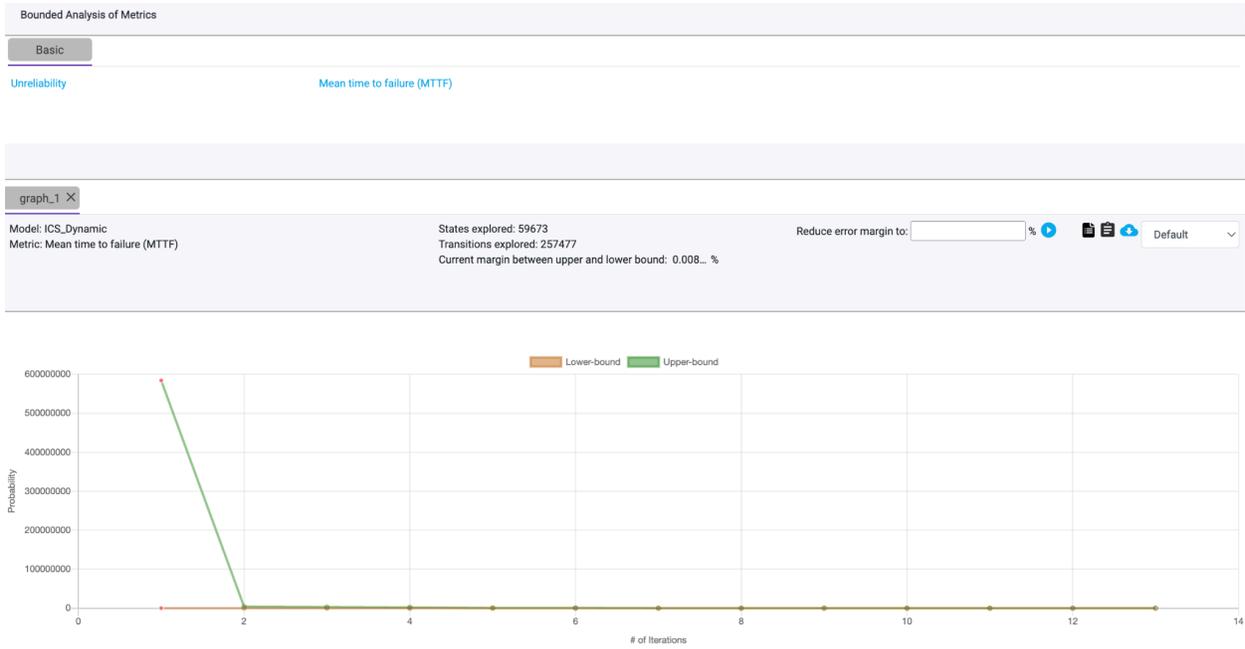
Graph name* i **Y-axis label***

graph_1 Probability

Cancel
Start

- All fields are filled up as described in the “Analysis” case with a few additions:
- “Error margin between upper and lower bound of the actual value”: A percentage error margin is entered in this field.

- Optionally enter “Graph name” and the label of its Y-axis. Note X-axis will always represent the number of iterations in this case.
- Bounded analysis is always done by the Markov technique.
- Click the “Start” button, the results will be displayed as:



The upper line in the graph shows the upper bound whereas the lower line shows the lower bound on the actual value of the metric.

- In addition, we show the number of generated states and the transitions explored so far.
- In case you are interested in further reducing the error margin, insert a new value in the text field and click the play button  .
- One can apply a log function on the values of the Y-axis by selecting it on the right side of the graph.
- The graph values can be downloaded by clicking on the  icon.
- Click the  icon to view configuration of the analysis.

Details

Fault Tree
ICS_Dynamic

Fault Tree Root
Root Element (Default)

Initial Condition
InitCond

Probabilistic Dependencies
V56A_FOD **Applied**
V56B_FOD **Applied**
V56C_FOD **Applied**
LINE_BREAK_FRI **Applied**
HEX_FRI **Applied**
VALVES_RUPTURE_FMD **Applied**

CCF Groups
V5ABC_CCF **Applied**
V6ABC_CCF **Applied**
HEXs_CCF **Applied**
Test **Not Applied**

Parameter Set
SMRs_Rates

Constants
MIN_PER_YEAR: 1
HTP_TPOINT: 0.02
ILPER_INC: 0.3
BLPER_INC: 0.3
MINPINT: 1

[Close](#)

- Click the  icon to view the analysis log.

Logs

```

Hybrid Analysis
Fault Tree Simplification : true

Applying V5ABC_CCF CCF Group

Applying V6ABC_CCF CCF Group

Applying HEXs_CCF CCF Group

Applying V56A_FOD Prob. Dependencies

Applying V56B_FOD Prob. Dependencies

Applying V56C_FOD Prob. Dependencies

Applying LINE_BREAK_FRI Prob. Dependencies

Applying HEX_FRI Prob. Dependencies

Applying VALVES_RUPTURE_FMD Prob. Dependencies

***** Replacing CCF Groups, Prob Dependencies and Inital Failed Data *****

Fault Tree:
DFT (Galileo): Download Open in new tab
JSON: Download Open in new tab Load in fault tree

***** Analysis Start *****

Fault Tree:
DFT (Galileo): Download Open in new tab
JSON: Download Open in new tab Load in fault tree

```

[Close](#)

- Click the “Download” link to download the generated artifact (DFT/DRN).
- Click the “Open in new tab” link to open the generated artifact in a new browser tab.
- Click the “Load in fault tree” link to load the generated fault tree in the current project.

Graphs

We provide an interface to plot and compare measures of interest e.g. reliability, MTTF, etc. against different parameters of interest. Click on the “Graphs” link under “Computing” in the left panel and then click “Reliability”. The following window will appear:

Graph

Metric
Unreliability : $P=? [t \leq \text{time_bound system_failed}]$

Fault tree
ICS_Dynamic

Fault tree root element ? Root Element (Default)

Initial condition*
InitCond

Metric Parameters

Name	Single point		Range			
	Value		Start	End	Step	
time_bound	<input type="radio"/>	1	<input checked="" type="radio"/>	0.1	1	0.1

Assign labelled events (of the model) to metric labels

Metric label	Model labelled event
system_failed	system_failed

Model parameter set* ?
SMRs_Rates

Constants

Name	Single point		Range			
	Value		Start	End	Step	
MIN_PER_YEAR	<input checked="" type="radio"/>	1	<input type="radio"/>	1	1	1
HTP_TPOINT	<input checked="" type="radio"/>	0.02	<input type="radio"/>	1	0.02	1
ILPER_INC	<input checked="" type="radio"/>	0.3	<input type="radio"/>	1	0.3	1

Simplify fault tree before analysis Analysis type: Markov Hybrid (Markov and/or BDD)

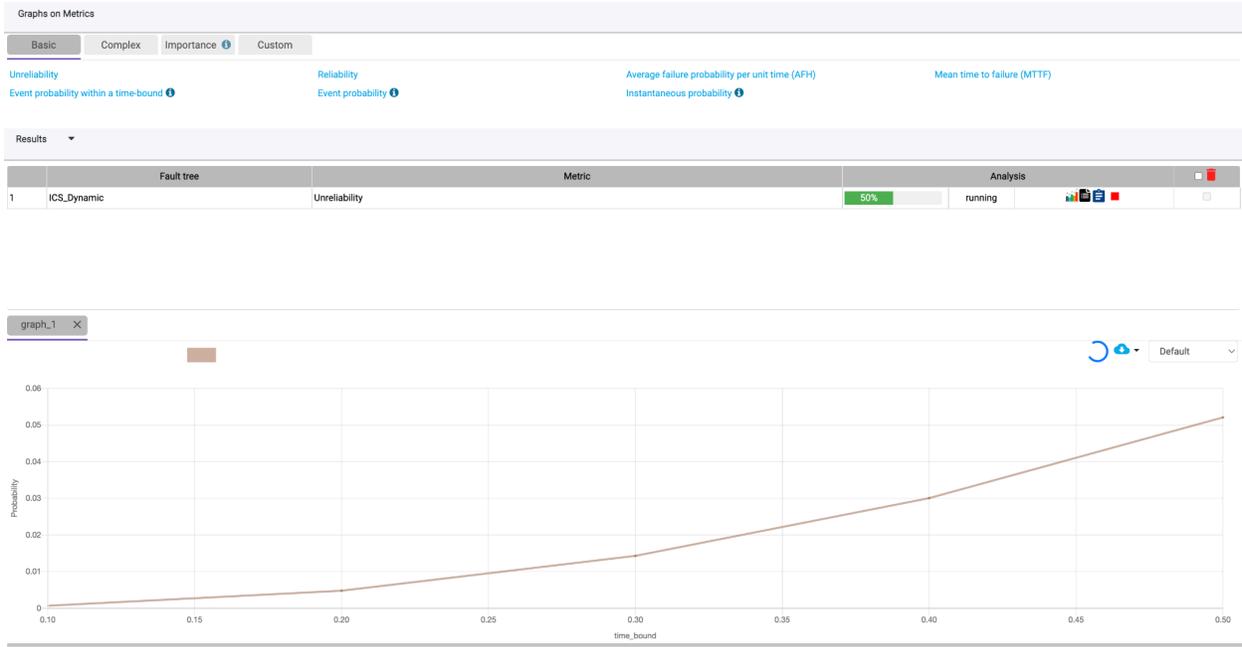
Graph New Existing

Name* ?
graph_1

Variable on X-axis X-axis offset
time_bound 0

Y-axis label* Y-axis offset
Probability 0

- All fields are filled up as described in the “Analysis” case with a few additions:
- One can specify a range of values of metric parameters as well as of Constants defined in the selected parameter set.
- A graph can be plotted on an existing graph as well that has the same variable on the X-axis.
- The variable on the X-axis of the graph can be selected either from the metric parameters or from the Constants of the selected parameter set.
- Click the “Start” button to display the graph:



- Click the  icon to rerun the analysis and draw a graph.
- Click the  icon to stop the running analysis.
- Click the  icon to view the configuration of the analysis.

Details

Fault Tree
ICS_Dynamic

Fault Tree Root
Root Element (Default)

Initial Condition
InitCond

Probabilistic Dependencies
V56A_FOD **Applied**
V56B_FOD **Applied**
V56C_FOD **Applied**
LINE_BREAK_FRI **Applied**
HEX_FRI **Applied**
VALVES_RUPTURE_FMD **Applied**

CCF Groups
V5ABC_CCF **Applied**
V6ABC_CCF **Applied**
HEXs_CCF **Applied**
Test **Not Applied**

Parameter Set
SMRs_Rates

Constants
MIN_PER_YEAR: 1
HTP_TPOINT: 0.02
ILPER_INC: 0.3
BLPER_INC: 0.3
MINPINT: 1

[Close](#)

- Click the  icon to view the analysis log.

Logs

Hybrid Analysis
Fault Tree Simplification : true

Applying V5ABC_CCF CCF Group

Applying V6ABC_CCF CCF Group

Applying HEXs_CCF CCF Group

Applying V56A_FOD Prob. Dependencies

Applying V56B_FOD Prob. Dependencies

Applying V56C_FOD Prob. Dependencies

Applying LINE_BREAK_FRI Prob. Dependencies

Applying HEX_FRI Prob. Dependencies

Applying VALVES_RUPTURE_FMD Prob. Dependencies

***** Replacing CCF Groups, Prob Dependencies and Inital Failed Data *****

Fault Tree:
DFT (Galileo): [Download](#) [Open in new tab](#)
JSON: [Download](#) [Open in new tab](#) [Load in fault tree](#)

***** Analysis Start *****

Fault Tree:
DFT (Galileo): [Download](#) [Open in new tab](#)
JSON: [Download](#) [Open in new tab](#) [Load in fault tree](#)

[Close](#)

- Click the “Download” link to download the generated artifact (DFT/DRN).
- Click the “Open in new tab” link to open the generated artifact in a new browser tab.
- Click the “Load in fault tree” link to load the generated fault tree in the current project.
- In the case of Importance measures, one can draw a plot for multiple components at the same time:

Graph

Metric
 Birnbaum Index (BI) : $\partial \text{Unr}(\text{system_failed}, \text{time_bound}) / \partial \text{Unr}(\text{component_failed}, \text{time_bound})$

Fault tree
 SCR_Dynamic

Fault tree root element
 Root Element (Default)

Initial condition*
 InitCond

Metric Parameters

Name	Single point		Range			
	Value		Start	End	Step	
time_bound	1		0.1	1	0.1	

Assign labelled events (of the model) to metric labels

Metric label	Model labelled event
system_failed	system_failed
component_failed	All Components

Model parameter set*
 SMRs_Rates

Constants

Name	Value	Start	End	Step
MIN_PER_YEAR	1	1	1	1
HTP_TPOINT	0.02	1	0.02	1
ILPER_LNC	0.3	1	0.3	1

Simplify fault tree before analysis
 Analysis type: Markov Hybrid (Markov and/or BDD)

Graph New Existing

Name*
 graph_3

Variable on X-axis
 time_bound

X-axis offset
 0

Y-axis label*
 Probability

Y-axis offset
 0

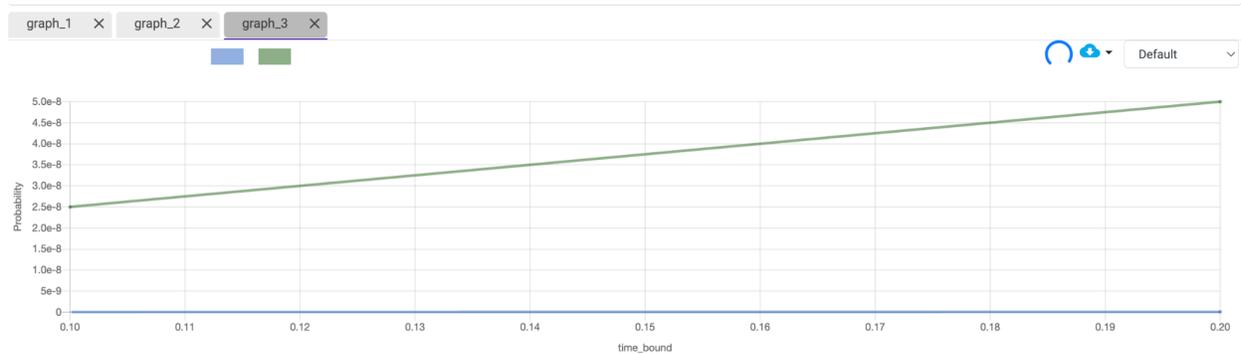
Graphs on Metrics

Basic | Complex | **Importance** | Custom

[Birnbaum Index \(BI\)](#) | [Criticality Importance \(CI\)](#) | [Risk Achievement Worth \(RAW\)](#) | [Risk Reduction Worth \(RRW\)](#)
[Diagnostics Importance Factor \(DIF\)](#) | [BAGT+](#) | [BAGT-](#)

Results

	Fault tree	Metric	Analysis	
3	SCR_Dynamic	Birnbaum Index (BI)	20% running	<input type="checkbox"/>
2	ICS_Dynamic	Birnbaum Index (BI)	60% stopped	<input type="checkbox"/>
1	ICS_Dynamic	Unreliability	70% stopped	<input type="checkbox"/>



Interactive simulation

The idea is to interactively visualize a sequence of failures in a fault tree. The user would start with a usual fault tree and could select one of the basic events (BE) that should fail first. Based on this, the status of each element (failed, operational, fail-safe, claiming in SPAREs, etc.) is redetermined and then visualized. Afterward, another BE can be selected to fail, and so forth. The main benefit of this feature is that the semantics of DFTs become much clearer as users can try out the behavior by themselves.

Click on the “Interactive Simulation” link under “Computing” in the left tab. The following screen will appear. Click on the icon  to start the simulation. The user will be prompted to select a fault tree, a parameter set, and an initial condition. Note that if an initial condition is selected, the resultant fault tree will be shown on a single page because of CCF groups and probabilistic dependencies among elements that lie on multiple pages.

Simulation

Fault tree

BipolarHVDC ▼

Before the simulation, data from all pages will be collected to create a uniform fault tree with its root element given on the main page.

Parameter set* i

HVDC_800KV_day ▼

Initial condition*

None ▼

Cancel
Start

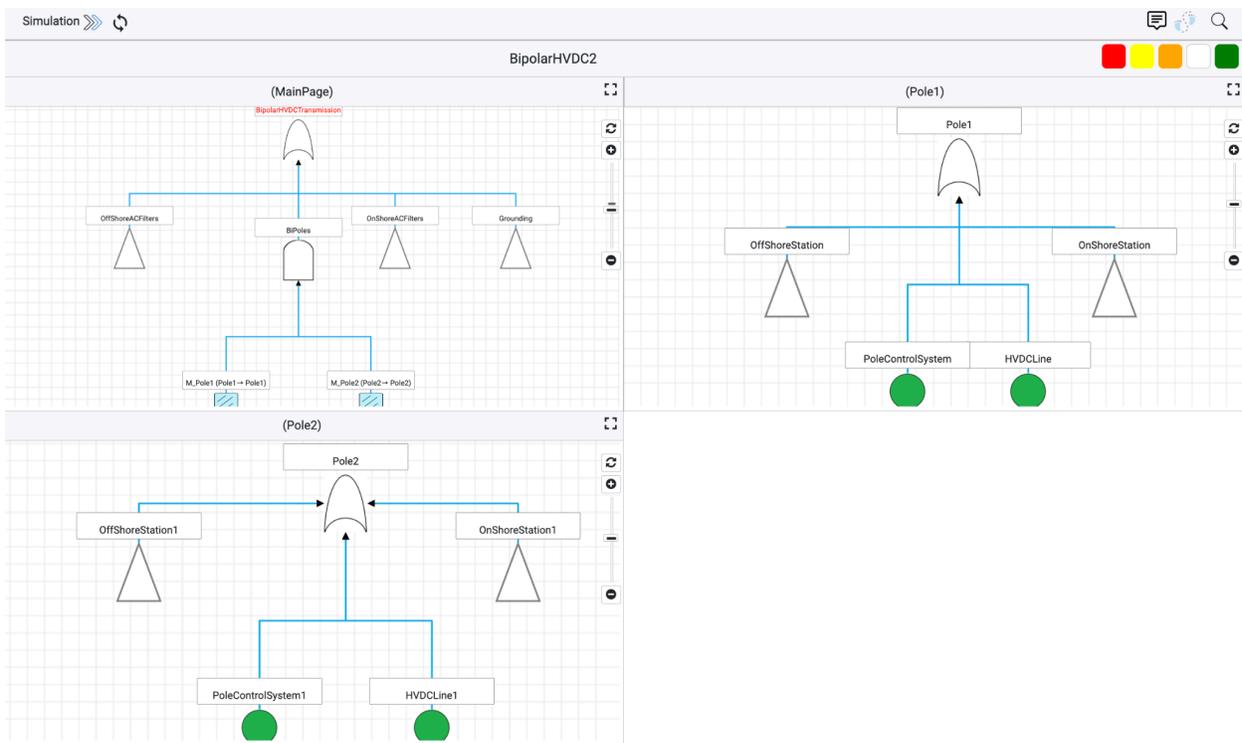
- Click the icon to start the simulation. The user will be prompted to select BEs, having constant probability distribution, that will be failed on start. On clicking the “Ok” button, the simulation will start.

BEs Status at Simulation's Start

BEs, having constant failure probability, that fail at simulation's start. i

Basic Event	Fail
(MainPage) I2	<input checked="" type="checkbox"/>
(MainPage) I3	<input checked="" type="checkbox"/>

Ok



- All basic events (BEs) that can fail are shown in green.
- The user clicks any green BE to fail it. Its color will be turned into Red. After this, BEs that are operational and cannot fail currently remain White, those that are in a fail-safe state are Orange, and those that are in a dont-care state are Yellow.
- The user keeps on failing green BEs, and in return, the failure keeps on moving up the tree until the top-level event turns Red showing the failure of the top-level event.
- The sequence of failures can be shown by clicking on the icon :

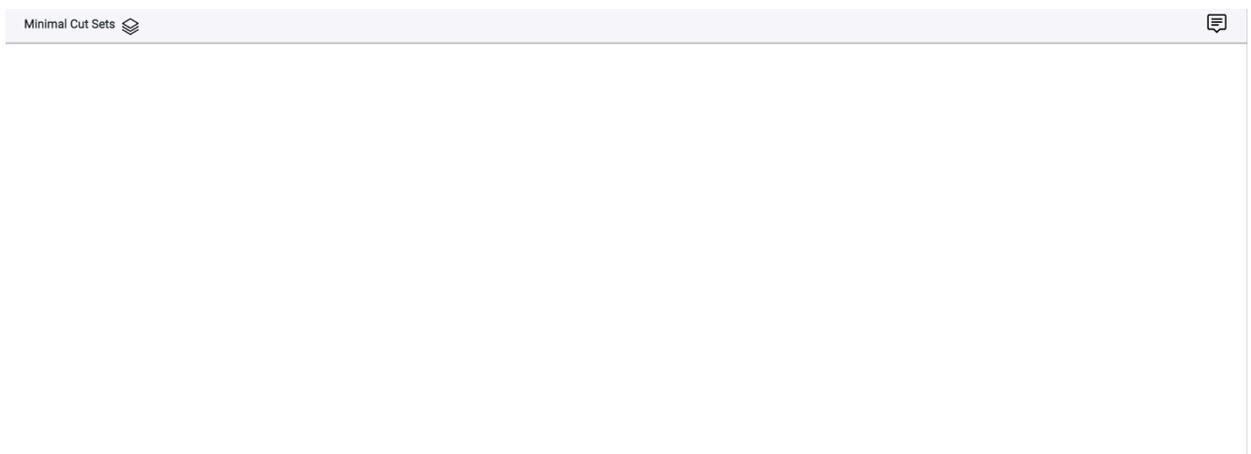


- Users can restart the simulation by clicking on the icon  .

Minimal cut set (for static fault trees)

Cut sets represent sets of BEs whose failure leads to the failure of the top-level element of a fault tree. A minimal cut set is a set whose proper subset cannot be a cut set itself. Cut sets cannot be calculated for dynamic fault trees because of the dynamic nature of the system.

Click on the “Minimal cut set” link under “Computing” in the left tab. The following screen will appear.



Click on the icon  to start. The user will be prompted to select a failure model and a parameter set as:

Minimal Cut Set

Fault tree

BipolarHVDC ▼

Parameter set* 

HVDC_800KV_day ▼

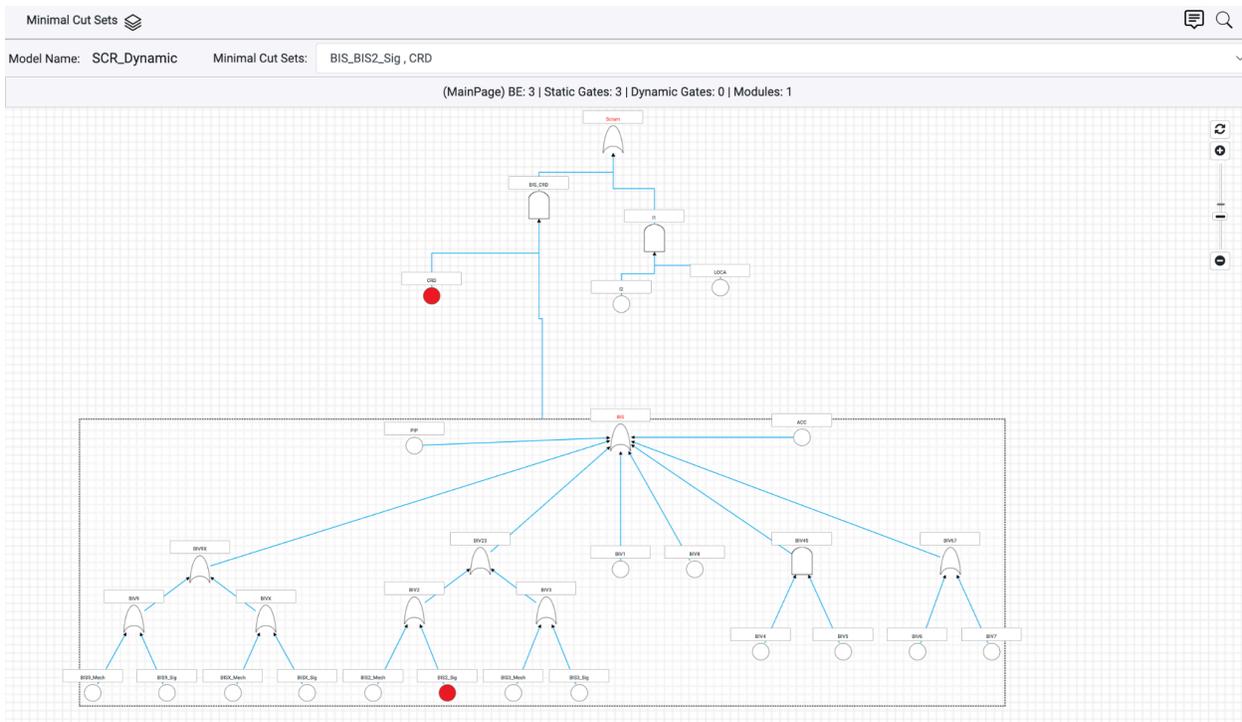
Initial condition*

None ▼

Cancel

Find

On clicking “Find”, minimal cut sets are computed and displayed on the screen as:



- All minimal cut sets will be shown in the dropdown.

- On clicking a cut set, the corresponding BEs will be highlighted (in Red) in the tree.

Event Tree Analysis

It contains all event trees along with their configurations (parameter sets, loss sets, consequence sets), and computing methods.

Configurations

Parameter Sets

Each parameter set contains a list of parameters that are key-value pairs. They are used to specify different quantities in event trees e.g. probabilities, etc. By changing their values several variants of event trees can be generated, which can then be compared with each other based on the results of metrics of interest. Each parameter set comprises:

- Constants
- Constant expressions

View

Click the “Parameter Sets” under “Configurations” in the left panel to view all existing parameter sets.

Parameter Sets			
Name	Reference manuals	Description	Actions
HVDC_800KV_day			
SMRs_Rates			
NPP_LOCA_Rates			
NPP_RRS_Rates			
ElectricPowerSupplyRates			
CentCompMFR2			
AircraftFuelDistributionSystem (2)			
HVDC_800KV_day1			

Creation

Click the “Add parameter set” button to create a new parameter.

Import

Click the “Import parameter set” to import the parameter set in .ps format (a format in which parameter sets are imported/exported in SAFEST).

Duplicate

Click the icon  to duplicate a parameter set.

Export

Click the  icon to export a parameter set in .ps format.

Update

Click a parameter set to update its details

Constants

LOCA_Constants

Constant  Constant expression 

Name*	Numeric value*	Description	
LOCA_Freq	2.51e-4	2.51e-4	   
SMR_LOCA_Freq	4.21E-04		   

Constants can only be numeric e.g. 4, 2.3, 4e-6 etc. Their value can be changed at the time of analysis. For example, graphs can be plotted for matrix results against ranges of values of constants.

- Click the “Add constant” button to enter a new row in the table.
- Click the “Export” button to export constants in a CSV format.
- Click the “Import” button to import constants from a CSV file.
- Click the “Find & replace” button to search sub-strings among Constants and replace them with a new string.

Find & Replace

Filter type
Name, Value

Search substring

Replace substring

[Replace](#) [Cancel](#)

- Click the  icon in the last column of any row to add a new row above it.
- Click the  icon to duplicate the row.
- Click “Evaluate” button to evaluate expressions in all tabs. The result will be displayed in a popup.

Evaluation

Constant

Name	Value	Description
ALARM_Rate_Factor	1	
POWER_Rate_Factor	1	
ECCS_Rate_Factor	1	
PIS_Rate_Factor	0.1667	0.1667

Constant expression

Name	Value	Description
K	1000	kilo
RODS	2.8e-9	Failure of all roads (rate)
ELEC_MGN_SWT	1.92e-9	Failure of electromagnetic switch to disengage (PFD)
RT3STK	0.000032	Relay T3 stuck (PFD)
SCRM_GATE	6.97e-7	Gate of slow scram fails
RT1FO	6.97e-7	Relay T1 fails to open
SECC	0.000032	Sensor fails to give signal

[Close](#) [Download](#)

- Click the “Save” button to save the data. This action will save data in all the tabs.

Constant Expressions

LOCA_Constants			
Constant		Constant expression	
Name*	Value (Expression)*	Description	
SCRAM_F	2.621515123258112e-13 + 5.386249406572089e-10		  
RIS_F	1.4279012841717482e-9 + 6.842946219469892e-11		  
ICS_F	4.024946711143525e-11 + 1.356583063080009e-7		  
BRSF	0.00001216878680857508	Before LOCA RIS failed within time t	  
RIS_LOCA_G_SO	0.0004209112063954996/(1-BRSF)	LOCA in RIS given RIS is operational within time t	  
RIS_FWD	1.4279012841717482e-9/RIS_LOCA_G_SO	RIS Failed within drive cycle after LOCA	  
BRSF	5.957784604784817e-10	Before LOCA RS failed within time t	  
RS_LOCA_G_SO	0.0004209113917750028/(1-BRSF)	LOCA in RS given RS is operational within time t	  
RS_FWD	2.621515123258112e-13/RS_LOCA_G_SO	RS failed within drive cycle after LOCA	  
BCCF	0.00003174494778730206	Before LOCA CC failed within time t	  
CC_LOCA_G_SO	0.0004209113706647805/(1-BCCF)	LOCA in CC given CC is operational within time t	  
CC_FWD	4.024946711143525e-11/CC_LOCA_G_SO	CC failed within drive cycle after LOCA	  

[Add expression](#) [Export](#) [Import](#) [Find & replace](#)

[Evaluate](#) [Save](#)

These are non-negative, real-value expressions, which can use constants (defined in Constants tab) e.g. $x + 2$ where x is a constant. The grammar of the expression is given [here](#).

- Click the “Add expression” button to enter a new row in the table.
- Click the “Export” button to export expressions in a CSV format.
- Click the “Import” button to import expressions from a CSV file.
- Click the “Find & replace” button to search sub-strings among Constant Expressions and replace them with a new string.

Find & Replace

Filter type

Search substring

Replace substring

[Replace](#) [Cancel](#)

- Click the  icon to duplicate the row.
- Click the  icon in the last column of any row to add a new row above it.
- Click the “Save” button to save the data. This action will save data in all the tabs.

Loss Sets

Loss Sets			
Name	Reference manuals	Description	Actions
RadioactiveReleases			   
LOCA_Losses14			   
LossQuantities2			   

[Add loss set](#) [Import loss set](#)

A loss set contains quantities along with their units and descriptions. These quantities can be assigned values at nodes/states of event trees. During analysis, their expected values are calculated by the analysis algorithms.

Click the “Loss Sets” in the left panel to view loss sets.

- Click the “Add loss set” button to create a new loss set.
- Click the “Import loss set” button to import the loss set in .rs format (a format in which loss sets are imported/exported in our tool).
- Click the  icon to duplicate the row.
- Click the  icon to export a loss set in .rs format.
- Click a loss set to view its details
 - Click the “Add loss” button to add a new loss quantity in the above table.
 - Click the “Export” button to export loss in a CSV format.
 - Click the “Import” button to import consequences in a CSV format.
 - Click the  icon to duplicate the row.
 - Click the  icon in the last column of any row to add a new row above it.
 - Click the “Save” button to save the data.

LossQuantities2			
Quantity	Unit	Description	
C	Lives		
R	Million Curies		
L	Sq miles		

[Add loss](#) [Export](#) [Import](#)

Save

Consequence Sets

A consequence set contains a list of outcomes along with their descriptions. These outcomes can be assigned to leaf nodes/states in event trees. During analysis, their expected frequencies/probabilities are calculated.

Click the “Consequence Sets” in the left panel to view consequence sets.

Consequence Sets			
Name	Reference manuals	Description	Actions
consequence_set_1			
LOCA_Consequences			
LOCA_Releases4			
SMR_LOCA_Consequences1			

[Add consequence set](#) [Import consequence set](#)

- Click the “Add consequence set” button to create a new consequence set.

- Click the “Import consequence set” to import a consequence set in .cs format (a format in which loss sets are imported/exported in our tool).
- Click the  icon to duplicate the row.
- Click the  icon to export a consequence set in .cs format.
- Click a consequence set to view its details
 - Click the “Add consequence” button to add a new consequence in the above table.
 - Click the “Export/Import” button to export/import consequences in a CSV format.
 - Click the  icon to duplicate the row.
 - Click the  icon in the last column of any row to add a new row above it.
 - Click the “Save” button to save the data.

LOCA_Consequences

Title 	Description		
ES1	No Release		  
ES2	Low Release		  
ES3	Low Release		  
ES4	Low Release		  
ES5	Low Release		  
ES6	High Release		  
ES7	High Release		  
ES8	High Release		  
ES9	Small Release		  
ES10	Small Release		  
ES11	Small Release		  
ES12	Medium Release		  
ES13	Medium Release		  
ES14	Medium Release		  
ES15	High Release		  
ES16	High Release		  
ES17	High Release		  







Event Trees

This section contains all event trees.

View

Click on the “Event Trees” in the left panel to display event trees in a table. A model that is worked upon the most can be selected as a default model by selecting the corresponding radio button.

Event tree	Consequence set	Loss set	Parameter set	FT events set	Reference manuals	Default	Actions
event_tree_1	consequence_set_1			SMR_TRIGGERING_EVENTS		<input checked="" type="radio"/>	  
LOCA ET	LOCA_Consequences	RadioactiveReleases	Constantsssss	NPP_Models		<input type="radio"/>	  
LOCA_PRA_With_Decision	LOCA_Releases4	LOCA_Losses14	LOCA_Constants	NPP_Models		<input type="radio"/>	  
SMR_LOCA_UPDATED	SMR_LOCA_Consequences1	LossQuantities2	LOCA_Constants	SMR_TRIGGERING_EVENTS		<input type="radio"/>	  

[Add event tree](#) [Import event tree](#)

Creation

Click the “Add even tree” to create a new event tree.

New Event Tree

Name*

Consequence set*

Loss set

Parameter set

FT events set

Reference manuals

Enter all mandatory fields and click the “Save” button.

Export

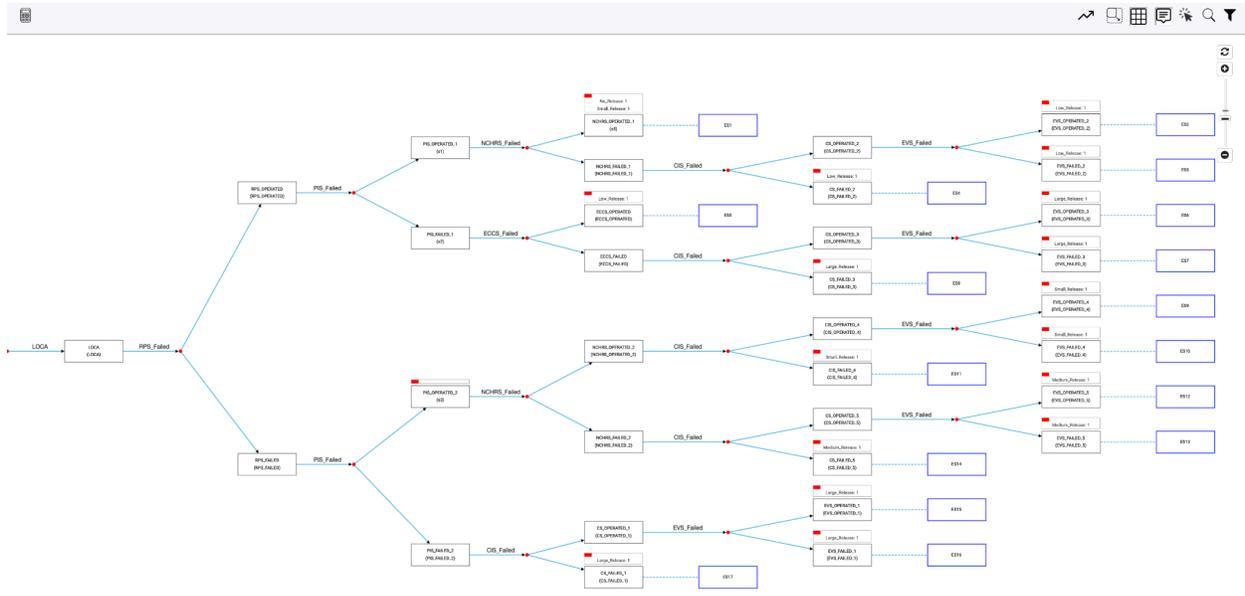
Click the  icon in the corresponding row to download the event tree model in .et format (a format used in the SAFEST tool to import/export event tree models).

Import

Click the “Import event tree” button to import an event tree model (saved in .et format) from your drive.

Update

Click on the model in the table to open it in the canvas.



- Click on the first arrow to update the information of “Accidental Event” (initiating event).
 - For the Accidental Event, select the respective radio button to enter its:
 - Probability
 - Frequency
 - FT triggering/functional event – The dropdown will be filled with all FT events/FT event expressions that exist in the FT events sets associated with the event tree. Select an FT event from the dropdown menu as an accidental event.
 - Enter the name of the event in the “Event name” field.

Accidental Event

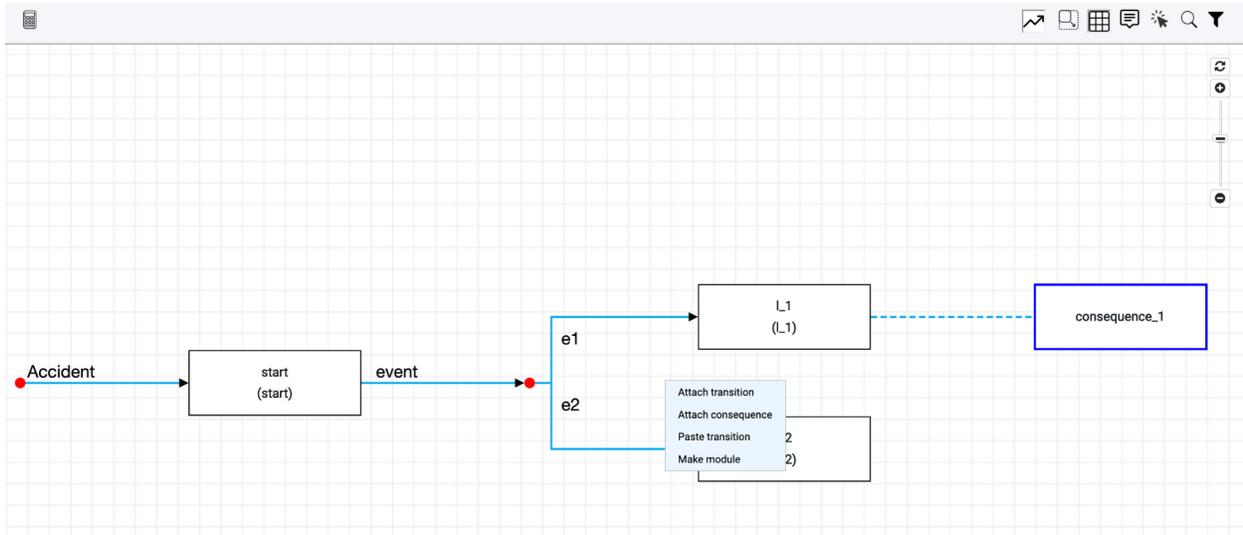
Probability ⓘ

Frequency (f)

FT triggering/functional event*

Event name (ε) *

- Right-click on a node to add a transition, a consequence, past a transition (which is already copied), or convert the sub-tree emanating from this node into a module.



- Click the “Attach transition” to add a new transition to the selected node. You can add multiple transitions to a given node. Note that no further transition can be attached to a node having a consequence attached to it.

Transition

Triggering event name

Transition Branches

Branch event type	Branch event (e)*	Branch probability* <small>p(e) represents the probability of event occurrence.</small>	Next state*
User defined		1	

Add

Description

Cancel Save

- Enter the event name that triggers the branch: triggering event name
- Click the “Add” button to add a new branch of the transition. One can add multiple branches but the sum of probabilities of all branches must be equal to 1.
- Select the branch event type that triggers the branch: User-defined or FT event branch.
 - User-defined branch
 - Enter event name, branch probability – which can be a constant expression from the associated parameter set – and next state name
 - FT event brach

- Select FT event from the “Branch event” dropdown. The branch probability is the probability of the selected event that will be calculated before analyzing the event tree.
- Click a transition to update it. The popup, which comes up while adding a new transition, will appear.
- Click on a transition branch to update it.

Transition Branch

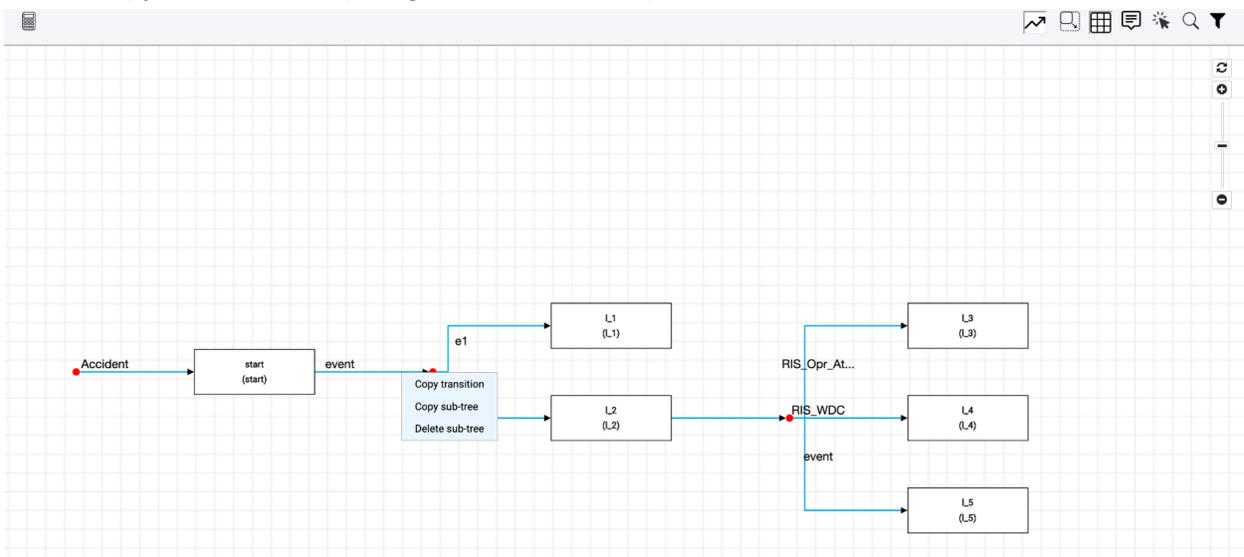
Branch event type

Branch event (ϵ)* ⓘ

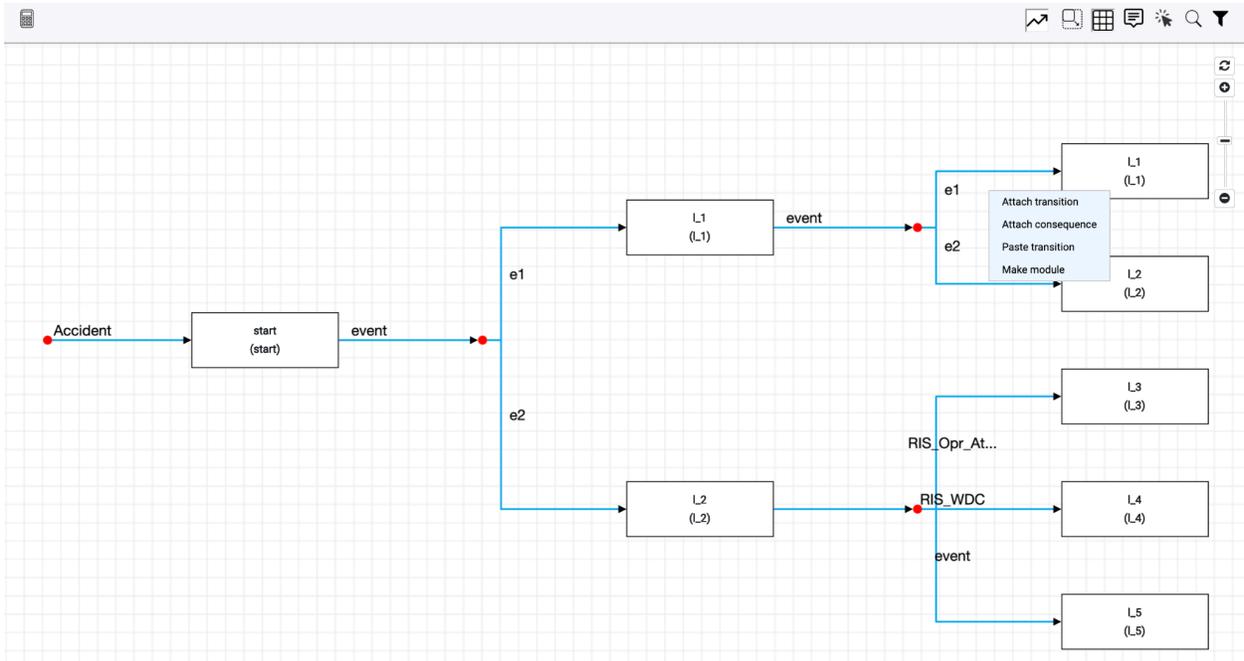
Branch probability* $\rho(\epsilon)$ represents the probability of event occurrence.

Next state

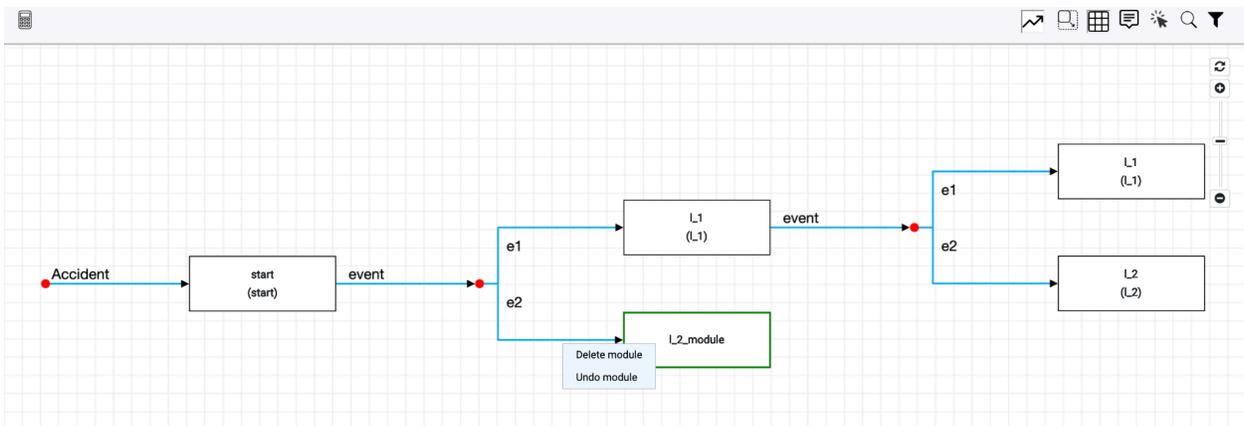
- Right-click on a transition to copy/delete a sub-tree originating from the transition, or copy the transition (along with its branches).



- Copy a transition/sub-tree and then right-click on a node to paste it. Note that transition branches cannot be copy-pasted individually.



- Click on “Make module” to convert the sub-tree emanating from the node into a module. This helps simplify the event tree.
 - Undo a module by right-clicking a module node and selecting “Undo module”.
 - Delete a module by right-clicking a module node and selecting “Delete module”.



- Click the “Attach consequence” to attach a consequence with a node. All consequences in the “Consequence Set” attached to the model will be available in the “Title” dropdown. Select one of the consequences and click the “Save” button. Note that a consequence can be attached to the leaf nodes of a tree.

Consequence

Title *

consequence_1

Description

Cancel
Save

- Click a node to update it.
 - Update the title of the node (not unique in the event tree)
 - Update the name of the node (unique in the event tree)
 - Update tag color and tag datetime
 - Add losses along with their values (which can be constant expressions).

State

Title*

NCHRS_OPERATED_1

Name*

s5

Tag **Tag datetime**

Red

dd/mm/yyyy, --:-- --

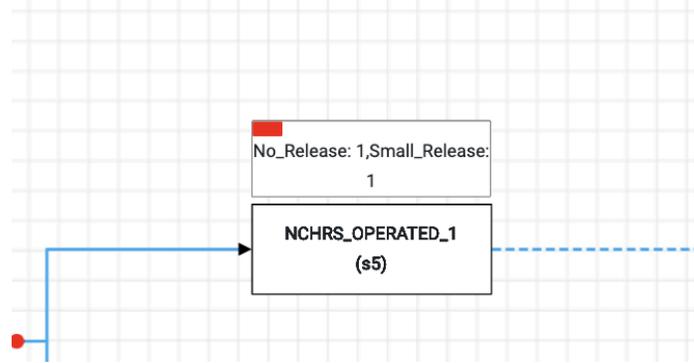
State losses

Quantity*	Value*	
No_Release	1	🗑️
Small_Release	1	🗑️

Add

Cancel
Save

- Click on the icon  to enable the navigator at the bottom of the screen.
- Click on the icon  to show the grid on the screen.
- Click on the icon  to show the summary information about each element on the screen.



- Click on the icon  to display summary information about an element on hovering.
- Click on the icon  to search for any element on the screen.
- Click on the icon  to search elements based on filters. A popup will appear to apply filters.
 - All fields that are filled up, their data is AND together to find the nodes. Within a field, the data is OR-together unless it is mentioned otherwise.
 - If any field is not filled up, it is not considered to be a part of the filtering process, and thus ignored.
- On clicking the “Search” button, the result will be displayed in the “Search results” table.

Advance Search

Filters

State name & Title & Losses All selected must be present & Consequence &

Tag

Search results

Index	Name	Title	Consequence	Losses	Tag	<input type="checkbox"/>
0	LOCA	LOCA				<input type="checkbox"/>
1	RPS_OPERATED	RPS_OPERATED				<input type="checkbox"/>
2	RPS_FAILED	RPS_FAILED				<input type="checkbox"/>
3	s1	PIS_OPERATED_1				<input type="checkbox"/>
4	s2	PIS_FAILED_1				<input type="checkbox"/>
5	s3	PIS_OPERATED_2				<input type="checkbox"/>
6	PIS_FAILED_2	PIS_FAILED_2				<input checked="" type="checkbox"/>
7	s5	NCHRS_OPERATED_1	EST			<input checked="" type="checkbox"/>
8	NCHRS_FAILED_1	NCHRS_FAILED_1		No_Release: 1, Small_Release: 1		<input type="checkbox"/>
9	CS_OPERATED_2	CS_OPERATED_2				<input type="checkbox"/>

- An element can be updated by clicking its name and opening the corresponding popup.
- By selecting elements of the same type in the “Search results” table, operations can be performed on them at once.
 - Update consequences (for leaf nodes)

Update Consequence

Selected states

Name	Title	Consequence	Losses	Tag
s5	NCHRS_OPERATED_1	ES1	No_Release: 1, Small_Release: 1	
EVS_OPERATED_2	EVS_OPERATED_2	ES2	Low_Release: 1	
EVS_FAILED_2	EVS_FAILED_2	ES3	Low_Release: 1	

New consequence

ES8

■ Update losses

Update Loss

Selected states

Name	Title	Consequence	Losses	Tag
s5	NCHRS_OPERATED_1	ES1	No_Release: 1, Small_Release: 1	
CS_FAILED_2	CS_FAILED_2	ES4	Low_Release: 1	<input type="text"/>
EVS_OPERATED_2	EVS_OPERATED_2	ES2	Low_Release: 1	<input type="text"/>
EVS_FAILED_2	EVS_FAILED_2	ES3	Low_Release: 1	<input type="text"/>
ECCS_OPERATED	ECCS_OPERATED	ES5	Low_Release: 1	<input type="text"/>
CS_FAILED_3	CS_FAILED_3	ES8	Large_Release: 1	<input type="text"/>
EVS_OPERATED_3	EVS_OPERATED_3	ES6	Large_Release: 1	<input type="text"/>
EVS_FAILED_3	EVS_FAILED_3	ES7	Large_Release: 1	<input type="text"/>
CIS_FAILED_4	CIS_FAILED_4	ES11	Small_Release: 1	<input type="text"/>

Update losses

Quantity	Value	Actions
No_Release	<input type="text"/>	Add <input type="button" value="v"/>
Low_Release	<input type="text"/>	Add <input type="button" value="v"/>
Small_Release	<input type="text"/>	Remove <input type="button" value="v"/>
Medium_Release	<input type="text"/>	Remove <input type="button" value="v"/>
Large_Release	<input type="text"/>	No change <input type="button" value="v"/>

■ Update tag

Update Tag

Selected states

Name	Title	Consequence	Losses	Tag
s5	NCHRS_OPERATED_1	ES1	No_Release: 1, Small_Release: 1	
CS_FAILED_2	CS_FAILED_2	ES4	Low_Release: 1	<input type="text"/>
EVS_OPERATED_2	EVS_OPERATED_2	ES2	Low_Release: 1	<input type="text"/>
EVS_FAILED_2	EVS_FAILED_2	ES3	Low_Release: 1	<input type="text"/>
ECCS_OPERATED	ECCS_OPERATED	ES5	Low_Release: 1	<input type="text"/>
CS_FAILED_3	CS_FAILED_3	ES8	Large_Release: 1	<input type="text"/>
EVS_OPERATED_3	EVS_OPERATED_3	ES6	Large_Release: 1	<input type="text"/>
EVS_FAILED_3	EVS_FAILED_3	ES7	Large_Release: 1	<input type="text"/>
CIS_FAILED_4	CIS_FAILED_4	ES11	Small_Release: 1	<input type="text"/>

Update tag

None

Computing

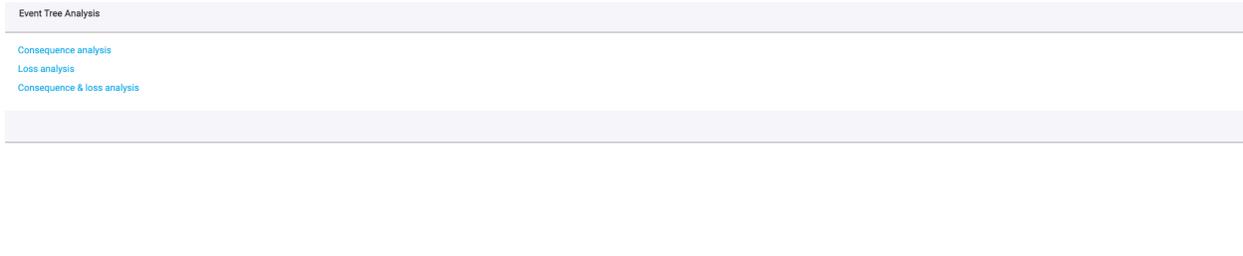
Event trees can be analyzed for consequence frequencies/probabilities and expected values of (loss) quantities.

- Analysis – the exact results of consequence frequencies/probabilities and expected values of (loss) quantities can be computed.

- Graphs – the exact results of consequence frequencies/probabilities and expected values of (loss) quantities can be graphed against time duration.

(Exact) Analysis

Click on the “Analysis” link under “Computing” in the left panel. The following window will appear.



Select the property that you want to verify. E.g. click “Consequence analysis”, and the following popup will appear:

Event Tree Analysis

Event tree*

event_tree_1

Metric

Accidental event (ϵ) frequency * consequence probability -- $f(\epsilon) * P=?$ [true U "consec"]

Parameter set* 

LOCA_Constants

Constants

Name	Value 
LOCA_Freq	2.51e-4
SMR_LOCA_Freq	4.21E-04

FT events set

SMR_TRIGGERING_EVENTS

FT events constants

Name	Value 
TIME_TO_LOCA	1
SAFE_OPERATIONAL_TIME	0.00274

Output tab*

Result_1

- Select the event tree model that you want to analyze from the “Event tree” dropdown – it shows all event tree models that exist under the “Even Trees” in the left panel.
- Change the parameter set if needed. The selected parameter set should contain all constants/expressions that have been used in the model as parameters.
- The constants defined in the selected parameter set (above) are shown in the table, which can be updated if needed.
- Change the FT events set if needed. The selected FT event set should contain all FT events/expressions that are you used to specify the branching probabilities in the event tree.
- The constants defined in the FT Event set (above) are shown in the table, which can be updated if needed.
- Enter the name of the tab where the results of the analysis will be displayed.

Logs

```

***** Replacing CCF Groups, Prob Dependencies and Inital Failed Data *****

Fault Tree:
DFT: Download Open in new tab
JSON: Download Open in new tab Load in fault tree

***** Analysis Start *****

Fault Tree:
DFT: Download Open in new tab
JSON: Download Open in new tab Load in fault tree

***** Identifying Dynamic Modules *****

Dynamic Modules:
Name: PIS
Id: 20240923104718428795

***** Compute Unreliability for Modules *****

Module Id: 20240923104718428795

***** Markov Analysis Unreliability *****

Fault Tree:
DFT: Download Open in new tab
JSON: Download Open in new tab Load in fault tree
Markov Analysis Unreliability Start:
DRN: Download
Markov Model Detail:
-----

```

[Close](#)

- Click the  icon to download the results in a CSV format.

Graphs

We provide an interface to plot consequence probabilities/frequencies or expected values of loss quantities against different parameters of interest. Click on the “Graphs” link under “Computing” in the left panel. Click the “Consequence/Expected Loss”, and the following window will appear:

Graph

Event tree
 event_tree_1

Metric
 Accidental event (e) frequency * consequence probability - f(e) * P=? [true U "consec"]

Max Min

Assign event tree consequences to metric label

Metric label	Consequences
consec	consequence_1

Parameter set* 
 LOCA_Constants

Constants

Name	Single point		Range			
		Value	Start	End	Step	
LOCA_Freq	<input checked="" type="radio"/>	2.51e-4	<input type="radio"/>	1	2.51e-4	1
SMR_LOCA_Freq	<input checked="" type="radio"/>	4.21E-04	<input type="radio"/>	1	4.21E-04	1

FT events set
 SMR_TRIGGERING_EVENTS

FT events constants

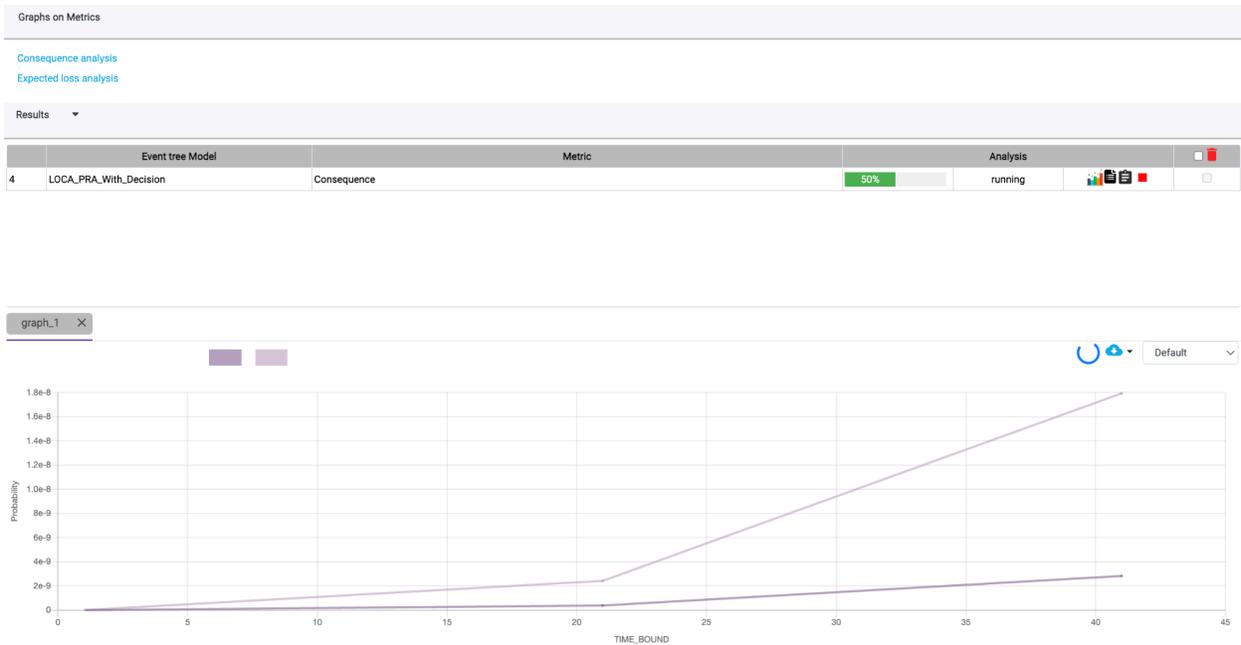
Name	Single point		Range			
		Value	Start	End	Step	
TIME_TO_LOCA	<input checked="" type="radio"/>	1	<input type="radio"/>	1	1	1
SAFE_OPERATIONAL_TIME	<input checked="" type="radio"/>	0.00274	<input type="radio"/>	1	0.00274	1

Graph New Existing

Name*  Variable on X-axis Y-axis label*
 graph_1 LOCA_Freq Probability

- “Event tree” dropdown: an event tree that is selected as a default in the “Event trees” page is automatically selected.
- Select whether the min, max, or both values of consequences probabilities/frequencies (expected loss) are to be computed.
- “Assign event tree consequences (quantities) to metric labels (parameter)”: Select (multiple) consequence(s) (quantities) from the dropdown for which we want to measure probabilities/frequencies (expected values).
- A parameter set that is attached to the selected event tree is automatically selected. It can be changed at this point to generate another variant of the model.
- One can specify a range of values of constants defined in the selected parameter set.
- An FT event set which is attached to the selected event tree is automatically selected. It can be changed at this point to generate another variant of the model.
- One can specify a range of values of constants defined in the selected FT event set.
- Select whether to draw a new graph or it is to be plotted on an existing graph that has the same variable on X-axis.
- The variable on the X-axis of the graph can be either time-bound or from the constraints of the selected parameter/FT event set.

- Click the “Start” button to display the graph:



- Click the  icon to stop the running analysis.
- Click the  icon to rerun the analysis and draw a graph.
- Click the  icon to view the configuration of the analysis.

Details

Event Tree
LOCA_PRA_With_Decision

Parameter Set
LOCA_Constants

Constants
LOCA_Freq: 2.51e-4
SMR_LOCA_Freq: 4.21E-04

FT events constants
TIME_BOUND: (Start: 1, End: 100, Step: 20)

Metric
Consequence (max)
Label -> Consequence
consec: CoreDamage_50pct, CoreDamage_100pct

[Close](#)

- Click the  icon to view the analysis log.

Logs

```

***** Replacing CCF Groups, Prob Dependencies and Inital Failed Data *****

Fault Tree:
DFT (Galileo): Download Open in new tab
JSON: Download Open in new tab Load in fault tree

***** Analysis Start *****

Fault Tree:
DFT (Galileo): Download Open in new tab
JSON: Download Open in new tab Load in fault tree

***** Identifying Dynamic Modules *****

Dynamic Modules:
Name: PIS
Id: 20240923104718428795

***** Compute Unreliability for Modules *****

Module Id: 20240923104718428795

***** Markov Analysis Unreliability *****

Fault Tree:
DFT (Galileo): Download Open in new tab
JSON: Download Open in new tab Load in fault tree
Markov Analysis Unreliability Start:
DRN: Download
Markov Model Detail:
-----
Model type: CTMC (sparse)
States: 4
Transitions: 6
Reward Models: none
State Labels: 4 labels
* PIS_dc -> 0 item(s)
* PIS_failed -> 1 item(s)

```

[Close](#)

- Click the “Download” link to download the generated artifact (DFT/DRN).
- Click the “Open in new tab” link to open the generated artifact in a new browser tab.
- Click the “Load in fault tree” link to load the generated fault tree in the current project.

Interfaces

Interfaces can be defined to use fault trees within event trees. Labeled events (basic or compound) of fault trees can be associated with the branches of event trees as triggering events. The probabilities of these events provide the branching probabilities of the related transitions. To do this, we choose fault tree events and define CSL metrics to compute their probabilities. During the analysis phase, the metrics are calculated on the fault trees to provide the branching probabilities of the linked transitions.

- Click on “FT Events sets” under “Interfaces” in the left panel.

FT Events Sets			
Name	Reference manuals	Description	Actions
NPP_Models			  
SMR_TRIGGERING_EVENTS			  

[Add FT events set](#)

- Click on the icon  to duplicate the FT event set.
- Click on the FT event set link to update it.
- Click “Add FT event set” to create a new event set. FT event set has:
 - Constants
 - Constant expressions
 - FT events, and
 - FT event expressions

Constants

SMR_TRIGGERING_EVENTS			
Constant 			
Name*	Value (Numeric Constants)*	Description	  
TIME_TO_LOCA	1	years	  
SAFE_OPERATIONAL_TIME	0.00274	24 hours = 0.00274 years	  
TIME_TO_LOCA	1	years	  
SAFE_OPERATIONAL_TIME	0.00274	24 hours = 0.00274 years	  

[Add constant](#) | [Export](#) | [Import](#) | [Find & replace](#)

[Evaluate](#) [Save](#)

Constants can only be numeric e.g. 4, 2.3, 4e-6 etc. Their value can be changed at the time of analysis. For example, graphs can be plotted for matrix results against ranges of values of constants.

- Click “Add constant” to enter a new row in the table.
- Click “Export” to export constants in a CSV format.
- Click “Import” to import constants from a CSV file.
- Click the “Find & replace” button to search sub-strings among Constants and replace them with a new string.

Find & Replace

Filter type

Search substring

Replace substring

- Click the  icon in the last column of any row to add a new row above it.
- Click the  icon to duplicate the row.
- Click the “Evaluate” button to evaluate expressions in all tabs. The result will be displayed in a popup.

Evaluation

Constant

Name	Value	Description
TIME_TO_LOCA	1	years
SAFE_OPERATIONAL_TIME	0.00274	24 hours = 0.00274 years

Constant expression

Name	Value	Description
Exp1	5	
Exp2	1.00274	

- Click the “Save” button to save the data. This action will save data in all the tabs.

Constant Expressions

SMR_TRIGGERING_EVENTS

Constant **+** Constant expression **+** FT event **+** FT event expression **+**

Name*	Value (Expression)*	Description	
Exp1	TIME_TO_LOCA * 5		 
Exp2	1+ SAFE_OPERATIONAL_TIME		 
Exp1	TIME_TO_LOCA * 5		 
Exp2	1+ SAFE_OPERATIONAL_TIME		 

+ Add expression **+** Export **+** Import **+** Find & replace

Evaluate **Save**

These are non-negative, real-value expressions, which can use constants (defined in Constants tab) e.g. $x + 2$ where x is a constant. The grammar of the expression is given [here](#).

- Click the “Add expression” button to enter a new row in the table.
- Click the “Export” button to export expressions in a CSV format.
- Click the “Import” button to import expressions from a CSV file.
- Click the “Find & replace” button to search sub-strings among Constant Expressions and replace them with a new string.

Find & Replace

Filter type
Name, Value

Search substring

Replace substring

Replace **Cancel**

- Click the  icon to duplicate the row.
- Click the  icon in the last column of any row to add a new row above it.
- Click “Evaluate” button to evaluate expressions in all tabs. The result will be displayed in a popup.

Evaluation

Constant			
Name	Value	Description	
TIME_TO_LOCA	1	years	
SAFE_OPERATIONAL_TIME	0.00274	24 hours = 0.00274 years	

Constant expression			
Name	Value	Description	
Exp1	5		
Exp2	1.00274		

- Click the “Save” button to save the data. This action will save data in all the tabs.

FT event

SMR_TRIGGERING_EVENTS

Name	Fault Tree	Metric	Description	
LOCA	LOCA	Unreliability		
RIS_Opr_At_LOCA	RIS_Dynamic	DegradedButFunctional	RIS is functional at the time of LOCA	
ICS_Opr_At_LOCA	ICS_Dynamic	DegradedButFunctional	ICS is functional at the time of LOCA	
SCR_Opr_At_LOCA	SCR_Dynamic	DegradedButFunctional	SCR is functional at the time of LOCA	
RIS_WDC_After_LOCA	RIS_Dynamic	Failure under limited operation in degradation (FLOD) Modified		
ICS_WDC_After_LOCA	ICS_Dynamic	Failure under limited operation in degradation (FLOD) Modified		
SCR_WDC_After_LOCA	SCR_Dynamic	Failure under limited operation in degradation (FLOD) Modified		

- Click “Add FT event” to create an FT event.

FT Event

Name *

Metric to compute on the root element of the fault tree*

Fault Tree*

Fault tree root element ⓘ

Initial Condition

Metric parameters

Name	Value ⓘ
time_bound	365

Assign labelled events (of the model) to metric labels

Metric label	Model labelled event
system_failed	system_failed

Model parameter set ⓘ

Constants

Name	Value ⓘ
MIN_PER_YEAR	1
HTP_TPOINT	0.02
ILPER_INC	0.3
BLPER_INC	0.3

Simplify fault tree before analysis

Description

- Enter an event name that should be unique among other FT events.
- Select a metric to quantify the event
- Select a fault tree on which the metric is to be computed
- Select the root element of the fault tree
- Select an Initial condition for the fault tree
- Specify values of metric parameters. Note that Constants and Constant Expressions defined in the first two tabs can be used as values of metric parameters. These values can be changed at the time of event tree analysis.
- Select a parameter set for the fault tree model, and change the values of the constants defined in the parameter set if needed.
- Click the Save button to save the FT event.

- Click the icon  to view the configuration of the FT event.
- Click the icon  to duplicate an FT event.

FT event expression

SMR_TRIGGERING_EVENTS

Constant  Constant expression  FT event  **FT event expression **

Name*	Value (Expression)*	Description	
RIS_Opr_At_LOCA_NL	RIS_Opr_At_LOCA/LOCA		  
RIS_WDC	RIS_WDC_AFTER_LOCA/RIS_Opr_At_LOCA_NL		  
ICS_Opr_At_LOCA_NL	ICS_Opr_At_LOCA/LOCA		  
SCR_Opr_At_LOCA_NL	SCR_Opr_At_LOCA/LOCA		  
ICS_WDC	ICS_WDC_AFTER_LOCA/ICS_Opr_At_LOCA_NL		  
SCR_WDC	SCR_WDC_AFTER_LOCA/SCR_Opr_At_LOCA_NL		  
RIS_Opr_At_LOCA_NL	RIS_Opr_At_LOCA/LOCA		  
RIS_WDC	RIS_WDC_AFTER_LOCA/RIS_Opr_At_LOCA_NL		  
ICS_Opr_At_LOCA_NL	ICS_Opr_At_LOCA/LOCA		  
SCR_Opr_At_LOCA_NL	SCR_Opr_At_LOCA/LOCA		  
ICS_WDC	ICS_WDC_AFTER_LOCA/ICS_Opr_At_LOCA_NL		  
SCR_WDC	SCR_WDC_AFTER_LOCA/SCR_Opr_At_LOCA_NL		  

 Add FT event expression  Find & replace

 Save

- Click the “Add FT event expression” to create a new row in the table.
- An expression can be defined using Constants, Constant expressions, and FT events defined in the previous tabs.
- Click the “Find & replace” button to search sub-strings among Constants and replace them with a new string.

Find & Replace

Filter type
Name, Value

Search substring

Replace substring

 Replace  Cancel

- Click the icon  to duplicate an FT event expression.
- Click the icon  to create a new row above the current row.

Manuals

Link of reference manuals can be created and then associated with elements of fault trees/event trees.

- Click on the Manuals link in the left panel.
 - Click the “Add manual” button to create a new row in the table.
 - Click the “Import/Export” button to import/export data in the table.
 - Click the icon  to duplicate an FT event expression.
 - Click the icon  to create a new row above the current row.

Reference Manuals		
Title*	URL*	
Modelcheckingpaper	https://dl.acm.org/doi/abs/10.1145/3552326.3587442	  
CTMCPaper	https://dl.acm.org/doi/abs/10.1145/3552326.3587442	  

 Add manual  Export  Import

 Save

Annotation of SysML Models with Safety Information

To annotate SysML model elements with safety information, we have created a few packages, which are to be used inside the SysML models against which fault trees are to be generated. These [packages](#) are:

- DGBMetadata: It contains a package DFTElements with the following sub-packages and elements:

- DFTGates package: It defines all gates that are used to construct fault trees.

```

package DFTGates {

  metadata def AND;
  metadata def OR;
  metadata def VOT {
    /* if any k-out-of-n components fail (input events),
       the system will fail (output event) n number of input events */
    attribute k : Number;
  }
  metadata def SPARE;
  metadata def PAND;
  metadata def POR;
  metadata def FDEP {
    /* The failure of the trigger_element renders the children of FDEP failed
       as per the value of probability attribute. The default value of probability
       is 1. */
    occurrence trigger_element;
    attribute probability: Real;
  }
  metadata def FSEQ;
  metadata def MUTEX;
}

```

- DFTBEs package: It defines all basic elements that may be used in fault trees.

```

package DFTBEs{
  abstract metadata def BE{
    /* The value of dormancy attribute is only relevant if the BE is a
       child of a spare spare gate. The default value of dormancy is 1.*/
    attribute dormancy:Real;
  }
  abstract metadata def BE_CONSTANT_DISTRIBUTION specializes BE {
    attribute prob:Real;
  }
  abstract metadata def BE_EXPONENTIAL_DISTRIBUTION specializes BE {
    attribute rate:Real;
  }
  abstract metadata def BE_ERLANG_DISTRIBUTION specializes BE {
    attribute rate:Real;
    attribute phases:Real;
  }
  abstract metadata def BE_NORMAL_DISTRIBUTION specializes BE {
    attribute mean:Real;
    attribute stddev:Real;
  }
  abstract metadata def BE_WEIBULL_DISTRIBUTION specializes BE {
    attribute rate:Real;
    attribute shape:Real;
  }
}

```

- TOP_LEVEL metadata: It is used to annotate an element of a fault tree as a top-level element. More than one element can be annotated as top-level elements. This helps generate multiple fault trees (for different scenarios) collectively that may share Gates and BEs.
- FailureModes: It defines all failure modes that may be used to annotate elements of SysML models with safety information. At the moment we allow failure modes to be modeled with the following failure distributions:

- Exponential distribution
- Erlang distribution
- Weibull distribution
- Log-normal distribution, and
- Constant distribution

Moreover, within this package, we allow to define model constants as (DFTParameters) enumerations. These constants can be used to define failure rates, probabilities, shapes, etc. of failure modes.

```

public import DGBMetadata::DFTElements::*;
/* DFTParameters enumeration defines constants used to annotat
failure rates/probabilites/shares/etc. of BEs in fault trees.
enum def DFTParameters :> Real {
  FIT1 = 0.000000001;
  FIT2 = 0.000000002;
  FIT3 = 0.000000003;
  FIT4 = 0.000000004;
  prob = 0.2;
  param1 = 10.2;
  param2 = 1.1;
}

metadata def FIT1 specializes BE_EXPONENTIAL_DISTRIBUTION{
  attribute redefines rate = DFTParameters::FIT1;
}
metadata def FIT2 specializes BE_EXPONENTIAL_DISTRIBUTION{
  attribute redefines rate = DFTParameters::FIT2;
}
metadata def FM1 specializes BE_CONSTANT_DISTRIBUTION{
  attribute redefines prob = DFTParameters::prob;
}
metadata def FIT3 specializes BE_ERLANG_DISTRIBUTION{
  attribute redefines rate = DFTParameters::FIT3;
  attribute redefines phases = 2;
}
metadata def FM_4 specializes BE_NORMAL_DISTRIBUTION{
  attribute redefines mean = DFTParameters::param1;
  attribute redefines stddev = DFTParameters::param2;
}
metadata def FIT4 specializes BE_WEIBULL_DISTRIBUTION{
  attribute redefines rate = DFTParameters::FIT4;
  attribute redefines shape = 3;
}

```

Laptop Example.

The following example explains how elements within the SysML model can be annotated to generate fault trees out of them.

```

package LaptopPackage {
  private import FailureModes::*;
  part Laptop {
    part CPU1 {
      metadata Failure:FIT2;
    }
    part CPU2 {
      metadata Failure:FIT1;
    }
    part cooling {
      metadata Failure:FIT1;
    }
    part plug {
      metadata Failure:FIT2;
    }
    part battery {
      metadata Failure:FIT2;
    }
    part switch {
      metadata HWF:FIT1;
    }
    metadata power:SPARE about plug::Failure, battery::Failure;
    metadata processor:AND about CPU1::Failure, CPU2::Failure;
    metadata laptop:OR about power, processor;
    metadata Dep:FDEP about CPU1::Failure, CPU2::Failure {
      trigger_element = cooling::Failure;
    }
    metadata TLE1:TOP_LEVEL about laptop;
    metadata TLE2:TOP_LEVEL about power;
  }
}

```

After the compilation of the SysML model annotated with safety information using our packages in Jupyter Notebook, run the following command to export the package in JSON format. **Currently, we support the latest version – v0.45.0 – of SysML 2.0: [SysML-v2-Release](#)**

```
%export <package_name>
```

After downloading, it can be uploaded inside the SAFEST tool at the “Failure Models” page under “Fault Tree Analysis” in the left panel:

Fault Trees							
Fault tree	Fault tree type	Reference manuals	Time-bound (Life cycle)	Description	Loaded	Default	Actions
BipolarHVDC	Dynamic	asdfd	365 days		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	   
ICS_Dynamic	Dynamic		1 years	Isolation Condenser System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
SCR_Dynamic	Dynamic		1 years	Boron Injection System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
RIS_Dynamic	Dynamic		1 years	Reactor Isolation Systems	<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
NPP_RPS	Dynamic		20000 hours	Reactor Protection System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
NPP_PIS	Dynamic		20000 hours	Pool Isolation System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
NPP_ECCS	Dynamic		20000 hours	Emergency Core Cooling System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
NPP_CIS	Dynamic		20000 hours	Containment System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
NPP_RRS	Dynamic		20000 hours	Reactor Regulation System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
NPP_EVS	Dynamic		20000 hours	Emergency Ventilation System	<input type="checkbox"/>	<input type="checkbox"/>	   
NPP_NCHRS	Dynamic		20000 hours	Natural Circulation Heat Removal Failure	<input type="checkbox"/>	<input type="checkbox"/>	   
NPP_PowerSupply_EDF	Dynamic		100 hours		<input type="checkbox"/>	<input type="checkbox"/>	   
CentCompSys_5	Dynamic		12 months		<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
AFDS	Dynamic		100 hours		<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
LOCA	Dynamic		1 years		<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
AFDS_2	Dynamic		100 hours		<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
BipolarHVDC1	Dynamic		365 days		<input checked="" type="checkbox"/>	<input type="checkbox"/>	   
BipolarHVDC2	Dynamic		365 days		<input checked="" type="checkbox"/>	<input type="checkbox"/>	   

 Add fault tree
  Import fault tree
  Import fault tree from SysML

Click the “Import failure model from SysML” button to extract failure models as well as parameter sets from the SysML model. The failure models are added to the list of existing failure models on the “Failure Models” page. Whereas all constants (DFTPParameters enumerations inside the SysML FailureModes package) are added to the existing parameter sets on the “Parameter Sets” page.

Grammars

Regular Expressions of Identifiers and Numeric Constants

- **Identifier (id):**
 - It is used to give a unique name to e.g. constants, expressions, etc.
 - It is a string of characters starting with a capital letter (A-Z), a small letter(a-z), or an underscore (_) followed by a capital letter(s), a small letter(s), underscore or digit(s) (0-9).
 - Note that identifiers cannot be from the list of keywords of a grammar.
- **Numeric constant (nc):**
 - Simple, decimals and exponential i.e 123, 123.123, 123e+1, 123e-1, 123e1, 123.123e+1, 123.123e-1, 123.123e1, 123.123E1, 0.12

Context Free Grammar (CFG) of Expressions

- $RE \rightarrow E \mid + nc \mid - nc$
- $E \rightarrow E \text{ OP } E \mid (E \text{ ? } E : E) \mid nc \mid id \mid (RE) \mid BF (RE, RE) \mid UF(RE) \mid ! E$
- $BF \rightarrow \text{pow, log, min, max}$
- $UF \rightarrow \text{floor, ceil, abs}$
- $OP \rightarrow \text{=>} \mid \& \mid = \mid != \mid >= \mid <= \mid < \mid > \mid + \mid - \mid * \mid / \mid \%$
- $OP \rightarrow \mid$

Where

- “id” is an identifier of an expression,
- “nc” is a numeric constant string, and
- **pow**, **log**, **min**, **max**, **floor**, **ceil**, and **abs** are grammar keywords.

Note: The above grammar can produce both boolean and real expressions; however, this tool only processes real expressions. In other words, while the grammar allows for expressions that may evaluate to either boolean (true/false) or real (numeric) values, the tool is specifically designed to handle only those expressions that result in real numbers. Boolean expressions, although included in the grammar, are not utilized by the tool.

Examples of real expressions:

- 2.2
- 13.12e-9
- 2 + x
- 3.9 * pow(x, y) + log (a, b)
- 4.5 / min(x*x, y+2) * max (a, b)
- 3 + floor(x) + ceil(y * a) + abs(b)
- (x > y ? 3 : a * b + c)

In these examples, each expression results in a real (numeric) value, aligning with the tool's requirements.

Context Free Grammar (CFG) of Boolean Expressions

- $E \rightarrow E \text{ OP } E \mid id \mid (E) \mid !id \mid !(E)$
- $OP \rightarrow \mid$
- $OP \rightarrow \&$

Where

- “id” is an identifier of an expression, and

Context Free Grammar (CFG) of Continuous Stochastic Logic (CSL)

- PROP → P OP2 Type [PathFormula] | T OP2 Type [RewardFormula] | LongRun OP2 Type [StateFormula]
- Type → =? | OP3 E
- LongRun → LRA | S
- PathFormula → OP4 BoundedExpression StateFormula | StateFormula OP5 BoundedExpression StateFormula
- BoundedExpression → ^ { Bound } | { Bound } | Bound | NULL
- Bound → [E,E] | OP3 TIME
- TIME → (E) | nc
- RewardFormula → I = E | C <= E | F StateFormula | LongRun
- StateFormula -> StateFormula OP6 StateFormula | P OP2 OP3 E [PathFormula] | LongRun OP2 OP3 E [StateFormula] | id | (StateFormula) | true | !StateFormula
- OP → => | & | | | = | != | <= | >= | > | < | + | - | * | / | %
- OP1 → + | -
- OP2 → min | max | NULL
- OP3 → <= | >= | > | <
- OP4 → G | F
- OP5 → U | W | R
- OP6 → | | &
- E → E OP E | id | nc | (E) | !(E) | (OP1 nc)
- NULL → empty string

Where

- “id” is an identifier of an expression,
- “nc” is a numeric constant string, and
- true, false, Pmin, Pmax, Smin, Smax, Tmin, Tmax, LRAmin, LRAmax, P, R, T, S, LRA, min, max, G, U, F, W, C, I, failed, system_failed are keywords of the grammar.