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

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

---

### Predefined samples

(1) Electromagnetic energy (ESE): 

- **Causes**: Battery has heat, Battery has current, Battery has voltage, Battery has resistance.
- **Hazards**: Battery has heat, Battery has current, Battery has voltage, Battery has resistance.
- **Sequence of Events**: Battery has heat, Battery has current, Battery has voltage, Battery has resistance.
- **Hazardous Situation**: Battery has heat, Battery has current, Battery has voltage, Battery has resistance.
- **FMEA Risk**: High

---

### Traceability between Design to Failure

- **Design**
  - Battery
  - Dispenser
  - Display
  - Control module
  - Pump
  - TISS / TISS

- **Failure Analysis**
  - Battery
  - Dispenser
  - Display
  - Control module
  - Pump
  - TISS / TISS

---

### Traceability between Design to Risk

- **Design**
  - Battery
  - Dispenser
  - Display
  - Control module
  - Pump
  - TISS / TISS

- **Risk Analysis**
  - Battery
  - Dispenser
  - Display
  - Control module
  - Pump
  - TISS / TISS
• 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