Arbor Fault Tree Analysis

User's Manual

Rev 8

Introduction

This guide describes how to use the Arbor Fault Tree Analysis Software. Arbor is a module in the Kenexis Integrated Safety Suite (KISS). KISS provides technical safety and security professionals with a cloud-based multi-user platform for the design of engineered safeguards.

Because new features are added frequently, you are encouraged to check the version number on the cover page of this manual to ensure that you are reading the most current version of this manual which corresponds with the active version of Arbor.

About Kenexis

Kenexis is an independent engineering consulting firm. We ensure the integrity of instrumented safeguards and industrial networks. Using skills in risk analysis, reliability engineering, and process engineering, we help establish the design and maintenance specification of instrumented safeguards, such as safety instrumented systems (SIS), alarm systems and fire and gas systems. We use the same skills for industrial control systems (ICS) network design, cyber security assessments, and industrial network performance analysis.

Table of Contents

Table of Contents

Section 0 – Quick Reference

This section contains a list of common symbols, terms and hotkey combinations used in Arbor. This section is intended to serve as a desk reference when working in Arbor.

0.1 Hotkeys

The following hotkey combinations are available when working on the Fault Tree Interface Page with the Main Workspace in focus.

> *IMPORTANT NOTE:*
> The Main Workspace can be brought into focus by left clicking anywhere on the graphical representation of the fault tree. For example, selecting a gate or event (as indicated by a red border around the object) will bring the Main Workspace into focus.

Hot Key	**Action**
Ctrl + Enter	Run Calculations
Plus / Equals	Zoom In
Minus / Underscore	Zoom Out
Q	Add New Gate Below Selected Node
W	Add New Event Below Selected Node
Ctrl + X	Cut Selected Node
Ctrl + C	Copy Selected Node
Ctrl + V	Paste Cut or Copied Node Below Selected Node
Delete	Delete Selected Node
Ctrl + Left Arrow	Move Selected Node Left (Relative to Siblings)
Ctrl + Right Arrow	Move Selected Node Right (Relative to Siblings)
Escape	Clear Node Selection

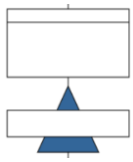
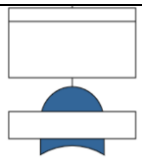
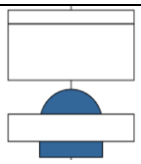
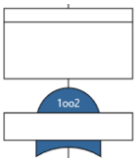
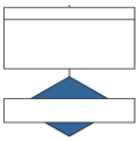
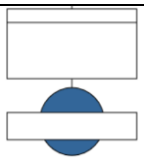
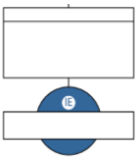
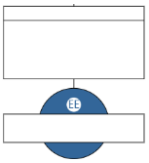
Section 0 – Quick Reference

0.2 Event Model Types

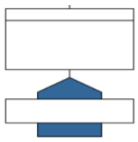
Event Model Type	Description
Constant	The user directly enters unavailability and Frequency Event Model Failure Rate = Event Frequency Event Model Unavailability = Event Unavailability
Covert	Used to model component failures that are not self-revealing or are not repaired immediately. Unrevealed or non-repaired failures remain present until the Test Interval is reached.
Overt	Used to model component failures that are self-revealing and are repaired immediately. Unavailability contribution from overt events is associated with downtime during repair.

Section 0 – Quick Reference

0.3 Event and Gate Symbols

Symbol	Description
	**Transfer Gate:** The Transfer gate allows the unavailability and frequency of a child node to pass through unchanged. If a Transfer gate has more than one child, it is underdefined and both unavailability and frequency will evaluate to zero.
	**Or Gate:** Any child of an OR gate in a failed state results in a failed state of the gate.
	**And Gate:** All children of an AND gate must be in a failed state for the gate to be in a failed state.
	**Vote Gate:** K-out-of-N child nodes in a failed state will results in a failed state for a Vote gate, where: K = Vote Count defined on the Gate Details Form N = The total number of children under the gate
	**Undefined Event:** An undefined event is an event which has been created but does not have an event model or Boolean calculation mode applied. Unavailability and frequency will always evaluate to zero for undefined events.
	**Defined Event:** The default event type. Both unavailability and frequency will be calculated for this event type using the selected event model for the event.
	**Initiating Event:** This is an event which has been defined as an initiating event on the event details form. Initiating events force the calculation engine to exclude unavailability and only calculate frequency for this event and all parent nodes above it in the tree.
	**Enabling Event:** This is an event which has been defined as an enabling event on the event details form. Enabling events force the calculation engine to exclude the frequency of this event from any cut sets in which it is contained.

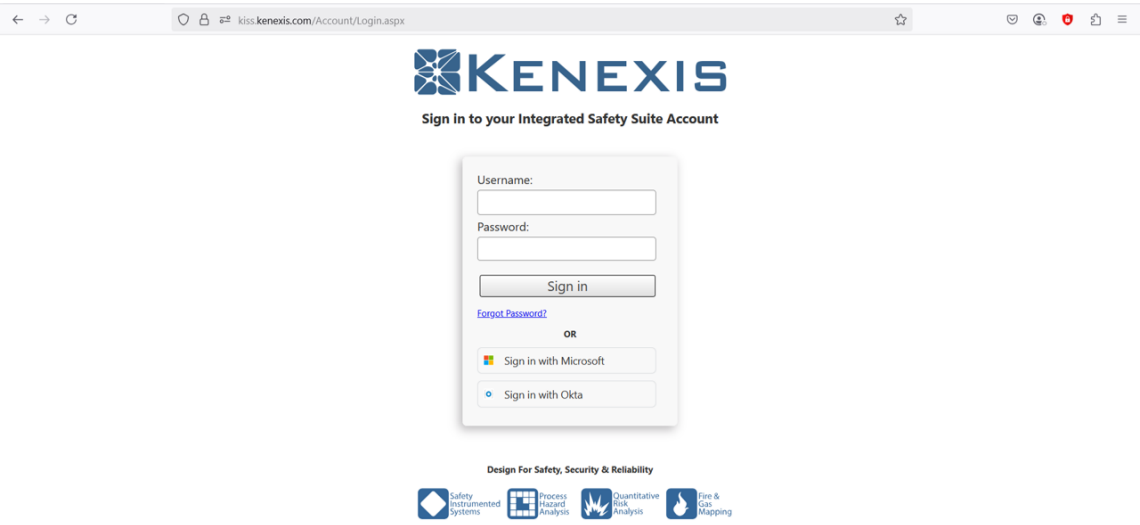
Section 0 – Quick Reference

	**House Event:** An event which has “always true” or “always false” set as the calculation mode on the event details form. House Events apply Boolean logic, where: Always True results in unavailability of one. Always False results in unavailability of zero.

Section 1 – Getting Started

1.1 Instructions for First Time Login

Welcome to Kenexis Integrated Safety Suite (KISS). If you are new to the Kenexis Integrated Safety Suite (KISS) you should have received a welcome package via email with your login credentials. Once you have received this package, it means that your account has been configured and is ready to use. You can access your account by directing your browser to https://kiss.kenexis.com. This will navigate your browser to the KISS login page, shown below.

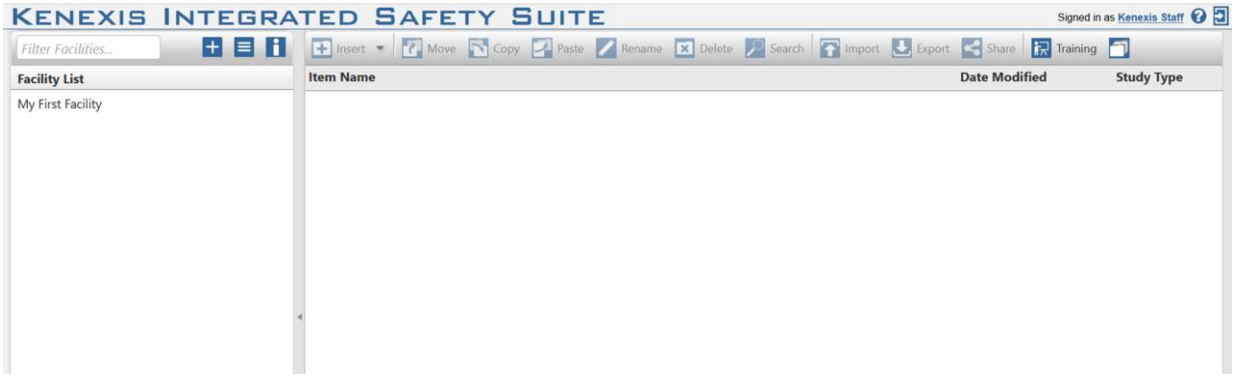


From here you can login using the login credentials provided in your KISS welcome email. If you've lost your temporary password, it can be restoring by using the "Forgot Password?" link. If you've lost your username, please contact support@kenexis.com for assistance.

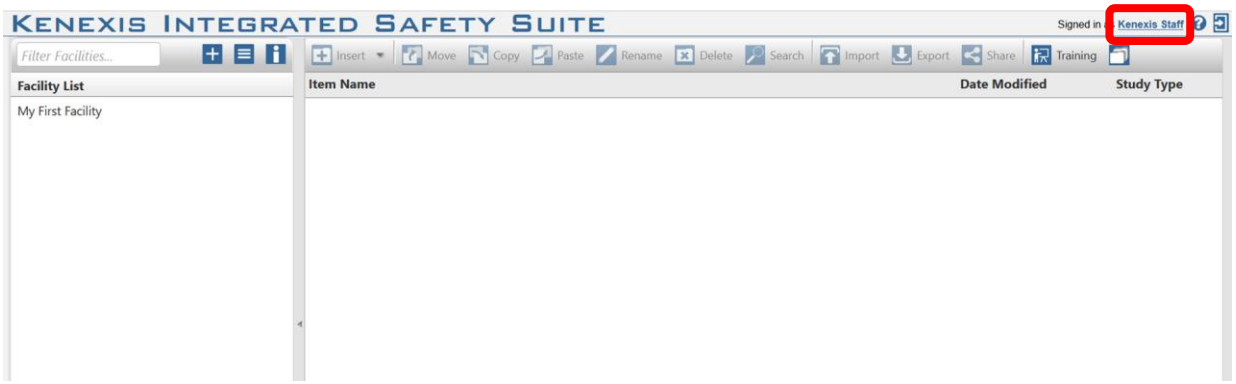
If your organization is set up to use single sign on, you can log in by clicking on the "Sign in with" button that is appropriate for your organization. In the figure, there are options to sign in with Microsoft Office 365 and Okta Verify.

Section 1 – Getting Started

After Successful login, you should arrive at the Study Manger page, shown below.

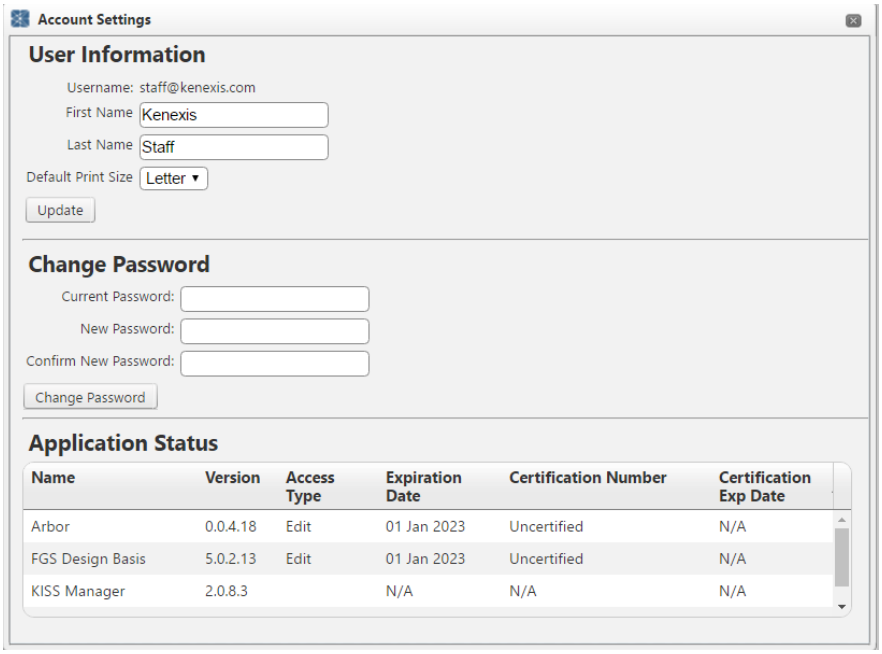


From here, it is highly recommended that you reset your temporary password. You can reset your password by clicking on your name in the top right corner.



This will open your account settings where you will have the option to change your password.

Section 1 – Getting Started



1.2 Login Troubles

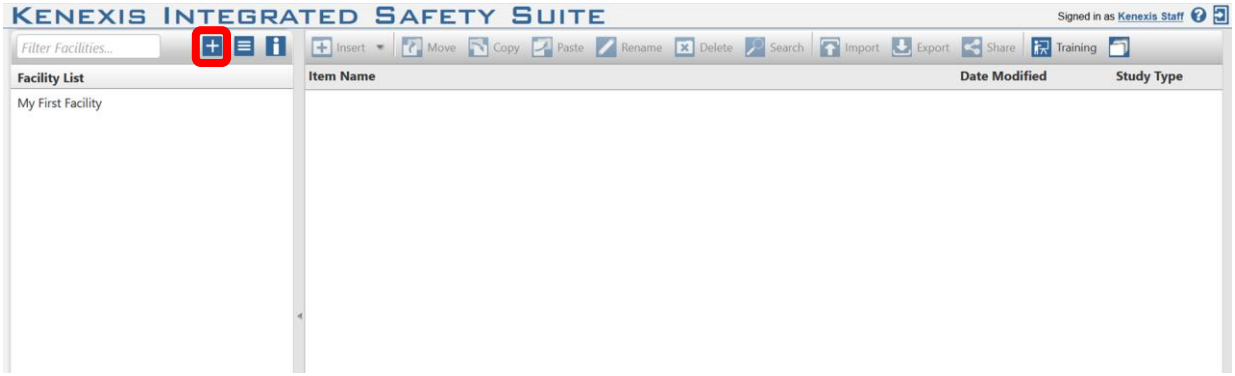
This section describes some of the common causes and solutions for trouble with logging into the Kenexis Integrated Safety Suite (KISS).

Problem #1: I forgot my password
Solution: Visit Kiss.Kenexis.com and click on the "Forgot Password?" link.

Problem #2: I forgot my username
Solution: Contact Support@Kenexis.com to restore your account

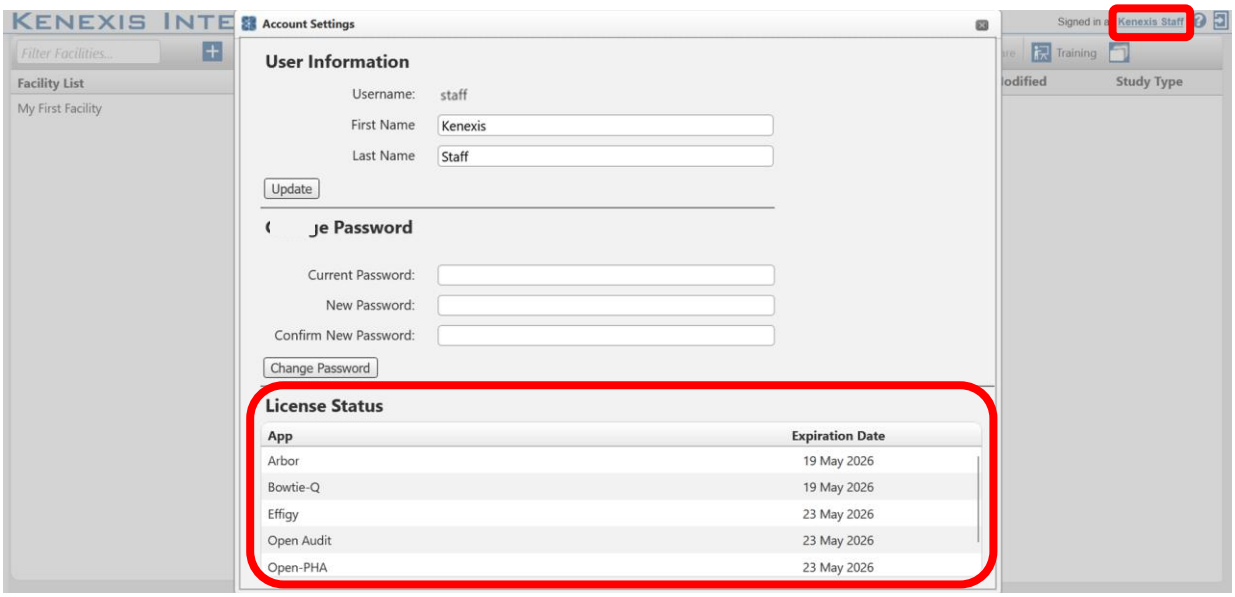
Problem #3: When I login I don't see any studies on the Study Manager Page
Solution: If you are not able to view any facilities or studies on the Study Manager page it is because you do not have access to any study information. Depending on your roles within your company you may have privileges to create a new facility by clicking on the Add Facility button (shown below).

Section 1 – Getting Started



If you are a first time user of Arbor and unfamiliar with the data structure you may want to consider following the "Creating Your First Study" tutorial.

Alternatively, if your account has been assigned read-only permissions you will need to contact your project manager/company administrator to grant you access to the desired studies. You can view your account permissions on your account settings window, which is accessed by clicking on your name in the top right corner.



Section 1 – Getting Started

1.3 Other Resources

In addition to the information provided in this user's manual, help and support for use of the Arbor Fault Tree Analysis Software can also be obtained from the following resources:

- Online or Instructor Based Training Course - A full list of these available courses can be found at www.kenexis.com/training.
    - Conceptual Design and SIL Verification
    - Using Arbor

- Books and other Kenexis publications relating to reliability engineering methodologies, including:
    - Books
        - Kenexis Safety Instrumented Systems Engineering Handbook
    - Papers and Magazine Articles
    - Kenexis Employee Blog Posts
- Live Support from Kenexis Staff. Support requests can be submitted to Kenexis staff via the Kenexis support system, which can be accessed from https://support.kenexis.com.

Section 2 - Interface

2.1 The Navigation Toolbar

The Navigation Toolbar serves as the primary means for navigating the Arbor study editor interface and appears on all pages in the editor. This section details the available buttons on the toolbar:

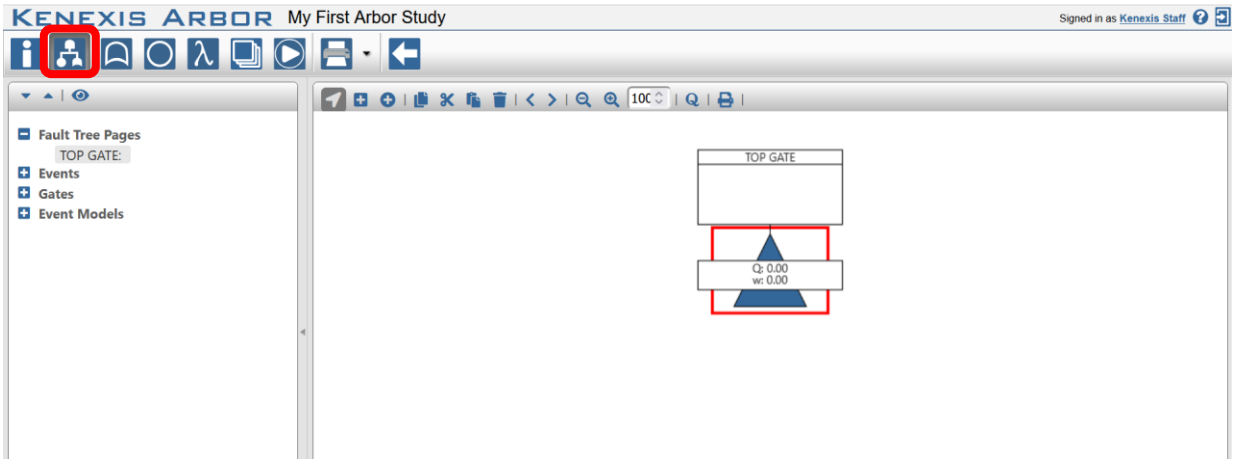
Button	Description
	The Overview button will navigate to the Study Dashboard page for the active study.
	The Fault Tree button will navigate to the fault tree view. From this view you can add, edit or delete objects and build fault tree relationships between gates, events, and event models.
	The Gates page will display a list of all gates for the current fault tree. Gates are used to represent the logical interactions between event failures and system failure.
	The Events page will display a list of all events for the current fault tree. Events are used to represent the components of a system which can fail.
	The Event Models page will display a list of all event models for the current fault tree. Event models are applied to events to characterize their failure rates and characteristics.
	The Minimum Cut Sets page will display the details of the minimum cut sets for any gate in the current fault tree. Each cut set can be expanded to display the details of the events which are included in the set.
	The run calculations button will recalculate all results for the current fault tree.

Section 2 - Interface

Button	Description
	The Print button is used to export information about objects for the current study. Use the dropdown icon to the right to display object types available for printing.
	The Back to Study List button will navigate to the Study Manager page.

2.2 The Fault Tree Interface

The fault tree interface is the primary interface for Arbor. This page is where most data entry takes place and is the interface where you will spend the most time when constructing a fault tree model. The Fault Tree Interface can be reached by clicking on the Fault Tree icon in the Navigation Toolbar (highlighted below).

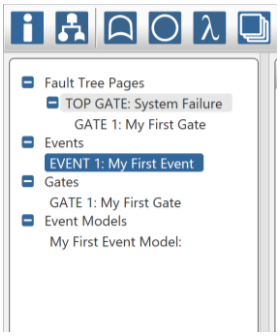


Section 2 - Interface

2.2.1 The Study Data Tree View

To the left of the interface is the Study Data Tree View. In this view you can see all events, gates and event models included in the current study as well as any paging of gates that has been defined.

Left clicking on any event, gate or event model in the tree view will highlight the selected object as shown to the right. A double-click will display the properties for the selected object in a dialog window.



Any gate which has been paged will be displayed in the "Fault Tree Pages" section of the Study Data Tree View in addition to the gates section.

Gates will be nested in the fault tree pages view depending on their parent – child relationships. In the above figure, GATE 1 is a child of TOP GATE and therefore is nested below it. Clicking on any gate in the Fault Tree Pages section will navigate the main workspace window to the selected gate, displaying all children of the paged gate. Paging is an effective method for creating viewable sections in a large tree by hiding children of gates with large amounts of data.

2.2.2 The Main Workspace Window

The Main Workspace Window displays the current fault tree. There is a collection of controls at the top of the workspace for interacting with the tree. These controls are shown below.

The three controls to the left of the panel allow you to define the mode of operation for interactions with the tree. There are three modes:

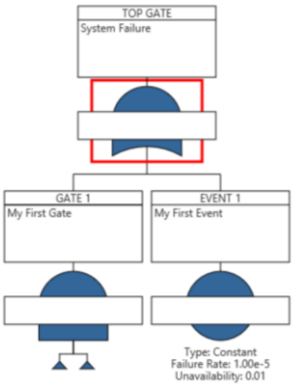
1. Select
2. Gate Insert
3. Event Insert

Section 2 - Interface

2.2.2.1 Working in Select Mode

Select Mode can be entered by clicking on the cursor icon in the header menu of the main workspace, as shown below:

Definition:
NODE – A Gate or Event



When in Select mode, left clicking on a gate or event will select it, making it the selected node. When a node is selected, it will be marked with a red outline, indicating that it is the selected node, as shown to the left.

A node can be de-selected by either selecting a different node, or by pressing the Escape key while the main workspace is in focus.

When a node is selected, several options are available to interact with it:

- **Display Properties:** Double-clicking the selected node will display its priories in a dialog window. Properties can be adjusted to affect the interactions of this node with the rest of the tree.
- **Copy:** The selected node can be copied by clicking the Copy button in the workspace header (the fourth button from the left). Alternatively, the node can be copied with the (ctrl + C) hotkey shortcut. Copied nodes can later be pasted into another section of the tree.
- **Cut:** Similar to copy, a selected node can be cut from the tree by clicking the Cut button in the workspace header (the fifth button from the right). Alternatively, the (ctrl + X) hotkey shortcut can be used. When a node is cut, the node and any of its children will render semi-transparent, indicating that any paste action will cut this node and its children from its current location and relocate it to the pasted location.
- **Paste:** If a node has either been copied or pasted previously, the Paste button (sixth from the right in the workspace header menu) will insert the cut/copied node as a

child of the currently selected node. Nodes can only be pasted as children of gates. Attempting to paste a node as a child of an event is not allowed. As with copying and cutting, pasting can also be performed using a hotkey shortcut (ctrl + V).

- **Delete:** The selected node can be removed from the fault tree by clicking the Delete button in the workspace header menu (seventh button from the right). This action can also be accomplished by pressing the Delete key while the workspace is in focus. If the selected node is the only instance of that node in the fault tree, the node will be permanently removed from the study. Similarly, and child nodes of the selected node will be permanently removed if the child nodes are not referenced at any locations outside of the child structure of the selected node. If the selected node, or any of its children have multiple instances the link between the selected node and its parent will be removed, however the additional instances will remain.
- **Move Left:** The selected node can be moved to the left relative to its siblings by clicking on the Move Left button in the workspace header menu (eighth button from the right). This can also be performed using the hotkey shortcut (ctrl + Left Arrow) when the main workspace is in focus.
- **Move Right:** The selected node can be moved to the right relative to its siblings by clicking on the Move Right button in the workspace header menu (ninth button from the right). This can also be performed using the hotkey shortcut (ctrl + Right Arrow) when the main workspace is in focus.

2.2.2.2 Working in Insert Mode

Insert Mode can be entered either by clicking on the Square Plus icon or the Circle Plus icon in the header menu of the main workspace shown below. Clicking on the Square Plus icon, as shown below, will enter Gate Insert Mode. Clicking on the Circle Plus icon will enter Event Insert Mode.

Once a study has been placed in Insert Mode, nodes can no longer be selected, as described in *Section 2.2.2.1*. When working in Insert Mode, a left mouse click on a gate in the fault tree will add either a new gate or a new event as a child of the node. The type of node added depends on the selected mode (Gate Insert Mode will insert gates, Event Insert Mode will insert events).

Insert Mode is often useful when beginning work on a new fault tree model. By working in Insert Mode, the logical representation of the tree can be constructed quickly with minimal

keystrokes. Once the tree is constructed, returning to Select Mode will allow you to display the properties for each gate and event, and allow you to populate the appropriate data.

New gates and events can also be added in Select Mode using hotkeys. With the main workspace in focus and a gate selected, pressing the Q key will insert a new gate and pressing the W key will insert a new event.

2.2.2.3 Adjusting the Zoom on the Main Workspace

The zoom of the main workspace can be adjusted using the zoom controls in the main workspace header menu shown below.

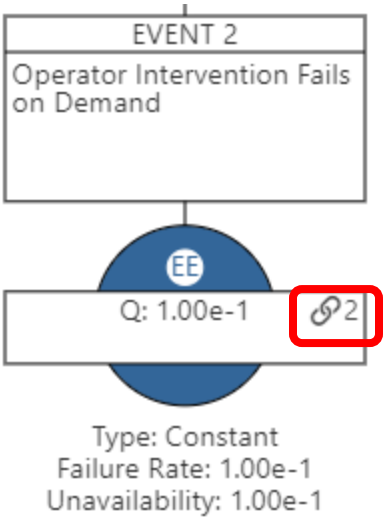
By default, the zoom of the main workspace is always reset on 100% when the fault tree is loaded. Clicking the Minus Magnifying Glass icon will zoom out 5%. Clicking the Plus Magnifying Glass will zoom in 5%. The current zoom setting is displayed in the text box to the right of the Magnifying Glass icons. In the above image, the toolbar is displaying 100% zoom, which is the default setting. The zoom can be adjusted manually by simply selecting the text in box and entering the desired zoom setting.

Finally, the zoom of the main workspace can be adjusted with hotkey combinations while the main workspace is in focus. The Minus/Underscore key will cause the window to zoom out, and the Plus/Equals key will cause the window to zoom in.

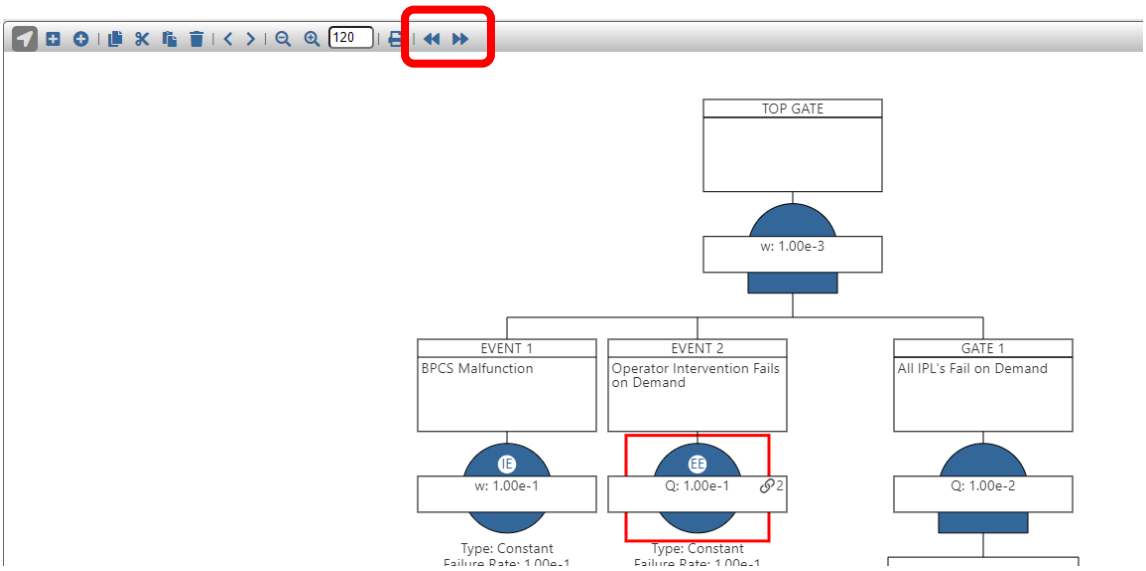
2.2.2.4 Working with Nodes that are Used in Multiple Locations

If a node is used in multiple locations in a fault tree, it will be indicated by a use count interface in the top right corner of the results section of the node.

Section 2 - Interface

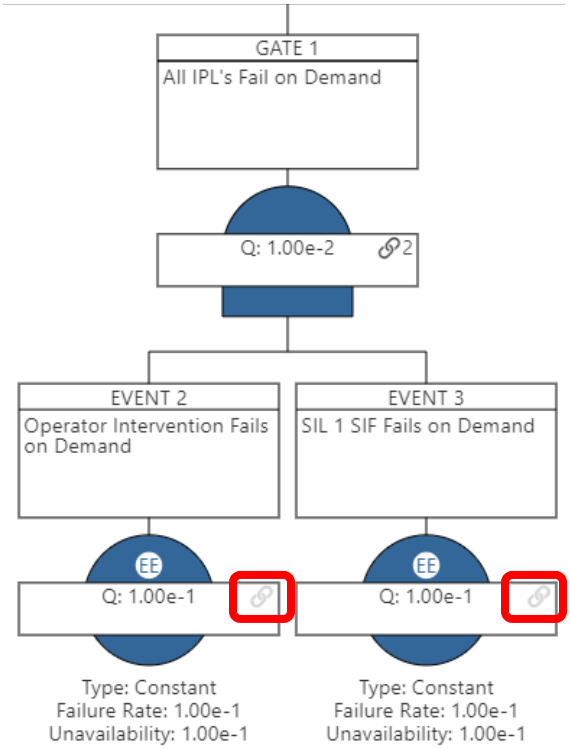


If a node is selected that is used in multiple locations, additional buttons will be displayed on the main workspace toolbar. These buttons allow you to quickly navigate between each instance of the node by selecting the previous or next occurrence.



Every node below a gate that is used in multiple locations will have a link icon without a use count, indicating that a parent node above it within the tree is used in multiple locations. The parent node that is used in multiple locations will also have a link icon with a use count. The icon is provided to inform you that any updates to this node will affect multiple branches of the tree, because a parent gate is used in another branch.

Section 2 - Interface



2.2.2.5 Toggle Unavailability and Risk Reduction Factor (RRF)

Often when using fault trees for analysis, for the purposes of calculating the probability of failure on demand for SIL verification, it is preferable to report the unavailability as a risk reduction factor (RRF), mathematically calculated as 1 divided by unavailability.

To switch between using unavailability and risk reduction factors for analysis, the unavailability and risk reduction factor views can be toggled in the main workspace by using the Toggle Unavailability/RRF button in the main workspace header menu as shown below.

By default, the main workspace is set to display the unavailability of events and gates.

Section 2 - Interface

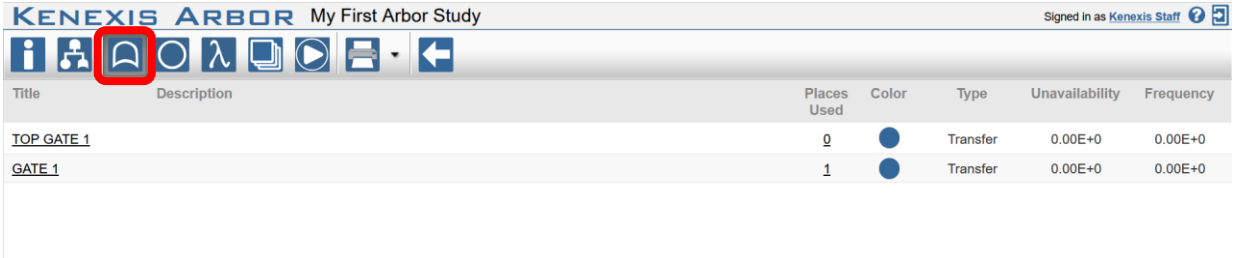
2.2.2.6 Saving the Fault Tree as an Image

To save the current fault tree as an image in *.png format, you can use the Save Fault Tree as Image button in the main workspace header menu.

The resulting image will be downloaded to your desktop.

2.3 The Gates Grid View

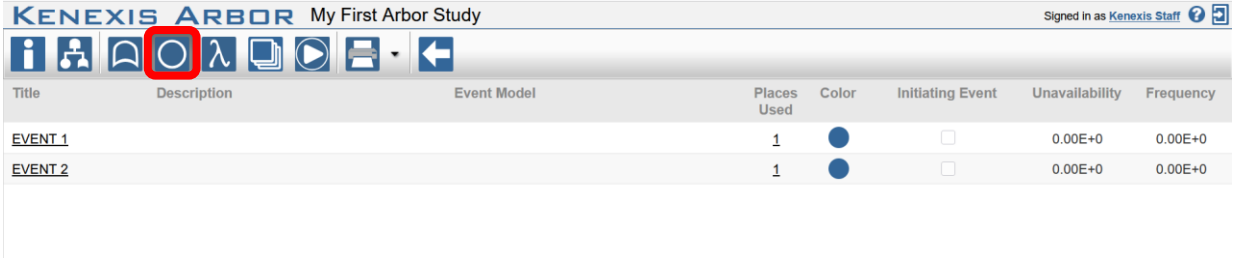
The Gates Grid View displays all gates in the current study. The Gates Grid View can be reached by clicking on the Gates icon in the Navigation Toolbar.



For large fault trees, it can be useful to display all gates in the tabular interface of the gates grid, which allows for quick comparison of unavailability results and frequency results between gates. From the Gates Grid View, the properties of a gate can be displayed by either double-clicking on a row of the grid, or by clicking on the gate title.

2.4 The Events Grid View

The Events Grid View displays all events in the current study. The Events Grid View can be reached by clicking on the Events icon in the Navigation Toolbar.



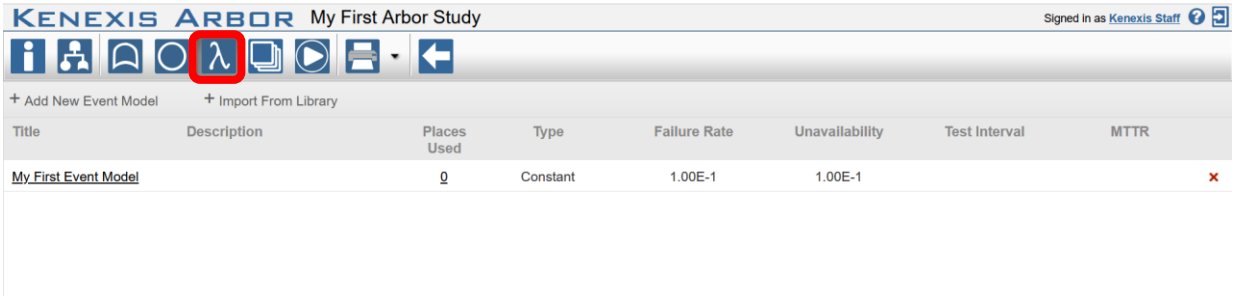
For large fault trees, it can be useful to display all events in the tabular interface of the events grid, which allows for quick comparison of unavailability or frequency results between events.

Section 2 - Interface

The events grid view can also be useful for quickly identifying where an event model has been applied throughout the study. From the Events Grid View, the properties of an event can be displayed by either double-clicking on a row of the grid, or by clicking on the event title.

2.5 The Event Models Grid View

The Event Models Grid View displays all Event Models in the current study. The Event Models Grid View can be reached by clicking on the Event Models icon in the Navigation Toolbar.



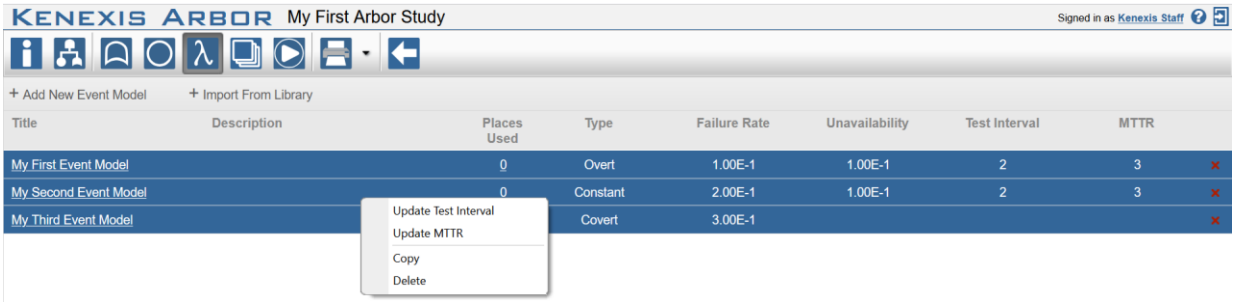
The Event Model Grid View can be used to quickly delete and/or update event models. An Event Model can be deleted by clicking on the Delete icon (red x) for a row of the grid. Care should be taken when deleting Event Models, as one or more events may rely on the Event Model as a source of failure rate data. As a general practice, event models should only be deleted when they are not linked to any events, or when the impact of deleting the model is well understood.

2.5.1 The Event Models Grid View Context Menu

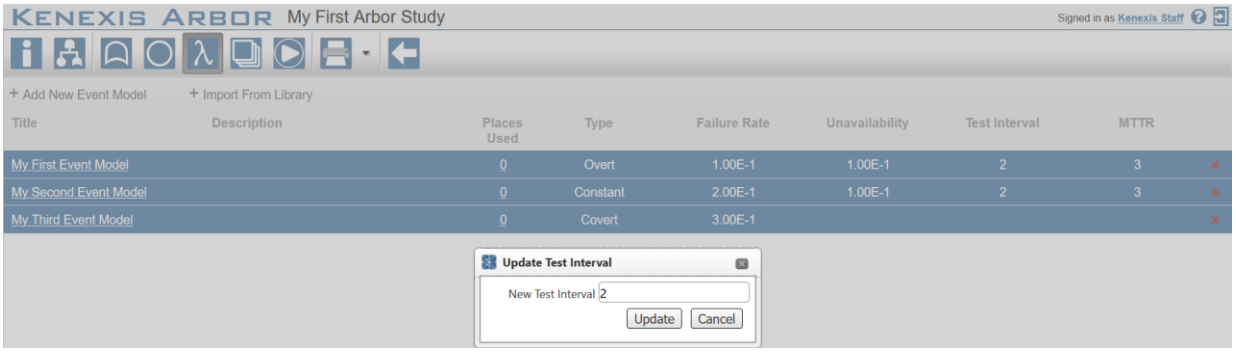
It is often useful to be able to adjust properties of many event models quickly. A common application is performing sensitivity analysis on the effects of test intervals or mean-time-to-repair (MTTR) for several devices. A context menu is available in the Event Models Grid View to speed up the process of making such changes.

Within the Event Models Grid View, a row can be selected by left clicking on the row. Many rows can be selected by holding the Shift or Ctrl keys while left clicking. With one or more rows selected, a right mouse click anywhere on the grid will display a context menu as shown below.

Section 2 - Interface

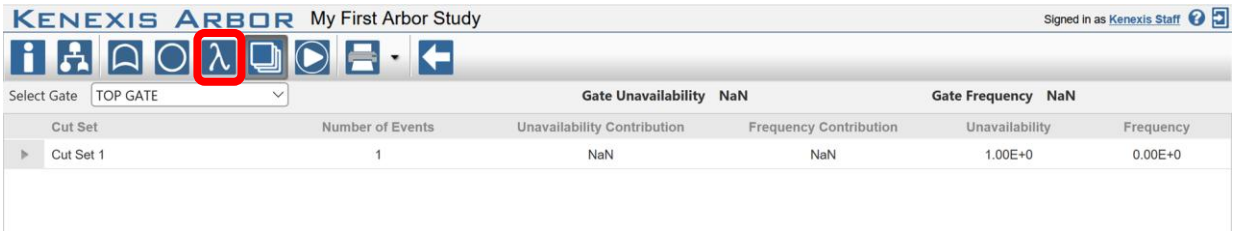


From the context menu, the Test Intervals or MTTRs for all selected events models can be changed with a single action. Selecting either "Update Test Interval" or "Update MTTR" will open a dialog window with a prompt for the new value to be applied to all selected event models as shown below:



2.6 The Minimum Cut Set Grid View

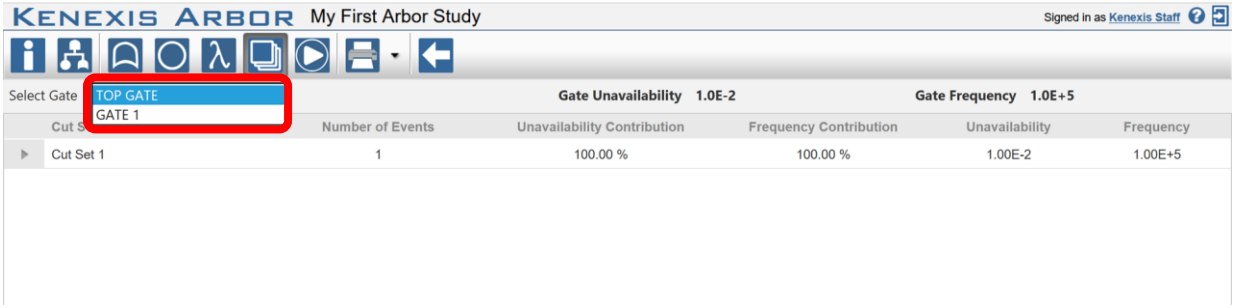
The Minimum Cut Set Grid View is used to display detailed results of the minimum cut set analysis of a fault tree. The Minimum Cut Set Grid View can be reached by clicking on the Minimum Cut Set icon in the Navigation Toolbar.



IMPORTANT NOTE:
Understanding minimum cut sets is critical to understanding the calculations performed in fault tree analysis. The calculation details of minimum cut set analysis are not described here. For calculation details see *Section 4* of this manual.

Section 2 - Interface

The Minimum Cut Set Grid View will display minimum cut sets for a single gate of a fault tree. The gate that has its cut sets displayed can be changed by selecting a gate from the dropdown menu above the grid.



The total unavailability and frequency for the selected gate is displayed above the grid to the right of the selected gate. When no results have been calculated, these values will display "Not A Number," or "NaN."

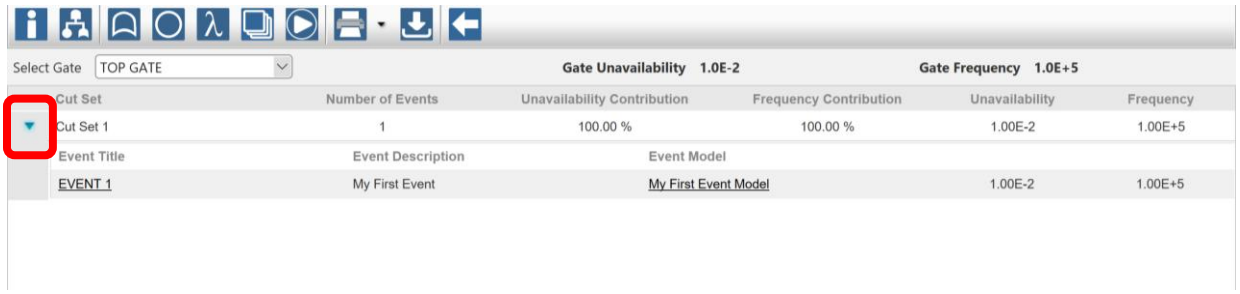
By default, cut sets will be ordered by their unavailability contributions to the selected gate. The first cut set in the grid will have the highest unavailability contribution, meaning it contributes the largest portion of the total unavailability for the selected gate.

Each cut set is given an index (Cut Set 1, Cut Set 2 … Cut Set N). This indexing is provided for display purposes only. For any given cut set, the index can and will change if the fault tree is modified and calculations are rerun. Indexes are generated at run time and are based on the unavailability contributions.

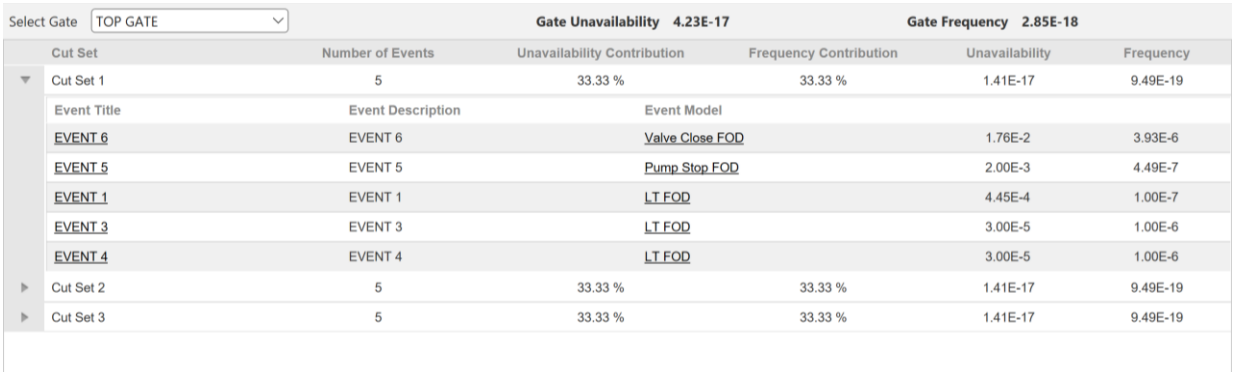
When reporting cut sets, it is advised to report cut sets based on the collections of events that contribute to them rather than Grid View indexes. These event combinations will only change if changes are made to gate types (and, or, vote, etc.). These generally occur less frequently than changes to event model properties, which do not affect the event combinations in each cut set.

To view additional details on a cut set, click on the expander icon at the left side of the grid. This action will display the event collection which contributes to the expanded cut set as shown below.

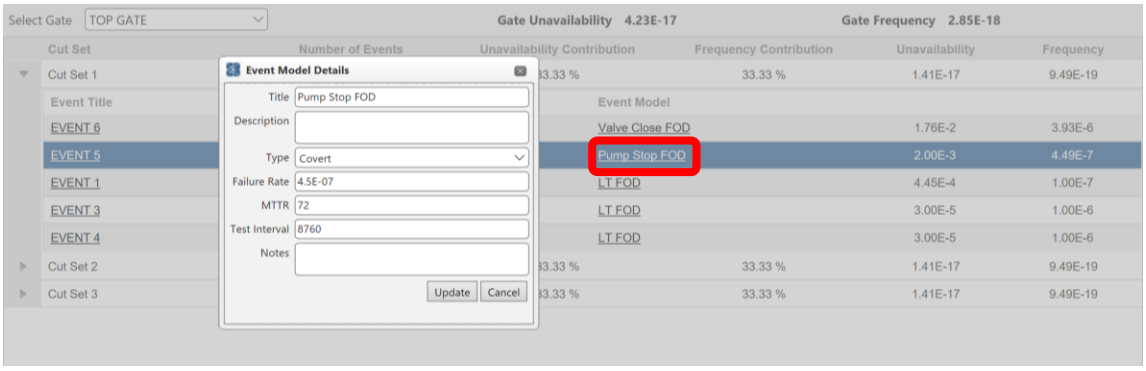
Section 2 - Interface



In the expanded view of a cut set, details of events and their corresponding event models are visible. In the above figure Cut Set 1 only contains a single event (EVENT 1), however for large trees these event collections will grow rapidly, particularly for highly fault tolerant systems. Below is an example of a Cut Set containing 5 events:



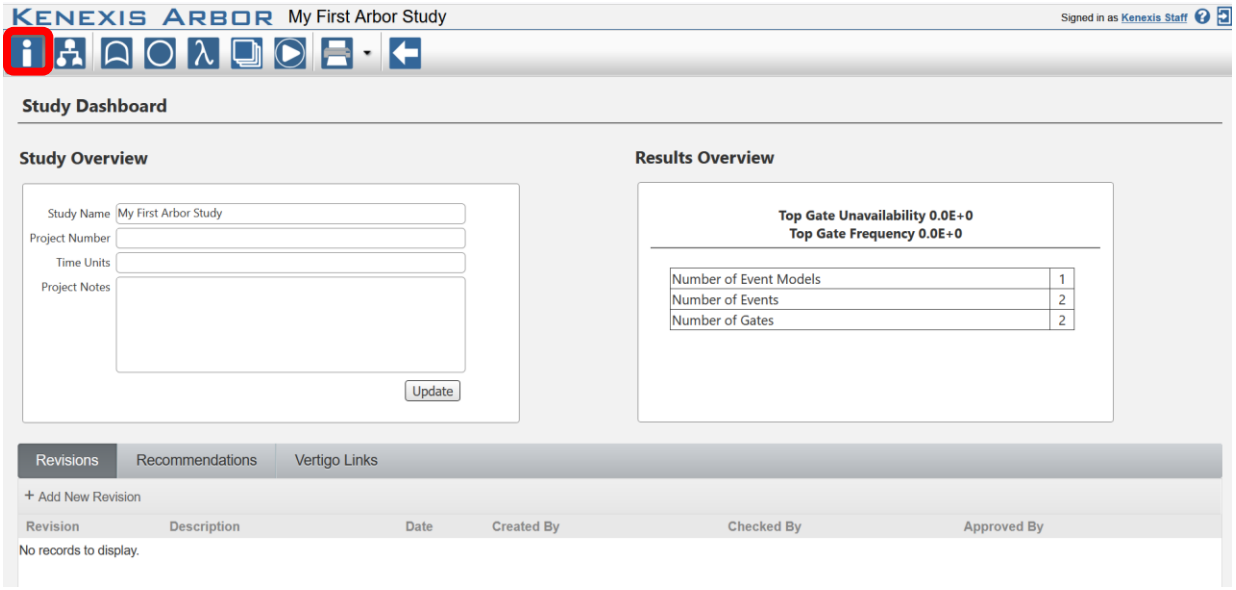
When a cut set is expanded, the properties of any Event or Event Model can be displayed by left clicking on the Event title or the Event Model title. This action will display a window where the properties of the selected object can be viewed and/or modified.



Section 2 - Interface

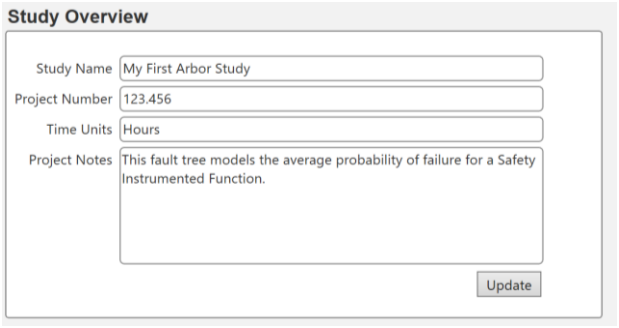
2.7 The Study Dashboard

The Study Dashboard provides a high-level overview of a fault tree study in Arbor. The Study Dashboard has three sections, the Study Overview, the Results Overview, and the Revisions & Recommendations Grid Views. The Study Dashboard can be reach by clicking on the Study Dashboard icon in the Navigation Toolbar.



2.7.1 Study Overview

The Study Overview is used to input administrative information about an Arbor study. None of the fields in the Study Overview section of the Study Dashboard affect the calculated results of a fault tree; these fields are provided for information tracking only. The following fields can be input in the study overview:



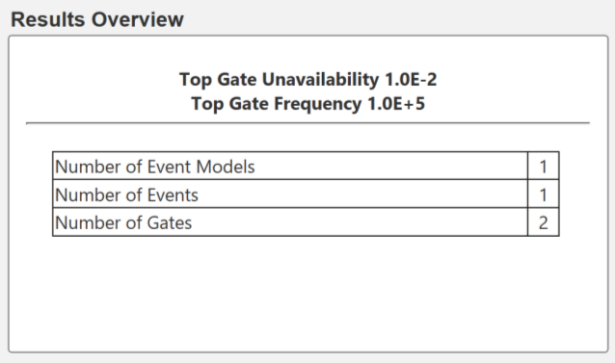
- **Study Name**: Study Name is a required field and is set when a study is created. The Study Name can be updated at any time from the Study Overview on the Study Dashboard. The Study Name will be displayed in the Study List page of the KISS Manager application.

- **Project Number**: This field is provided to track a project number for project management purposes.
- **Time Units**: Arbor calculations are unitless, meaning that it is the user's responsibility to ensure that all failure rates, frequencies, test intervals and MTTRs are entered in a consistent unit of time. The Time Units field is provided in the Study Overview to allow you to explicitly state the units of time used in a study. Populating this field can be particularly helpful when working collaboratively, as it will provide other users with a clear definition of the units of time used in a study.
- **Project Notes:** Any notes specific for a study can be entered here.

Hit the Update button to save any changes made in the Study Overview.

2.7.2 Results Overview

The Results Overview section of the Study Dashboard provides a summary of the results of a study at a glance. The Results Overview includes unavailability and frequency information about the top gate of the fault tree and a count of the gates, events, and event models included in the analysis.



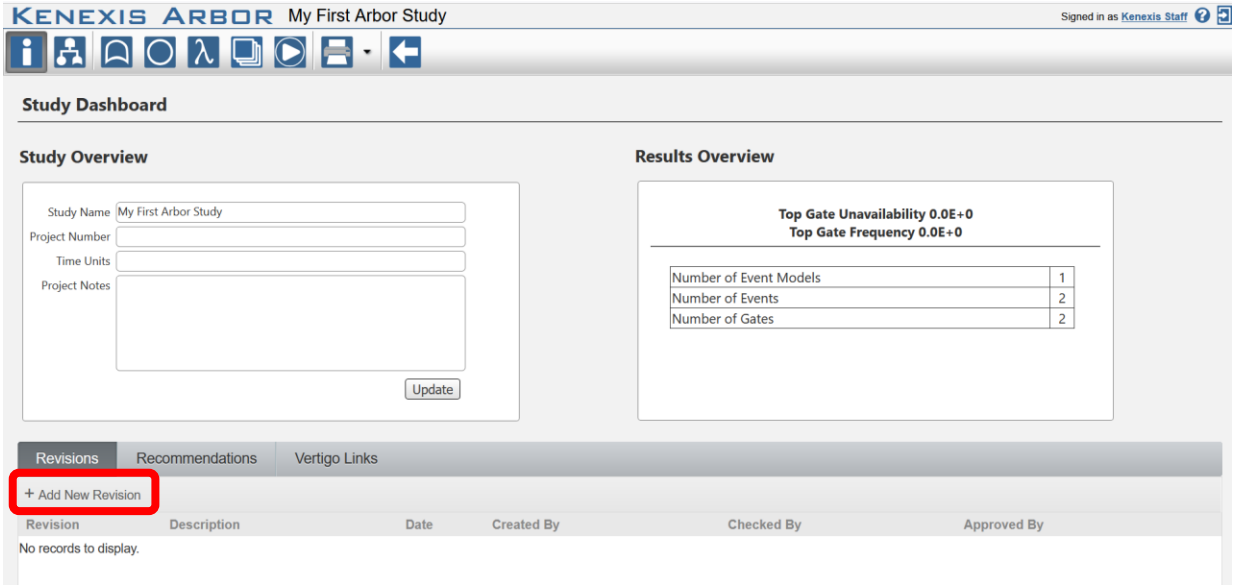
2.7.3 The Revisions Grid View

The Revisions Grid View is used to add, edit, and delete revisions. Each Arbor study can have one or more revisions linked to the study. Revisions are useful for tracking changes to the fault tree analysis model and documenting the personnel response for making those change as well as the parties responsible for checking and approving the work.

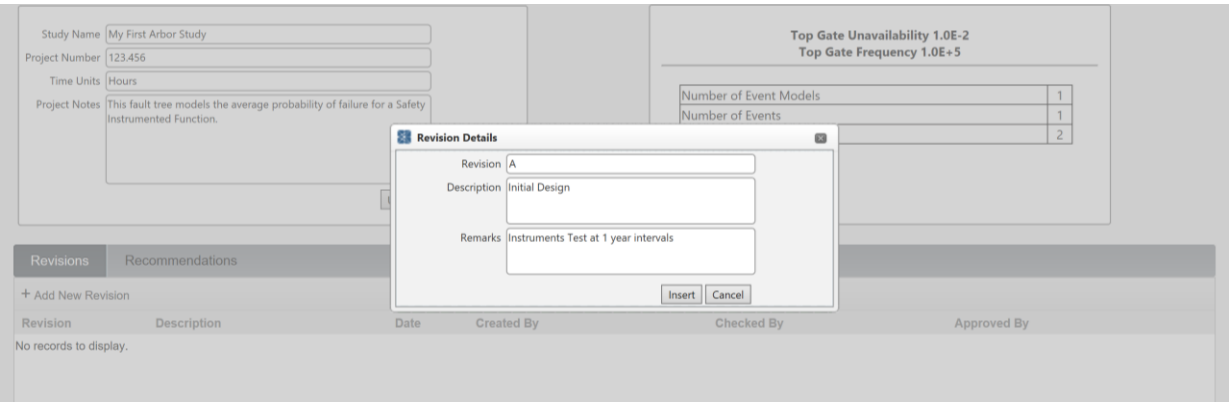
2.7.3.1 Adding a Revision

A revision can be added to an Arbor study by clicking on the Add New Revision button in the header of the revisions grid view as shown below.

Section 2 - Interface



Adding a revision will open the Revision Details window where a revision number, description, and remarks can be added.

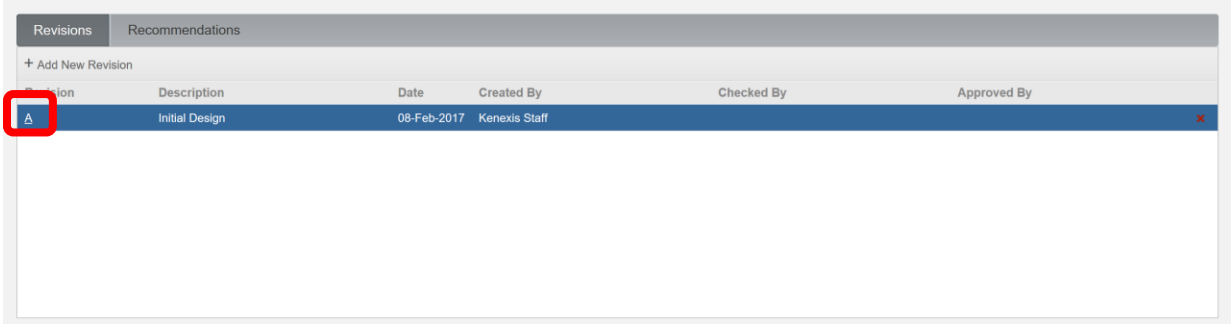


Clicking Insert in the Revision Details window will add the revision to the revisions grid. When a revision is added the revision date will automatically be populated as will the "Created By" field in the revisions grid view. The "Created By" field will be populated with the name of the user who inserted the revision.

2.7.3.2 Updating a Revision – Checking and Approving

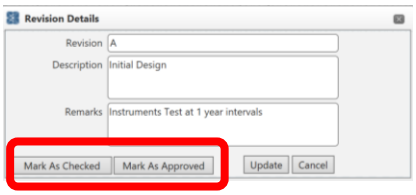
Existing revisions can be updated by either clicking on the revision number or double-clicking on a row in the Revision Grid View.

Section 2 - Interface



Updating a revision will open the Revision Details window in Update Mode. When the Revision Details is opened in Update Mode, two additional buttons will appear. These buttons are:

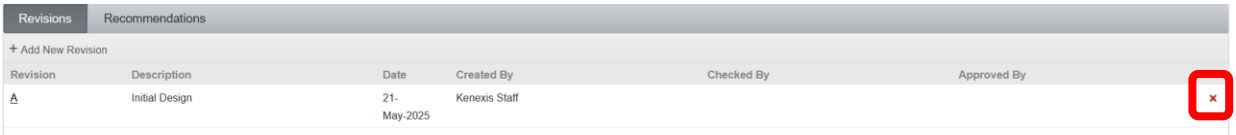
- Mark As Checked
- Mark As Approved



These two additional buttons are used to check and to approve revisions. As with the creation of revisions the names of the checker and approver will be automatically populated based on the name of the user who clicks the checked / approved button. After a revision has been checked or approved, the name of the user(s) who performed the corresponding action will appear in the Revisions Grid View.

2.7.3.3 Deleting a Revision

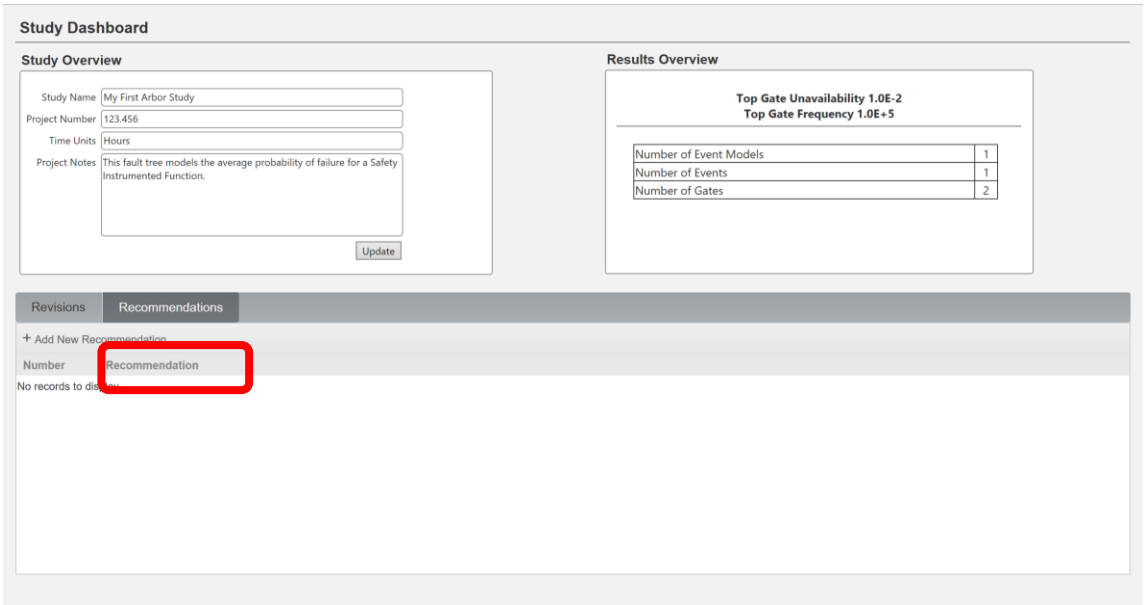
Revisions can be deleted by clicking on the Delete icon (red x) at the far-right side of the Revisions Grid View.



2.7.4 The Recommendations Grid View

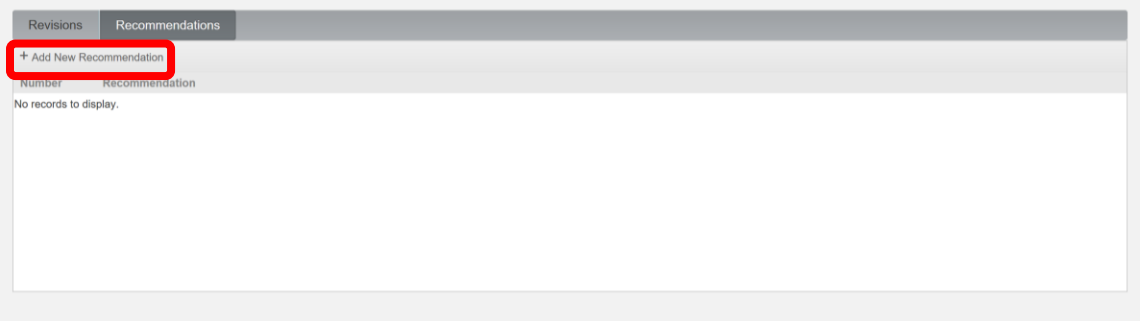
The Recommendations Grid View is used to add, edit and delete recommendations. Each Arbor study can have one or more recommendations linked to the study. Revisions are useful for documenting proposed changes to a system design based on the result of fault tree analysis modeling. The Recommendations Grid View can be shown by clicking on the Recommendations tab on the Study Dashboard.

Section 2 - Interface



2.7.4.1 Adding a Recommendation

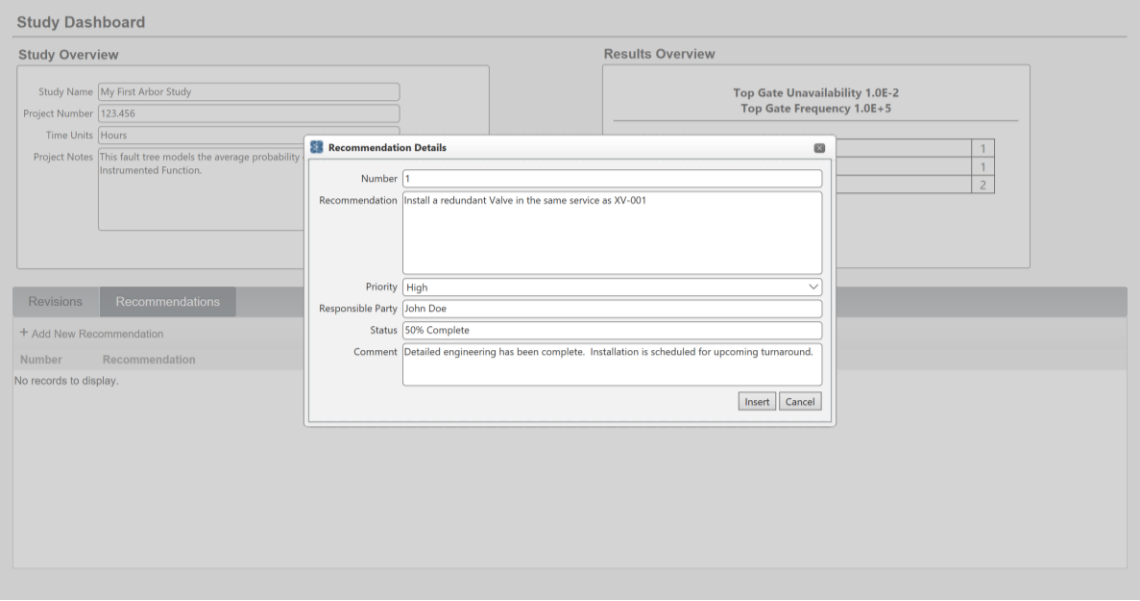
A recommendation can be added to an Arbor study by clicking on the Add New Recommendation button in the header of the Recommendations Grid View as shown below:



Adding a recommendation will open the Recommendation Details window where the following information about a recommendation can be entered.

- **Recommendation Number:** A unique identifier used for recommendation tracking. By default, the recommendation number will automatically enumerate to the first integer value greater than zero which is not currently being used in the list of recommendations for a study.
- **Recommendation:** Details of the recommended actions
- **Priority**: Priority of the recommendation relative to other recommendations. Typically, high priority recommendations will require a more prompt response than low priority recommendations.

- **Responsible Party**: The person, organization or department responsible for addressing the recommendation actions.
- **Status**: The status of implementation of the recommendation
- **Comments**: Any additional comments regarding the recommendation



Clicking Insert in the Recommendation Details window will add the recommendation to the Recommendations Grid View.

2.7.4.2 Updating a Recommendation

Existing Recommendations can be updated by either clicking on the recommendation number, or by double-clicking on a row in the Recommendations Grid View.

Updating a recommendation will open the Recommendation Details window in Update Mode.

2.7.4.3 Deleting a Recommendation

Recommendations can be deleted by clicking on the Delete icon (red x) at the far-right side of the recommendations grid view.

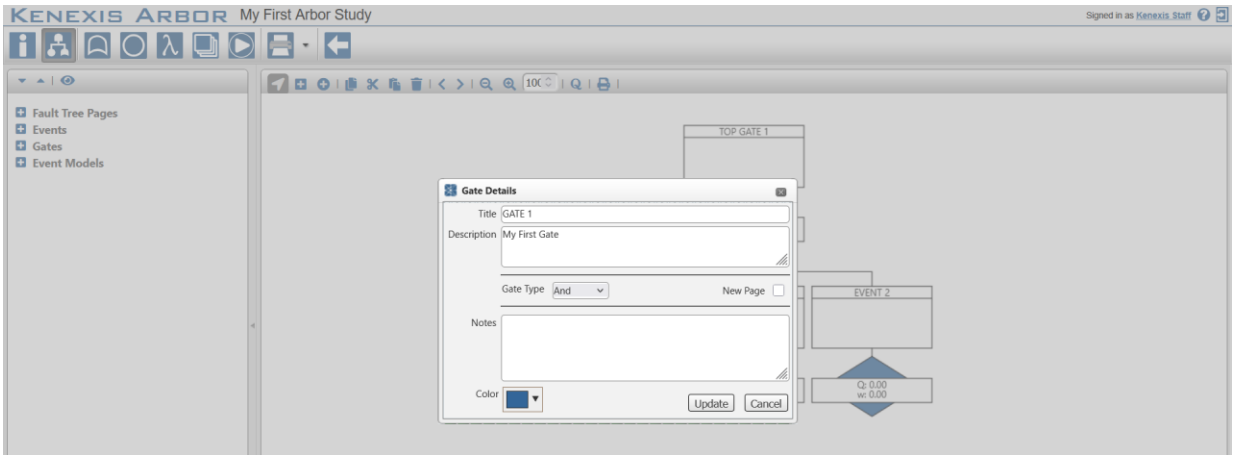
Section 2 - Interface

2.8 The Gate Details Form

The Gate Details form is a window for entering information about the properties of a gate. There are several ways to reach the Gate Details form, including:

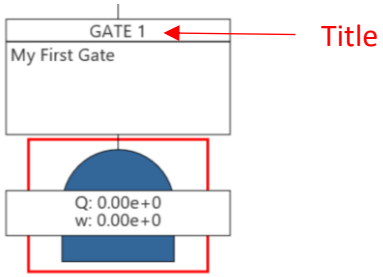
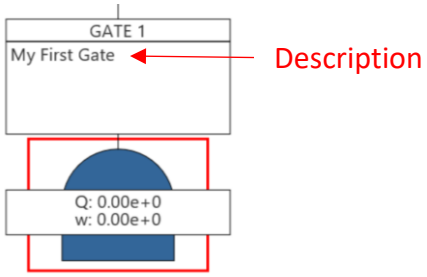
- From the Fault Tree Interface:
  - double-click on a gate title in the study tree view on the left side of the page
  - while in select mode, double-click on a gate in the main workspace (fault tree view)
- From the Gate Grid View:
  - double-click on a row of the grid
  - click on the title of a gate

The Gate Details form is shown below:



The following properties for a gate can be set from the Gate Details form:

Section 2 - Interface

Title	The title of the gate. The gate title is displayed in the top section of the gate details on the fault tree model. When a new gate is created the gate title is set by default.  The default title for a gate is GATE #, where # is an integer value which is automatically enumerated. When a gate is created, # will be set to the lowest integer value greater than zero which has not already been used in the study. It is highly recommended that gate titles be unique, however this is not a requirement.
Description	A description of the gate. The gate description is displayed in the lower section of the gate details on the fault tree model. The gate description is generally used to describe the combination of events which contribute the unavailability and frequency for the gate. 
Gate Type	The gate type defines the logical relationship between a gate and its children. The following gate types are supported in Arbor: • **Or Gate:** Gate is in a faulted state if any child node is in a faulted state. • **And Gate:** Gate is in a faulted state if all children nodes are in a faulted state. • **Vote Gate:** Gate is in a faulted state if “n” child nodes are in a faulted state, where “n” is the vote count defined in the gate details form. The vote count input will be displayed dynamically when the gate type is set to vote on the Gate Details Form.

	NOTE: This can be counter-intuitive for voting gates with more than 3 child nodes. For example, in control systems terminology, a 2oo4 vote to trip requires 3 devices to be in a faulted state for the system to be in a faulted state. This configuration would be a vote count of 3oo4 in Arbor. • **Transfer Gate:** If the gate has one child, the unavailability and frequency for the gate will be set to the unavailability and frequency of the child node. If the node has more than one child a transfer gate is in an undefined state and the gate unavailability and frequency will be set to zero.
New Page	Defines pagination for the gate. If new page is checked the gate will be paginated. When painted, all child nodes of the gate will be displayed on a new fault tree page in the Fault Tree Interface. Pagination is appropriate for large fault tree. Paginating a gate can help break a large tree into separate sections that relate logically, so that collections of related nodes can be more easily viewed together.
Notes	Any notes or comments relating to the gate.
Color	The color of the gate, as it appears on the fault tree diagram. The color defaults to Kenexis Blue but can be changed to any number of preprogrammed colors.

Once you have modified the desired details, hit the Update button to apply your changes, or hit the Cancel button to leave the Gate Details form.

2.9 The Event Details Form

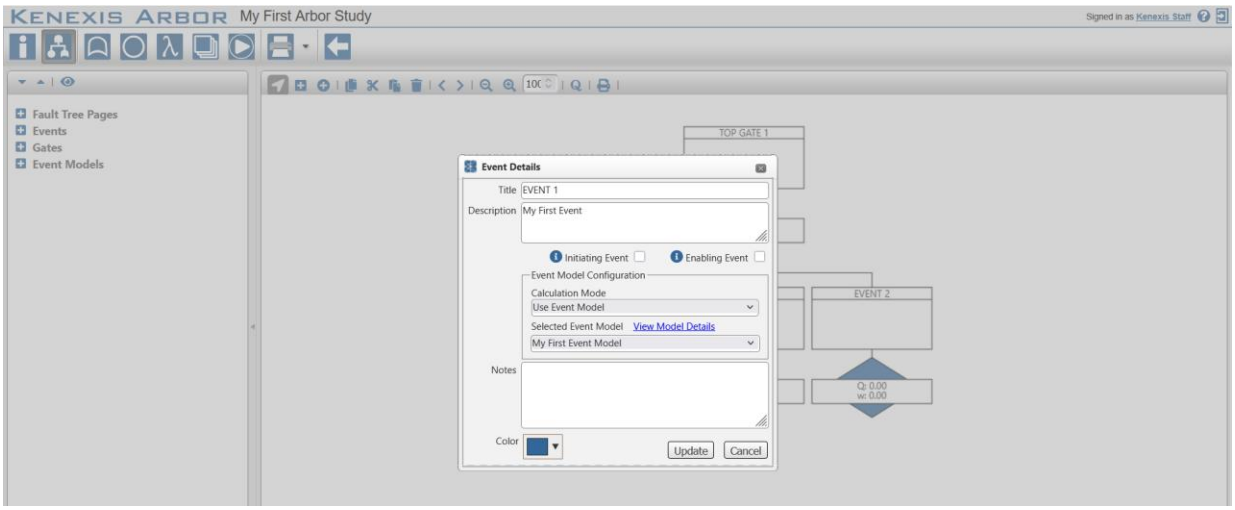
The Event Details form is a window for entering information about the properties of an event. There are several ways to reach the Event Details form, including:

- From the Fault Tree Interface:
  - double-click on an event title in the study tree view on the left side of the page
  - while in select mode, double-click on an event in the main workspace (fault tree view)
- From the Event Grid View:

- double-click on a row of the grid
- click on the title of an event

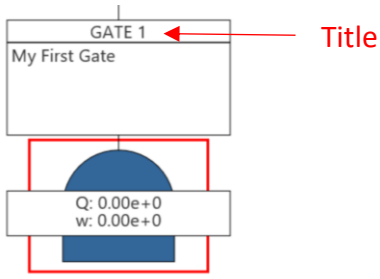
- From the Cut Set Grid View:
  - double-click on an event row of the grid while a cut set is expanded
  - click on the title of an event while a cut set is expanded

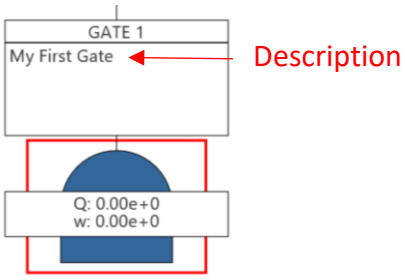
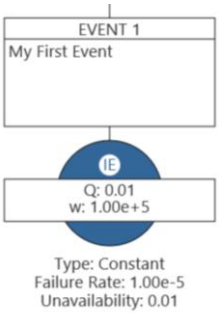
The Event Details form is shown below:

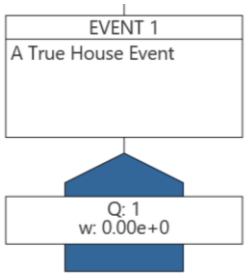


The following properties for an event can be set from the Event Details form:

Title	The title of the event. The event title is displayed in the top section of the event details on the fault tree model. When a new event is created the event title is set by default. The default title for an event is EVENT #, where # is an integer value that is automatically enumerated. When an event is created, # will be set to the lowest integer value greater than zero which has not already been used in the study. It is highly



	recommended that event titles be unique, however this is not a requirement.
Description	A description of the event. The event description is displayed in the lower section of the event details on the fault tree model. The event description is generally used to describe the event model, which contributes to the unavailability and frequency for the event. 
Initiating Event	Checking the Initiating Event checkbox will force Arbor to handle an event as an initiating event. For initiating events, the event unavailability is ignored and only frequency is used for calculation. Any parent, grandparent, etc. of an initiating event will only report frequency. Initiating events should only be used when the result of concern for the Top Gate is frequency as unavailability will never be calculated for the Top Gate if an initiating event is defined anywhere in the tree.  When an event has been defined as an initiating event, it will be decorated with a small badge reading "IE," indicating it is an initiating event. For more information on the use of initiating events, see *Section 4.2.4* of this manual.
Enabling Event	Checking the Enabling Event checkbox will force Arbor to handle an event as an enabling event. For enabling events, the event only contributes to cut set unavailability and is excluded

	in the frequency calculations. Any parent, grandparent, etc. of an enabling event will only report unavailability. Enabling events should be used when the failure of the event alone does not result in a failure of the system being modeled.  When an event has been defined as an enabling event, it will be decorated with a small badge reading "EE," indicating it is an initiating event. For more information on the use of enabling events, see *Section 4.2.5* of this manual.
Calculation Mode	By default, event unavailability and frequency are calculated using the event model applied to an event. The calculation mode dropdown menu allows you to override this default behavior by applying Boolean (true/false) logic. Setting the calculation mode for an event to "Always True" or "Always False" will apply Boolean logic. Events will render as house events when Boolean logic is applied. When a house event is set to true, the unavailability will always evaluate to 1. When a house event is set to false, the unavailability will always evaluate to 0.  Frequency for house events will always evaluate to 0 regardless of whether the logic is set to true or false.
Selected Event Model	The selected event model dropdown menu allows you to apply an existing event model to an event or add a new event model to apply to the event. A new event model can either be imported from a failure rate library by selected "Add New from

	Library…" or can be created manually by selecting "Add New…". Selecting to add a new event model will open a dialog to guide you through the event model creation process. For more information on the import of event models or creation of event models, see *Section 2.10*.
Notes	Any notes or comments relating to the event.
Color	The color of the event, as it appears on the fault tree diagram. The color defaults to Kenexis Blue but can be changed to any number of preprogrammed colors.

Once you have modified the desired details, hit the Update button to apply your changes, or hit the Cancel button to leave the Event Details form.

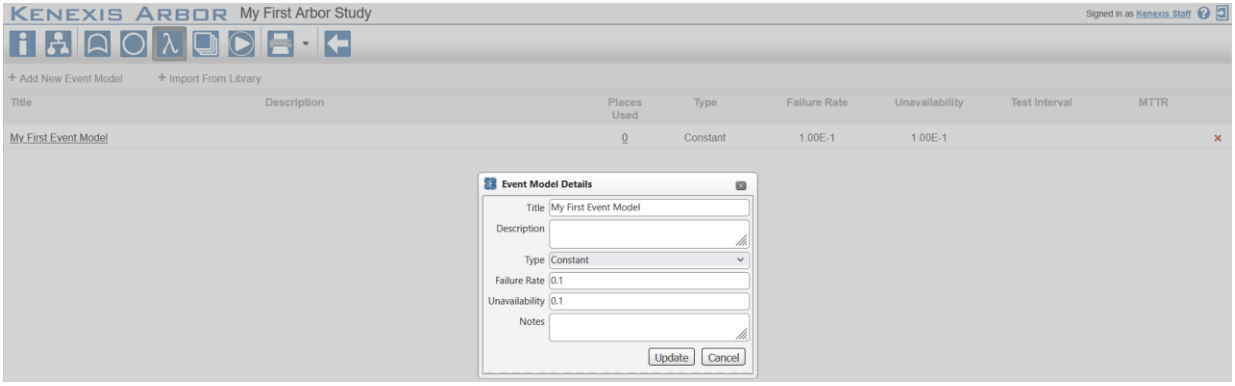
2.10 The Event Model Details Form

The Event Model Details form is a window for entering information about the properties of an event model. There are several ways to reach the Event Model Details form, including:

- From the Fault Tree Interface:
  - double-click on an event model title in the study tree view on the left side of the page.
- From the Event Models Grid View:
  - double-click on a row of the grid
  - click on the title of an event model
- From the Cut Set Grid View:
  - click on the title of an event model while a cut set is expanded
- From the Event Details Form:
  - select "Add New…" from the selected event model dropdown menu.

The Event Model Details form is shown below:

Section 2 - Interface



The following properties for an event model can be set from the Event Model Details form:

Title	The title of the event model. It is recommended that this title be unique, however it is not required.
Description	A Description of the event model. The description is generally used to describe the component failure(s) that the event model represents.
Type	The event model type dropdown is used to select from three event model types available in Arbor • Constant • Overt • Covert Changing the selected type will update the Event Model Details form to display the numerical inputs required to calculate frequency and unavailability for the event model. Calculation details for each event model type are provided in *Section 4.1* of this manual.
Failure Rate	The rate of failure of the device being represented by the event model. Failure Rate is entered in units of failures per unit time (e.g. failures per hour).
Unavailability	The unavailability of the event model. Unavailability is only used for the Constant event model type.
Test Interval	The time interval between functional testing of the device being represented by the event model. Test Interval is entered in units of

	time (e.g. hours). Test intervals are required for the Covert event model type.
MTTR	MTTR stands for the mean time to repair. MTTR represents the average time period required to repair a failed component and return it to an available state. MTTR is entered in units of time (e.g. hours). The MTTR is required for both the Overt and Covert event model types.
Mission Time	The Mission Time is the total time of operation for a component. Mission Time is entered in units of time (e.g. hours). Mission Time is required for the Overt event model type.
Notes	Any notes or comments relating to the event model.

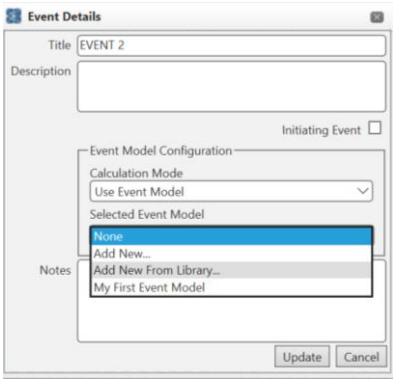
Once you have modified the desired details, hit the Update button to apply your changes, or hit the Cancel button to leave the Event Model Details form.

2.11 The Failure Rate Library Import Form

The Failure Rate Library Import form is a window for importing event model failure rate data from the Kenexis Integrated Safety Suite libraries.

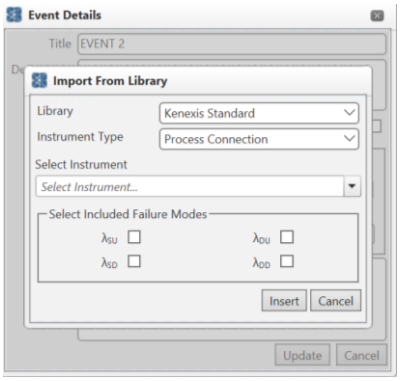
The Failure Rate Library Import form can only be reached by selecting “Add New From Library…” from the Event Details form.

When “Add New From Library…” is selected, the Failure Rate Library Import form will open automatically.

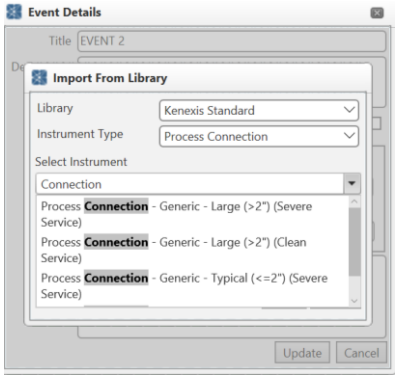


Section 2 - Interface

When the form is opened, you will be prompted to select both a library and an instrument type. The libraries available to Arbor are the same failure rate libraries used by Vertigo, the KISS application for SIS Lifecycle Management. If you are also a Vertigo user, any library data you have defined for use in Vertigo will also be available in Arbor.



Once the library and instrument type have been selected, the Select Instruments combo-box can be used to filter instruments by typing all or part of the instrument name into the box. Below, Process Connection in the Kenexis Standard library has been filtered on the word "Connection."



Selecting the desired instrument can be done by double-clicking on the instrument. You can use the provided scrollbar to navigate the combo-box dropdown menu.

After selecting the instrument, the included failure modes must be selected. In the Kenexis failure rate libraries, failure rates at broken down into four separate categories.

- λ_{SU} Safe Undetected Failures
- λ_{SD} Safe Detected Failures
- λ_{DU} Dangerous Undetected Failures
- λ_{DD} Dangerous Detected Failures

Selecting the appropriate failure mode(s) depend on the type of failures you intend to model in the event where the failure rate will be applied. The following rules-of-thumb will apply for most cases.

- When using the Covert Event model type, the undetected failure rates (λ_{SU} and λ_{DU}) are typically the failure modes of interest.

- When using the Overt Event mode type, the detected failure rates (λ_{SD} and λ_{DD}) are typically the failure modes of interest.
- When using the Constant Event model, it is commonly the case that the total failure rate is of interest. In this case, all four failure modes would be included.

Once the failure modes have been selected and the Insert button has been clicked, a new event model will be generated with the title, description and failure rate populated from the selected library item on the Failure Rate Library Import form. If you wish to exit without saving, you may click the Cancel button. After inserting your event model from the Failure Rate Library, any additional properties required for the event model can be added as described in *Section 2.10* of this manual.

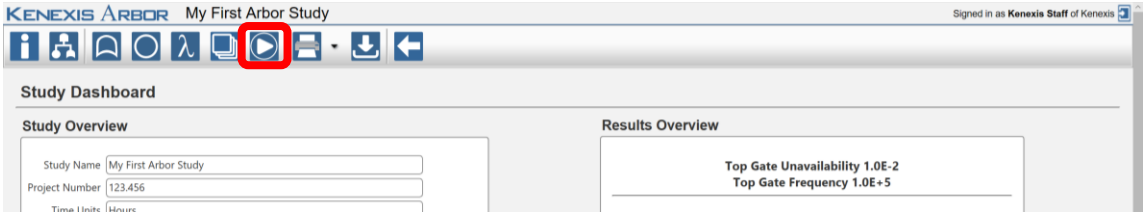
By default, all user accounts have access to the Kenexis Standard Library. This library contains a large collection of failure rate data for a variety of industrial control system components. The data in the Kenexis Standard library is maintained by Kenexis to ensure that the most current and accurate data is always available to KISS users.

If the Kenexis Standard library does not contain a component that you need, your Arbor license also includes the ability for you to create your own custom failure rate libraries. When a custom failure rate library is created, data in that library will be available to all applicable studies in KISS that may utilize the failure rate libraries, including Arbor and Vertigo. Within custom libraries, you also have the option to grant library access to your colleagues working within the Kenexis Integrated Safety Suite. Libraries can be a powerful tool in ensuring that all members of a project team are applying accurate and consistent failure rate data.

Instructions on creating and managing libraries are not contained in this manual. Libraries are part of the KISS Manager module of the Instrumented Safeguard Suite. Information on creating and managing libraries can be found in the KISS Manager User's Manual.

2.12 Running Calculations

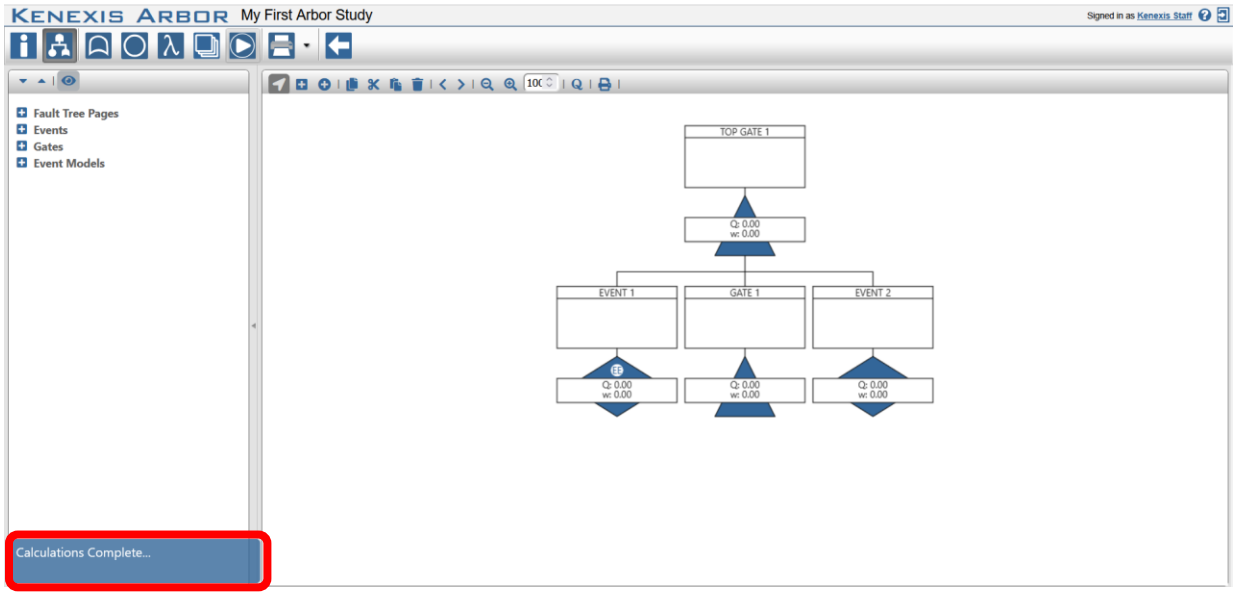
Calculations are performed by clicking the Run Calculations icon in the Navigation Toolbar.



Section 2 - Interface

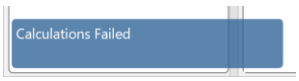
When changes are made to gates, events or event models the existing calculations will often be invalidated, requiring calculations to be performed. Calculations in Arbor typically run quickly, in under 5 seconds. However, there is no limit to the size of a fault tree in Arbor and very large event trees will cause calculation times to grow exponentially. For this reason, calculations are not performed automatically after any change that would invalidate the top gate results. Before reporting results, the Run Calculations button should always be clicked to ensure that the state of the results is current.

In addition to the Run Calculations button on the Navigation Toolbar, while working on the fault tree interface, calculations can be run by using the hotkey combination (Ctrl + Enter) while the main workspace is in focus. The fault tree interface will generate user messages confirming the completion of calculations in the lower left corner of the window, as shown below:



When working from any other page in Arbor, running calculations will cause the page to reload, refreshing the data on the page.

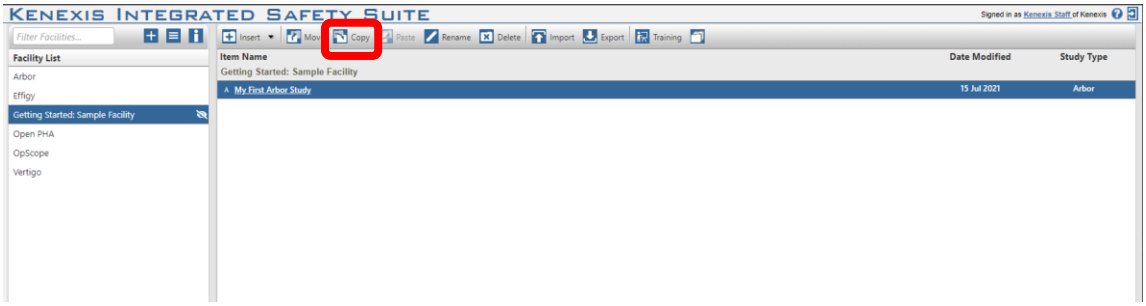
There are several checks that occur at calculation-time to ensure that your fault tree contains valid data. If one or more of these checks fail, Arbor will generate a user message (either in the lower left corner or in a popup window) informing you why the calculations could not be performed, as shown below:



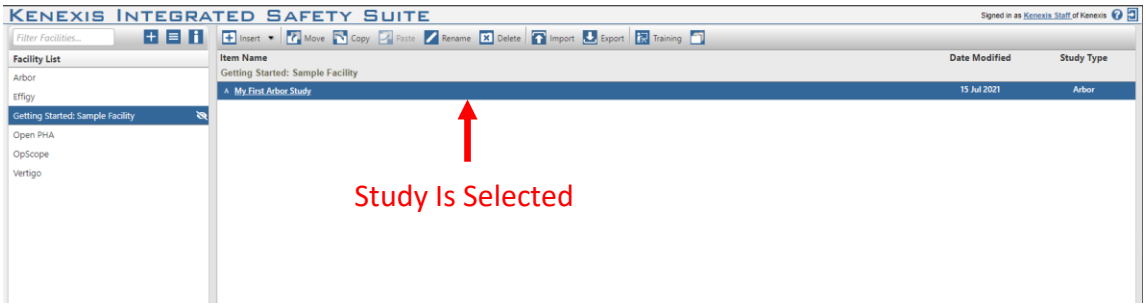
Section 2 - Interface

2.13 Copying a Study

An Arbor study can be copied from the KISS Study Manager page. The KISS Study Manager page is the main page in the KISS Manager application and the default landing page when logging into your KISS account, shown below.



Studies can be copied by clicking on the Copy button in the main Navigation Toolbar, highlighted above. If there is no study selected, the Copy button will be disabled and rendered with transparency, as shown in the above figure. Once an Arbor study is selected, the Copy button will enable, allowing the selected study to be copied, as shown below. An Arbor study can be selected from the Study List by left clicking on the row of the desired study. When selected, the row will be highlighted blue.

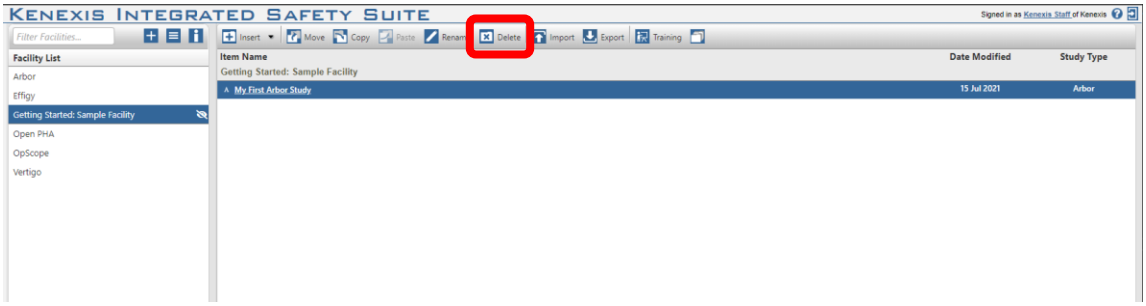


Studies can only be copied within the facility where they were created. When a study is copied the new instance of the study will be renamed to “Study Name – Copy”. Where Study Name is the name of the original study. To create a copied instance of a study outside of the facility where it was created, use the Study Data Import / Export functionality described in *Section 2.15* of this manual.

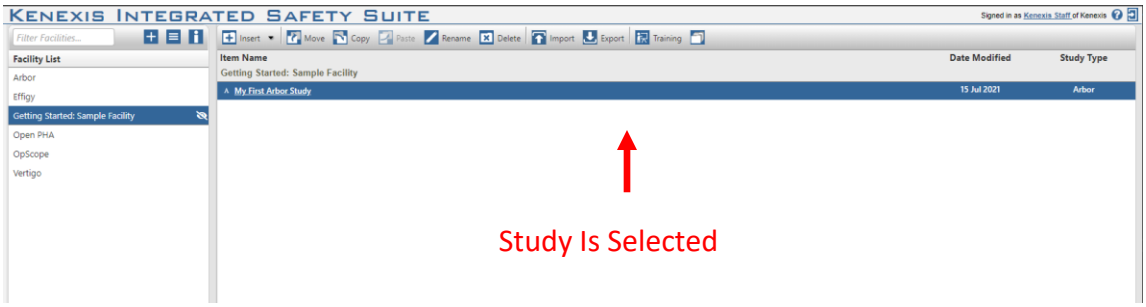
Section 2 - Interface

2.14 Deleting a Study

An Arbor study can be deleted from the KISS Study Manager page. The KISS Study Manager page is the main page in the KISS Manager application and the default landing page when logging into your KISS account, shown below.



Studies can be deleted by clicking on the Delete button in the main Navigation Toolbar, highlighted above. If there is no study selected, the Delete button will be disabled and rendered with transparency. Once an Arbor study is selected, the Delete button will enable, allowing the selected study to be deleted, as shown below. An Arbor study can be selected from the Study List by left clicking on the row of the desired study. When selected, the row will be highlighted blue.

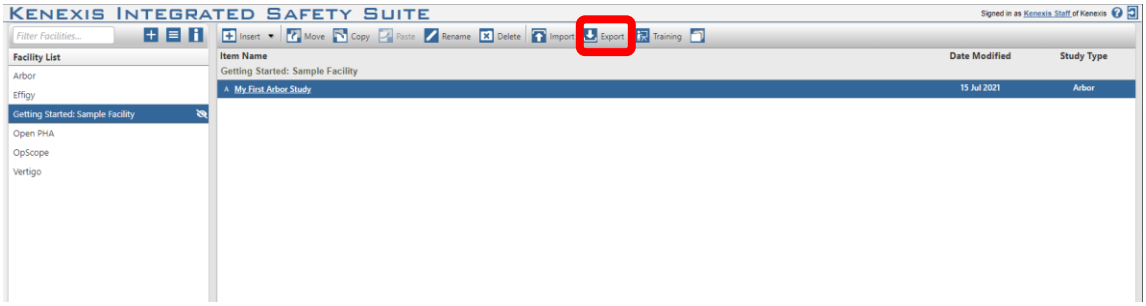


2.15 Exporting & Importing Study Data

2.15.1 Exporting

An Arbor study can be exported from the Study Manager page in the KISS Manager. Arbor studies are exported in a proprietary binary file format, *.arb. These files can't be edited. Studies can be exported by clicking on the Export button selected in the main Navigation Toolbar. The Export button will be disabled unless a study has been selected. See *Sections 2.13/14* on copying and deleting studies for details on selecting studies on the Study Manager page.

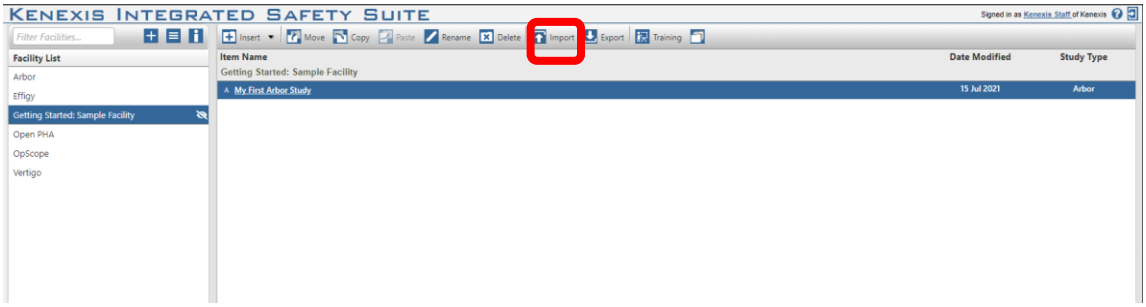
Section 2 - Interface



When the Export button is clicked, a *.arb file will be downloaded containing the name of your study. This file contains all the data associated with the Arbor study being exported. This file can later be imported using the method described below.

2.15.2 Importing

An Arbor study can be imported from the Study Manager page in the KISS Manager. The import functionality is primarily used by Kenexis for a variety of maintenance tasks but is also provided publicly to allow studies to be copied across facilities or servers.



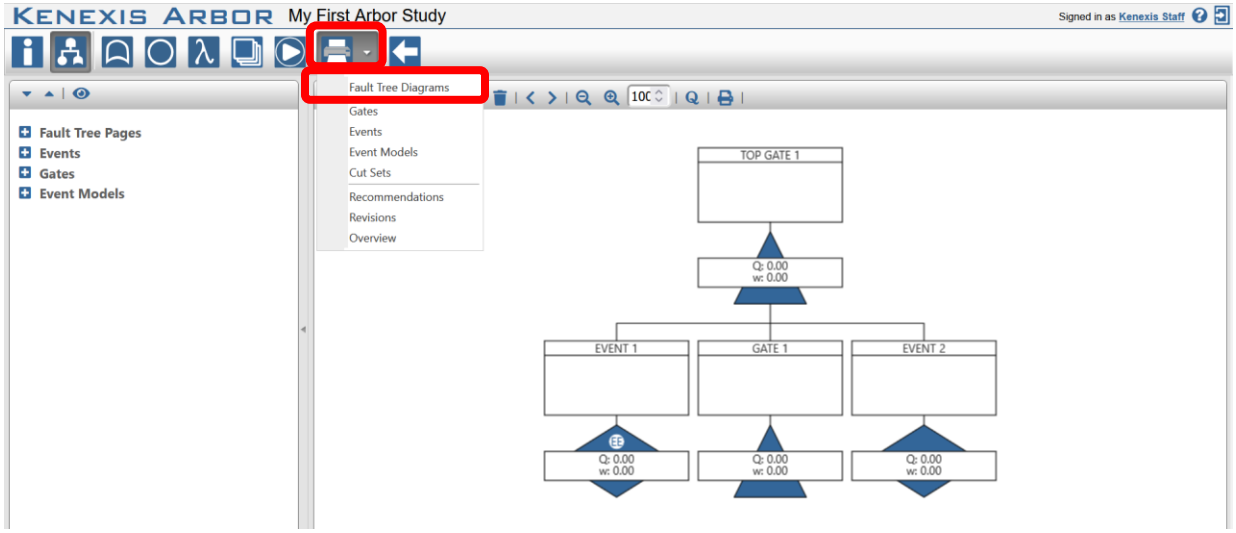
Studies can be imported by clicking on the Import button in the main Navigation Toolbar, highlighted above. The Import button will be disabled unless a study has been selected. In addition, before importing a study, you must select a facility from the facility list on the left side of the interface. Studies cannot be imported without first selecting a destination facility for the study. Once a facility has been selected, the facility will be highlighted blue in the facility list, and the Import button will be enabled.

Clicking the Import button will open a file selection dialog that can be used to select the *.arb study you would like to import. If the data contained in the *.arb file is valid, the import will be performed, and the imported study will be automatically opened in Arbor.

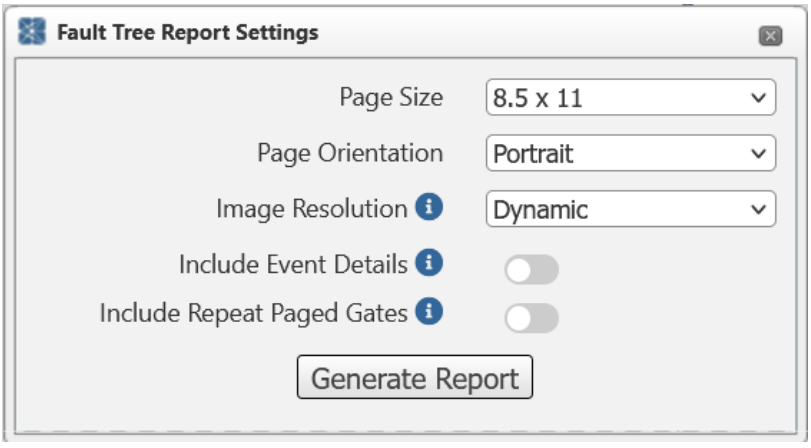
Section 3 – Reporting

3.1 Generating a Fault Tree Report

Generating a report containing a graphic representation of the fault tree can be done from anywhere within Arbor by clicking on the Print dropdown menu in the Navigation Toolbar. This will expand a dropdown menu where you can select whether to report your fault tree diagrams, the grid views for gates, events, event models, and cut sets, or the recommendation or revision history, or an overview of the study. For reporting options other than Fault Tree Diagrams, see *Section 3.2* of this manual.



Choosing to generate a Fault Tree Diagrams report will generate a Microsoft Word (*.docx) file. When the Fault Tree Diagrams option is chosen, the Fault Tree Report Settings form is opened.



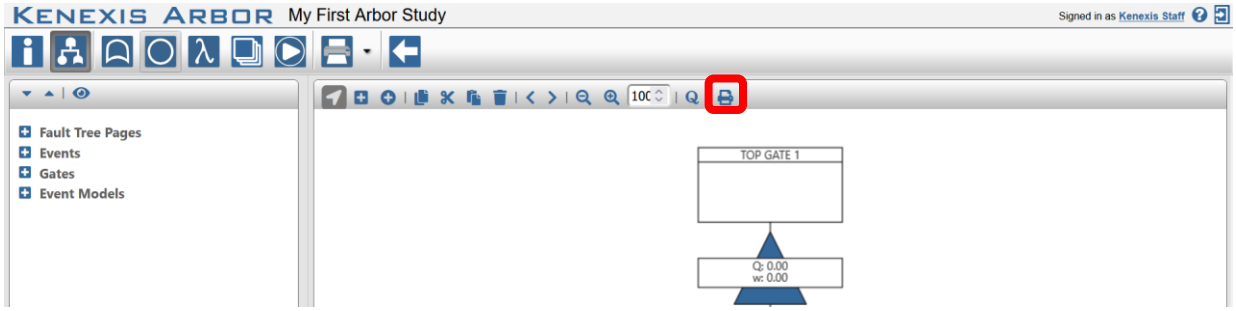
From the Fault Tree Report Settings form, you can choose the page size of your report (either 8.5 x 11 or 11 x 17), the page orientation of your report (either portrait or landscape), the

image resolution of your report, whether event details are included, and whether paged gates are printed once or multiple times.

The Image Resolution options include Dynamic and Maximum. The Dynamic resolution option scales images to fit the report page to reduce file size. The Maximum resolution option embeds images at their maximum resolution to allow for scaling without the loss of image fidelity. The choice between these image resolution options is up to user preference.

When toggled on, the Include Event Details option includes a table under each page of the event tree in the final report with details on the events shown in that page. When toggled on, the Include Repeat Paged Gates option prints paged gates reused throughout the diagram multiple times. These options allow you to fully customize your Fault Tree reports. When you've made your desired choices, click the Generate Report button.

In addition to the fault tree reporting functionality, snapshots of the visible fault tree page can be generated by clicking on the Print button in the main workspace menu, as shown below:



Clicking the Print button will download an image file containing the fault tree in *.png format.

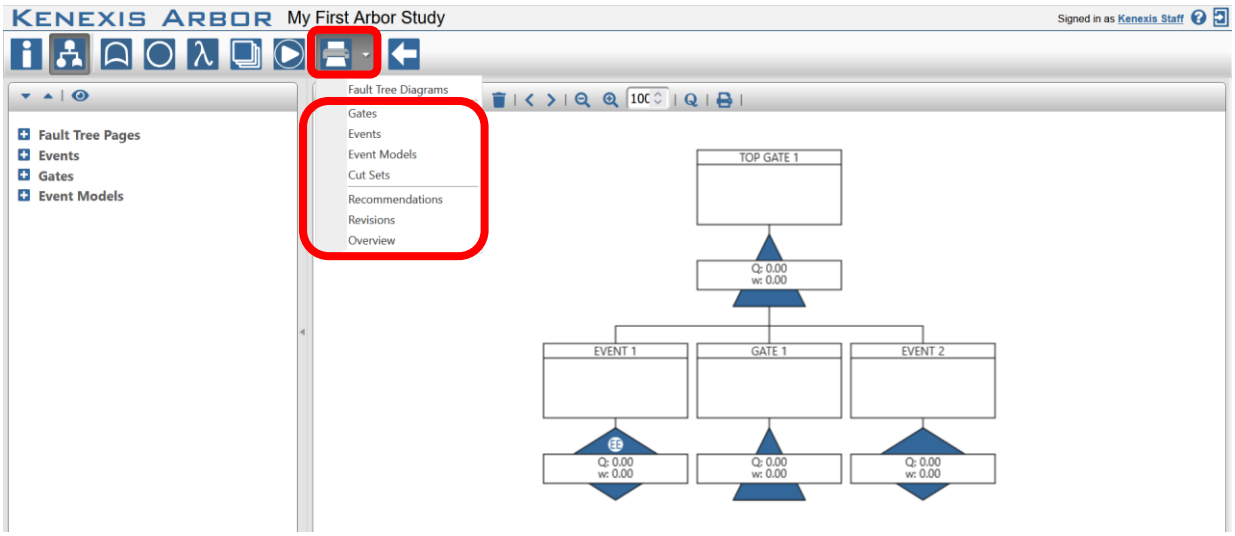
The resolution of the snapshot can be modified by adjusting the main workspace zoom using the zoom controls in the main workspace menu, as described in *Section 2.2.2.3* of this manual. Increasing the zoom will increase the resolution of the produced image, reducing the zoom will reduce resolution.

3.2 Generating a Tabular Report

Reports can be generated in tabular formats for gates, events, event models, minimum cut sets, recommendations, revisions, and for an overview of the study. Tabular reports are generated in Microsoft Excel file format (*.xlsx).

Section 3 – Reporting

To generate a tabular report, click on the Print dropdown menu in the Navigation Toolbar. This will expand a dropdown menu where you can select the object type you would like to be reported.



Clicking on an object type in the print dropdown will start a download of the tabular report. The resulting tabular report will display the corresponding grid views for the object type selected. For the Overview tabular report, the result will include a table of the study name, project number, time units, project notes, the top gate unavailability and frequency, and the number of gates, events, and event models used in the Arbor study.

Section 4 – Calculation Details

This section details the calculations methods used by Arbor to determine unavailability and frequencies for gates, events, and event models.

4.1 Event Model Calculations

Event models are used to characterize failure characteristics for an event. An event is used to characterize one component of a system. Collections of events, along with the logical relationships between those events (as defined by the gates of a fault tree) are used to calculate unavailability and frequency of failure for a system (the top gate of a fault tree).

Three event model types are available in Arbor. These event model types are:

- Constant
- Covert
- Overt

The following sections detail the calculation details for each event model type. The unavailability and frequency calculated for an event model are applied to all events in a study that use that event model (as defined on the Event Details Form).

4.1.1 Constant Event Model Calculations

The Constant Event Model should be used when you want to directly enter unavailability and frequency for an event model. The Constant Event Model is the simplest of the event models in Arbor. When creating a Constant Event Model, you will be prompted to enter the failure rate and the unavailability of the event model. The relationship between these inputs and the unavailability and frequency calculated for any event applying a constant event model is simple. The unavailability and frequency of an event can be calculated using the following formulas:

$$w_e = \lambda_{em}$$

$$Q_e = Q_{em}$$

Where:

w_e = Event Frequency — λ_{em} = Event Model Failure Rate

Q_e = Event Unavailability — Q_{em} = Event Model Unavailability

Some typical applications for using the Constant Event Model include:

- Modeling a system power failure that is estimated to occur at a fixed frequency.

- Modeling an initiating event frequency in Layer of Protection Analysis (LOPA). For example, a process control loop is typically assumed to fail at a failure rate of 0.1 per year. Using a Constant Event Model with a failure rate of 0.1 and setting the associated event as an initiating event can be used to model this scenario.
- Modeling an Independent Protection Layer (IPL) in LOPA. For example, operator response to an alarm is typically assumed to be 90% effective (unavailability = 0.1). A Constant Event Model with an unavailability of 0.1 can be used to model this scenario.
- Modeling the unavailability of a fire and gas detection system due to an uncovered fire or gas results. This scenario typically involves calculation of detector coverage using the Effigy Fire and Gas Mapping application of KISS. The unavailability of the constant event would be set to one minus the detector coverage factor calculated by Effigy.
- Modeling any fixed probability, such as modeling the probability of a given set of meteorological conditions. For example, suppose the wind blows from the North 25% of this time. A Constant Event Model with an unavailability of 0.25 can be used to model this scenario.

4.1.2 Covert Event Model Calculations

The Covert Event Model should be used when you want to model a component that fails and remains in a failed state until the component is tested, with testing occurring at predefined test intervals. The Covert Event Model assumes a constant failure rate and calculates the mean unavailability and frequency over a time interval given by the event model test interval.

The following equation is used to calculate the event unavailability for a Covert Event Model:

$$Q = \frac{\lambda * TI - \left(1 - e^{-\lambda * TI}\right) + \lambda * MTTR * \left(1 - e^{-\lambda * TI}\right)}{\lambda * TI + \lambda * MTTR * \left(1 - e^{-\lambda * TI}\right)}$$

Where:

Q = Event Unavailability λ = Event Model Failure Rate

TI = Event Model Test Interval MTTR = Event Model MTTR

The following equation is used to calculate the event frequency for a Covert Event Model:

$$w = \lambda * (1 - Q)$$

Where:

w = Event Frequency λ = Event Model Failure Rate

Q = Event Unavailability

Section 4 – Calculation Details

Some typical applications for the Covert Event Model include:

- Modeling the PFD_{avg} for a component as part of a Safety Integrity Level (SIL) Verification calculation for integration with the Vertigo SIS Lifecycle Management application.
- Modeling the PFD_{avg} for fire or gas detection components as part of an FGS availability analysis in a performance-based fire and gas system assessment.

4.1.3 Overt Event Model Calculations

The Overt Event Model should be used when modeling an immediately diagnosable component failure, with an initiated maintenance action to repair the failed component. The Overt Event Model assumes both a constant failure rate and constant repair time, usually the mean time to repair (MTTR).

The following equation is used to calculate unavailability for the Overt Event Model:

$$Q = \left[\frac{\lambda}{\lambda + \frac{1}{MTTR}}\right] * \left[1 - e^{-1*\left(\lambda + \frac{1}{MTTR}\right)*T_m}\right]$$

Where:

Q = Event Unavailability λ = Event Model Failure Rate

MTTR = Event Model MTTR T_m = Mission Time

The following equation is used to calculate frequency for the Overt Event Model:

$$w = \lambda * (1 - Q)$$

Where:

w = Event Frequency λ = Event Model Failure Rate

Q = Event Unavailability

Section 4 – Calculation Details

Some typical applications for the Overt Event Model include:

- Modeling the failures of basic process control loop components in a focused quantitative risk assessment.
- Modeling the unavailability of a pump due to maintenance.
- Modeling the unavailability of a programmable logic controller component in a fault tolerant system where the component failure is detectable but does not result in a system trip.

4.2 Gate Calculations

The unavailability and frequency for each gate in an Arbor study can be calculated using minimal cut set analysis. Minimal cut set analysis is the process of identifying the minimum combinations of basic events in a failed state that are required to yield a failed state for the system, given the logical relationship between gates and events. This section contains a brief description of the minimal cut set analysis process sufficient for understanding the principles at work in Arbor. A more complete description of the process can be found in the following technical reference:

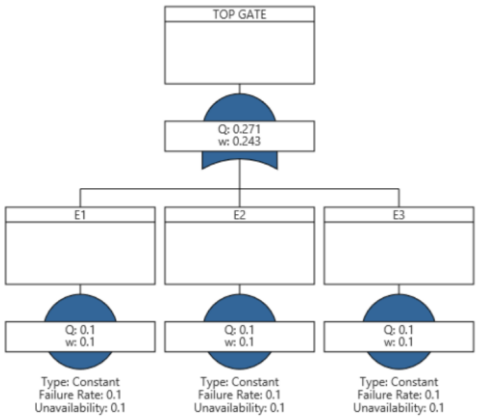
- *Guidelines for Chemical Process Quantitative Risk Analysis. New York: Institute of Chemical Engineers, 2000. Print.*

4.2.1 Minimal Cut Set Analysis

A cut set is defined as any combination of failed events which can result in failure at the gate level. A minimal cut set is a special case of a cut set which is unique and not contained within the definition of any other cut set for a given gate. Calculating minimal cut sets is important in fault tree analysis because ignoring the uniqueness of cut sets can result in a gross overestimation of gate unavailability and frequency.

Take, for example, the simple fault tree shown below:

Section 4 – Calculation Details



In this tree, there are three events E1, E2 and E3. The top gate is an OR gate, meaning that a failure of any one of the three events will result in failure of the top gate. For this simple fault tree, there are seven cut sets as follows:

1. E1
2. E2
3. E3
4. E1 and E2
5. E1 and E3
6. E2 and E3
7. E1 and E2 and E3

Of the above cut sets, only the first three are unique, making them the minimal cut sets for the top gate. Sets 4 through 7 are not minimum cut sets because each set already contains an event within the first three cut sets. In simple terms, the simultaneous failure of E1 and E2 is not a concern because the failure of a single component, either E1 or E2, will lead to a system failure.

A collection of minimal cut sets for a gate is generated by first creating the complete cut set list and then by minimizing that list by applying a set of rule-based Boolean expressions to exclude cut sets that are not minimal. The minimum cut set generation rules are shown below, where A, B, and C represent basic events.

Section 4 – Calculation Details

Rule	Mathematical Form
Communitive Rule	A*B = B*A A + B = B + A
Associative Rule	A*(B + C) = (A*B) + C A + (B + C) = (A + B) + C
Distributive Rule	A*(B + C) = A*B + A*C A + (B*C) = (A + B)*(A + C)
Idempotent Rule	A*A = A A + A = A
Rule of Absorption	A*(A + B) = A A + A*B = A

Reference: Guidelines for Chemical Process Quantitative Risk Analysis. New York: Institute of Chemical Engineers, 2000. Print.

4.2.2 Calculating Cut Set Unavailability & Frequency

Once a minimal cut set has been generated, the unavailability and frequency for the cut set can be calculated by applying the mutually exclusive unavailability and frequency equations.

By default, Arbor performs unavailability calculations for cut sets containing events with Covert Event Model types in accordance with *IEC 61508-6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3*, and with the recommended practice in *ISA-TR84.00.02 – Part 3 Safety Instrument Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques Part 3: Determining the SIL of a SIF via Fault Tree Analysis*. Guidance from these documents requires that unavailability calculations for a system be performed using a method of averaging after logic is applied for covert failure modes. The unavailability and frequency for a cut set can be calculated using the following equations:

$$Q_{cs} = \frac{2^m \prod_{j=1}^{m} Q_j}{m+1} \prod_{i=1}^{n} Q_i$$

Where:

Q_{cs} = Unavailability of the Cut Set

Q_j = Unavailability of Event j

Q_i = Unavailability of Non-Covert Event i

m = Number of Covert Events in the Cut Set

n = Number of Non-Covert Events in the Cut Set

$$w_{cs} = \sum_{j=1}^{n} w_j \prod_{\substack{i=1 \\ i \neq j}}^{n} Q_i$$

Where:

w_{cs} = Frequency of the Cut Set

n = Number of Events in the Cut Set

Q_i = Unavailability of Event i

w_j = Frequency of Event j

4.2.3 Calculating Gate Unavailability and Frequency

The unavailability and frequency for a gate can be calculated by applying the Esary-Proschan equations for unavailability and frequency. The default application of these equations is:

$$Q_g = \prod_{i=1}^{n} Q_i \left[1 - \prod_{j=1}^{m} (1 - Q_{cs,j}) \right]$$

Where:

Q_g = Unavailability of the Gate

n = Number of Events Common to All Cut Sets

Q_i = Unavailability of Common Event i

m = Number of Cut Sets for the Gate

$Q_{cs,j}$ = Unavailability of Cut Set j (Excluding Common Events)

$$w_g = \sum_{j=1}^{n} w_{cs,j} \prod_{\substack{i=1 \\ i \neq j}}^{n} (1 - Q_{cs,i})$$

Where:

w_g = Frequency of the Gate

n = Number of Cut Sets

$w_{cs,j}$ = Frequency of Cut Set j

$Q_{cs,i}$ = Unavailability of Cut Set i

Section 4 – Calculation Details

4.2.4 Calculations for Initiating Events

Events can be defined as initiating events to inform the calculation engine that the only result of interest is frequency for that event and any gates above that event in the tree.

Initiating events are instantaneous in nature. Therefore, all initiating events must be mutually exclusive, and a cut set is not allowed to contain more than one initiating event. At cut set generation, Arbor will check for cut sets that contain multiple initiating events. If a cut set is detected with multiple initiating events, the calculations will stop, and a user message will be displayed detailing the issue.

Because initiating events are instantaneous and mutually exclusive, they are handled differently in calculations, as the unavailability of an initiating event is zero. When calculating unavailability for a cut set, the unavailability of an initiating event is excluded from the product of unavailability's equation such that the equation for calculating cut set unavailability becomes:

$$Q_{cs} = \prod_{i=1}^{n} Q_i$$

Where:
Q_{cs} = Unavailability of the Cut Set
n = Number of Events in the Cut Set, Excluding Initiating Events
Q_i = Unavailability of Event i

If all cut sets for a gate contain a common initiating event, the calculation for gate unavailability and frequency must be modified to avoid overestimation of the gate frequency with the Esary-Proschan equation. The following equations are used to calculate gate unavailability and frequency for a gate containing a common initiating event in all cut sets:

$$Q_g = \prod_{i=1}^{n} Q_i \left[1 - \prod_{j=1}^{m} (1 - Q_{cs,j})\right]$$

Where:
Q_g = Unavailability of the Gate
n = Number of Basic Events Common to All Cut Sets, Excluding Initiating Events
Q_i = Unavailability of Common Event i
m = Number of Cut Sets for the Gate

$Q_{cs,j}$ = Unavailability of Cut Set j (Excluding Common Events)

$$w_g = Q_g \sum_{i=1}^{n} w_i$$

Where:

w_g = Frequency of the Gate

n = Number of Common Initiating Events

w_i = Frequency of Common Initiating Event i

4.2.5 Calculations for Enabling Events

Events can be defined as enabling events to inform the calculation engine to exclude the frequency for any cut sets that contain the event. Setting an event as an enabling event does not affect the calculations used to calculate unavailability or frequency for cut sets or gates described earlier in this section. The effect of setting an event as an enabling event is simply that the frequency for that event is excluded from the summation of frequencies in any cut set calculations. Events can either be set as initiating events or enabling events, but not both.