

Model-based Reliability and Safety Analysis, fosters Agility in Design of Mission-Critical Systems

Carmelo Tommasi
Commercial Director, Italy
No Magic Europe
Milan, Italy
Carmelo.tommasi@nomagic.com

Nerijus Jankevicius
Product Manager
No Magic Europe
Kaunas, Lithuania
nerijus.jankevicius@nomagic.com

Andrius Armonas
Product Manager
No Magic Europe
Kaunas, Lithuania
andrius.armonas@nomagic.com

Copyright © held by the author.

Abstract—In Systems Engineering Verification and Testing for Reliability and Safety are the most complex, error-prone and expensive tasks. This paper explains how Model Based Systems Engineering Techniques and Methodologies, powered by SysML, can facilitate Agility in Design for Reliability and Safety of Mission-Critical Systems in several Industries like Aerospace, Medical, Automotive, Transportation.

We highlight how Model Based Systems Engineering is increasingly key in traditionally conservative industries like e.g. Aerospace where Safety is of the utmost importance but Systems Engineering Design has always neglected new techniques and trends. Indeed recently DO-178B/ED-12B, the primary document for safety approval of aerospace systems, has been updated to the “C” version, where an entire supplement, “DO-331/ED-216: Model Based Development and Verification supplement” is reserved to the use of Model-Based Techniques to Avionic Safety.

To assert the application in various industries of these automation/MBSE techniques, one example from a critical industry like Medical has been used. The example, based on an insulin pump system design, explains the value users get from taking Model-Based approach to safety and reliability analysis and integrating it into MBSE toolkit, with big benefits of reusing most of analysis item in the same project new versions or new projects.

Keywords—MBSE; Model Based Systems Engineering; Model Based Reliability and Safety Analysis; SysML; Mission and Safety Critical Systems Design; Requirements Automated Verification; Reliability Analysis; Safety Analysis; Functional Analysis; FMEA; FMECA; Systems Reliability and Safety

I. INTRODUCTION

In this article, we will discuss how to apply MBSE approach to safety and reliability analysis and integrate them into MBSE toolkit. Scope of this article are 2 important topics Reliability and Safety, key for Cyber security, nevertheless we will not touch Cybersecurity in this presentation.

DEFINITIONS (from mentioned standards):

Reliability: ability of a functional unit to perform a required function under given conditions for a given time interval (from ISO/IEC 2382:2015 Information Technology)

Safety: freedom from unacceptable risk (definition from IEC 61508:2010 EEP safety-related systems)

For a company dealing with Reliability/Safety, it is important to work with customers because many companies were creating their own safety tools.

We will show the work done so far.

Main activities for a Model-Based Systems Engineering Tool Supplier are: (i) work with customers, analyse their implementations and merge them (ii) Analyse standards on safety and reliability (iii) Analyse scientific and industrial papers on this topics (iv) look at Research tools e.g. Excel – we are also looking at Model Based tools

It is also key to cooperate with standardization body OMG: in fact OMG is working on a new profile about Safety. OMG SafeML working group – they are standardizing the safety profile. No Magic is part of this group. So there will be an official profile for safety and will be integrated in SysML

SafeML is a SysML profile for integrating safety information with system design information, as an aid to information consistency and communication between development teams and between members of a team. It can be used for:

- tracing from hazards through the safety measures used to the verification steps taken to test those measures; and
- documenting the analyzed hazards and their safety measures to certification authorities.
- communicating from safety engineers to system engineers the hazards that must be

considered while designing to meet requirements, as identified through hazard and safety analysis processes; and

- communicating from system engineers to safety engineers the hazards that the system is designed to manage, including the safety measures used.

The goal of SafeML is to allow the intuitive documentation of hazard and safety analyses results and safety measures in the system model. This can improve consistency between multiple analyses and aid in communicating the results of analyses. SafeML focuses on making this information visible in the system design.

SafeML is designed to be used in conjunction with SysML. SysML provides the diagrams and element types necessary for design modelling, while SafeML provides the element types used to add safety information to the model.

The most popular methods are FMEA (**Failure Mode, and Effects Analysis**) /FMECA (**Failure Mode, Effects, and Criticality Analysis**).

Another method of Analysis is FTA (**Fault Tree Analysis**) and will be available this year in the tool.

Another key Analysis is **Functional safety, risk/hazard analysis**. We will deal particularly with FMEA and Risk/Hazard Analysis.

FMEA (Failure Mode and Effect Analysis) is a method designed to: identify potential failure modes for a product or process, assess the risk associated with those failure modes, rank the issues in terms of importance and identify and carry out corrective actions to address the most serious concerns.

On the other hand, the objective of functional safety Analysis is a design which is free from unacceptable risk of:

- physical injury or
- damage to the health of people either directly or indirectly (through damage to property or to the environment)

The Vertical segments where Reliability and Safety analysis are key are the most mission – and safety critical: Medical, Automotive, Rail, and Aerospace

Whilst FMEA, FMECA, FTA are implemented in all industries more or less in the same way, so it is easy to provide a common solution. On the other way for Functional safety and risk/hazard analysis, each domain has its own standard. See Fig. 1

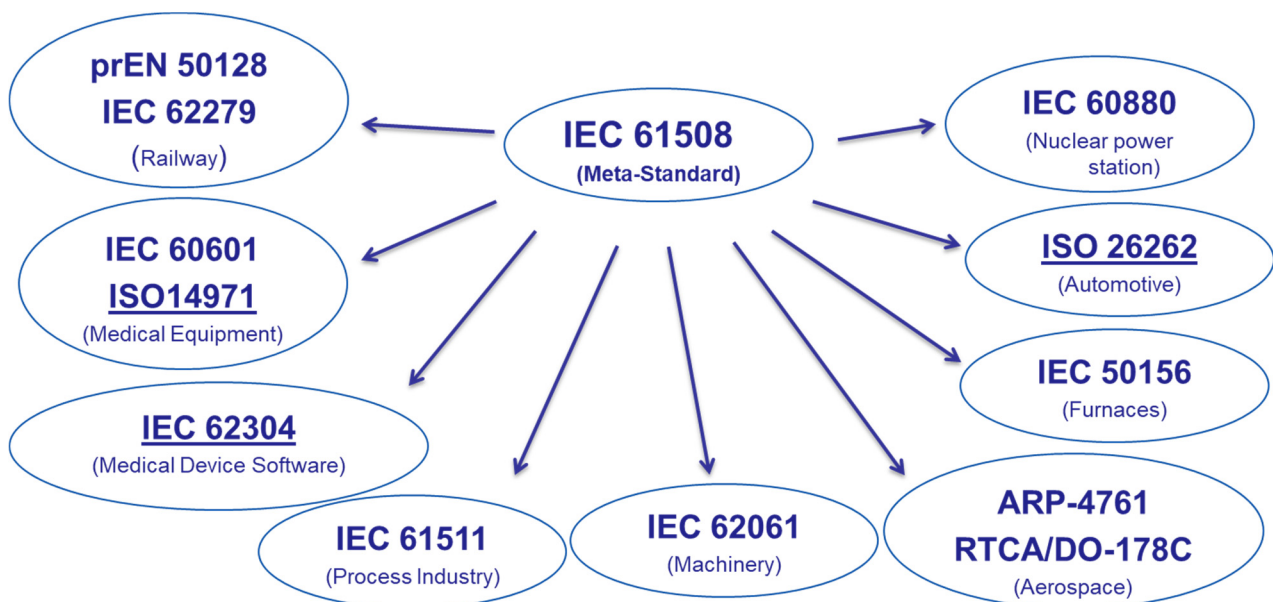


Fig. 1 - Safety Standards by Verticals

Each industry has developed domain specific ISO standards, derived from IEC 61508 that reflect more

accurately the needs and challenges within their domain.

We will show some solution for a specific industry, even if we support all segments.

II. EVOLUTION OF STANDARDS VS. MODEL BASED

Even in segments particularly conservative like DO-178B avionnic certification standard, Model-Based methodology has been introduced by the new version DO-178C.

In fact DO-178B had no explicit provisions about Model-Based techniques, it assumes “structured design”, Maximize Determinism & Visibility, is very weak on Model-Based Design traceability and it is weak on structural coverage application to Models.

On the other hand DO-178C (through its supplement DO-331) allow controlled modelling, bound Model-Based Design acceptability, foster and emphasize overall traceability, emphasize detailed Model Based Design standards, allows credit for some model simulation activities and when using Auto Code Generation.

III. WHY MODELING?

So why modeling? Mil-aero/Medical/Transport applications are among the most complex, most critical and are often mission-critical, safety-critical or both; they are invariably event-driven (real-time), developers model their requirements and designs and have built structured analysis & design models for decades; more recently, have used object-oriented techniques

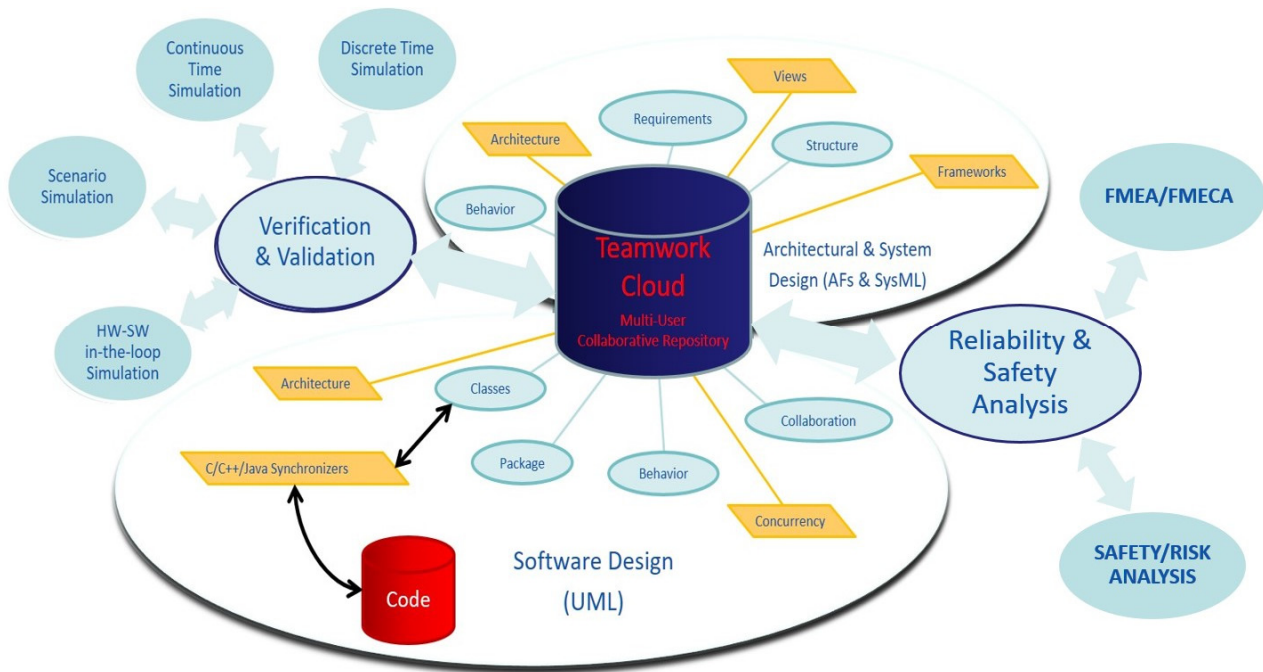


Fig. 2 - Model-Based approach for System Design & Simulation

In a Model-Based environment all data are stored in a Centralized Repository and organized in an easy workable and understandable model. The underlying database allows an instant traceability of all elements using a formal notation like UML mainly for software applications, Architectural frameworks (DoDAF, MoDAF, NAF, UPDM, UAF) for Systems of Systems and SysML for Systems.

In this environment you can build various views of your design, its architecture and can make a really Model-Based Verification & Validation of your model, but not only that, you can really perform a Model-Based Reliability and Safety Analysis of your design, as we will show in this presentation

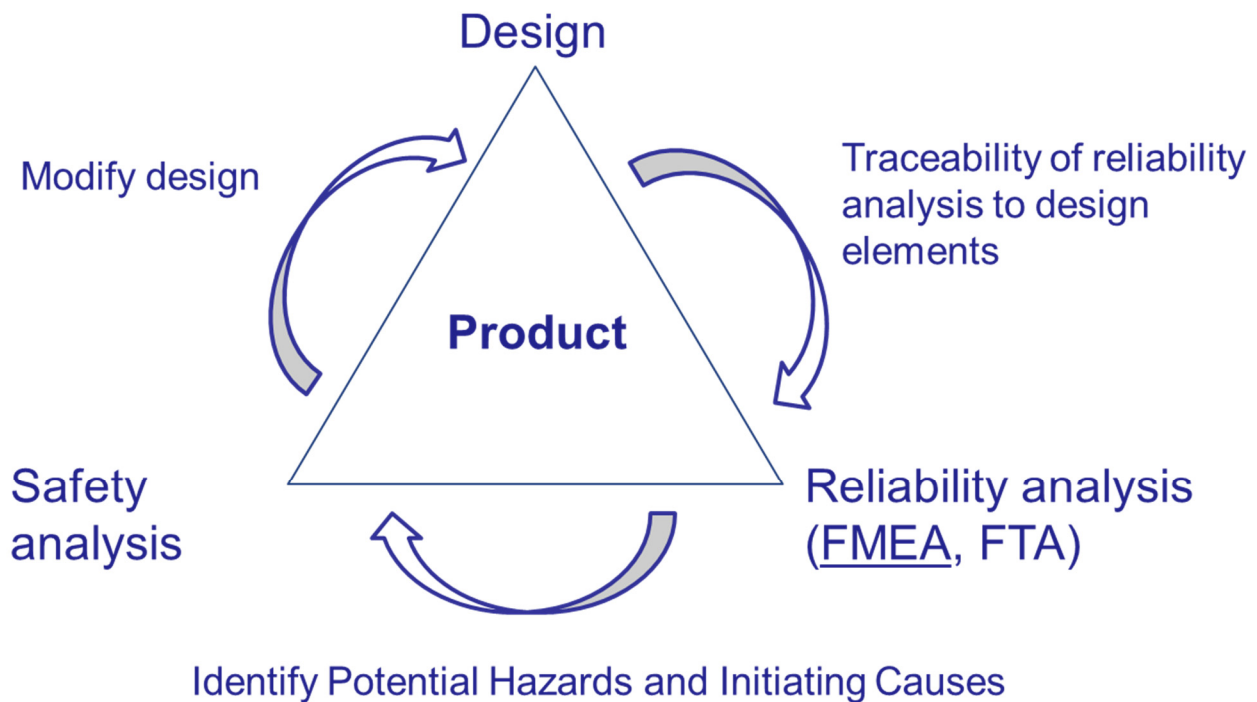


Fig. 3 – Design-Reliability Analysis-Safety Analysis LIFECYCLE

IV. TYING DESIGN, SAFETY AND RELIABILITY ANALYSIS

A simple but very common scenario in Model-Based Testing, used e.g. designing medical devices, starts from MODELING the system, with the Model Based Systems Engineering tool, in this case No Magic CAMEO System Modeler.

There are 2 additional teams working in parallel with the System Engineers.

The first group is the Reliability Cross-Functional Team and the second group is the Safety Cross-Functional Team. Those 3 groups exchange a lot of information among them.

E.g. the Design of an Insulin injection Pump System contains a package called “Design” containing a very simple model of the insulin injection pump system: a Display a Battery, a Beeper, a TVSS, a Dispenser, a Control Module and a Sensor.

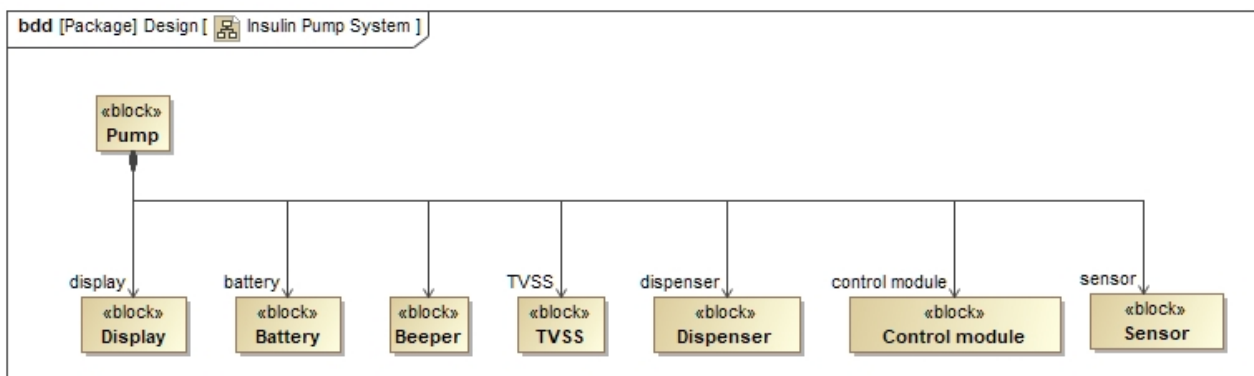


Fig. 4 – Insulin Pump System Structure

The Design team performs the Systems Engineering design and The Reliability cross-functional team performs FMEA and FTA Reliability analysis.

In the model there is another package named “Reliability Analysis”. Expanding that package you can find another one named FMEA. Internally there is

a table called FMEA (see Fig. 5, FMEA Table, folded in 3 parts for a better reading).

An FMEA table allow to analyze the reliability aspect in your design. As FMEA items are text-based, this table provides a convenient way to fill-in FMEA item info using a spreadsheet-like tabular format. Each row in the table represents an FMEA item, but the items are “living” model elements, then they are full REUSABLE. The table columns represent the

properties of each FMEA item in the table. With this table it is possible to:

- Create a new FMEA item directly in the table or import an existing one from your model into the table.
- Directly edit the properties of FMEA items in the table
- Directly generate a failure report, renumber FMEA item IDs or export the table into a CSV or HTML file format







































#	Id	△ Name	Classification	Item	Failure Mode	Local Effect Of Failure			Final Effect Of Failure				
1	F-1	 F1	electrical	 battery : Battery	 Unable to be charged				 Underdose or overdose				
2	F-2	 F2	electrical	 battery : Battery	 Voltage error				 Therapy delay				
3	F-3	 F3	electrical	 battery : Battery	 Unable to be charged				 Therapy delay				
4	F-4	 F4	electrical	 dispenser : Dispenser	 Pumps inaccurate size/rate of dose (including "fail to pump...	 Air in line							
5	F-5	 F5	electrical	 display : Display	 Broken keypad				 Therapy delay				
6	F-6	 F6	electrical	 sensor : Sensor	 Drop in sensitivity	 High glucose-level undetected  Low glucose-level undetected							
SEV	Cause Of Failure			OCC	Prevention Control	Detection Control	DET	OxD	RPN	Hazard Analysis Reference			
4	 Battery degraded			1	 Meter designed to ISO00124	 Charging test 02-1111	1	1.0	4.0	 R-1 Discharged battery leads to coma or death			
4	 Battery depleted			4	 Meter designed to ISO00124		3	12.0	48.0				
3	 Battery overcharged			1			1	1.0	3.0				
4	 Failure to release inside air, lower inside air pressure.			2			2	4.0	16.0				
3	 Incorrect operation			1			1	1.0	3.0				
4	 Battery degraded  Flawed sensor			2			3	6.0	24.0				
Requires Hazard Analysis	Recommended Action			Mitigation		Responsibility	Target Completion Date	Action Taken	Reduced SEV	Reduced OCC	Reduced DET	Reduced OxD	Reduced RPN
<input checked="" type="checkbox"/> true	Add display view to monitor battery charging level			 1 Alarm when battery has sank					4	1	1	1.0	4.0
<input checked="" type="checkbox"/> true	Add display view to monitor battery status			 3 Alarm when battery does not charge a		Barry John	03/15/2016		4	2	1	2.0	8.0
<input type="checkbox"/> false									3	1	1	1.0	3.0
<input checked="" type="checkbox"/> true									4	2	2	4.0	16.0
<input type="checkbox"/> false									3	1	1	1.0	3.0
<input type="checkbox"/> false									4	2	3	6.0	24.0

Fig. 5 – FMEA Table

This table is very similar to a one it is possible to have in Excel or other tools, with the same fields. So the conceptual transition from using a tabular tool to a model based tool is as easy as possible.

Each row represents an analysis item.

An analysis item is composed by various parameters: It starts with an ID, which is unique and customizable in the prefix and in the numbering schema, then it is possible to assign a friendly Name to it. This is not normally needed in Excel, but it is in modeling tool, because the friendly name will be visible in the diagrams. Classification (sometime called “Discipline”) permits to choose among type of failure: electrical, mechanical, software. Then there is the “item”. This is pretty standard and indicates the item that can fail. Typically it is a Part or a Block, but it can be as well a function, an Activity or an Action. To

assign a Part or a Block, an Activity or even a Requirement to the item you can drag and drop items from the Model-tree straight to the table. Then the next parameter is “Failure Mode”. In this particular case: how the battery can fail? It may not be charged.

The next parameters are the “effects”: Local effects of Failure (the effects on the local item) and Final Effects of Failure (the effect on the overall system). Then a parameter evaluates the “severity”, the seriousness of the failure mode: 4 is very high, 3 is a bit lower, but the level grades can be fully customizable according to company methodology.

The column “Cause of Failure” is an indication of a design weakness, the consequence of which is the failure mode. What is really important is that the “Cause”s are REUSABLE, because they are MODEL elements, you can search in the model and find in the

package “Failure Modes” under “Reliability Analysis”. This is very different from what you can do in Excel or other tabular tools. If a new item is added, it is possible to drag the model elements like Cause of Failure, Effects of Failure (Local & Final), Failure Modes, etc.. additionally if the name of any of these model items is changed, it changes in all the model, all the Tables, and everywhere. In Excel it is really difficult to maintain consistency among all elements of the analysis. It is key to have all those elements REUSABLE. You can use them in a new project or in a new version of the project. E.g. if a new version of the Insulin pump is being designed it is expected that most of Causes and Effects come from the previous analysis, so it is possible to automatically check if the previous analysis was exploited well enough.

Next column, OCC, Occurrency, is a property showing likelihood that a specific cause may occur. OCC can be customizable like 1-5 or 1-10.

Then there is Prevention Control (prevention of an occurrence of a failure mode, reusable) and Detection Control (how to detect the occurrence of a failure mode, reusable). Then DET, the rating of the “detectability” of an occurrence of failure mode, OxD, the product of Occurrence and Detectability ratings. Obviously, this property is customizable because every company has its own corporate-defined functions and parameters. Finally, there is RPN Risk Priority Number product of OCC, SEV and DET. Of course, this is also customizable.

In the “Safety Analysis Configuration”, it is possible to set the min and max values of all the above functions and to customize them via JavaScript.

We will come later to the following 2 columns, they are key for a cross-activity of all design and testing teams

Then there are the Recommended Actions (how to reduce a Risk Priority Number) and, very important, Mitigation, where it is possible to establish a link to the Safety Requirements by simply dragging the related requirement from the package “Safety Requirements”.

Finally, there are service properties like “Responsibility”, “Target Completion Date”, “Action Taken” and a set of “Reduced” values of functions (SEV, OCC, DET, OxD and RPN) after Mitigation.

Going back to Fig. 3, “TYING DESIGN, SAFETY AND RELIABILITY ANALYSIS”, we covered Reliability Analysis pretty much, analyzing all Design elements and tracing them to Reliability Requirements and other safety elements.

As said the Safety cross functional team uses their own standards, different for Aerospace, Medical, Rail, Automotive.

Going back to the model there is a package called “Safety Analysis” with a few sub packages, including “Risks”. Inside this package there is the “Risk Table”, see Fig. 6, the Table has been folded in 2 for a better reading.

#	Id	FMEA Reference	Initiating Cause	Hazard	Sequence Of Event	
1	R-1	F-1 F1	Discharged battery leads to coma or death	A Dose	Battery has sank	T
2	R-2		Discharged battery leads to decreased consciousness	A Dose	Battery has sank	T
3	R-3		Discharged battery leads to minor organ damage	A Dose	Battery has sank	T
4	R-4		R4	B Electromagnetic energy(ESD)	(1) Electrostatically charg...	F

Hazardous Situation	Harm	S	P1	P2	P	D	C	PU	Risk	Use Related
The user receives less insulin than required to maintain desirable BG levels	Coma, Death	4	3	4	3.0	1	1	1	High	<input type="checkbox"/> false
The user receives less insulin than required to maintain desirable BG levels	Decreased consciousness	3	3	3	3.0	1	1	1	Medium	<input type="checkbox"/> false
The user receives less insulin than required to maintain desirable BG levels	Minor organ damage	2	3	2	2.0	1	1	1	Low	<input type="checkbox"/> false
Failure to deliver insulin unknown to patient with elevated blood glucose level	Coma, Death	4	2	3	2.0	1	1	1	Medium	<input type="checkbox"/> false

Fig. 6 – RISKS Table

The table reports standard parameters taken into account when dealing with Medical devices.

In the second column, after numbering, there is a customizable Id. Then there is a reference to FMEA Initiating Cause and a Hazard column.

It is necessary to ask the question: what can be a Hazard when designing an insulin pump, e.g. the Dose or the Electromagnetic Energy, etc. As in FMEA, all the concepts expressed in the Risk table are REUSABLE. Therefore, in a company it is possible to create a set of Hazards for cross-corporate use.

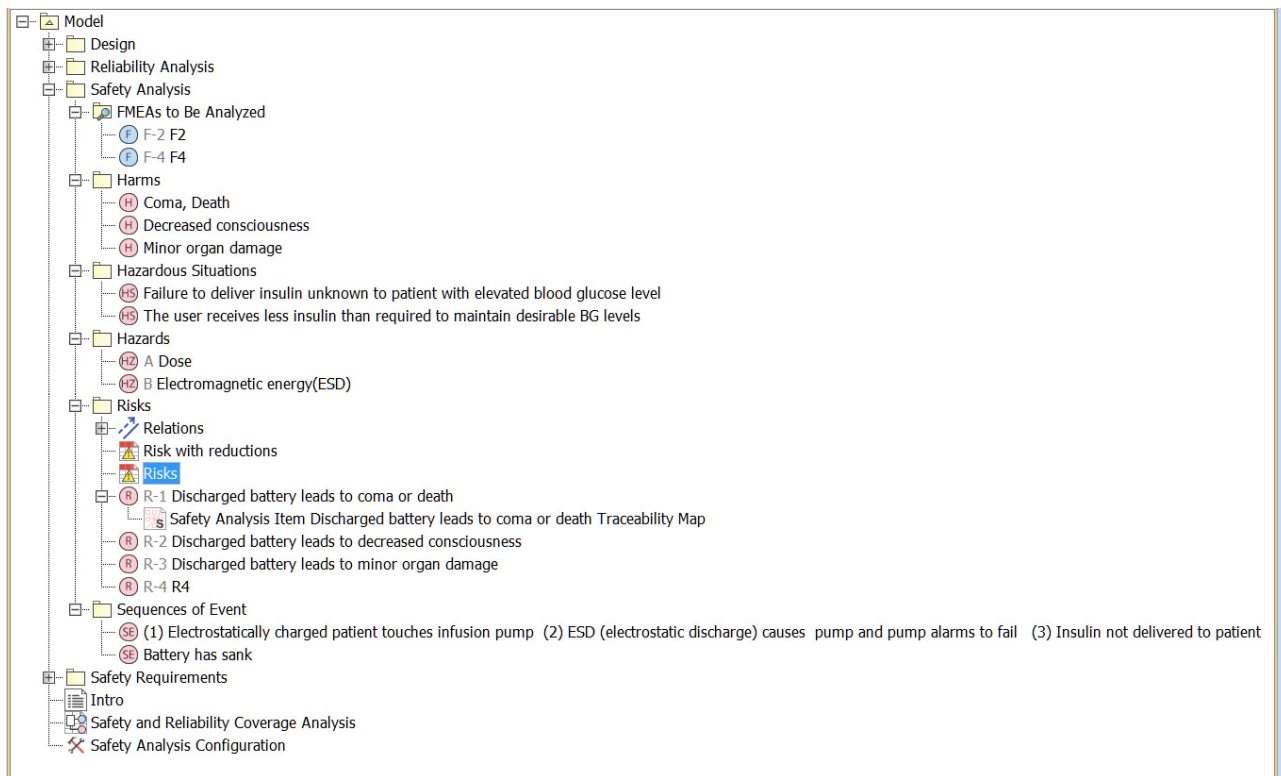


Fig. 7 – Safety Analysis Package

all the concepts are resumed in the Fig. 7. It is possible to see Harms, Hazardous Situations, Hazards, Sequence of Events, containing reusable model elements that can be easily dragged to the Risk Table and reused in other versions of the Insulin Pump design and other new designs.

This is key to maintain a big consistency all through this analysis.

Considering all the parameters and the Harm, it is possible to set a “Severity Level” S, where min & max values are customizable.

Then again, mandated by the standard, there are 2 probabilities, P1 and P2: P1 is the probability that the Cross-Functional Team has a certain Hazard after getting the related “Sequence of Event”. P2 is how likely is a Harm to occur given a certain “Sequence of Event”. P is the product of P1 by P2.

Then there are other parameters:

D, “Detectability”: likelihood of discovering and correcting a hazard or failure mode before it causes a harm.

C, “Correctability” the rate of relative ease of mitigation a certain risk.

PU, “Product Utility” the rate showing the clinical benefits of a product taking into accounts the risks it holds.

Not every company uses all these parameters. If some are not used in the analysis, it is possible to skip them and not show in the Risk Table, because all the columns can be hidden.

And finally the Table shows the Risk, which is automatically calculated as a function and can be customized or just be the product of the previous parameters.

The last column tells if the Hazard is related to how the user uses the device, e.g. he forgets to charge the battery, etc. In the future there will be a link to Use Cases because Use Cases represent HOW the user interacts with the system and in some way in the model that will be an ACTION subject to a risk and there will be a reference directly from here.

Back to the FMEA Table, where the Reliability Cross-Functional Team is performing its analysis, for some items, failure modes can cause failure or consequences like injuries or death.

Therefore, if the Reliability Engineer think that the item requires attention from Safety Cross-Functional Team then can check the tick box.

In this way, the Safety people have a package called “FMEAs to Be Analyzed”. This is a “smart” package: i.e. it shows elements by query.

Why in the Fig. 7 there are 2 items instead of three? Because there is already one risk which addresses this

particular item, so the elements that must be analyzed are only two. In fact in the Risk table there is a back-reference to the FMEA item F1.

Going back to the Risk Table and dragging from “FMEAs to Be Analyzed” package to FMEA reference F-2, then R-2 will appear in Risk Table, Hazard Analysis reference and F-2 will disappear from “FMEAs to Be Analyzed” package. And then there will be only one item left for the review.

It is very easy for Reliability Cross-Functional Team members to see the ticked items that are not covered by an Hazard Analysis Reference. On the other hand the Safety Cross-Functional Team members can easily see what items need attention by looking at the content of the “FMEAs to Be Analyzed” package.

The Table “Risk with Reduction” is useful to determine how to reduce risks.

Some of the risks have been identified, some are high, other medium priority, etc. There is first a column “Risk Control Measures Description” with a brief, qualitative description of the proposed method to control the Risk and then, in the “Risk Control Measure” column it can be created, as in FMEA, it is possible to create reusable safety requirements and here there is a reference to them. E.g. in this case it is possible to install an alarm in the system when battery has sank and the user should recharge the pump.

According to this methodology, there is a package where the mitigation requirements needed, which are ordinary SysML requirements, are created and collected.

Starting from those requirements it is possible to create new model elements satisfying such requirements. E.g. in this case, a “Beeper” block has been created.

Then, after this action, the mitigated parameters, S, P1, P2, P, PU are evaluated again.

In this example it is possible to see that in the first row the risk rating went from HIGH to LOW, so mitigating that risk has been successful.

Going back to Fig. 3 – Design-Reliability Analysis-Safety Analysis LIFECYCLE – there is a very strong link between Reliability and Safety analysis. Also from Safety Analysis new requirements are created and therefore from those requirements new design elements are created which require additional Reliability Analysis that may imply additional Safety Analysis. This can introduce additional design elements and so on going along this full Life Cycle.

It is possible to do all these actions in one single tool which is basically a Model Based Systems Engineering

tool bringing big benefits and AGILITY in the system design.

This methodology provides for another couple of diagrams that reinforce the benefits of conducting reliability and safety analysis in one single MODEL-BASED tool.

One is the Traceability Matrix showing which design elements are covered by FMEA items. E.g. in this table it is possible to notice that “Control Module” has not been covered by one FMEA item, etc. this type of analysis is very difficult to perform in Excel.

Another very important diagram is the Traceability Matrix between the design elements and the Risks, showing which design parts have not been covered by Risk Analysis.

Finally, another important table is the Safety and Reliability Coverage Analysis Table, showing in one table which design elements are covered by Safety Analysis and which are covered by Reliability Analysis. Here you can also see which Safety and Reliability Analysis items are linked together.

So just to summarize the Model-based safety and reliability analysis features are:

- Perform Safety analysis for devices and software (e.g. for Medical according to IEC 62304 and ISO 14971:2007 medical standards, etc.)
- Performing Reliability analysis via FMEA
- Ability to automatically link design to reliability analysis, reliability analysis to safety analysis, safety analysis to design for maximum design effectiveness and Agility.
- Supply of Predefined reports for safety and reliability analysis
- Full customizability allowing the users to add their own data columns and customize risk calculation rules and reports. This allow to create solid corporate safety and reliability analysis procedures and methodologies.

V. BENEFITS OF MODEL-BASED SAFETY AND RELIABILITY ANALYSIS.

It is necessary to spend less effort to demonstrate to the regulatory bodies (e.g. U.S. FDA, Food and Drug Administration for Medical devices, or U.S. FAA, Federal Aviation Administration or European EASA, European Aviation Safety Agency, for Aerospace) that risks are addressed by safety requirements/risk control measures, design elements, critical quality attributes (CQA). In the document world, it is time-consuming and error-prone to validate the document to ensure that

each risk is properly addressed by making changes in the design.

It is possible to easily automate the model validation and the analysis of the design to ensure that the entire design went through safety and reliability analysis. This brings to really reduce time and increase agility of the design in the reliability and Safety design phases and a better management leads to a more precise and EARLY detections of risks and faults and in the end safer design models.

This brings to an increased agility between design, safety and reliability analysis phases: a lot 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 a lot more precise detections of risks and faults and safer, more reliable products.

Additionally, it is ensured shorter safety and reliability analysis through two-way traceability between safety and reliability analyses allowing a better interaction between Reliability and Safety Cross Functional Teams. In practice, separate cross-functional teams are working on safety and reliability analysis and it is important that the Safety Cross-Functional Team can effectively review and analyze fatal faults identified

during the reliability analysis. On the other hand, reliability analysis cross-functional team needs to be aware that fatal faults they identified have been reviewed and addressed by the safety analysis cross-functional team.

VI. REFERENCES

- [1] A. Kossiakov, Systems Engineering Principles And Practice, John Wiley.
- [2] NoMagic, Cameo Systems Modeler User Guide, No Magic Inc.
- [3] NoMagic, Creating a Report Template to Use in MagicDraw, No Magic Inc.
- [4] P. C. Jorgensen, The Craft of Model-Based Testing, CRC Press.