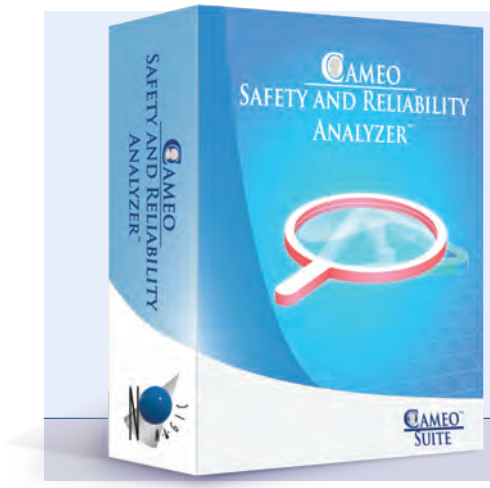


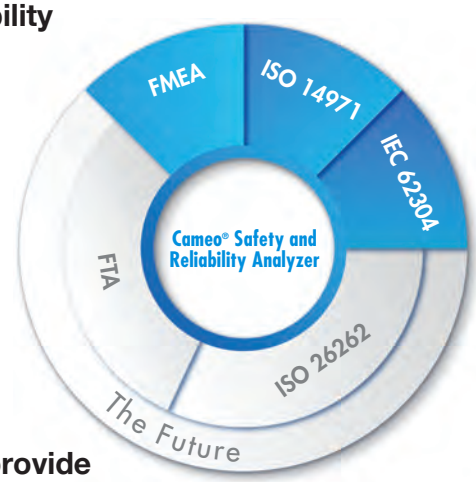
Cameo® Safety and Reliability Analyzer

A Model-based Approach to Safety and Reliability Analysis

The Cameo Safety and Reliability Analyzer Plugin enables a model-based approach to safety and reliability analysis. This new functionality integrates into the No Magic MBSE toolkit.

The Cameo Safety and Reliability Analyzer plugin supports:

- Failure mode and effects analysis (FMEA) according to IEC 60812:2006 standard
- Hazard analysis according to the following medical standards:
  - IEC 62304
  - ISO 14971:2007



As the plugin evolves, it will provide support for the following:

- Fault Tree Analysis (FTA)
- ISO 26262 (Road vehicles – functional safety)

> "This profile looks great and would definitely make this analysis easier to perform on future programs. I really like the matrix views that can be auto-generated to see the FMEA and Safety items related to the elements of the architecture. I also like the connection between FMEA and safety items – it makes that traceability a lot easier to capture and to review than with an Excel approach. I think this is definitely a capability that my organization will make use of."
>
> - ***Candace Miano**, Systems Engineer, Space Systems, Lockheed Martin Corporation*

Cameo® Safety and Reliability Analyzer

- **Helps demonstrate** that risks are addressed by safety requirements/risk control measures, design elements, critical quality attributes (CQA)
- **Validates the model** to ensure that the entire design passes safety and reliability analysis
- **Provides increased agility** between design, safety and reliability analysis phases:
  - Frequent exchange of information between safety and reliability analysis cross-functional teams
  - Shorter development cycles followed by shorter safety and reliability analysis cycles, leading to more precise detection of risks and faults
  - More reliable products
- **Ensures traceability** of risks to requirements, design elements, critical quality attributes (CQA) and other artifacts. Traceability from design elements to FMEA is also realized, including two-way traceability between FMEA and risks/hazard analysis.

Features

The **Cameo Safety and Reliability Analyzer** plugin currently supports the following features:

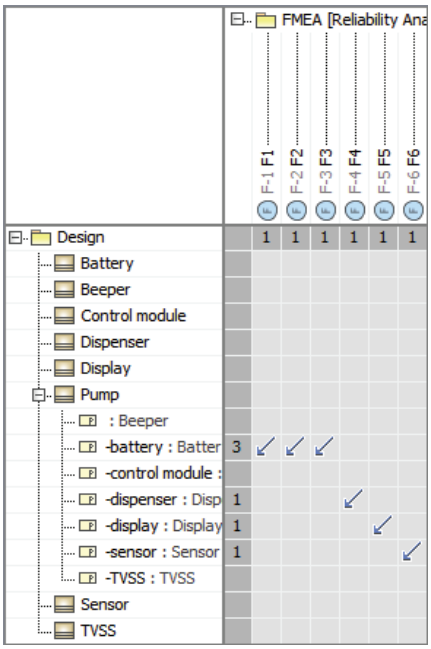
- Reliability analysis via FMEA

#	Name	Item	Subsystem	Failure Mode	Local Effect Of Failure	Final Effect Of Failure	SEV	Cause Of Failure	OCC	Prevention Control	Detection Control	DET	OxD	RPN	Hazard Analysis Reference	Requires Hazard Analysis	Recommended Action	Mitigation	Responsibility	Target Completion Date	Action Taken	Reduced SEV	Reduced OCC	Reduced DET	Reduced OxD	Reduced RPN
1	F1	battery : Battery	Pump	Unable to be charged		Underdose or overdose	4.0	Battery degraded	1.0	Meter designed to ISO00124	Charging test 02:1111	1.0	1.0	4.0	R-1 Discharged battery leads to coma or death	true	Add display view to monitor battery charging level	: Alarm when				4.0	1.0	1.0	1.0	4.0
2	F2	battery : Battery	Pump	Voltage error		Therapy delay	4.0	Battery depleted	4.0	Meter designed to ISO00124		3.0	12.0	48.0		true			Barry John	03/15/2016		4.0	2.0	1.0	2.0	8.0
3	F3	battery : Battery	Pump	Unable to be charged		Therapy delay	3.0	Battery overcharged	1.0			1.0	1.0	3.0		false						3.0	1.0	1.0	1.0	3.0
4	F4	dispenser : Dispenser	Pump	Pumps inaccurate size/rate of dose (including "fail to pump"), operating abnormally	Air in line		4.0	Failure to release ins	2.0			2.0	4.0	16.0		true						4.0	2.0	2.0	4.0	16.0
5	F5	display : Display	Pump	Broken keypad		Therapy delay	3.0	Incorrect operation	1.0			1.0	1.0	3.0		false						3.0	1.0	1.0	1.0	3.0
6	F6	sensor : Sensor	Pump	Drop in sensitivity	High glucose-level undetectec Low glucose-level undetected		4.0	Battery degraded Flawed sensor	2.0			3.0	6.0	24.0		false						4.0	2.0	3.0	6.0	24.0

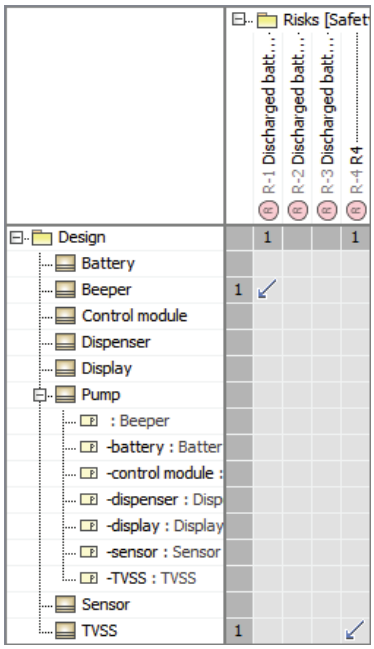
- Safety analysis for medical devices and software according to IEC 62304 and ISO 14971:2007 medical standards

#	FMEA Reference	Initiating Cause	Hazard	Sequence Of Event	Hazardous Situation	Harm	S	P1	P2	P	D	C	PU	Risk	Use Related
1	F-1 F1	Discharged battery leads to coma or death	A Dose	Battery has sank	The user receives less insulin than required to maintain desirable BG levels	Coma, Death	4.0	3.0	4.0	3.0	1.0	1.0	1.0	High	false
2		Discharged battery leads to decreased consciousness	A Dose	Battery has sank	The user receives less insulin than required to maintain desirable BG levels	Decreased consciousness	3.0	3.0	3.0	3.0	1.0	1.0	1.0	Medium	false
3		Discharged battery leads to minor organ	A Dose	Battery has sank	The user receives less insulin than required to maintain desirable BG levels	Minor organ damage	2.0	3.0	2.0	2.0	1.0	1.0	1.0	Low	false
4		R4	B Electromagnetic energy(ESD)	(1) Electrostatically charged patient touches infusion pump (2) ESD (electrostatic discharge) causes pump and pump alarms to fail (3) Insulin not delivered to patient	Failure to deliver insulin unknown to patient with elevated blood glucose level	Coma, Death	4.0	2.0	3.0	2.0	1.0	1.0	1.0	Medium	false

- Predefined samples (Medical FMEA and Hazard Analysis and Automotive FMEA) to demonstrate model-based safety and reliability analysis advantages over document-based approach for a wide audience of systems engineers from different domains



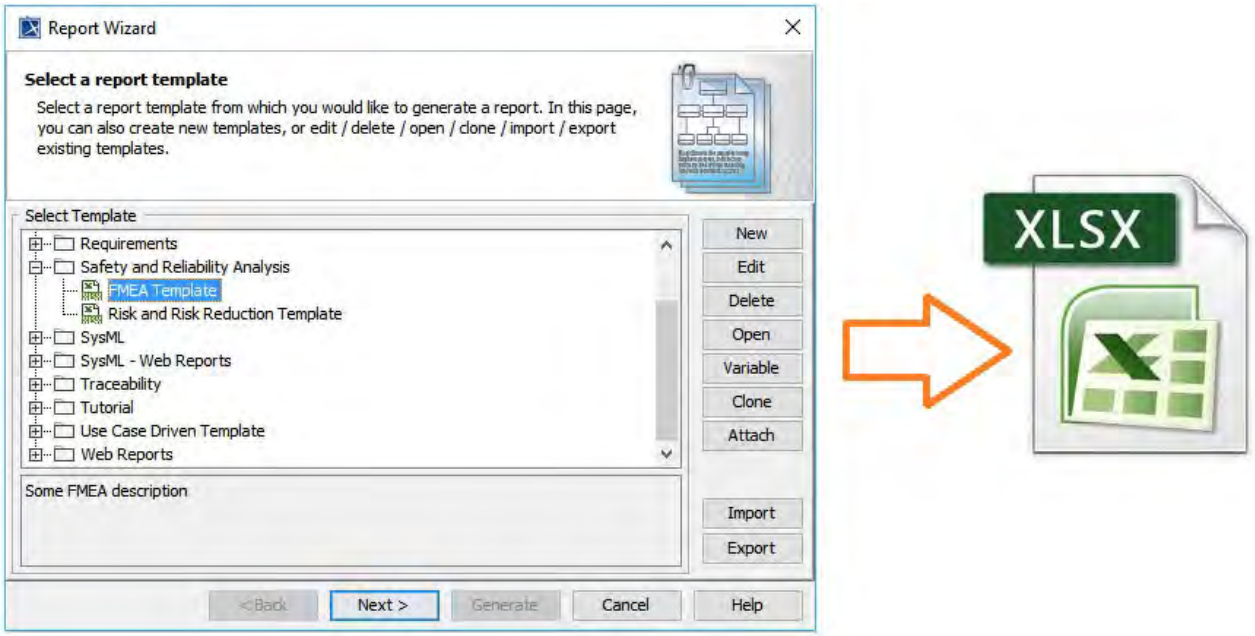
Traceability between Design to Failure



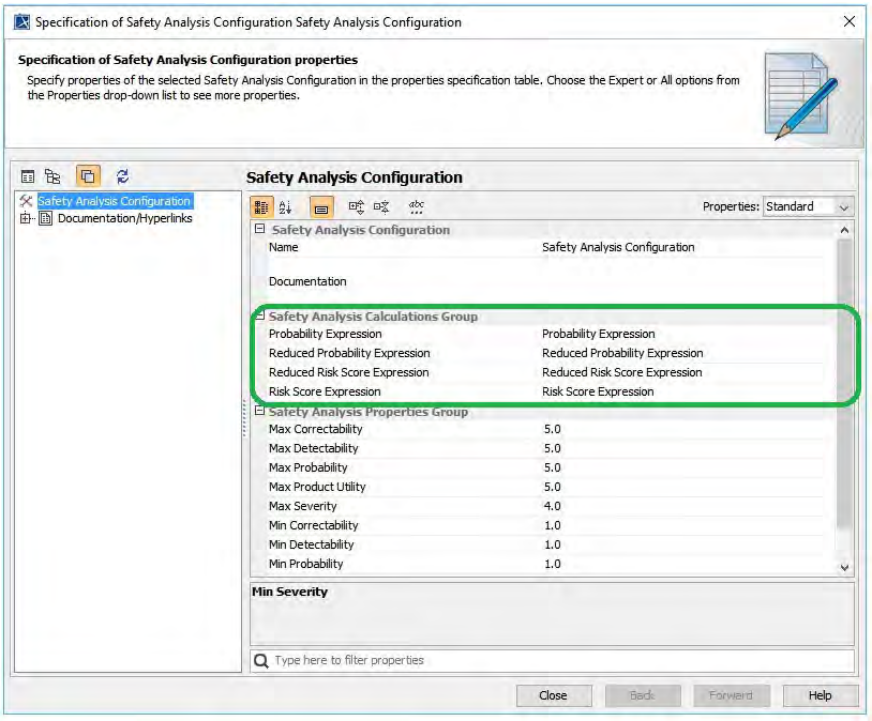
Traceability between Design to Risk

Features ...continued

- Predefined reports for safety and reliability analysis



- The plugin is customizable, allowing users to add their own data columns and customize risk calculation rules and reports

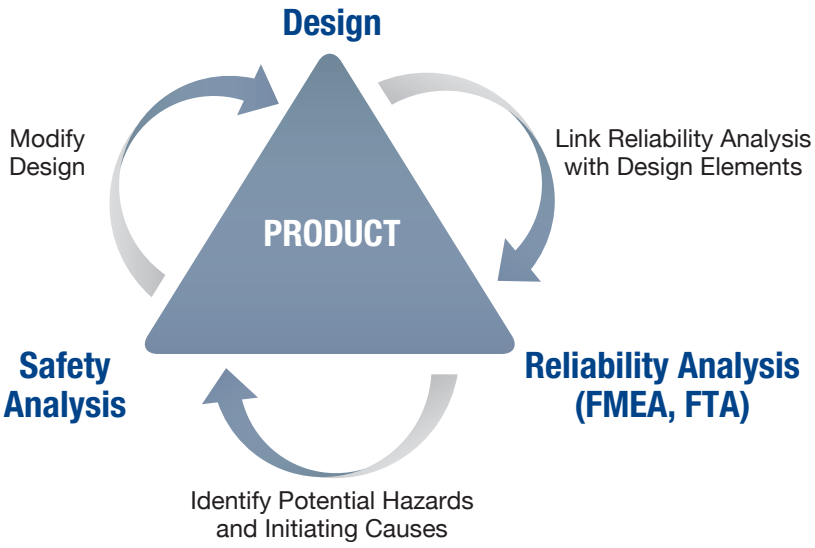


Process Description

For analyzing the safety and reliability of your model, we recommend the following workflow:

1. Create or use an existing model of your system design. The model of your design depends on your particular case.
2. Define failure modes of your particular case for each design element and perform the FMEA analysis.
3. Identify possible risks and use them for further risk analysis.
4. Address the risks in your system design (by introducing new design elements) for controlling and reducing potential hazards.

The safety analysis process is cyclical and requires constant review, as depicted in the figure on the right.



Project Templates

There are two templates predefined in the plugin:

- **FMEA Project** (Failure Mode Effects Analysis Project). Select this template if you need the reliability analysis only.
- **Safety and Reliability Analysis Project** (FMEA Project included). Select this template if you need both the FMEA and risk analysis.

Both templates contain predefined packages and diagrams to start performing risk analysis. Depending on the template, Design, Reliability Analysis, Risk Analysis and Safety Requirements top-level packages are created, followed by appropriate sub packages.

Compatibility

The **Cameo Safety and Reliability Analyzer Plugin** is compatible with the following **No Magic** products:

- MagicDraw (Standard, Professional, Architect and Enterprise editions)
- Cameo Systems Modeler
- Cameo Enterprise Architecture

For more information about Cameo Safety and Reliability Analyzer, go to
http://www.nomagic.com/products/magicdraw-no-cost-add-ons/cameo-safety-and-reliability-analyzer-plugin

The Truth is in the Models™

No Magic, Inc.
One Allen Center
700 Central Expressway South, Suite 110
Allen, Texas 75013
Phone 214.291.9100
E-mail: sales@nomagic.com
www.nomagic.com