A SAFETY ALLOCATION METHODOLOGY FOR A NEW TRAIN DEVELOPMENT

Philippe Cozzarin (Rolling Stock Safety Expert), Pascal Guesdon (Alstom Safety Director), Raoul Roland (Train Metier & Solutions RAMS Director)

ALSTOM

SUMMARY

Safety allocation starts from the preliminary design phase and shall be flexible to manage during the earlier phases the inputs from the Design team and the Suppliers and later those coming from the Regulation and the Operators. At the earlier phase, an efficient way to drive the design is to:

- Differentiate allocation and demonstration
  Safety allocation is linked to the risk analysis and evaluation. The Event Tree Analysis (ETA) is an appropriate tool to allocate functional safety requirements whereas the Fault Tree Analysis can be used for demonstration purpose.
- Define at the right level the functional requirements including the expected safety performances
  The Safety Integrity Level (SIL) allocation contributes to the definition of the system architecture. The notion of Risk Reduction Factor (RRF) associated to safety barriers is used. Its link with the SIL removes the need to specify the Safe Down Time (SDT) or latency time when the detailed design is not known.
  The event tree allows going to the right level of the architecture to apportion the requirements of each stakeholder.
- Understand the concept of SIL
  SIL addresses random and systematic failures. Tuning the SDT (to reduce the Hazard Rate and then the SIL) addresses only the random failure requirement but not the systematic failure one. A link between RRF and SIL avoid this misuse.

INTRODUCTION

The Market is more and more competitive and pushes manufacturers to be proactive in order to comply with more and more stringent requirements on cost, delivery schedule, service reliability, new technologies and services. This constant pressure to decrease costs and increase efficiency drives the industry to move to a product oriented approach. A foundation of a product oriented approach is a frozen technical specification including the Safety requirements. A same product can then be integrated in different train level architectures fulfilling the different market needs. Then, sub-systems having robust functional safety requirements can be easily managed at train level through the methodology presented in this paper.

The proposed safety allocation is part of a global risk assessment methodology relying on 10 steps:

- Step 1. Define the System
- Step 2. Identify the potential hazards/accidents
- Step 3. Preliminary Risk Analysis
- Step 4. Set a Demonstration Strategy
- Step 5. Perform a Risk Evaluation
- Step 6. Perform an Hazard Causal Analysis

- Step 7. Confirm the functional independence
- Step 8. Refine the Safety Integrity objectives
- Step 9. Issue the functional safety requirements
- Step 10. Evaluate the compliance with safety requirements (demonstration)

Subsystems contributing somehow to reach an acceptable safety level are managed by Safety Requirements describing all type of measures to be put in place for reducing the severity and/or the frequency until getting an acceptable risk level. One can define 3 families of safety requirements:

- Functional Safety Requirements define a function (sensor, treatment and actuator) that contributes to reduce the risk in a given context. When a Driver action is needed (e.g. ordering the Emergency Brake), the Driver is part of the function.
- Technical Safety Requirements define design constraints (e.g. the locking system on sliding doors shall withstand a force in the opening direction of 1 200 N).
- Contextual/Operational Safety Requirements define a relationship between the system and its environment (e.g. mission profile, staff qualification)

A safety requirement being a safety function contributing to mitigate the risk can be defined at different system levels:

- Railway system level: A requirement defined by the overall line integrator (e.g. to brake to stop the train before the point to protect) is then apportioned to the train (e.g. to brake to stop the train on signalling order)
- At train level: A requirement defined by the Car Builder to mitigate an accident scenario at train level (e.g. to cut-off traction when all doors are not closed and locked)
- At sub-system level: A requirement defined by the designer of the sub-system (e.g. to cut-off HVAC electrical supply in case of too high temperature detected)

Safety requirements are defined in accordance with the Safety Acceptance Principle selected among those set by the European Common Safety Method **[2]**:

- Application of Codes of practices: Compliance with recognized technical standards and rules,
- Similarity analysis with reference system(s): Proven in use approach, comparison with similar systems operated in a similar operating environment with a similar mission profile. This principle considers the non-regression of the safety performance with other in-revenue service products or systems used as reference: it allows the re-use of proven techniques, technologies, equipment or operating & maintenance principles without the requirement for re-doing a complete safety demonstration.
- Explicit risk estimation: Assess the accident scenario with all the mitigation measures (layers of protection) to demonstrate the Safety Target is met. It relies usually on a risk acceptability matrix.

This paper focuses on the functional safety requirement allocation (from steps 6 to 8) including a way to draw and quantify the risk model to allocate functional safety requirements that can be managed efficiently from the design phase up to decommissioning.

1. NECESSARY STEPS BEFORE DETAILED FUNCTIONAL ALLOCATION ACTIVITIES

Functional safety requirements depend on the system analysed, context and operational rules. The first step is to define the system to be analysed, its main functions, performances, interfaces, limits of responsibility and operational characteristics **(step 1. System definition).**

The foundation of the risk assessment (whatever the risk acceptance principle used) is the identification of the hazards/accident at the boundary of the system **(step 2. Identification of the potential hazards/accidents).**

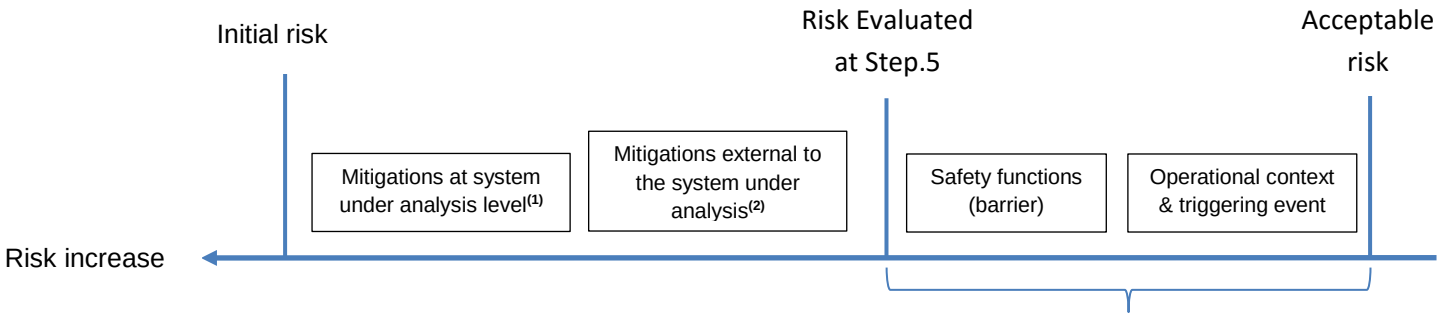
In a deductive approach, the causes that could lead to the hazard/accident are identified (e.g. the failure of sub-systems, functions and interfaces including human error). At the end of this step, the scenario of accident from the initial event (causes) to the accident is defined **(Step 3. Preliminary Risk Analysis).**

The Risk Acceptance Principle, to be used to manage the corresponding Hazard, is selected and the first set of risk reduction means including those managed by other is defined **(Step 4. Set a Demonstration Strategy)**.

The risk is evaluated considering the severity of the accident and the frequency taking into account the risk acceptance principle and mitigations defined at the previous step **(Step 5. Perform a Risk Evaluation)**. When the risk is not acceptable, further risk reduction means need to be defined.

2. SAFETY FUNCTIONAL ALLOCATION

When designing a new system (at conceptual design phase), the preliminary steps allow identifying the scenario of accident requiring detailed analysis to reduce the risk up to an acceptable level. This applies when the risk acceptance principle "explicit demonstration" has been selected. The risk reduction concept is summarized by the Figure 1.

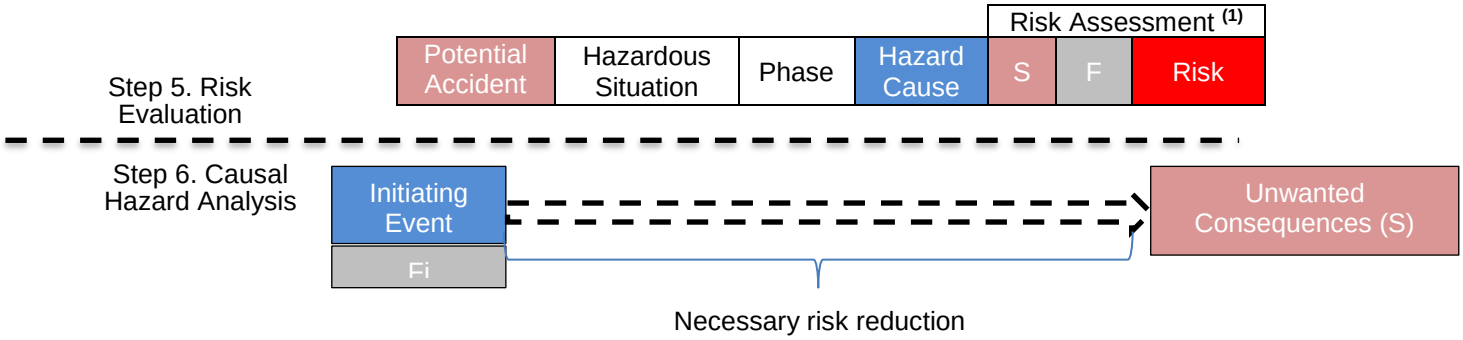


(1) At system under analysis level, the mitigations are mainly those regarding:
- the application of codes of practice principle
- the comparison with similar systems principle
- the safety requirements regarding the hazard cause (e.g. feared event, functional safety requirement)

(2) The mitigations are mainly those regarding operational context and function/barrier independent from the cause

Figure 1: Risk Reduction Concept

The functional safety allocation is anchored to the risk analysis and evaluation performed at the step 5 (Figure 2):
- The cause with the associated frequency is the initial event of the hazard causal analysis
- The potential accident with the associated severity is the credible consequence of the causal analysis



(1) A risk matrix (frequency/severity) is used

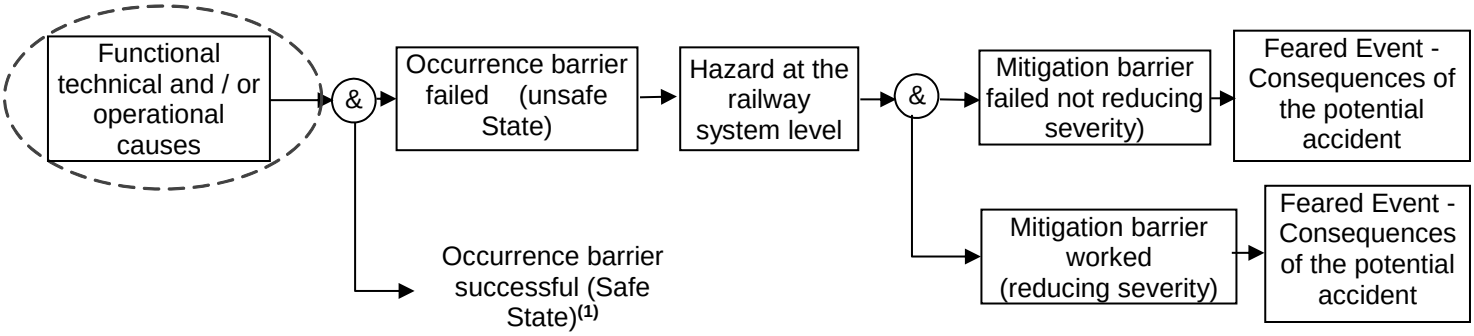
Figure 2: Link between Risk Evaluation and Causal Hazard Analysis

One may identify 2 cases:

- If the failure mode of the system under consideration has a failure rate which associated to the severity leads to an acceptable risk, no further risk reduction needed. In this case the requirement should be a functional failure mode in a defined context.
  However, when a system is complex and integrates several sub-systems (like a train), the definition of a too high level requirement or a hazard at train level is not the right way to allocate the functional safety requirement and manage it. The aim is to get a right level of confidence that for a given hazard, the identified scenarios of accident are under control (not to make a sum of the scenarios leading to the hazard). As stated by CSM **[2]**, "for technical systems where a functional failure has a credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 1E-9 per operating hour". Then, no requirement more demanding than 1E-9/h (or respectively 1E-7/h for critical consequences as stated in CSM amended version **[3]**) is expected.
- If the failure mode of the system under consideration has a failure rate which associated to the severity leads to an unacceptable risk identified at Step 5, additional safety layer of protections (safety functions) and operational context shall be identified and/or defined to reach an acceptable level. The step 6 Hazard causal analysis consists in drawing the risk model by including barriers and also the operational context when applicable. The behaviour and features expected from each layer of protection contributing to reduce the risk is defined, with regard to safety, through a set of requirements.

2.1 To Draw a Qualitative Event Tree

An Event Tree Analysis is an efficient way to model the scenario allowing to share with others (like Operator, System Engineering and Suppliers). This analysis is performed in parallel to the risk evaluation. Each event in series shall be independent. These Events are placed in order to respect the logical way of the accident scenario allowing a holistic view of the sequence of events. The scenario is drawn from the initiating event leading to the accident (domino effect) taking into account the different Safety functions/barriers and context. Drawing an event tree pushes to think about existing or new barriers/safety functions and to define their functional performances (e.g. response time).



(1): usually the paths leading to a safe state are not represented.

Figure 3: Qualitative Risk Model Represented by an Event Tree Analysis

The Event Tree shall be drawn before the architecture is frozen. It is an iterative way of working until the architecture and the Event Tree are finalized with the functional safety requirements and associated assumptions defined. At this phase of the project, the aim is to get a safe architecture which is a foundation for the further safety activities.

It is necessary to split functional failures leading to a hazard (e.g. train speed displayed lower than the real speed) from those which do not lead directly to the hazard but reducing the risk (e.g. loss of fire detection). If one function is clearly identified as a barrier (not a "cause" defined at risk evaluation phase) it cannot be the initial event like the fire detection. If there is no possibility to identify one barrier (both functions being either cause or barrier), 2 scenarios can be drawn using as a cause the failure mode of the 2 functions.

Operational context is also modelled. When applicable, the analysis shall take into account the combination of the probability of the operational mode and the technical hazard. For example when taking credit of a function which is considered as safety related regarding evacuation the model should consider the functional failure and the probability to be in an evacuation mode through an "AND" gate (i.e. in series in the event tree).

2.2 To quantify the Event Tree

The quantification of the event tree consists in the derivation of the HR of the initial event up to the final event (i.e. the accident). HR being defined per hour or kilometre, the derivation is done by using the Risk Reduction Factor (RRF) which is a non-dimensional figure.

The RRF represents the efficiency of the barrier in mitigating the risk. It can be seen as a probability that a safety barrier fulfils its expected behaviour in mitigating correctly the risk. RRF can be seen as the inverse of PFD (Probability of Failure on Demand) as introduced in the IEC61508 [1].

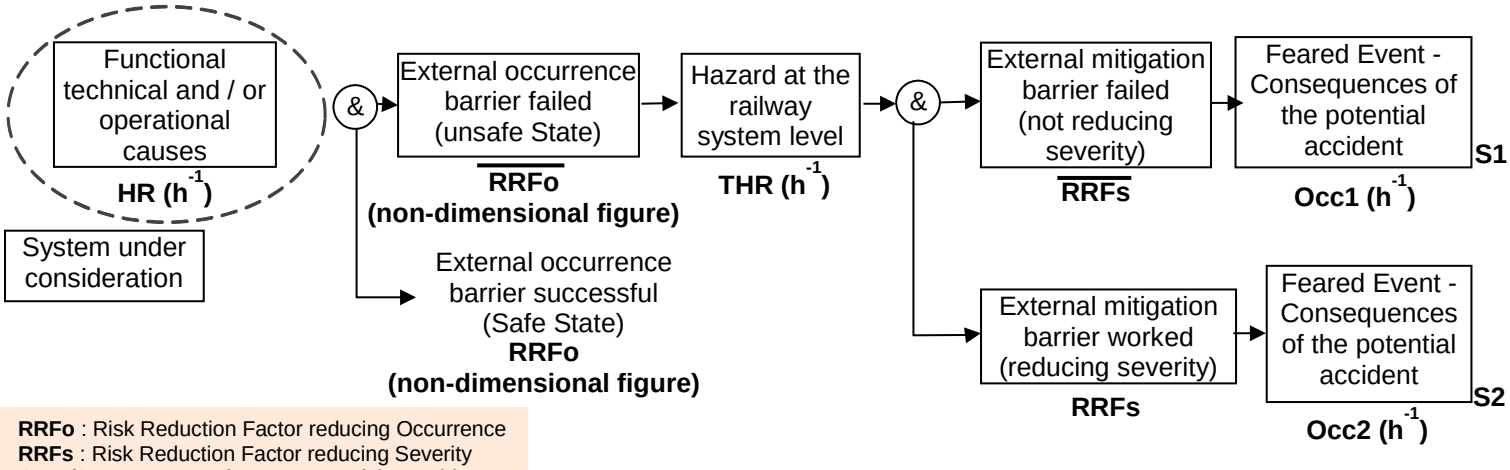
RRF comprises the aspects of HR and SDT of the Barrier, therefore at design phase, they may vary as long as the RRF is reached. When designing a new system, defining architecture without specifying the SDT provide degrees of freedom and prevent issues at later project phases.

Deriving the SIL allocated to the functions implementing the Barrier from the RRF, covers the systematic and random failures. In this case, SIL allocation relies only on a quantitative approach (no need of specific rules regarding combinations of SIL functions). Changing the SDT does not affect the allocated SIL. The SIL allocation is no more relying on the assumption taken on SDT. One can remark a very short SDT (e.g. 1s detection time) leads to allocate a very permissive SIL. This approach forbids claiming that it is possible to reach a target at 1E-9/h with two redundant SIL0 functions.

Hazard Rate (HR) [event / hour]	Risk Reduction Factor effectiveness (RRF)	Safety Integrity Level (SIL)
$10^{-9} \leq HR < 10^{-8}$	$10\,000 < RRF \leq 100\,000$	4
$10\text{-}8 \leq HR < 10\text{-}7$	$1\,000 < RRF \leq 10\,000$	3
$10\text{-}7 \leq HR < 10\text{-}6$	$100 < RRF \leq 1\,000$	2
$10\text{-}6 \leq HR < 10\text{-}5$	$10 < RRF \leq 100$	1
$10\text{-}5 \leq HR$	$RRF \leq 10$	Basic Integrity

Table 1 : HR or RRF versus SIL Correspondences

The qualitative risk model (Figure 3) can be easily quantified:



RRFo : Risk Reduction Factor reducing Occurrence
RRFs : Risk Reduction Factor reducing Severity
Occ1/2 : Frequency of occurrence of the accident

Figure 4 : Quantitative Risk Model Represented by an Event Tree Analysis

The HR of the initial event shall be controlled. If it is not the case (e.g. due to an external cause not controlled), the hazard shall be assumed permanent and the failure of the barrier has to be considered as the actual hazard to be prevented.

The efficiency of the barriers in reducing the hazard rate is expressed by the formula:

Equation 1: $$THR = HR \times \prod_{1}^{n} \frac{1}{RRFon}$$

With $RRFo_n$ the Risk Reduction Factor of the n **independent barriers** implemented to reduce the occurrence of the hazard/accident coming from a functional technical and / or operational cause.

One can deduce the 2 equations to be resolved to reach an acceptable risk level for the risk model defined by the (Figure 4):

Equation 2: $$HR \times \frac{1}{RRFo} \times \frac{1}{RRFs} \leq OCC1$$

Equation 3: $$HR \times \frac{1}{RRFo} \times \left(1 - \frac{1}{RRFs}\right) \leq OCC2$$

One the equations are known, the weight of each event contributing to reduce the risk is defined and the frequency of the potential accident/hazard is calculated starting from:

- Frequency of Initial Event (HR) coming from the step 5.
  Pay attention that having a too high frequency of occurrence for the initial event (higher than 1E-4/h) leads to stringent safety requirements when using the RRF to allocate the SIL. Then in this case the safety function/barrier should be considered as the initial event and the SIL defined in accordance with the HR refer to Table 1.
- The severity coming from the step 5.
  The acceptable occurrences of the potential accident (OCC1/2) are defined from the risk matrix using as input the severity.

Once having defined the context event probability, it is possible to apportion to the barriers an integrity requirement in term of RRF. This RRF is defined from 1 to 100 000 and the link with SIL is defined by Table 1.
One can deduce the RRF from the result without safety barrier and the target occurrence (RRF = HR/OCC x context probability).

Even if a conservative approach leads to consider no risk reduction for a context (100%), they shall be represented in the Event Tree in order to provide confidence on the model and avoid further unfruitful discussions (e.g. percentage of time the train is crowded).

2.3 To Compare Result with the Target

The quantification of the risk model integrates inputs from the stakeholders and order of magnitude coming from return of experience. It is an iterative way of working to get the more efficient solution including the economical aspect.

Then, when the target is not reached the further actions are to:

- Analyse how the scenario of accident has been managed on previous project/application to ensure the risk acceptance principle “explicit demonstration” is the right one and the model drawn is correct
- Get valuable inputs from the suppliers to update the model and the quantification
- Be more stringent on the frequency of initial event
- Be more stringent on the risk reduction factors of the safety functions/barriers
- Define additional safety functions/barriers
- Define additional operational constraints

The choice of the lever will depend on the cost and cycle impact at project level.

Once the target is reached the functional safety requirements are defined and recorded in the Hazard Log.

2.4 To Confirm the Functional Independence (Step 7)

The mandatory condition to demonstrate safety is at this stage, to make sure that all items and sub-systems identified and contributing into the ETA model will not fail simultaneously (e.g. due to single failure/common failure mode).

Common hardware and software failure mode shall be both analysed during design phase in order to confirm absence of simultaneous failure of several sub-systems/components taking into account in series in the event tree drawn. If not the SIL of the overall function shall be allocated to the development of each sub-system/component function.

2.5 To Refine the Safety Integrity Objectives (Step 8)

Safety barriers (functions) could be apportioned into different sub-functions when several sub-systems are involved. The apportionment process started during the risk assessment and evaluation phase stops when each apportioned function (product) is no more under the design authority of the Integrator.

A function C is performed by a function “A” relying on 2 sub-functions “A_1” and “A_2” and an independent function B is modelled as follow:

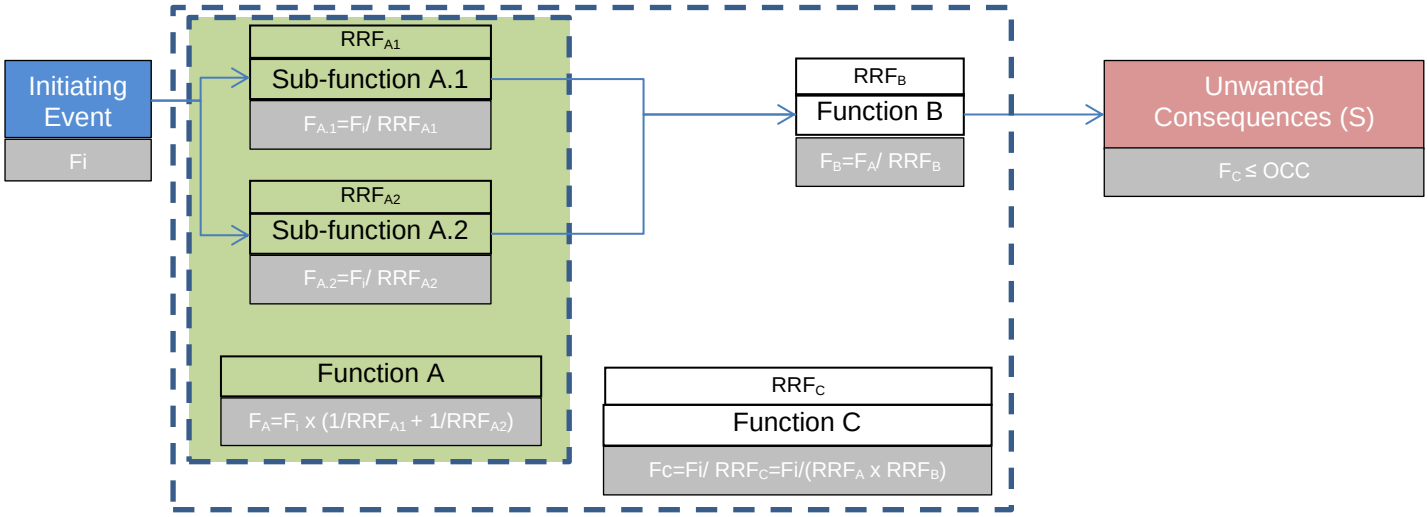


Figure 5 : Apportionment to Sub-Functions

The apportionment from a high functional requirement to the lowest level of functional independence where SIL is allocated based on RRF or HR (Table 1) is easy and based only on quantitative calculation,

2.6 To Issue the Functional Safety Requirements (Step 9)

When a function contributes to reduce the risk of several scenarios, the more stringent requirement in terms of HR, RRF and SIL must be applied to that function.
Then, the function shall be defined by an action verb. In order to get the right level of confidence on the capability of the function to mitigate the risk as expected, the functional safety requirement shall include:

- the input, treatment and output
- the technical performances expected (e.g. time response)
- SIL (for E/PE implemented functions)
- random targets (HR and RRF)

Previous drifts lead to allocate directly SIL to software without defining any particular function (sometimes miscalled Software SIL). It does not contribute to reduce the risk given no safety requirement on safety related functions if any. Software is part of a safety function which includes also the E/PE hardware, “sensor” and “actuator”. The definition of the function protecting against the realization of a given hazard scenario is a key to:

- get the right commitment from the owner
- design it
- validate it
  - by tests (technical performances),
  - by applying a robust process (systematic failure)
  - by performing probabilistic demonstration (random failure)
- manage its performances up to dismantlement

The evaluation of compliance with RRF requirement (demonstration - Step 10) uses the formula below [1]. Specific software tools allow performing this calculation like the HR one.

Equation 4: $$\mathrm{RRF}_{avg} = \frac{T}{MDT(T)} = \frac{T}{\int_0^T Usf(t)}$$

With,

- T = Proof Test Interval (SDT or latency time)
- MDT(t) = Mean Down Time
- Usf(t) = Instantaneous unavailability

One can deduce the RRF for a configuration 1oo1 and 1oo2:

- 1oo1 => Equation 5: $\mathrm{RRF}_{\mathrm{avg}} = \frac{1}{\lambda \times T}$
- 1oo2 => Equation 6: $\mathrm{RRF}_{\mathrm{avg}} = \frac{3}{\lambda_A \times \lambda_B \times T^2}$

A RRF target set at 10 000 and then leading to a SIL3 requirement for a function relying on an E/PE system by using the Table 1, can be demonstrated by a λ=1E-5/h and a proof test (T) performed every 10h (daily test at the beginning of the mission).

CONCLUSION

At the earlier phase of a project, defining functional safety requirements allow to set-up a lean architecture and to take credit of the performances of the sub-systems already on shelf. The risk model is drawn in an iterative way mixing top down approach and bottom up one. Regarding Safety, the effort can be put on several functions and the optimum regarding cost cannot be reached when applying only a top-down approach. It is efficient to build the event tree first with the standard functional performances of the sub-systems (should be communicated and part of the technical description with the associated Safety Related Application Conditions if any).

During the design phase up to the beginning of the commercial operation, a direct link between the functional requirements and the risk model allows easy updates and proactivity. Then, the event tree analysis can be handed over to the Operator to ensure each scenario remains acceptable and to assess the safety issues identified in operation.

SIL allocation is a team activity. It is not a task of an expert independent from the product development. The involvement of all the actors is needed (e.g. system engineer). Then, communication is a key and the rules shall remain easy to apply. Every Event Tree can be modelled by a Fault Tree (historically a demonstration tool) however the Event Tree, and the use of the notion of RRF, allows to:

- Segregate the cause (initial event) from a barrier,
- Model the scenario in a sequential way which is easier to share and challenge by other stakeholders,
- Allocate SIL without specifying the proof test interval,
- Avoid misuse such as allocating a SIL0 based on too short test interval,
- Update event frequency and scenario based on return of experience.

NOMENCLATURE

CSM: Common Safety Method
E/PE: Electronic/Programmable Electronic
ETA: Event Tree Analysis
HR: Hazard Rate
RRF: Risk Reduction Factor
SDT: Safe Down Time
SIL: Safety Integrity Level

REFERENCES

[1] IEC61508-6 Clause B.4.4
[2] REGULATION (EU) No 402/2013 of 30 April 2013
[3] REGULATION (EU) No 2015/1136 of 13 July 2015