SAFETWICE

SafeTree

A reliability software designed for Fault Tree Analysis

Contents

1 Introduction

SafeTree is part of the SafeSuite family of products, a powerful tool for the development of projects meeting common industry's safety standards.

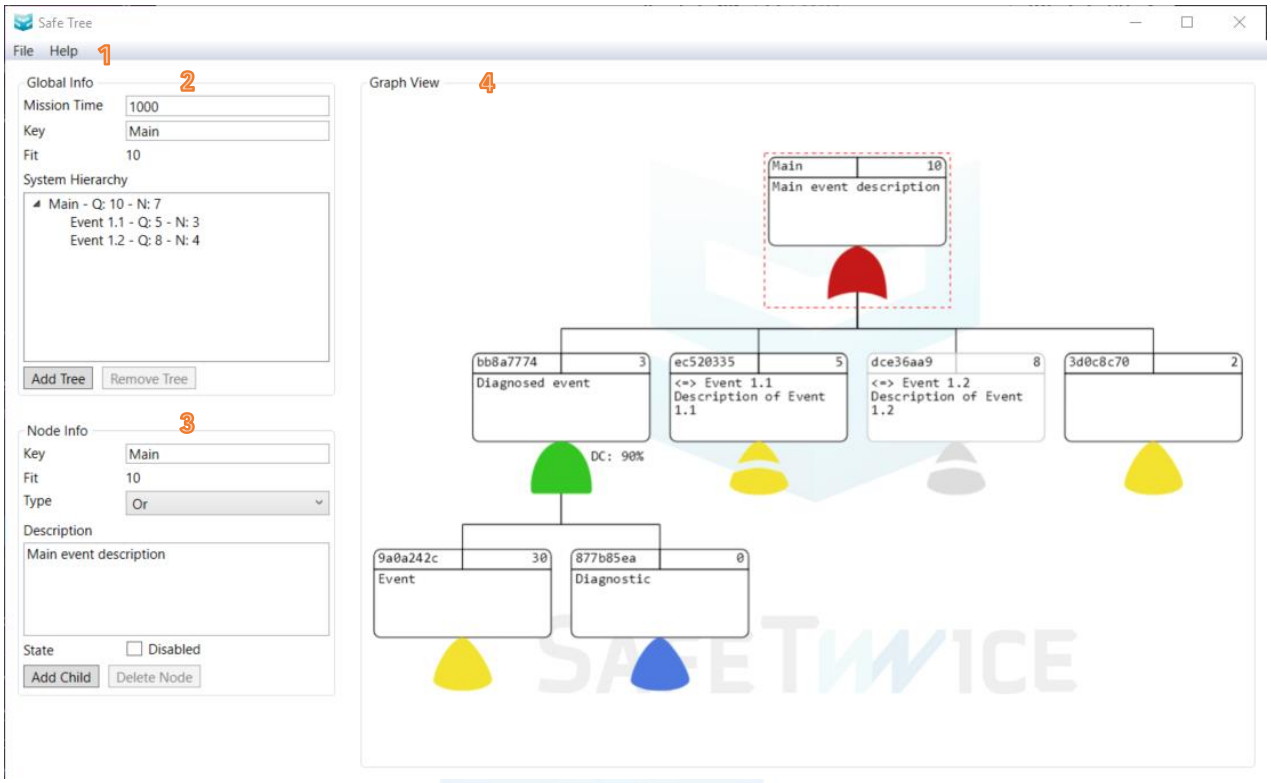
SafeTree provides a tool for Qualitative Fault Tree Analysis (FTA), which is a top-down deductive analysis method in which safety-concerned top-level events are decomposed in a series of lower-level events combined in a well-determined fashion; and for Quantitative Fault Tree Analysis, which delivers a global failure rate for top-level events depending on the drawn tree topology.

1.1 Features

- **Support for different event types: failure, diagnosis and hardware endpoints.**
- **Automatic tree layout and drawing. Robust, single-view interface.**
- **Immediate failure rate recalculation.**
- **Simple, efficient navigation: zooming, panning, branch switching.**
- **Simple child branch management: duplicate, connect, disconnect trees.**
- **Enable/disable branches for quick impact assessment.**
- **Print to paper or PDF.**
- **Save/Load data in custom format enabling app-specific features.**
- **Support for software endpoints for informative and process integrity purposes.**

2 Usage

2.1 Application parts



1. **Menu**
    a. **File > (New | Load | Save | Print | Exit)**
    b. **Help > (About | License)**
2. **Global Info panel**
3. **Node Info panel**
4. **Graph View**

2.2 Licensing

The application has three licensing states:

- **Unlicensed/invalid/expired license: in other words, no license.**
- **Demo license: expires after a time interval (14 days).**
- **Full license: lifetime license.**

The "No license" state blocks the Save, Import, Export features. Loading is still possible for demo purposes, but severely limits the application's usability.

A license can be requested with the "Help > License" dialog. The dialog shows brief instructions, which are hereby developed:

1. Select the desired license type: either "Demo" or "Full". The full license requires an order ID.
2. Click the "Generate" button, which creates several files and opens their location on disk.
3. Send the file named "LicenseRequest.dat" to the e-mail address support@safetwice.com
4. The e-mail will be replied (if all is correct) with a file "License.dat". Copy this file to the same place where the request is located.
5. Close and reopen the program for the license to get detected.

NOTICE: the license folder can be quickly found with the "Find" button in the "License" dialog. It should be in "C:\Users\<USER>\AppData\Local\SafeTwice\SafeTree\License".

NOTICE: to be able to regenerate the license request, if required, delete from disk the files "LicenseRequest.dat" and "PrivateKey".

NOTICE: the ".dat" extension is important. Add it in case it is missing in the "LicenseRequest" or "License" files. Otherwise the application will not properly recognize the license.

NOTICE: a license is only valid for the computer it was generated in.

2.3 Global Info panel

The aim of this panel is to display information of interest to the user at any point of the development process. It shows the current top-level event failure rate, as well as the name and the tree structure at a glance. New trees are added and deleted from here.

- Mission Time: required FTA parameter for diagnosed events. Units in hours.
- Key: top-level event name.
- Fit: read-only global failure rate top-level event. Units in FIT (failures in 10E9 hours).
- System Hierarchy: shows available trees. There can be top-level events and lower-level events, i.e. child branches. The items show their name, total branch failure rate (Q)

(failures in 10E9 hours) and number of included events (N). Right-clicking on an item displays its context menu: "Copy Key", "Duplicate".

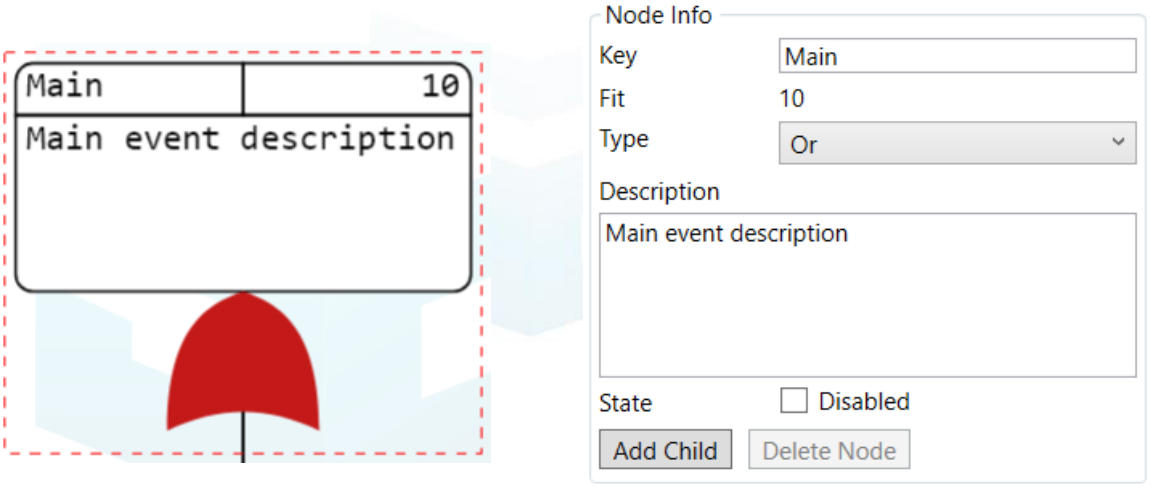
- System Hierarchy > Copy Key: copy currently selected tree key (name).
- System Hierarchy > Duplicate: copy selected tree, changing event names (uniqueness).

- Add Tree: adds a new top-level tree to the list.
- Remove Tree: deletes the currently selected tree and all subtrees.

2.4 Node Info panel

This panel shows information specific to the currently selected node, i.e. the one surrounded by a red dashed line. There are four main types of nodes: Or, And, End Point, Diagnosed.

2.4.1 Or Gate

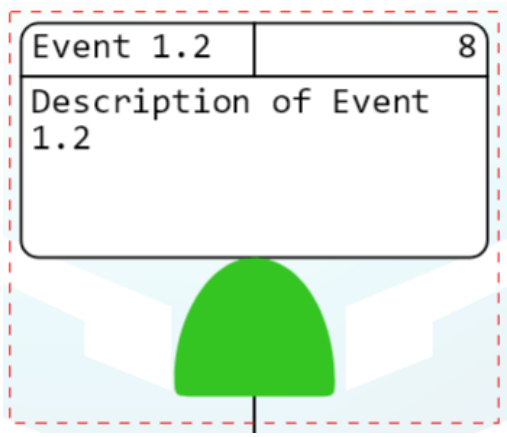


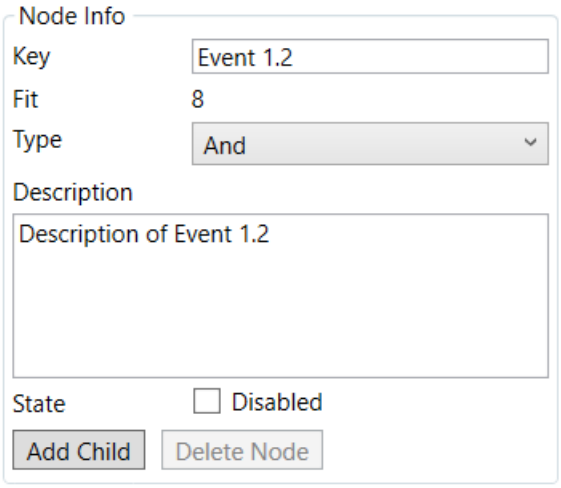
This gate sums the FIT values of child nodes.

- Key: editable node name.
- Fit: read-only node FIT value.
- Type: event type.
- Description: event description.
- State: allows disabling a branch to ignore its value in higher-level calculations.
- Add Child: add new child event.
- Delete Node: delete this event and all descendants.

NOTICE: OR gates are typically used to describe the contribution from lower-level events to a common top-level event.

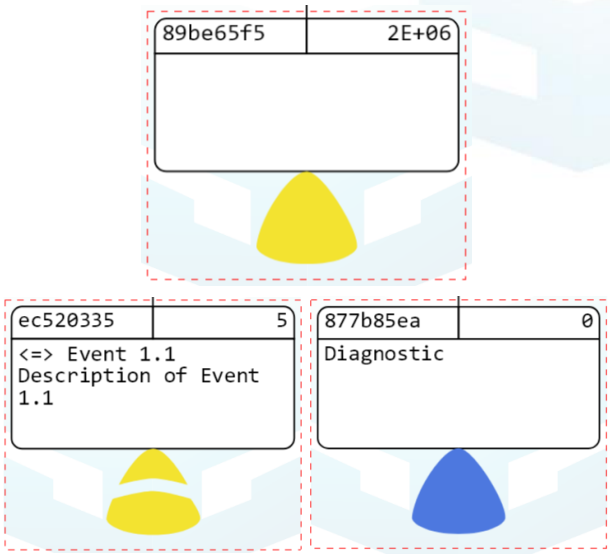
2.4.2 And Gate

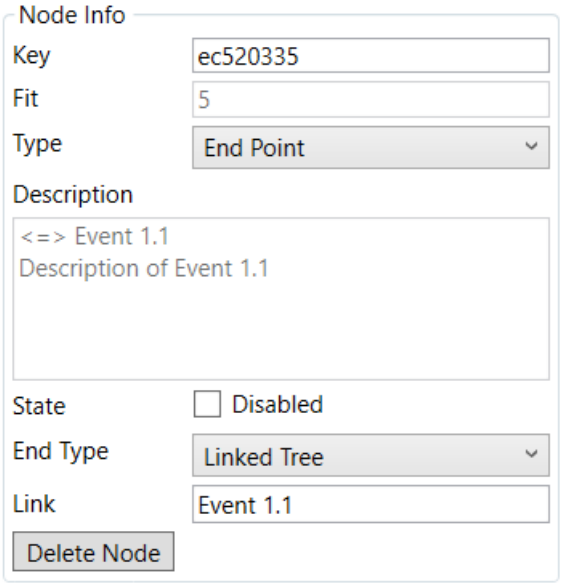




This gate multiplies FIT values of child nodes. This node's properties are the same as the "Or" gate.

2.4.3 End Point Gate





This gate provides an actual FIT value for higher-level gates, hence its "Fit" field is editable. There are three subtypes of end point nodes ("End Type"):

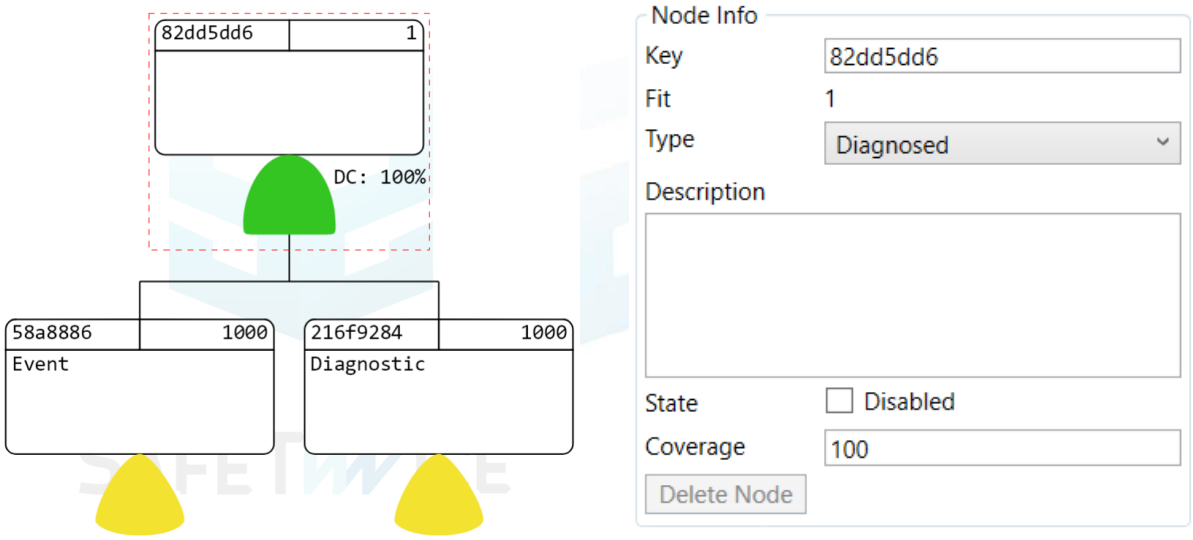
- **Normal (yellow): editable FIT value.**

- **Linked Tree (yellow, split): used as linking point for child trees. Use top node's key of target tree as "Link" value. It can be copied from the System Hierarchy or written directly. The "Description" is read-only in this mode, displaying the link target.**
- **Software (blue): read-only zero FIT value. Used mainly as diagnostic node, clearly showing its type at a glance. By definition, correctly written SW diagnostics are error-free, i.e. have zero FITs.**

The rest of the fields are similar to other node's fields.

NOTICE: End Point gates are typically used to describe bottom-level events for which a determined failure rate is available.

2.4.4 Diagnosed Gate



This gate combines an event branch (λ_E) with a diagnostic branch (λ_D) which can fail at a given rate (DC – Diagnostic "Coverage"). For automotive (ISO-26262) this is usually 60%, 90% or 99%. When at 100%, it simply works as an And gate. The global "Mission Time" (T) parameter is used by this gate internally:

$$\lambda = \lambda_E(1 - \mathrm{DC}) + \lambda_E \mathrm{DC} \lambda_D \mathrm{T}$$

Note that children node types can be changed normally to suit any topology.

This gate is actually a combination of the other gates, but it is frequently used and therefore nice to have by default.

Note: the event branch is always on the left, and the diagnostic on the right. Bear it in mind in case the default descriptions are replaced.

NOTICE: Diagnosed gates (or AND gates) are typically used to describe dual point failures: a higher event is described as a lower-event failure rate weighted by a diagnostic mechanism (wich is described by a diagnostic coverage ratio and a failure rate for the diagnostic mechanism itself).

2.5 View workflow

The application is designed for the workflow that is hereby explained.

Initially there is a single tree. Nodes can be added only to "And" and "Or" gates. A node can be deleted with the "Delete Node" button, removing also all descendants. A node type can be changed at any point, but this deletes descendants. Disable nodes with the "State" to bypass them.

When a tree grows to big or for modularity purposes, a new tree can be created with the "Add Tree" button. Trees can be deleted when selected, with the "Remove Tree" button. A tree can be duplicated using the context menu item "Duplicate" in the "System Hierarchy".

Trees can be linked together by means of an "End Point" node of type "Linked Tree". Only top-level trees can be linked (uniquely linked), i.e. those not already linked. This prevents circular references and does not limit design complexity. When linked, a tree appears as a child of its parent.

Note: be careful with delete operations since there is currently no undo operation.

Note: event keys must be unique, which in enforced by the application. This ensures traceability.

Quick tips

- **The Graph View can be panned (hold left button) and zoomed (scroll wheel).**
- **Nodes in the Graph View are selected with the left mouse button.**
- **Reset the view with the context menu item in the Graph View.**
- **Items in the System Hierarchy have a context menu for "Copy Key", "Duplicate".**
- **Press "Enter" in any input box to commit changes without having to change focus.**
- **All text can be copy/pasted as usual.**

2.6 Save/load

The project file has ".fta" extension. Save/load of project files is done through the "File" menu.

2.7 Print

Printing enables exporting all trees to paper or PDF, as chosen through the system's print dialog. A simple information box is added to the top of all pages displaying top-level node name, description, page index, and project name.