A component-based methodology to quantify the Safety Integrity Level

Authors: Davy Maes[1], Bey-Temsamani Abdellatif[1], Bjorn Aelvoet[2]
[1] Flanders Make
[2] DANA Holding Corporation

1. Abstract

In the design process of a safety related system, three main steps are necessary: (i) Hazard and risk analysis, which amongst others results in a number of safety functions that have to be implemented, (ii) conceptual design which specifies a design that will implement the safety functions, (iii) evaluation of the safety functions where the Safety Integrity Level (SIL), for example, needs to be quantified (ref. functional safety standard “IEC 26262”). This last step requires considering reliability information of the safety-instrumented system.

Analyzing the current applied approaches that industries follow to quantify the Safety Integrity Level, some issues are observed. First of all, the additional safety information is not structured in the same way as in the design concept. As a consequence, it is difficult to relate the safety information to the different components in the design concept. When design iterations are required, it is hard to know which safety information is affected.

A second issue is the lack of re-use. Although some tools, like FTA (Fault Tree Analysis), offer the ability to specify failure propagation patterns, it was found that such patterns were not used in the failure specifications of the different safety functions.

At Flanders Make, these issues have been investigated in the framework of the industrial project Experimental Validation for Safety Integrity Level (VAL4SIL) resulting in the development of a new model-based safety methodology to deal with the aforementioned issues.

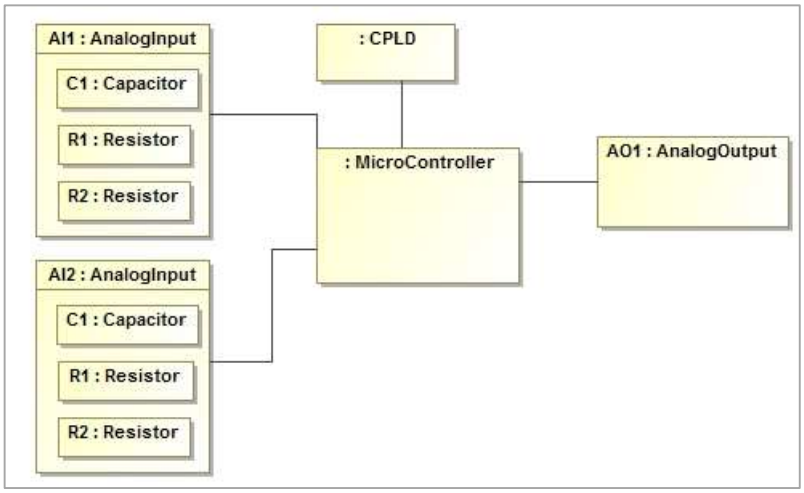
2. SIL quantification – Industrial case

The model-based safety analysis methodology is validated on a use case of Dana Belgium NV of the Off-Highway Systems Group - Dana Holding Corp. The controls department in Bruges, Belgium is entrusted with the development of the control system for a wide range of driveline systems for the world market, and functions as a 'state-of-the-art' research- and development center in the international group.

The use case is a control system of a transmission. The inputs to this control system are (i) a switch to set the gear in forward, neutral or reverse, and (ii) a switch for up and down switching. Two safety functions are defined

(i) Safety functions to prevent an inadvertent up or down shift.
(ii) Safety functions to prevent an inadvertent forward or reverse switch.

In the safety analysis of these safety functions, Dana needs to perform SIL quantification on the control hardware. A simplified system concept for the controller is the following:



Important to note is that the system concept contains a hierarchical decomposition that typically spans more than one decomposition layer. In the example, the system is decomposed in a number of physical components. The AI1 is then further decomposed in another set of physical components.

In the design, two analog inputs, AI1 and AI2, are identified. Typically they share the same design (have the same decomposition). In a typical system modeling language, like SysML (www.omgsysml.org), a generic type concept is used to model this. The definition of this generic type is re-used. In the example, AI1 and AI2 can be considered as instances of the generic AnalogInput (AI) type.

Reliability analysis is done using excel in this use case. For each safety function a separate excel file is constructed. Furthermore, the reliability of each subsystem (1st hierarchical layer) is specified in a separate table. Structuring is done informally by assuming that the Ref column represents a part and the possible failure column represents a failure of that part. The combination of the two must be unique. For each part of the analog input, an overall Failure In Time (FIT) value is retrieved from a reliability handbook (e.g. MIL-217F) (λ_{all}). The failure mode distribution is also retrieved from such a handbook. For each failure, the impact (Impact column) of the failure on the system is estimated. The impact value specifies that the given component failures leads to a dangerous system failure (100% in the table) or to a non-dangerous failure (0% in the table). Additionally a value for the Diagnostic Coverage (DC) is determined. This value tells if the component failure is detected by a separate component/algorithm. Out of bound values for sensors could for instance be detected by a very simple diagnostic check. Based on this information, derived values like the dangerous detected FIT rate (λ_{dd}) are calculated.
The result is shown in the following pictures:

Ref	λall [FIT]	Possible failure	Failure mode distr.	Impact [%]	DC [%]	λsd	λsu	λdd	λdu
R1	2.33	open	20%	100%	0%	0	0	0	0.466
R1	2.33	short	80%	0%	0%	0	1.864	0	0
R2	2.33	open	20%	0%	0%	0	0.466	0	0
R2	2.33	short	80%	0%	0%	0	1.864	0	0
C1	0.7287	short	70%	100%	0%	0	0	0	0.51009
C1	0.7287	open	10%	0%	0%	0	0.07287	0	0
C1	0.7287	drift	20%	0%	0%	0	0.14574	0	0

Figure 1: snapshot of analog input 1 specification for safety function 1

Ref	λall [FIT]	Possible failure	Failure mode distr.	Impact [%]	DC [%]	λsd	λsu	λdd	λdu
R1	2.33	open	20%	100%	0%	0	0	0	0.466
R1	2.33	short	80%	0%	0%	0	1.864	0	0
R2	2.33	open	20%	0%	0%	0	0.466	0	0
R2	2.33	short	80%	0%	0%	0	1.864	0	0
C1	0.7287	short	70%	100%	100%	0	0	0.5101	0
C1	0.7287	open	10%	0%	0%	0	0.07287	0	0
C1	0.7287	drift	20%	0%	0%	0	0.14574	0	0

Figure 2: Snapshot of analog input 2 specification for safety function 2

From the example it should be clear that Excel doesn't have native concepts to represent such hierarchy. At the same time, Excel does not have the 'component' concept that allows one to specify a generic type for the analog inputs as it is done in SysML. There is no re-use between the two analog inputs nor between analyses of two safety functions. When something changes in the system concept, e.g. adding an additional resistor to the analog input type, a corresponding change has to be done at multiple places in the safety excel sheets. The same is true for generic changes in the safety analysis, e.g. updating the overall FIT rates of the resistors with more accurate information from field results.

Additionally, we see that the impact and diagnostic coverage is specified directly on the lowest level, e.g. for each resistor. Doing so, is on the one hand complicated: To estimate the impact of a resistor failure one has to analyze how this failure impacts the system. On the other hand, it also prevents to re-use the resistor specification. Another resistor within the system could have a different impact.

To summarize, analysis shows that the safety information is not structured the same way as the system concept is structured. This makes it difficult to relate changes to the system concept to changes to be done in the safety analysis. This becomes more apparent if methodologies like fault trees or reliability block diagrams are used. The lack of re-using information in the safety analysis is another problem.

3. Developed Model-based safety analysis methodology

To solve the above mentioned problems, Flanders Make proposes to structure the safety information in re-usable components matching the component structure of the safety system design. To demonstrate the concepts, Flanders Make developed a prototype Domain-Specific Tool (DSL tool). At this moment a textual representation was chosen because this is easier to implement than a graphical representation. Figure 3 illustrates the decomposition of a system in parts that are specified as re-usable reference parts, e.g. AnalogInput.

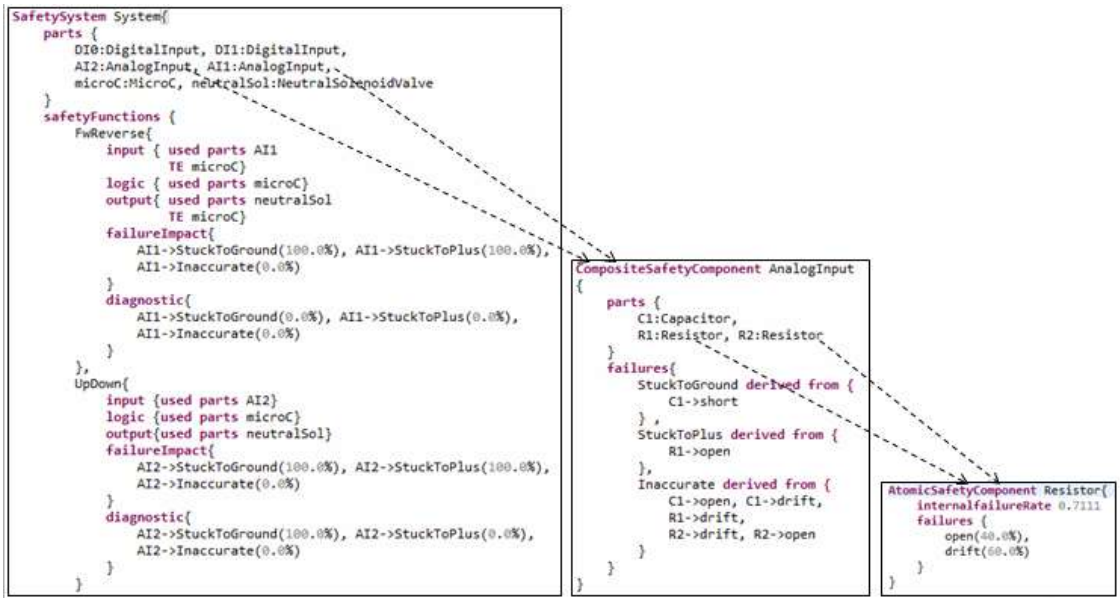


Figure 3: componentized failure specification using a textual DSL

To be able to make use of such a re-usable component structure, one must prevent specifying context-specific information in the re-usable components. Above, one can demonstrate for instance that the impact of a resistor failure depends on the safety function where it is used and thus may not be specified on the resistor component. Instead, the impact must be specified on system level. Having to specify the impact of each resistor on system level would breach our component boundaries. A better alternative is to add the specification of failure propagations to each component. If we specify the propagation of every failure of a component's part to a failure of the component, see AnalogInput example, then we can also re-use this failure propagation. On system level, impact analysis only has to be specified for the direct parts of the system.

If a new resistor has to be added to the analog inputs, only the specification of the AnalogInput has to be changed. This change will then automatically update the safety analysis of all our safety functions where an analog input is used.

The proposed new approach has two benefits. (i) The safety information and the system concept have the same structure. This makes it easy to correlate the safety information to the different parts of the system concept. (ii) The safety information is specified in a re-usable structure. As a consequence it will be much easier to guarantee consistency of the safety information.

The value of the first benefit is difficult to quantify. One way to quantify this is the following. Suppose a change is made to the design concept, how much information of the fault tree has to process to find the corresponding place in the fault tree. Taking the ratio between the original situation and the new approach, a rate of 1/20 can easily be achieved for a small system. This means that with the new approach only 5% of information has to be processed compared to the original situation (100%).

In order to quantify the second benefit, the number of words that are required to specify the reliability analysis are compared between the original method and the new methodology. The results can be found in the following table:

Parts of System	Old method	New method	%
1 analog input	279	308	110%
1 digital input	220	225	102%
2 analog inputs	558	321	57%
1 safety function*	2885	1473	51%
2 safety functions*	5770	1564	27%
*One safety functions exists of: 2 analog inputs, 1 digital input, 1 micro-processor, 1 CPLD, 1 analog output			

Figure 4: comparison of word count

This table shows that for very small systems, there is a slight overhead because of the additional structure that is introduced. However, when the system grows, the re-use offered by the new approach becomes dominant. Note that the entire safety function specification is even bigger than what is shown in the table.

Also note that the safety information is formally written down in a DSL, this allows extensive validation ("well-formedness" of the safety model). This is another benefit of the proposed approach. Example, when specifying the failure propagations of the analog input, the DSL only allows to use failures of components that are part of the analog input which results in an error-free specification.

4. Comparison to FTA's and RBD's tools

In another use case that, for confidentiality reasons is not published, the new developed mode-based methodology was compared with fault tree analysis (FTA) and reliability block diagrams (RBD). Although, tools (e.g. BlockSim) that implement these methodologies natively do have more support to specify reliability information, they have the same limitation regarding structuring the reliability information. They do not structure the safety information in the same way SysML structures the system concept. They also don't have the additional concepts that are required in safety analysis, i.e. impact analysis and diagnostic coverage.

5. Conclusions and future outlook

By analyzing the state of the practice, Flanders Make found that currently used methodologies to do safety analysis are cumbersome. This is mainly caused by the lack of re-usable concepts, mix of context-specific information and different structure of reliability models and concept design models. Each of these problems are tackled by the proposed Flanders Make methodology.

The proposed method has been applied on two example use cases, showing the potential of re-use. Dana Belgium NV is now further exploiting this methodology in their design of new products.

In a new project, Automotive Safety Integrity Level II (ASIL 2), Flanders Make is investigating the application of the core principles to other types of failure analysis, e.g. Failure Mode and Effect Analysis (FMEA). Additionally, a prototype tool with a graphical interface will be implemented.