Safety integrity level allocation shared or divergent practices in the railway domain

Kiswendsida Abel Ouedraogo, Julie Beugin, El Miloudi El Koursi, Joffrey Clarhaut, Dominique Renaux, Frédéric Lisiecki

PARIS
2 ▶ 7
OCTOBER
2016
INTERNATIONAL
RAILWAY SAFETY COUNCIL

SAFETY INTEGRITY LEVEL ALLOCATION SHARED OR DIVERGENT PRACTICES IN THE RAILWAY DOMAIN

Kiswendsida Abel Ouedraogo, Julie Beugin, El-Miloudi El-Koursi
Univ. Lille Nord de France, F-59000 Lille, France
IFSTTAR, COSYS, ESTAS, 20 Rue Elisée Reclus – BP 70317 – 59666 Villeneuve d'Ascq Cedex, France

Joffrey Clarhaut, Dominique Renaux
University of Valenciennes. LAMIH, Le Mont Houy, 59313 Valenciennes, Cedex 9

Frederic Lisiecki
EPSF, 60 rue de la Vallée, 80 000 Amiens

SUMMARY

In the E.U, safety railway system design and operational terms are governed by directives, regulations, decrees, standards to ensure the safety of the global system. However, based on its own technical and operational concepts, each state member of the E.U. has developed its own safety rules. By the way, this situation results in divergent practices and develops a need to harmonize methods and rail safety targets through the adoption of Technical Specifications for Interoperability (TSI), the definition of Common Safety Targets (CST) and the definition of a Common Safety Method (CSM). Through a risk management process, the residual risk reduction implies to allocate safety targets for each various parts of the railway system with SIL (Safety Integrity Level). After identifying specific uses of SIL allocation, the authors present some consultation results. These results are obtained from discussion with various rail stakeholders (like rail operators, rail manufacturers and notified bodies). The objective is to highlight shared points and divergent ones related to SIL allocation and to propose a harmonized SIL allocation methodology in the railway domain. This methodology implementation in the form of a practical application guide will help rail stakeholders, involved in the SIL allocation (rail manufacturers, system integrators, etc.), to answer this particular problematic.

INTRODUCTION

Rail system safety remains a major concern in railway domain; the design and exploitation conditions of the railway systems are governed, in Europe, by rules described in legal texts (directives, regulations, decrees, etc.) and by a normative reference that require system safety demonstration. Member states have developed their own rules and safety standards mainly at national level based on national technical and operational concepts. Therefore, differences exist and can affect the optimum functioning of rail transport in the EU. Some steps have been taken to support the safety process harmonization as: the adoption of subsystems Technical Specifications for Interoperability (TSI), the definition of the Common Safety Targets (CST) and the definition of the Common Safety Method (CSM). The harmonization of railway methods and safety targets continues in agreement with the standards references as EN5012X (under review). These railway safety standards describe the safety aspects to be applied to the various levels of the railway system life cycle based on a risk management process which implies SIL allocation to the system various safety-related functions in order to control the complete system residual risk. The generic concept of SIL was introduced for the Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related systems by taking into account system requirement specification.

Nevertheless, various methodologies are adopted to perform the SIL allocation to system safety-related functions. The basic difference in these methodologies stems usually from the risk evaluation procedure which varies from a

rigorous quantitative estimation to a simple qualitative evaluation. Furthermore, there are several issues in the need to harmonize SIL allocation methodologies and they are inherent to the safety integrity level uses such as:

- The poor harmonization of definitions across the different standards which utilize the SIL concept;
- The derivation of SIL based on reliability estimates and system complexity.

This article aims to present the discussions results stemming from various rail stakeholders' consultations on their SIL use and/or allocation practices. In particular this research summarizes shared and divergent practices in the SIL allocation leading to a homogeneous allocation methodology proposition in order to provide a guide to French national rail authority EPSF for different actors concerned by SIL allocation problem in railway safety systems. As the methodology description and its implementation are presented in detail in [1], some retained principles will be recalled briefly in this article to focus primarily on the shared and divergent practices issues.

FROM THE ALLOCATION OF SAFETY TARGETS TO SAFETY INTEGRITY LEVELS ALLOCATION WITHIN A RAILWAY RISK MANAGEMENT PROCESS

The approach for designing safe global rail system or defined subsystem includes a risk analysis and hazard control phases [2]. For any railway technical system, an acceptable safety level must be ensured thus the so-called Hourglass Model has been introduced (cf. Figure 1), offering a supportive viewpoint to the sequence of life-cycle phases. The Hourglass Model provides an overview of the major safety-related activities that are needed during the development of a technical system, including the corresponding responsibility areas. Risk analysis in railway is generally based on the distinct involved actors' roles. The purpose of this model is to enhance co-operation between the relevant stakeholders, clarifying responsibilities and interfaces. The technical system is developed by one or several suppliers; therefore the functional risk assessment is the responsibility of the operator. The hazard control, for hazards associated purely with the technical system, is the responsibility of the supplier. These two stakeholders shall comply with the prevailing legal requirements [3, 4].

In practice and according to the context of every project, several entities intervene. The division of the responsibilities between the entities is not clearly defined and definitive, in order to have some design latitude (objectives, different rolling stock exploitation rules) and to facilitate innovation. The entities which intervene are classified in 2 groups, the first one being the customer of the other one and this reciprocity finding itself at various levels of definition of the system:

– The project owner is the entity carrying the need. It defines the objective of the project, its planning calendar and the budget dedicated to this project.

– The project manager is the entity chosen by the project owner according to a contract, for the project realization in compliance with the deadlines and quality conditions as well as costs fixed by the aforementioned project.

1. Risk assessment

Risk assessment is a process covering risk analysis and risk evaluation [5] for the system under consideration. The risk analysis includes hazardous situation identification (conditions leading to an accident) with the associated operating environments, consequence analysis and selection of risk acceptance criterion principles. The accident is defined as an event or series of unexpected events leading to death, injury or to environment damages [3]. The consequence analysis identifies links between hazards and accidents for every accident scenario (through cause-consequence diagrams and event trees for example). The risk acceptability of the system under assessment shall be evaluated by using one or more of the following risk acceptance principles:

- Principle n°1: Applying Codes of Practice (CoP); the acceptability is proven by obeying to the codes or the rules: like TSI and associated norms, the national rules, the mutual recognition agreement protocols;
- Principle n°2: Comparison with similar systems (reference systems). The system acceptability is based on "proven in use" of its similar parts concerned to the railway reference system. This principle is known as the GAME ("Globalement Au Moins Equivalent" for globally at least equivalent) principle.
- Principle n°3: Explicit risk estimation: the applicant needs to establish a complete demonstration in order to set explicit risk estimation (quantitative or qualitative).

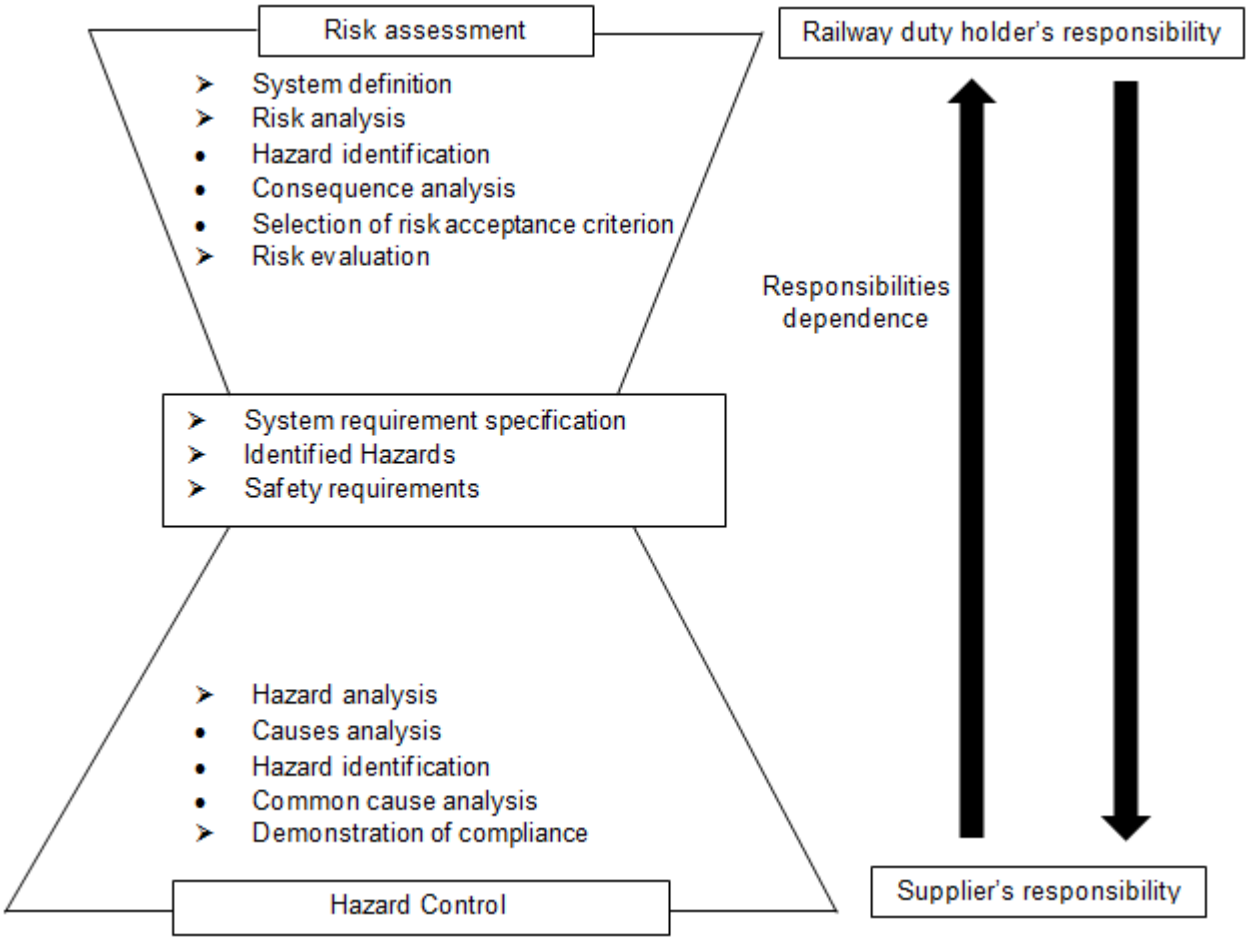

Figure 1. The hourglass model for risk management within railway, adapted from [3]

Explicit risk estimation is usually executed [6]:

- When Codes of Practice (CoP) or reference systems cannot be fully applied to control risks to an acceptable level. This occurs typically when the system under assessment is entirely new or where there are deviations from a code of practice or a similar reference system;
- When the chosen design strategy does not allow codes of practice or similar reference system uses, including desire to design a never used and more economical system (*e.g.*, train positioning with an onboard satellite localization system that is less expensive to maintain than distributed trackside beacons).

This risk assessment phase allows specifying the system requirements by establishing the list of identified hazards and a set of requirements on safety-related functions, subsystems or operating rules.

2. Hazard control

The second phase of the risk management process is hazard control and consists in ensuring/demonstrating that the specified system is in compliance with safety requirements. For that, the system internal causes are analyzed and determined and then the appropriate measures are implemented.

Risks related to safety-related function failures and systems that implement these functions, are controlled by complying with a set of technical measures required by regulations or standards. Risks induced by the E/E/PE systems are processed by a risk assessment followed by safety target allocations (often associated with frequency categories). Risks related to mechanical or pneumatic systems are processed by CoP or reference systems. The concept of risk acceptability level has been developed into the industrial IEC 61508 and railway EN 50126 standards. A matrix combining the accident severities and occurrence frequencies is used to set the risk acceptability levels. An acceptable maximum rate of the considered hazard occurrence noted THR (Tolerable Hazard Rate) is determined by a number of events per hour [2].

In principle, the operator should specify the THR so that the system designer is able to determine whether their system design is capable of meeting the target. In practice, the operator will define targets at the railway system level and may need to work together with the railway suppliers to define THR at the technical hazard level [3]. The next step is to determine the SIL of the safety-related functions based on safety targets allocated initially using THR. THR are associated to each hazard.

3. SIL concept

The Safety Integrity Levels are discrete levels defined to specify safety requirements for safety-related functions carried out by E/E/PE systems. A given SIL between SIL 1 and SIL 4 is linked to qualitative and quantitative requirement specifications for a safety-related function that are defined according to the random and the systematic failures related to the E/E/PE safety-related systems that perform the function [3]. SIL 4 is related to the most demanding requirements to counteract the hazard causes arising from these two kinds of failures. SIL 0 is occasionally defined for functions with no safety requirements.

The next section presents the SIL use/allocation practices stemming from consultations with various railway actors within our harmonized methodology for SIL allocation development. The obtained methodology is a research project proposal and not a national rule; these works were not intended to develop an additional method (many methods are already available) but to propose a methodology based on several existing practices and widely used while formalizing the implicit principles used.

SIL USE/ALLOCATION PRACTICES ACCORDING TO RAILWAY ACTORS

In Table 1, three main points (among others) describe a SIL particular use. In Table 2, on each line, practices providing guidance to the allocation approaches are presented (the columns are merged when there are consensus on the practice). These points of views and practices are most often different and sometimes contradictory depending on choices made by involved railway stakeholders. Whether they are rail duty holder, manufacturers, or notified bodies for railway certification.

The current standards attempt to harmonize risk analysis processes and their associated process (hazard, accident scenarios and hazard cause identification; safety target allocation, etc.) in order to strengthen the weaknesses of existing methods for instance including railway domain mutations (*e.g.*, new responsibility distribution; new technologies development onboard trains, on track or at the control stations). These changes aim to get more efficient systems but however result in more complex systems, especially for the safety analysis

[2]. It results in many discussions on approach evolution to be adopted in the revised standards, especially for the latest prEN50126 standard draft which is currently on investigation.

Description of a SIL particular use	**Point of view 1**	**Point of view 2**	**Remarks**
1. SIL 0 use additionally to other levels (SIL 1 to SIL 4)	SIL 0 is allocated to non-safety related functions. These functions, however, are considered as a first step to risk reduction. This type of function, although developed with a low level of confidence, brings a minimum but useful risk reduction (*e.g.*, reduction of the accident occurrence less than or equal to a factor of 10).	Functions that have an impact on safety (safety-related) should be allocated to a minimum SIL1.	- Standard EN 50128-2001 uses SIL 0 for non-safety related functions performed by software while the 2011 version uses the SIL 0 for functions that have an impact on safety, although this impact is low. - Standard prEN 50126 introduced the concept of *basic integrity* (not yet adopted). This notion is based on the point of view 1.
2. SIL for a function combining two dependent or independent sub-functions among each other	The THR logic only is considered. Then a SIL is allocated according to THR range associated to the function regarding the independence of its sub-functions.	Functions with a low-level of SIL can be combined to obtain a function with a higher SIL level (*e.g.*, a SIL 4 function can be obtained by two independent SIL2 sub-functions)	The concept of independence is not clearly achieved yet (in standard prEN 50126) because if there is dependency, the model that fits it is needed. The approach of EN50126 is still under discussion and might evolve.
3. Function involving a human operator	Human operator is taken into account in the studies (impact on SIL allocation) by considering it as a reliable (resilient) or, in contrast, unreliable.	Human operator is excluded.	In "acquire an emergency break request" function case, a set of solutions is possible as, request triggered by the driver after an alarm in the cab or by an automatic detection mechanism. The corresponding SIL might be the same regardless the solution.

Table 1. Different identified points of views related to SIL uses

Allocation approach characteristic	**Practice 1**	**Practice 2**	**Remarks and Examples**
1. Consequence severity associated to the function failure for SIL allocation	Allocation approaches show a direct link between SIL and the severity of functional failure.	The Function demand rate (depending on hazard occurrence frequency) associated with the severity if it fails, allows a SIL determination.	- Practice 1 tends to be banned. - Practice 2 can be illustrated by the following example: the overspeed protection is not critical if there is no overspeed situation.
2. Level of breakdown of accident causes in functional causes for SIL allocation (*i.e.*, stop level?)	Identification of all functional failure causes leading to the hazard (hazard upstream causes, *i.e.*, events when combined lead to the hazard)	Identification of each scenario from a given accident (hazard downstream causes, *i.e.*, events following the hazard occurrence until an accident) in which event combinations from	- In practice 2, a preliminary step is to use the risk graph as a method for allowing a prior SIL allocation ('conservative' results), *i.e.*, it leads to levels which the associated safety requirements are more constraining than actually needed. In this approach, if the risk graph result identifies the need to implement a very high level safety-related function, another

		technical, human or operational origin can jointly occur.	tool for a more detailed decomposition might be used (as an event graph or a fault tree). In addition, the risk graph is limited because it only considers one possibility of harm avoidance although several others could exist.
3. Item concerned by a safety target allocation (target obtained prior to the SIL)	Allocating a target on the identified functions from the system under consideration (*e.g.*, rolling stock), *i.e.*, the weight that is distributed to functions failures initially intended to reduce the risk; due to their failure, they no longer provide this reduction.	Allocation of a safety target related to hazard (in a specific accident scenario) by apportioning the risk reduction weight on the human, operational or technical components which perform a safety-related function.	- Example for **practice 2**: for overspeed hazard, there will be a risk part that will be supported by the infrastructure, another by the operator and another by the rolling stock. **- Remark associating demonstration to allocation concepts:** allocation can be seen as only defining safety requirements related to barriers (technical/human/organizational) handling a hazard; these barriers are defined following the accident scenario analysis (**practice 2**). Allocating risk reduction weight to the system safety-related functions (to comply with the hazard safety requirements, **practice 1**), can be seen as a demonstration approach rather than an allocation one based on the fact that we seek to show whether the system meets the requirements or not. The boundary between allocation and demonstration does not appear so clearly in the practices; indeed, at the European level, a safety target can be allocated to a hazard (dangerous situation) or, a contractor can ask directly a function with a SIL x. **- Remark on the SSIL:** The notion of Software SIL has disappeared in standard EN 50128-2011 and prEN50126 as SIL is allocated to a safety-related function.
4. Allocation practices in various accident scenarios involving the same function	For a specific accident scenario (when a trigger event such as an overspeed may lead to an accident with an unacceptable risk if a safety component is not involved), a technical component implementation among others facing the risk generated by the trigger event, allows to handle a final tolerated residual risk. If the same function is active in several scenarios, the most constraining requirement from all scenarios is used.		To illustrate two accident scenarios (*e.g.*, the accident being an obstacle collision) with a different context but involving the same function (automatic emergency braking) for the same dangerous situation (obstacles presence): in a first case, the train driver can trigger the emergency brake when he sees the obstacle. In a 2nd case braking can be triggered as soon as the train losses its catenary power supply cut off by the control center for example. Safety weight assigned on the human and technical components will be different from one case to another (the driver can support a risk reduction weight). Each case will lead, regarding the retained weight, to a different allocation of safety requirement on the function; the most constraining target is then retained.

Table 2. Different identified SIL allocation practices

Ref. Table 2	**Operators**	**Notified Bodies**	**Manufacturers**
1.	**Practice 2:** Depending on the hazard consequences severity, a safety target associated to the hazard is defined in terms of occurrence. If the accident is catastrophic, given the European regulation 402/2013 on Common Safety Method, a function failure leading directly to the hazard occurrence has to be $10E^{-9}$ per hour; if it's critical, the occurrence has to be $10E^{-7}$ per hour (these values refer to the CSM-Design Targets, which exclude human factors and operating rules as safety measures).		
2.	**Remark:** For the operator, SIL	**Practice 1:**- There is an activity	**Practice 2:**- The system actor at the

	allocations provided by the manufacturers include a large heterogeneity in the details provided. But regardless the used modeling tree view, what is essential is that everyone understands each other. The necessary breakdowns level is the one that ensures the demonstration; the sufficient level depends on the manufacturer (need or not of detailed sub-systems, for example with actuator mechanisms related to brake control).	prior to THR determination made by the infrastructure manager or the operator for a given function failure mode (some THR are defined by European legal texts as TSI). From a THR, the manufacturer will analyze how to design its system, to select its product in order to meet this target. - In a functional allocation approach, the requirement is on function. Before defining a SIL, the requirement is defined regardless of the system technology in use. The requirement on the function is common and can be seen as being achieved by a "box". If an E/E/PE system is used to perform this "box", the requirement is expressed in terms of SIL. In this case, it involves specific steps for the systematic failures control.	highest level can only allocate functional requirements to lower level actors. Then it is the latter ones responsibility, by their design choices, to perform a safety analysis in order to identify if their system is safe or not (*e.g.*, Energy by hydrogen or electricity storage); the manufacturer from its product, demonstrates a target achievement (demonstration approach rather than allocation). - The actor managing the whole railway system actually defines the weight to allocate to the safety-related function based on technical, human or operational features (not only technical). - There are particular cases. For example, a SIL 4 function, achieved through track beacons, also requires the same safety level for the onboard part in rolling stock, information support, etc.
3.	**Practice 1:** The infrastructure manager or the operator has the responsibility to control external events (especially risk reduction brought by the system external barriers,). Indeed, the rolling stock is not subject to the same external events according to the operated lines (conventional line, automated line, driverless line with specific procedures). The possibility to release THR target regarding external events is the operator or the infrastructure manager responsibility.	**- Practice 1 and 2:** Based on observations at European level: a safety target can be allocated to a hazard (dangerous situation) or an operator may sometimes claims directly SIL x for a function. In particular this is observed for urban guided transport depending on the rail network size and depending on the operator engineering expertise. One might specify only the highest accident risk level (*e.g.*, number of injuries per year). In this case, the manufacturer, who is involved in the preliminary safety study, can perform a fault tree beginning with the individual risk until specifying weight in the tree. - The German SIRF (*Sicherheitsrichtlinie Fahrzeug* - rolling stock safety regulations) approach is based on the THR apportionment from the accident analysis.	**Practice 2:** THR safety targets should be assigned to a hazard considering the accident implying this hazard (scenario), and then different actors have to reach this target at the system level (in the overall rail system). The actors might then show that the THR are achieved. **Remark:** - The Safe Down Time (SDT) intervenes as soon as there is an "AND" gate in a fault tree. It is part of the items that must be allocated. The SDT has a direct impact on the THR choice: the lower the SDTis, the higher the rate is.
4.			**Specifications on accident scenarios:** These scenarios are jointly defined between the manufacturer and its suppliers to fix a safety target. At the rolling stock level, the manufacturer receives information on the safety performance of supplier's equipment in order to verify if the proposed equipment performance can be selected or if new more robust equipment should be developed.

Table 3. Different actor's reactions on SIL allocation practices mentioned in Table 2

Given these uses and practices related to SIL, the following section presents the choices retained in the methodology for SIL allocation to safety-related functions.

CHOICES RETAINED IN THE METHODOLOGY

1. Methodology general aspects

The proposed methodology is established through two processes and their different steps are based on practical rules and hypotheses to be tested. Its implementation begins with the use of THR quantitative safety targets. These quantitative targets allow taking into account the Common Safety Method – Design Targets (CSM-DT) values associated to technical systems design recently defined by European Railway Agency (ERA). Although THR is a quantitative criterion, it is a target measure with respect to both systematic and random failure integrity. It is accepted that only random failure integrity will be possible to quantify; qualitative measures and judgements will be necessary to justify that the systematic integrity requirements are met. This is mainly covered by the SIL (and the measures derived from the SIL) (see standard EN50129 and prEN50126).

The methodology is illustrated by the overview in Figure 2. This is a macro view highlighting two main processes. In process 1, the THR apportioning rules are applied to the safety-related functions. On the one hand, these rules are based on the logical combinations of these functions. On the other hand, to take into account technical conditions (last safety weak link, functional dependencies, technological complexity, etc.), specific rules implicitly used in existing practices, are defined for readjusting some THR values. SIL allocation based on apportioned and validated THR values, are finally established in process 2.

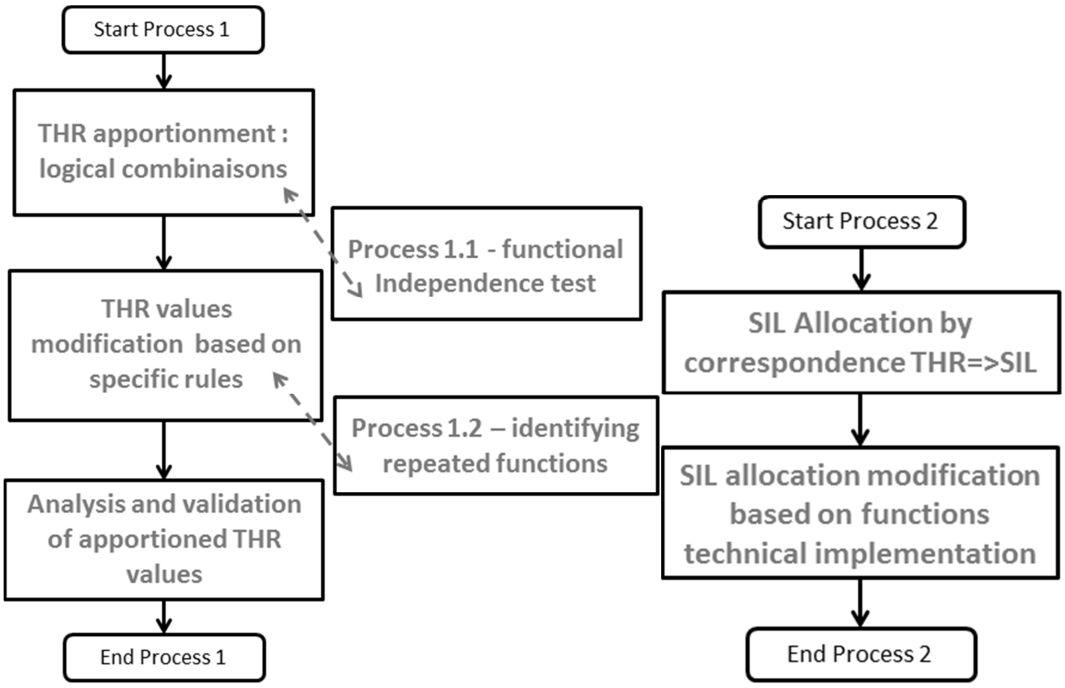

Figure 2. Overview of process 1 & 2: THR apportionment and SIL allocation

The Fault Tree Analysis explicitly expresses how equipment failure, operation errors, and external factors lead to system failures therefore is commonly used to analyse system safety. It is used as a quantitative method because it shows the cause-consequence links of the system functions but in certain cases, other methods can be used.

2. process 1 based on the THR

The THR is associated to a particular hazard; it's a main criterion within SIL allocation in the railway domain. A hazard with a tolerable rate results from combinations or sequences of failures under control within the system in a particular operational context.

In this process, the system elements are considered from the functional point of view as several hardware/software architectures are possible. In the railway standards there is no explicit indication/rule or provided guidance on how to reduce or manage the SIL allocation considering dependable architectural solutions, as is done in the IEC 61508 generic standard. For a particular sub-function with a specific SIL, supplier architecture solutions may be different but equally satisfactory [7].

THR (safety target associated to hazard occurrence in the considered accident scenario) apportioning rules are applied to the safety-related functions or sub-functions. On the one hand, these rules are based on the logical combinations of these safety-related functions. On the other hand, to take into account technical conditions (last safety weak link, functional dependencies, technological complexity, etc.), specific rules implicitly used in existing practices, are defined for readjusting some THR values.

After the THR values readjustments based on the specific rules, a "Down-Top" quantitative analysis and validation is performed to verify compliance with the THR (safety target) apportionment for each corresponding hazard. This validation is intended to eventually make changes in SIL allocation process by considering specific technical architectures. When the safety target THR is not achieved, the risk acceptability need to be demonstrate (expert arguments, GAME, etc.)

SIL allocation based on apportioned and validated THR values is finally established in process 2.

3. process 2 for SIL allocation

Safety target refers to a function failure rate, while SIL refers to a function: for each failure mode of a given function can be assigned a safety target as a THR and then a SIL being allocated to this function, based the most restrictive THR. The SIL allocation to safety-related functions is performed through THR => SIL correspondence (see Table A.1 from standard EN 50129).

How train functions and/or subsystems are implemented (functions technical design on the hardware/software architecture) has also an impact on the SIL allocation. Specific allocation rules taking into account these implementation conditions (complex technical solutions, mutual intrusion of implemented functions, restrictive or not safety requirements) are also defined in this latter process including a function with constraining quantitative requirements more than 10^{-9}/h, the need to involve methods and technical or operational measures applicable to SIL 4, or to allocate at least a SIL 1 to a function with safety quantitative requirements low than THR≥10^{-5}/h.

4. Methodology possible evolutions according to the changes in regulations

The prEN50126 standard draft (under review and subject to changes) advocates the use of the Tolerable Functional Failure Rate (TFFR) concept for safety-related functions and the THR for hazards, separating the hazard layer from functions layer. The proposed generic methodology can be adapted by setting a THR (not modifiable) for each identified hazards and an apportionment in terms of TFFR to safety-related functions and sub-functions.

CONCLUSION

This article has highlighted and focused on the practices for SIL allocation in railways given the concerned actors experience, the related literature review and works in passed research projects as MODUrban or MODTRAIN. Different points of views related to SIL uses, different identified SIL allocation practices and the associated actor's

reactions on these allocation practices are described with examples. The retained practices are included in a guide describing a methodology for a harmonized SIL allocation method.

ACKNOWLEDGEMENTS

The authors would like to thank various operators, manufacturers and notified bodies for their relevant and detailed feedbacks and remarks on the proposed methodological guide. It allows improving the methodology through their professional expertise and highlighting the still open various points.

REFERENCES

1. Ouedraogo KA, Beugin J, El-Koursi EM., Clarhaut J, Renaux D, Lisiecki F. Harmonized methodology for Safety Integrity Level allocation in a generic TCMS application. ESREL 2015 - European safety and reliability conference, pp 3579-3587, September 7-10, Zürich, Switzerland.
2. Blas A, Boulanger JL. How to enhance the risk analysis methods and the allocation of THR, SIL and other safety objectives. Lambda-Mu 16, Avignon, October 6-10, 2008.
3. prEN50126. Railways applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). CENELEC standard project. Part 2. 2015.
4. Braband J. Allocation of safety integrity requirements for railway signalling applications. ESREL '99 - European safety and reliability conference, Munich-Garching, Germany. In Schüller and Kafka (eds), pp 1237-1242.
5. Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009. Commission implementing regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013
6. ERA. Guide for the application of the commission regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in article 6(3)(a) of the railway safety directive, ERA/GUI/01-2008/SAF, European Railway Agency, Valenciennes, 2009.
7. Blanquart JP, Astruc JM, Baufreton P, Boulanger et al. Criticality categories across safety standards in different domains. 6th conference on Embedded Real Time Software and Systems, 2012.