Integrating Safety and Reliability Analysis into MBSE: overview of the new proposed OMG standard

Geoffrey Biggs
AIST
1-1-1 Umezono, Tsukuba, Ibaraki, Japan
+81-029-861-5984
geoffrey.biggs@aist.go.jp

Andrius Armonas
No Magic Europe
Savanoriu pr. 363, Kaunas, Lithuania
+370-652-27762
andrius.armonas@nomagic.com

Tomas Juknevicius
No Magic Europe
Savanoriu pr. 363, Kaunas, Lithuania
+370-686-83427
tomas.juknevicius@nomagic.com

Kyle Post
Ford Motor Company
20000 Rotunda Drive, Dearborn, MI, USA
48124
+1-313-805-0020
kpost1@ford.com

Abstract. Model-Based Systems Engineering (MBSE) is gaining popularity in organizations creating complex systems where it is crucial to collaborate in a multi-disciplinary environment. SysML, being one of the key MBSE components, has a good foundation for capturing requirements, architecture, constraints, views and viewpoints. It allows linking different types of models that come from different engineering disciplines. However, inherent safety and reliability aspects of a system are not addressed by the SysML language. A new group at the OMG has been created by industry experts in this area to address these aspects in a new standard. In this paper, with the intent to get feedback from the systems engineering community, the members of the newly formed group present the current state of the Safety and Reliability Analysis Profile for UML submission, which extends the SysML language with the tools for modelling safety and reliability aspects. This paper also explains the value users get from taking a model-based approach to safety and reliability analysis and integrating it into the MBSE toolkit. Open issues and challenges are also discussed.

Introduction

In 2017, a new group consisting of both industry and academia formed at the OMG to define a new standard profile for UML that addresses safety and reliability aspects of a system. This is an important aspect of systems engineering that the SysML language is not capable of.

A Request for Proposals was published by the OMG in March, 2017. The RFP calls for a UML profile that provides SysML with the capability to model safety information, such as hazards and the harms they may cause, model reliability analyses, including Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA), and use structured argument notation to organize the model and specify assurance cases.

The same group of contributors who created the RFP are responsible for drafting the specification. An initial version of the specification was submitted to the OMG on the 28th of August, 2017, in accordance with the OMG procedure. The group is currently revising the specification to meet remaining requirements from the RFP, bring consistency to the currently-disparate capabilities, and provide greater coverage of industry needs. This is a rapidly evolving piece of work.

At the time of writing, the submission group consists of representatives from 88solutions, Japan's National Institute of Advanced Industrial Science and Technology, France's Alternative Energies and Atomic Energy Commission (CEA), Change Vision Inc., Ford Motor Company, GfSE e.V. (the German chapter for systems engineering, Gesellschaft für Systems Engineering), MITRE, Multi Agency Collaboration Environment (MACE), NASA's Jet Propulsion Laboratory, No Magic, Inc., and oose Innovative Informatik eG. An increasingly-large number of other contributors provide irregular additional feedback and comments vital to producing a specification that covers a number of fields that are related in their approach to safety and reliability but still have important differences.

The need for a standardized UML profile for addressing safety and reliability aspects emerged long ago –group members have seen a number of commercial-grade model-based safety and reliability solution implementations being developed during the recent years and successfully used in practice. Some of the members (Ford, AIST, CEA) already have their own implementations with overlapping feature sets. One of the key goals for the new OMG group is to reconcile these different approaches so that the industry does not need to repeatedly design support for safety and reliability in their tools.

In this paper, we present the current state and content of the draft specification. We also present the potential value of using a model-based approach for safety and reliability analysis. The value is tightly connected to how model-based safety and reliability analysis is tied into existing modeling languages. We provide a small demonstration of utilizing one part of the profile, describing an approach that provides real users with value. We also describe the roadmap for the continuing development of this new profile.

Scope of the specification

In accordance with the RFP, the scope of the new profile provides model-based support for the following activities (OMG 2017a).

- Capturing/creating safety and reliability information in the system model.
- Reasoning on and analysis of this safety and reliability information.
  - directly on the model.
  - indirectly via model transformations to transfer data to and from external tools.
- Visualizing this safety and reliability information.
- Verifying the consistency and completeness of this safety and reliability information.
- Tracing safety/reliability/system information within the safety/reliability information itself as well as to related model elements (e.g. requirements, design elements, parametric models, test cases, and test results).

These are broadly broken down into modelling safety information, modelling reliability analyses, and using a structured argument notation to explain the system model and construct assurance cases. The profile is intended to be used in conjunction with SysML (Friedenthal, Moore & Steiner 2014).

The submission defines "safety" as "freedom from unacceptable risk" (taken from IEC 61508:2010 (IEC 2010)). "Reliability" is defined as the ability of a functional unit to perform a required function under given conditions for a given time interval (taken from ISO/IEC 2382:2015 (ISO/IEC 2015)).

One of the fundamental decisions made by the submission group is to rely on existing ISO and IEC standards. The aim of this group is not to develop a new approach to safety and reliability, nor is it to provide a profile that covers all known safety and reliability analysis techniques. Instead, the profile aims to provide a foundation for the model-based treatment of safety and reliability in a system model, and build on top of that standards-compliant packages for modelling safety and reliability in specific domains.

For safety, the RFP calls for support for at least one of the aerospace (DO-178C (RTCA 2012a) and DO-331 (RTCA 2012b)), automotive (ISO 26262 (ISO 2011)), medical (IEC 62304, IEC 60601-1, and ISO 14971 (IEC 2015a, 2015b; ISO 2007)) and railway (EN 50128 (CEN 2012) and EN 50126 (CEN2017)) domains. These are all mature domains and, with the exception of aerospace, they share a common root for their international safety standards in the IEC 61508 standard. Although there are other domains that are similarly mature (for example, the nuclear domain), limitations on the knowledge and experience of contributors prevented those domains being specifically included. The current draft specification provides explicit support for the automotive domain. The medical domain is also intended to be explicitly supported, and it is hoped that at least partial support for aerospace will be included. Additional domains beyond the four called for in the RFP are able to be supported if a contributor with experience in that domain comes forward; the submission group is not trying to be exclusive but rather prefers to produce a submission with fewer domains now but that can be extended easily, rather than to produce a specification that covers many domains but none of them satisfactorily to the needs of industry. The profile is being structured such that adding support for a new domain is straightforward.

For reliability, the specification aims for providing in-model support for reliability analysis techniques. The RFP requires support for two analysis techniques: Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA). Both have a long history, are well-understood, are widely-used, and have international standards defining the information and processes involved (IEC 61025 for FTA (IEC 2006b) and IEC 60812 for FMEA/FMECA (IEC 2006a)). The submission team considers the availability of a standardized version of a technique important for providing support for a widely-usable variant of that technique in the profile. The RFP makes allowance for additional techniques, and the submission team has already included a package for the preliminary Functional Hazard Analysis technique provided by one contributor.

For a structured argument notation, the specification uses the Goal Structuring Notation (GSN 2011). The submission group considers GSN to be the most widely-accepted visual notation for assurance cases. Its compatibility with the OMG's Structured Assurance Case Metamodel (SACM) specification provides further benefit (OMG 2017b).

Problem being solved and value to users

There are several problems with current approaches to creating, applying and managing the large quantities of information about a critical system. The current methods used are largely textual reports, large tables, specialist analysis reports, and verbal communication. These methods may be ambiguous, can lead to misunderstandings, and do not guarantee consistency, particularly when changes are made to a part of the design or an analysis. Furthermore, these issues make it difficult to perform safety and reliability analyses that are complete, consistent and accurate enough to meet the safety and reliability needs of systems and to ensure that they are compliant with relevant standards and methodologies.

Comparing the problems of the current methods with the relevant capabilities of a model-based approach illustrates several important benefits for safety and reliability engineers as well as systems engineers.

- The imprecise representation of safety and reliability information as text leads to difficulty in linking this information to system design information. In particular, a lack of coherent traceability between inputs and results of analyses, and the safety/reliability features in the system model compromises the consistency of this information and the resulting system.
- Information stored in a single model is easier to maintain in a consistent state. Synchronising document versions is no longer required if all data is modelled and stored in a single model. Similarly, methods such as tracking IDs are no longer needed for traceability.

- Voluminous textual safety data is difficult to parse, cross check, verify and validate. Text has no formal semantics, and so may be interpreted differently by different stakeholders with different training or experience. Modelled information can be searched, cross-checked, and transformed into any display format that suits the data as desired. Rather than being stuck with a particular format, as current methods are, modelled information separates the presentation of data from the data itself.
- The lack of formal semantics for text makes automated processing of safety and reliability information prohibitively difficult, limiting the potential of automated processing tools, such as for identifying faults that still require analysis, identifying the impacts of changes in a safety analysis or system design (impact analysis), calculating metrics over the information, demonstrating to certification bodies that the entire system has been analyzed and all known risks have been managed, and calculating different Risk Priority Number acceptance thresholds for use in the reliability information based on the system information in the same model.
- Unstructured textual reports and custom spreadsheets typically prevent information being automatically transferred between tools, for example transferring the results of a Fault Tree Analysis from the tool used to perform it into the tool used to prepare a certification report. Modelled information can be transformed into and from other formats (although there may be limits due to the content of a particular format), enabling automatic information exchange between tools and eliminating a potential source of errors.
- Safety and reliability information stored in unstructured formats cannot easily be re-used. Companies typically build up a large base of knowledge regarding safety and reliability in their business domain, and this knowledge forms a significant asset. Modelled information can be more readily imported into a new project without error.

Model-Based Systems Engineering is solving these problems and providing these benefits for system design information. However, today's MBSE toolkits focus on the design phase of systems, which is typically performed by the systems engineers. When developing critical systems, safety and reliability analyses are performed in parallel to the design activities. Cross-functional teams consisting of systems engineers, safety engineers, and field engineers gather to analyze potential risks and hazards of the system being developed. The results of these analyses are typically addressed by making changes to the design. This means that the design activities and the safety and reliability activities are highly coupled. A solely design-oriented, unintegrated MBSE toolkit is therefore insufficient for critical systems.

The document-based nature of safety and reliability engineering in contrast to the increasing support for systems engineering using model-based techniques. As mentioned in the introduction, some organizations have already developed model-based approaches in an attempt to solve this problem. Where model-based methods exist, such as the safety modeling capabilities of EAST-ADL (EAST-ADL Association n.d.), they are typically limited in scope to a particular domain or restricted to a particular tool.

The new specification under development at the OMG promises to bring the advantages of Model-Based Systems Engineering to safety and reliability engineering in standardized, integrated tool chains.

Profile structure and content

The profile organization is shown in Figure 1. It contains packages that each focus on one aspect of the profile's goals. They are broadly separated into three top-level packages representing the three areas, safety, reliability and structured argument notation. Forming a foundation for the entire profile is the "Core concepts" package, which contains highly abstract constructs used by multiple packages of the profile. Examples include the "hazard" concept, the "failure" concept, and a relationship linking causes and effects. Several of these concepts are expected to be useful beyond the safety and reliability domains, such as in the security domain (with necessary vocabulary changes accomplished using mechanisms such as stereotyping). This structure is important to ensure that a failure modelled in the safety part of a model is the same entity as that failure modelled in, for example, FTA.

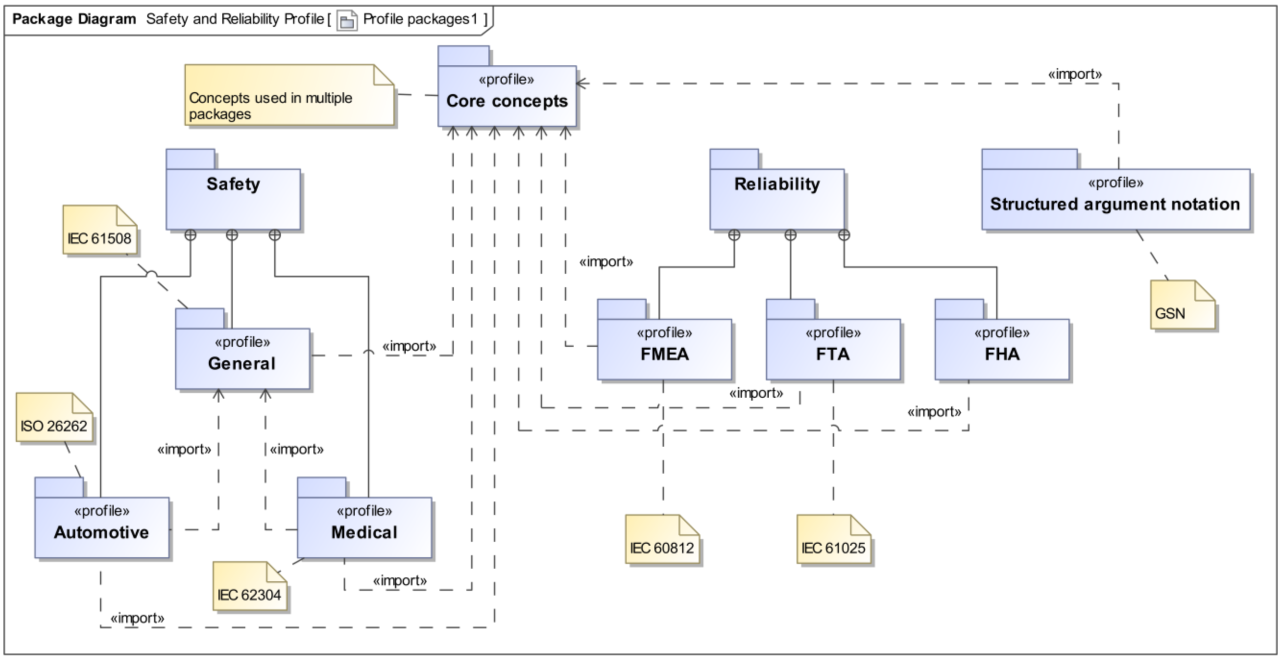

Figure 1. Profile organization

The safety packages are divided up into a generic safety package, which follows IEC 61508, and domain-specific packages for the automotive and medical domains, each of which comply with the standards in their domains, ISO 26262 and IEC 62304, respectively. This structure mimics the standards themselves, which derive from IEC 61508. It provides for the translatability of safety information between domains to the maximum degree possible. This structure also provides a framework into which additional domains can be fitted while maintaining the same level of compatibility as the domains supported in the initial version of the specification.

The reliability packages contain the support for reliability analysis methods. In contrast to the safety packages, the structure is mainly organizational. The concepts reused between packages typically come from the "Core concepts" package rather than being unique to reliability.

Finally, the "Structured argument notation" package sits beside the others, due to its status as a tool for organizing and explaining an integrated system/safety/reliability model.

At the time of writing, the most progress has been made in the automotive package, the FMEA package (used for medical safety), the FTA package, and the structured argument notation package. Current work is focusing on fulling out the core concepts package to provide a foundation for unifying the other packages.

General safety package

Just as the generalized IEC 61508 standard for safety-critical systems sits at the foundation of a collection of domain-specific safety standards, the profile will include a general safety package that provides the foundation for the domain-specific safety packages.

Although the general safety package can be used directly to model the safety-related aspects of a system, its main purpose is to provide two things.

1. A common foundation for the domain-specific safety modelling packages, allowing the movement of information between domains for cross-domain issues. This is particularly important as different domains may use the same concepts with different vocabulary, and a common foundation can provide a way to translate between these.
2. An available foundation on which additional domains with safety concerns, not included in the profile as-is, can be built by users with that need. For example, a tool vendor could build an additional package for the railway domain (for which the EN 50126 and EN 50128 standards are available) by building on the general safety foundation. This both reduces effort to add an additional domain and allows additional domain packages to be compatible with the existing profile packages. Due to a lack of the necessary expertise amongst the submission team members, there are no current plans to add additional domains, but additional domains will be considered if expertise becomes available.

We do not currently have a general safety package based on IEC 61508. At the time of writing, the profile's general safety package is more abstract and does not include all the necessary concepts. The creation of an IEC 61508-based general safety package will be done through the contributions of a contributor with experience in this area, as well as through working down from the abstractions in the "core concepts" package and working up from the domain-specific concepts in the automotive and medical safety packages.

Automotive safety package

The Automotive Safety package contains elements, relationships and diagrams for working with Functional Safety as specified by ISO 26262. ISO 26262 is a risk-based standard derived from IEC 61508. The automotive package is split into the three sections: hazard and risk assessment, safety requirements, and safety related systems engineering elements. The Automotive Safety package is meant to be used in conjunction with SysML as it adds elements to enrich the system model with safety relevant information. An example of this is shown in Figure 2, which depicts a SysML requirements diagram which displays the relations between the safety goals and safety requirements.

This paper focuses on the Hazard and Risk Assessment (HARA) portion of the automotive safety package. The Automotive Safety profile provides additional elements for item definition, safety requirements development, and architecture development which are not shown in this paper.

The HARA related profile elements provide the attributes needed to identify the associated functional risk as indicated by the Automotive Safety Integrity Level (ASIL). The level of risk is denoted by the following: QM, A, B, C, D. The lowest level of risk is represented by QM which identifies that the standard quality management process is sufficient, while an ASIL of D represents the highest level of risk. The output of the HARA is a defined set of Safety Goals with their corresponding ASILs.

The starting point for a HARA is to identify malfunctioning behaviors. One method is to conduct a Hazard and Operability Study (HAZOP) on the high-level behaviors. The profile provides elements to conduct the HAZOP on use cases or functions in a table format (Figure 3), which is typical practice.

In addition to the table format a graphical representation is available (Figure 4) where the guide words are represented as triggering event dependencies. The graphical notation is useful for understanding the relations between the data.

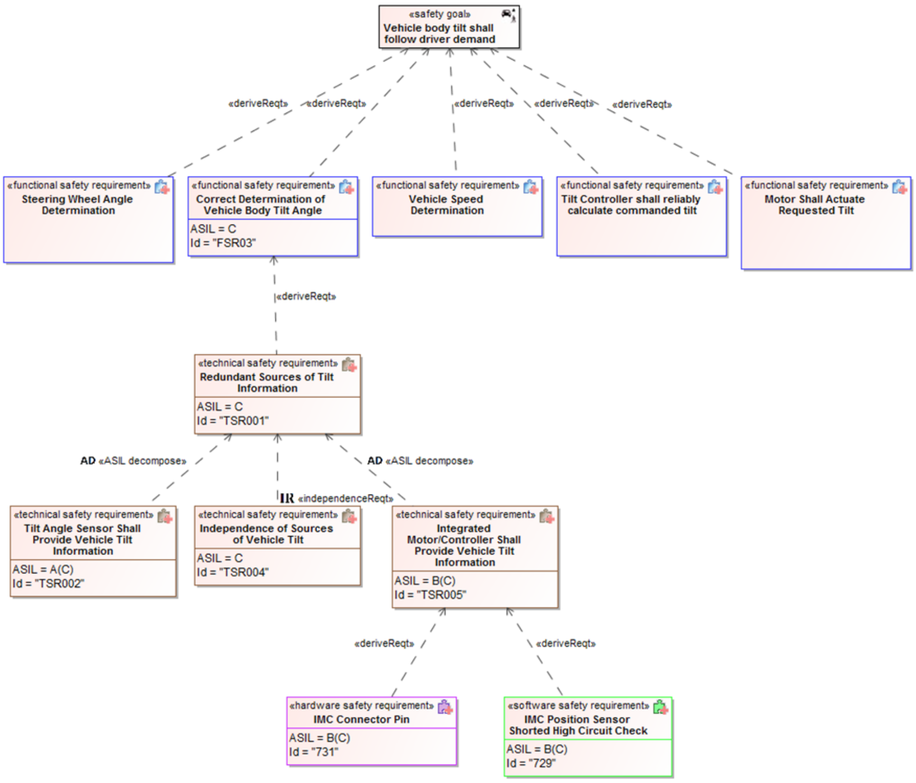

Figure 2. Graphical HAZOP Example

#	Name	Unintended	More	Intermittent	Inverted
1	Tilt the Vehicle	Vehicle body tilts when not required	Vehicle body tilts more than required	Vehicle body tilts intermittently	Vehicle body tilts c

Figure 3. Tabular HAZOP Example

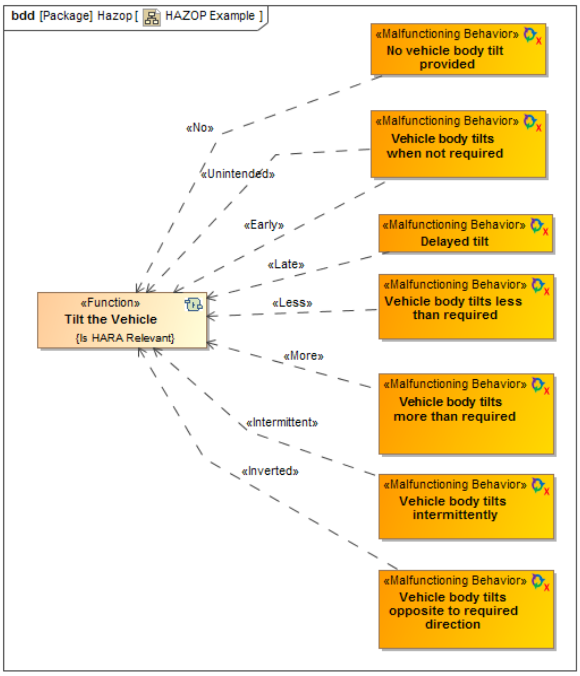

Figure 4. HAZOP diagram

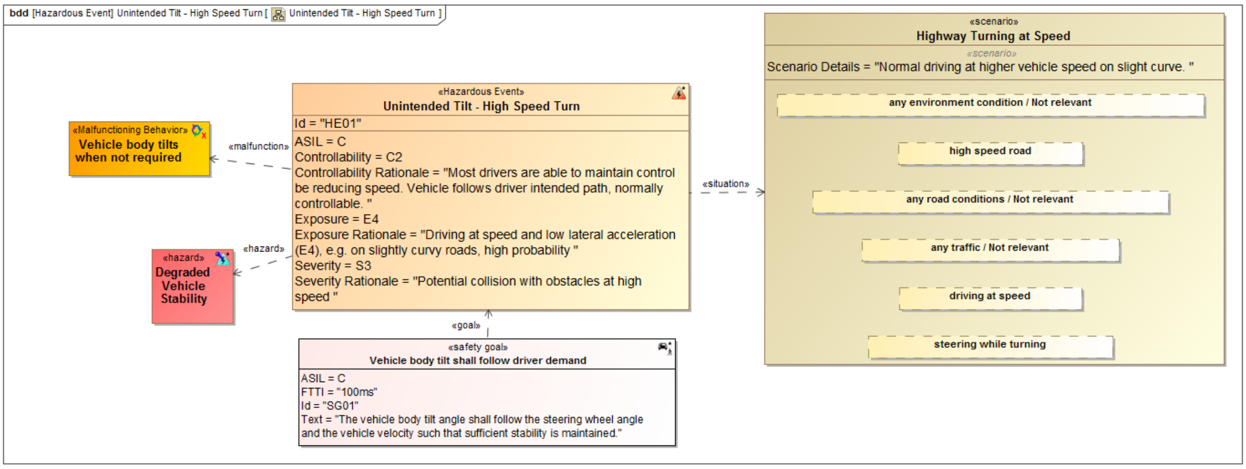

Figure 5. Hazard Analysis and Risk Assessment Diagram

#	Name	Id	Malfunctioning Behavior	Scenario	Hazard	Assumptions	Severity	Severity Ratic
1	Unintended Tilt - High Speed Turn	HE01	Vehicle body tilts when not required	Highway Turning at Speed	Degraded Vehicle Stability		S3	Potential collisi
2	Unintended Tilt - Service	HE02	Vehicle body tilts when not required	Service	Contact with Moving Parts		S2	Vehicle tilts, pc
3	More Tilt - High Speed Turn	HE03	Vehicle body tilts more than required	Highway Turning at Speed	No Hazard	727 Effect of excess tilt	S0	No potential fo
4	Less Tilt - Highway exit ramp with wet surface	HE04	Vehicle body tilts less than required	Highway - Medium traction ...	Degraded Vehicle Stability		S3	Potential collisi

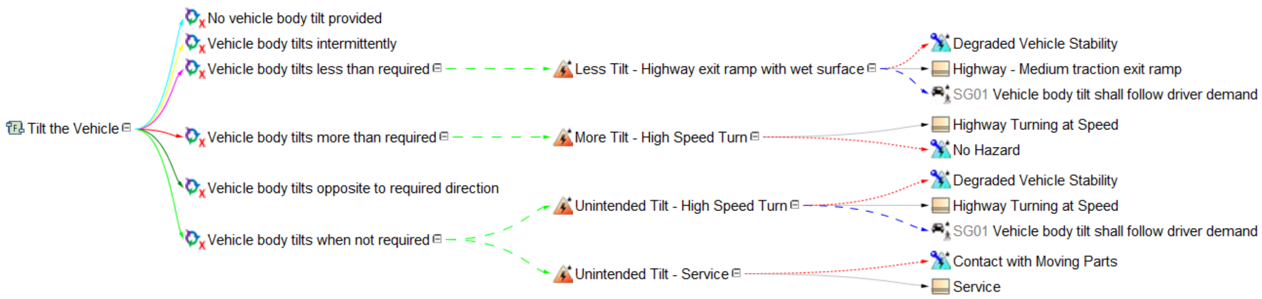

Figure 6. HARA data relationships across multiple hazardous events shown in two display formats (line colours indicate relationship type; legend not shown)

The malfunctioning behaviors identified in the HAZOP are fed into the HARA, combining with operational situations to detail potential hazardous events. A hazardous event is where the ASIL is determined by the severity, exposure, and controllability per ISO 26262. Figure 5 shows the information in a diagram for a single hazardous event. A safety goal is shown along with its relation to the hazardous event. The standard approach to a HARA in industry is to create a table to develop the HARA. This method is also supported by the profile.

By constructing the HARA in a model the data can be reused across various hazardous events and included in libraries to use across projects. Figure 6 shows the same four hazardous events displayed in a table and organized by the relations of the elements. The reuse of the malfunctioning behavior "Vehicle body tilts when not required" can be seen between the two "Unintended Tilt" hazardous events. By displaying the data in graphical form is also easier to see that the two related "Unintended Tilt" hazardous events have different hazards. The "Unintended Tilt" related to service has a hazard of "Contact with Moving Parts" while the "Unintended Tilt" related to highway driving has a different hazard of "Degraded Vehicle Stability".

Medical safety package

The medical safety package contains a simple profile designed to capture the (medical) safety analysis data. It is targeted at users who are performing a medical safety analysis according to the IEC 62304 and ISO 14971:2007 standards in a tabular format, to enable transition to model-centric form. The safety analysis dovetails into reliability analysis (FMEA/FMECA), i.e. failures that can potentially harm the user physically are further analyzed using FMEA/FMECA.

The main concept of the profile is a SafetyAnalysisItem, implemented as a stereotype on UML class. SafetyAnalysisItem represents a single item-of-concern for medical safety analysis. Each item has a link to the initiating FMEA analysis item, and through it the items (parts, blocks, functions, etc.) of the systems model that are being analyzed.

Each Safety AnalysisItem has an InitiatingCause, analogous to an FMEA CauseOfFailure; a SequenceOfEvents, which are events leading to the hazardous situation; a Hazard, a potential source of harm; a HazardousSituation, a situation that has a user exposed to one or more hazards, leading to the potential for harm to occur; a Harm, the actual injury to the person. Each of these items is modeled as (stereotyped) model elements, not just simple text, making them available for automated processing and reuse. Numerical analysis of the safety item is captured in properties.

The medical safety package is in many ways similar to the FMEA package, described below. One significant conceptual difference is that FMEA analysis considers failure as a single step transition, while medical risk analysis has a more nuanced two-step view, requiring a hazardous situation before harm is caused. Due to this, medical safety analysis has two probability numbers where FMEA has just one. The profile will integrate these two approaches to allow the medical and FMEA packages to reuse information between packages where possible.

Once the numerical analysis is complete, counter-measures may be added to the model as necessary. These are risk control measures (requirements addressing this particular risk) and mitigators (system model elements, addressing this particular risk). Their impact on the numerical risk analysis is calculated and added to the model.

Failure Mode and Effects Analysis (FMEA) package

The FMEA package contains a simple profile designed to capture reliability analysis data in a model-centric form. The current industry approach is to perform an FMEA/FMECA analysis in a tabular (Excel-like) document. Moving to a model-centric format gives many benefits, as described earlier.

The FMEA package consists of the main concept, "FMEAItem", implemented as a stereotype on a UML class.

FMEAItem represents a single item-of-concern for reliability analysis. FMEAItem has a relationship to an item in the system model. This represents the item whose reliability is being analyzed; this can by any aspect of the system, such as a block, a part, or a function.

FMEAItem has links to:

- FailureMode, describing in what way the system has failed (e.g. a car lamp does not turn on);
- CauseOfFailure, describing the initiating cause (e.g. filament burnout);
- Local and final EffectOfFailure (e.g. driving at night is hindered); and
- Prevention and DetectionControl.

Note that having these concepts as separate model items allows for libraries, which may be reusable or even standardized. This can simplify FMEA/FMECA analysis for a new system that is similar to systems analyzed in the past. Common types of failure causes can be catalogued for system component types, such as rust for metal components exposed to atmosphere, or tin whiskers for electronic components. Failure modes can be treated in a similar way, such as "valve stuck open" or "valve stuck closed" for systems that include valves.

The FMEAItem has three important characteristics.

- Severity (stemming from Effect); higher values indicate more severe consequences of this failure.
- Occurrence (stemming from Cause); higher values indicate higher probability of occurrence of this failure.
- Detectability (stemming from detection control); higher values indicate that this failure is *harder* to detect.

Note that, depending on company policy, the severity, occurrence and detectability of an FMEAItem can either be strictly dependent on the effect, cause and detection control, or that FMEAItem can override or have its own values. For example, even though the “rust” failure cause may have a standardized value for probability, the FMEAItem for a particular system part may want to specify different, lower or higher probability.

These three characteristics are combined, usually by simple multiplication into a single number – the Risk Priority Number (RPN).

The company then sets a threshold RPN value. Exceeding that value indicates that this FMEAItem has a high impact on reliability and steps must be taken to reduce it that impact. The steps can be anything from changing/adding requirements to a large redesigning of the relevant systems.

After these steps are taken, the FMEAItem can then be updated with reduced severity, occurrence, and/or detectability numbers and the new, reduced RPN can be calculated to ensure that this reliability concern is properly addressed. In the same manner, if a reliability analyst deems the FMEAItem to have an impact not just on the reliability of the system but also on safety, they can mark this FMEAItem as requiring further analysis from the risk analysis team.

Further information on this package is provided in the sample application, described later.

Fault Tree Analysis package

In addition to support for FMEA/FMECA, the profile also supports another major analysis method, Fault Tree Analysis (FTA). The support for FTA is based on the IEC 61025 standard for Fault Tree Analysis. Although, as with FMEA, there are many variations of FTA, by basing our support on this standard we ensure that we provide a form of FTA that is based on best practice and is accepted by practitioners.

The FTA package provides stereotypes for the entities specified in IEC 61025. These are a set of events, shown in Figure 7, and a set of logic gates for joining them, shown in Figure 8.

The FTA package currently provides a pure version of the IEC 61025 standard with no integration with other packages. Although integration with all packages is important, for the FTA package integration and compatibility with the FMEA package is most important. These two analyses are complimentary and are often used together. It is therefore vital for the usefulness of the profile that, for example, an event in a fault tree can be the same model element as a failure in an FMEA. This form of integration will lead to greater consistency in the modelled analysis information and play an important part in the profile’s contribution to increasing consistency in safety and reliability information overall.

FTA has a long history and there are many existing tools available for working with fault trees, especially for performing the calculations necessary for a quantitative fault tree. The RFP has as a goal the ability to import and export FTA information between such tools and the model. No work has currently been done towards this goal, but compliance with IEC 61025 is expected to enable it.

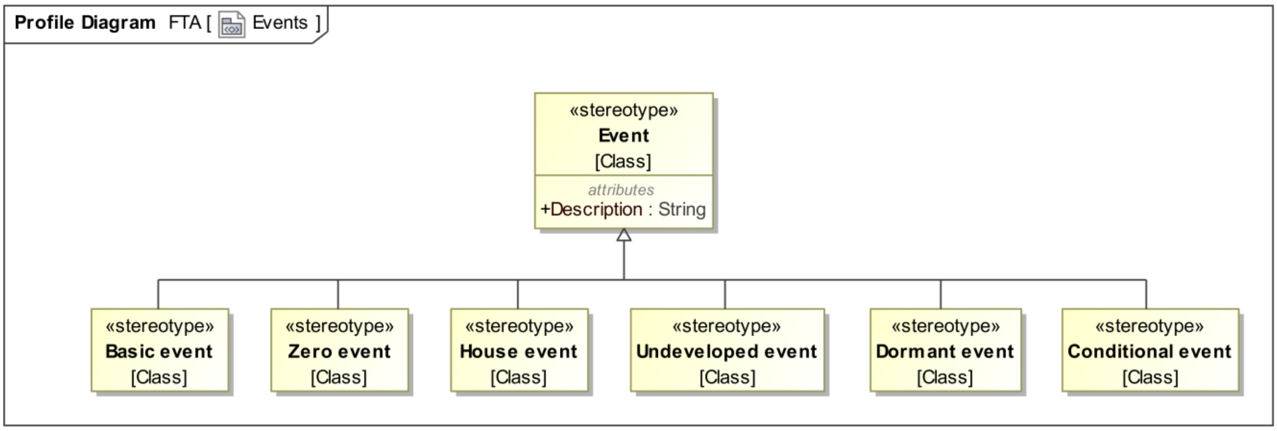

Figure 7. The event stereotypes in the FTA package.

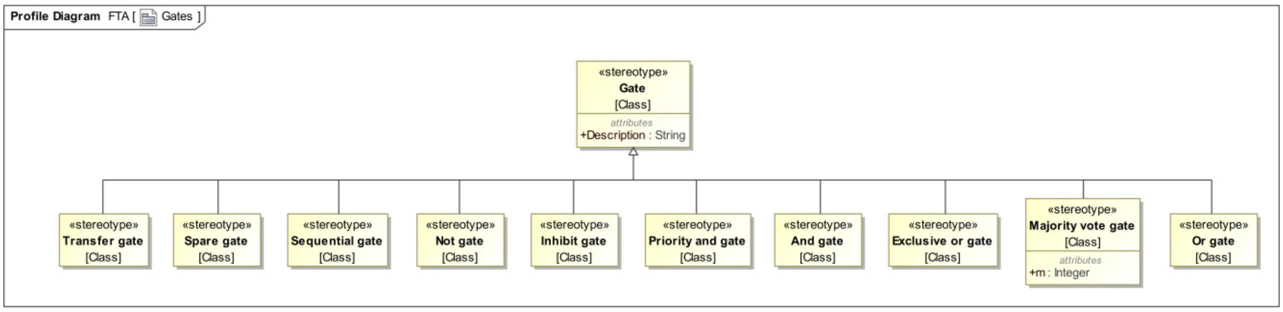

Figure 8. The logic gate stereotypes in the FTA package.

Structured Argument Notation package

The use of structured argument notations, such as the Goal Structuring Notation (GSN) and the Claims, Arguments and Evidence (CAE) notation (Adelard LLP n.d.) has grown in recent years. The ability of these notations to make an argument clear and relatively unambiguous is an important benefit when constructing a safety assurance case. Some have further found that combining a structured argument notation with SysML provides a powerful tool for structuring system models with regards to their safety requirements in a self-explanatory way. For this reason, our profile includes a package to provide a visual structured argument notation.

The notation is currently based on GSN. A package in the profile, "Structured Argument Notation" (SAN), provides stereotypes that can be used to record an argument directly in the system model using GSN. These are shown in Figure 9. Although not yet present in the profile, we also intend to include the correct visual notation for use with these stereotypes, as the visualization of the argument is an important factor in making the argument understandable.

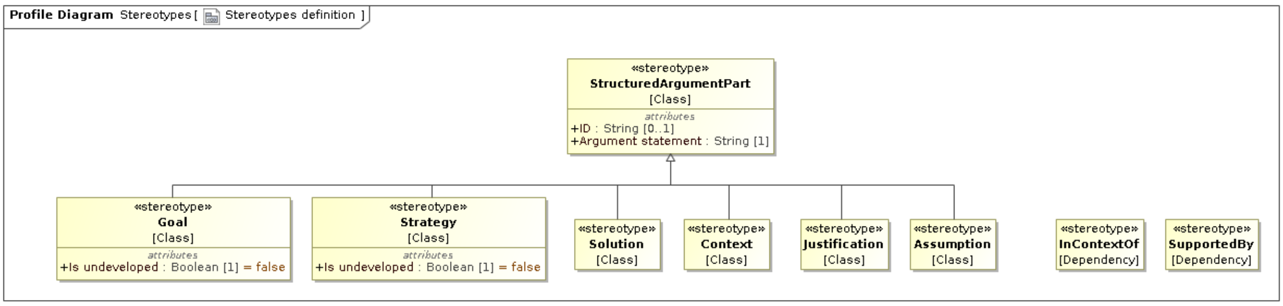

Figure 9. The stereotypes included in the "Structured Argument Notation" package, which allow for including GSN-like structured arguments in a system model.

Fortunately, GSN is a simple notation, despite its expressive power. This makes the SAN package very small when compared with the other parts of the profile. Despite this, it adds a unique capability for modelling explanations that the other packages in the profile cannot provide.

The stereotypes can be used in conjunction with SysML elements to record the "why" of how the system is designed and constructed. Such information is often not included in the model, making understanding difficult without the assistance of documentation external to the model or someone who already has an understanding of the model. Furthermore, through model transforms the information modelled using the SAN package's stereotypes can be transformed into the OMG's Structured Assurance Case Metamodel and from there into input for specialized structured argument tools.

FMEA profile application use case

To demonstrate use of the profile we present an example of performing an FMEA/FMECA. We start with a simple SysML model of a hybrid vehicle (see Figure 10). This model is maintained by systems engineers.

For the FMEA analysis, the cross-functional team working on reliability analysis will analyze all parts of the system to understand how each of those parts can fail, what will be the local and final effects of failure, what are the causes of failure, and what prevention and detection controls are possible. They will also perform a quantitative analysis by identifying severity, occurrence, detectability as well as the Risk Priority Number (RPN) for each failure (see Figure 11).

In the example depicted in Figure 11, the FMEA analysis is performed in a MBSE toolkit and is presented in a tabular form, similar to traditional FMEA tables. Every row represents an FMEA item. An FMEA item has references to other model elements that either come from the SysML model or from a library of reusable FMEA components, such as failure modes, causes of failures, and controls.

In Figure 11, the first row (#1) shows the analysis of the "airbag" part. The FMEA item is directly linked to the relevant SysML model part. This allows for automatically checking which parts have not yet been linked to any FMEA items. For example, if the system model evolves and new parts get added, it is trivial to validate whether or not the FMEA analysis is complete (see Figure 12).

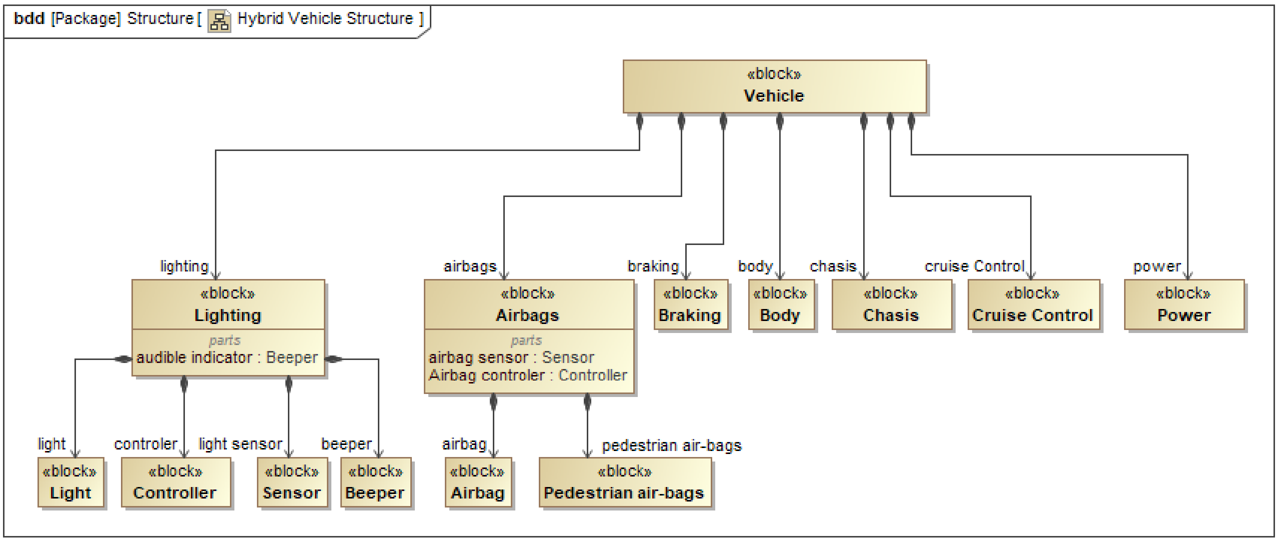

Figure 10. Hybrid vehicle structural breakdown

#	Item	Failure Mode	Local Effect Of Failure	Final Effect Of Failure	SEV	Cause Of Failure	OCC	Prevention Control	Detection Control	DET	OxD	RPN
1	airbag : Airbag	Bag does not open on impact		Injure Passenger	4	Sensor is not functioning properly Broken wire Controller is not functioning properly	4	Designed per material st	Environmental stress tes	4	16.0	64.0
2	light : Light	Light does not turn on	Car inoperable at night Car inoperable under bad weather		3	Battery dead	2			3	6.0	18.0
3	light : Light	Light does not turn on	Car inoperable at night Car inoperable under bad weather		3	Broken wire	2			3	6.0	18.0
4	light : Light	Light does not turn off	Car won't start		3	Short circuit in switch	2			3	6.0	18.0
5	light : Light	Light does not turn on	Car inoperable at night Car inoperable under bad weather		3	Headlight out	2			1	2.0	6.0
6	light : Light	Light does not turn off	Car won't start		2	Operator error (left on)	2			2	4.0	8.0
7	light : Light	Light does not turn on	Car inoperable at night Car inoperable under bad weather		2	Switch broken	2			1	2.0	4.0
8	light : Light	Light does not turn on	Car inoperable at night Car inoperable under bad weather		2	Switch corroded	2	Designed per material st		3	6.0	12.0

Figure 11. Hybrid vehicle FMEA

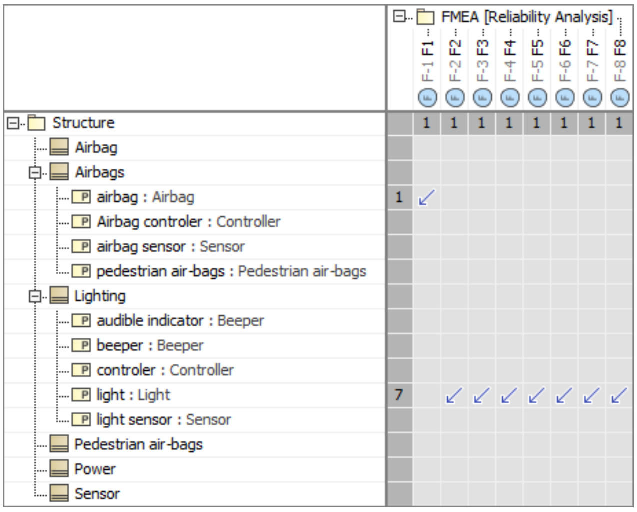

Figure 12. Hybrid Vehicle FMEA coverage analysis

The airbag part can lead to the failure mode “Bag does not open on impact”, which is itself a separate element that can be used not only in an FMEA analysis of the current system, but also in other projects or versions of that system. This is an advantage in comparison to document-based FMEA analysis as reuse is ensured by the modeling environment and no data copying is needed.

“Local effect of failure” is the effect on the component itself, while “Final effect of failure” is the effect of the failure mode on the function as perceived by the customer. Both are reusable elements. There can be many causes for each failure mode, and causes are similarly reusable. The same holds for prevention and detection controls.

Initial values for severity, occurrence, and detectability are taken from final effect of failure, cause of failure, and detection control correspondingly and can be adjusted in this specific context/system. RPN can automatically calculated.

After the highest risks are identified, FMEA items are augmented with information including the recommended action, responsibility, and target completion date. A link is created to SysML requirements which mitigate that risk. For example, in Figure 13 row #1, to mitigate the risk two new requirements are created.

#	Item	Failure Mode	RPN	Recommended Action	Mitigation	Responsibility	Target Completion Date	Reduced SEV	Reduced OCC	Reduced DET	Reduced OxD	Reduced RPN
1	airbag : Airbag	Bag does not open on impact	64.0	Add redundant sensor to monitor impact. Light to notify system is malfunctioning.	1 Impact detect 2 In case of a sy	Barry John	03/15/2016	4	4	2	8.0	32.0
2	light : Light	Light does not turn on	18.0					2	2	3	6.0	12.0
3	light : Light	Light does not turn on	18.0					2	2	3	6.0	12.0
4	light : Light	Light does not turn off	18.0	Redesign: Add audible indicator when driver's d	3 An audible ind			2	2	3	6.0	12.0
5	light : Light	Light does not turn on	6.0	Redesign: add visual lights-on display in console				2	2	1	2.0	4.0
6	light : Light	Light does not turn off	8.0	Redesign: Add audible indicator when driver's d	3 An audible ind			2	2	2	4.0	8.0
7	light : Light	Light does not turn on	4.0					2	2	1	2.0	4.0
8	light : Light	Light does not turn on	12.0					2	2	3	6.0	12.0

Figure 13. Hybrid vehicle FMEA with reductions

1. Impact detection should be based on multiple sensors.
2. In case of a system malfunction, a notification light should be illuminated.

These two new SysML requirements will be linked to the improved design model parts that satisfy these new requirements. The linkage of FMEA items to requirements enables automated FMEA coverage analysis: it becomes possible to check if risks with a high priority number are properly addressed by introducing new requirements and thus parts into the system design, and to quickly find what those parts are and inspect them.

Reduced values for severity, occurrence, and detectability are specified for each FMEA item so that the reduced RPN can be calculated. Having these calculations in the model allows for validating the FMEA analysis, checking whether FMEA items with a high RPN have been properly addressed, and confirming that the new, reduced RPNs are within acceptable limits.

Roadmap

The OMG standardization process requires a final submission to be accepted by the OMG, followed by a one-year "finalization" period during which bugs in the specification can be fixed but no major changes are allowed. We are currently early in the specification development process and, at the time of writing, do not expect to enter the finalization phase prior to the end of June, 2018.

The specification currently consists of a set of disjoint packages that cover most of the requirements from the Request for Proposals published by the OMG. Our next steps involve identifying commonalities between the packages to build out the abstractions to be contained in the "core concepts" package, followed by reworking the other packages to build on these abstractions. We also intend to produce several models to test and refine the profile.

Conclusions

With the increasingly popularity of Model-Based Systems Engineering, it is worth extending the benefits it offers beyond pure systems engineering to other aspects of designing critical systems. Through the application of model-based techniques to the management of safety-relevant system information and safety and reliability analysis methods, the under-development profile described in this paper enables a more automated, less time- and resource-intensive, and above all more trustworthy approach to critical systems design. The profile's packages, with their organization that supports domain-specific information while still enabling the general application of the concepts, will provide engineers dealing with safety- and reliability-related tasks with a broad new toolbox. Furthermore, the use of model-based techniques ensures that this toolbox can be easily extended with new capabilities, and support added for additional domains without compromising the existing ones. Although the profile is still under development, with inconsistencies and overlaps between packages, and the standardization process at the OMG has some time left to go, as the example presented here shows the profile already has much to offer.

References

Adelard LLP n.d., *Claims, Arguments and Evidence (CAE)*, viewed 9 November 2017, from https://www.adelard.com/asce/choosing-asce/cae.html.

CEN, 2012, *Railway applications - Communications, signaling and processing systems*, (EN 50128), European Committee for Standardization, Brussels, Belgium.

CEN, 2017, *Railway applications – The specification and demonstration of reliability, availability, maintainability and safety*, (EN 50126), European Committee for Standardization, Brussels, Belgium.

EAST-ADL Association n.d., *EAST-ADL Association*, viewed 9 November 2017, from http://www.east-adl.info.

Friedenthal, S., Moore, A., & Steiner, R., 2014, *A Practical Guide to SysML*, 3rd edn., Morgan Kaufmann, Waltham, MA.

GSN, 2011, *GSN community standard version 1*, viewed 9 November 2017, from http://www.goalstructuringnotation.info.

IEC, 2006a, *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*, (IEC 60812:2006), International Electrotechnical Commission, Geneva, Switzerland.

———, 2006b, *Fault tree analysis (FTA)*, (IEC 61025:2006), International Electrotechnical Commission, Geneva, Switzerland.

———, 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, (IEC 61508:2010), International Electrotechnical Commission, Geneva, Switzerland.

———, 2015a, *Medical device software - Software life cycle processes*, (IEC 62304:2006+A1:2015), International Electrotechnical Commission, Geneva, Switzerland.

———, 2015b, *Medical electrical equipment - Part 1: General requirements for basic safety and essential performance*, (IEC 60601-1), International Electrotechnical Commission, Geneva, Switzerland.

ISO, 2007, *Medical devices — Application of risk management to medical devices*, (ISO 14971:2007), International Organization for Standardization, Geneva, Switzerland.

———, 2011, Road vehicles - Functional safety, (ISO 26262:2011), International Organization for Standardization, Geneva, Switzerland.

ISO/IEC, 2015, *Information technology - Vocabulary*, (ISO/IEC 2382:2015), International Organization for Standardization and International Electrotechnical Commission, Geneva, Switzerland.

OMG, 2017a, *Safety and Reliability for UML Request for Proposals*, (ad/17-05-05), Object Management Group. Needham, MA (USA), from http://www.omg.org/cgi-bin/doc.cgi?ad/2017-3-5.

———, 2017b, *Structured Assurance Case Metamodel specification version 2.0 Beta 3*, (ptc/17-07-03), Object Management Group. Needham, MA (USA), from http://www.omg.org/spec/SACM/.

RTCA, 2012a, *Software considerations in airborne systems and equipment certification*, (DO-178C), Radio Technical Commission for Aeronautics, Washington DC (USA).

———, 2012b, Model-based development and verification supplement to DO-178C and DO-278A, (DO-331), Radio Technical Commission for Aeronautics, Washington DC (USA).