

Harmonized methodology for Safety Integrity Level allocation in a generic TCMS application

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

▶ **To cite this version:**

Kiswendsida Abel Ouedraogo, Julie Beugin, El Miloudi El Koursi, Joffrey Clarhaut, Dominique Renaux, et al.. Harmonized methodology for Safety Integrity Level allocation in a generic TCMS application. ESREL 2015 - European safety and reliability conference, Sep 2015, Zürich, Switzerland. pp.3579-3587. hal-01471416

HAL Id: hal-01471416
https://hal.science/hal-01471416

Submitted on 20 Feb 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

OUEDRAOGO, Kiswendsida Abel, BEUGIN, Julie, EL KOURSI, El Miloudi, CLARHAUT, Joffrey, RENAUX, Dominique, LISIECKI, Frédéric, 2015, Harmonized methodology for Safety Integrity Level allocation in a generic TCMS application, ESREL 2015 - European safety and reliability conference, Zürich, SUISSE, 2015-09-07, 8p

Harmonized methodology for Safety Integrity Level allocation in a generic TCMS application

K.A. Ouedraogo[1,2], J. Beugin[1,2], E.-M. El-Koursi[1,2], J. Clarhaut[3], D. Renaux[3] & F. Lisiecki[4]

[1]*Univ. Lille Nord de France, F-59000 Lille, France*

[2]*IFSTTAR, COSYS, ESTAS, 20 Rue Elisée Reclus – BP 70317 – 59666 Villeneuve d'Ascq Cedex, France*

[3]*LAMIH - Auto UMR CNRS 8201, University of Valenciennes and Hainaut-Cambresis*
Le Mont Houy – F-59313 Valenciennes Cedex 9, France

[4]*EPSF, Regulations Directorate – Rules and Standards Units*
60 Rue de la Vallée CS 11758, 80017 Amiens Cedex 1, France

ABSTRACT: This article presents a generic methodology for SIL allocation to railway rolling stock safety-related functions to solve the SIL concept application issues. This methodology is based on the flowchart formalism already used in CSM European regulation. It starts with the use of quantitative safety requirements, particularly the Tolerable Hazard Rate (THR). The THR apportioning rules are applied. On the one hand, the rules are related to logical combinations of safety-related functions preventing hazard occurrence. 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 process based on apportioned and validated THR values is finally established. Generic "Passengers doors" and "Emergency brake" sub-systems are examined in terms of SIL allocation to the safety-related functions and the methodology is validated by compliance with the safety requirement objectives.

1 INTRODUCTION

Rail systems safety remains a major concern in railway domain, where accidents can result in significant damages on the system and on the environment and cause many victims (e.g. railway accidents of summer 2013 in France, in Spain and in Switzerland). In Europe, the design and operation conditions of these systems are now governed by the rules described in legal texts (directives, regulations, decrees, etc.) and by a normative reference that require system safety demonstration. The reference documents are composed of specific European standards (the EN 50126,8,9 soon replaced by the unique EN 50126 multi-parts standard) derived from the functional safety generic standard IEC 61508 (2011); and it describes the safety aspects to be applied to different levels of the rail system life cycle. Railway standards recommend the application of the risk management process upstream of the rail system design. It involves setting safety levels in terms of SILs (Safety Integrity Levels) to most of system parts. A given SIL between SIL 0 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 systems that perform the function (prEN 50126 2012 – part 2, §10.2). SIL 4 is related to the most demanding requirements to counteract the hazard causes arising from these two kinds of failures.

However several sector safety standards derived from the IEC 61508 differ in their derivation of SILs resulting then to misunderstand the SIL allocation process. A state of the art and consultations have been completed explaining some practices employed in the railway domain compared to other domains in order to clarify, for railway actors, the SIL allocation process, especially concerning TCMS (Train Control and Monitoring Systems) that manage all the hardware and software parts inside trains (Ouedraogo et al. 2014). Specific rules implicitly used for SIL allocation process in TCMS have been identified/formalized and integrated in the proposed methodology.

Firstly, this paper will present how SILs are used within the harmonized risk management process for railway systems in the European Union. Then, the methodology aiming to harmonize SIL allocation in a generic TCMS application is described in detail. The "Passengers doors" and "Emergency brake" sub-systems are retained as application studies and the obtained SIL allocation results are presented.

2 SIL USE IN THE HARMONIZED RISK MANAGEMENT PROCESS

Railway safety is part of the various European Union texts recommending an unified European rail network in which future transportation systems will be interoperable (directive 2004/49/EC amended by directive 2008/110/EC for railways safety and harmonization principles of safety approval; decision 2009/460/EC on common safety method for assessing safety achievement). Member states have

developed their own rules and safety standards mainly at national level based on national technical and operational concepts. Differences exist and can affect the optimum functioning of rail transport in the EU and the approval of a system by some National Safety Authorities (MODSafe, 2010; MODURBAN, 2006). 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 unification of railway methods and safety objectives continues with the establishment of CSM Design Targets for technical systems (CSM-DT). The CSM regulation (402/2013/EU) defines a harmonized and generic risk management process to be applied to new rail systems in agreement with the EN5012x standards or to systems with a significant change that has an impact on safety. After the definition of the system under assessment, the risk management process, a global iterative process is depicted in regulation 402/2013/EU: appendix. In this process SIL can specify safety requirements to safety-related functions given the conclusions of the risk analysis and evaluation that derive global safety objectives associated to hazards, some objectives being defined in terms of Tolerable Hazard Rate (THR). Then, function ability performed by a safety-related system to comply with SIL must be validated. Operating procedures, testing and maintenance must also comply with the requirements of SIL. According to sectors, there are different methods to allocate SIL depending on standard in use, national practices and regulations, project's and operator's methods in use or available data (Rouvroye 2001, Smith & Simpson 2004, MIL-STD-882 E 2012, IEEE 1012 2012, IEC 62061 2005, IEC 61511 2003). Those mostly employed in railway domain are the well-known risk matrix and the risk graph, even if they are mainly used to derive safety requirements in general.

The methodology for SIL allocation presented hereafter is dedicated to railway rolling stock safety-related functions and aims to solve the SIL concept application issues. Each step of the methodology is illustrated by TCMS examples. Particular attention is drawn to the fact that this methodology should fit into the context of European regulation harmonization especially, the CSM regulation risk management process. SIL associated measures allow specific safety requirements for E/E/PE sub-systems in the CSM process to be laid down.

3 METHODOLOGY FOR SAFETY INTEGRITY LEVELS ALLOCATION

The generic methodology is based on the flowchart formalism already used in CSM regulation. It is principally dedicated to allocate SIL when the explicit risk acceptance principle is used, SIL allocation being direct for other principles (codes of practice, use of a reference system). It applies also to rolling stock safety-related functions rather than signalling functions even if the principles are still applicable to the latter. Indeed, for a signalling system that intervenes as final barrier against the rolling stock device failures, the allocation process is often direct by setting the highest SIL. For a rolling stock that combines different types of functions whose failures indirectly lead to risks, the methodology has to handle complex functional interactions.

The methodology includes steps based on practical rules and hypotheses to be tested, with the aim of an effective application. It starts with the use of quantitative safety objectives associated to hazard situations, particularly THR as they are considered in many analyses and as the regulation CSM-DT are quantitative. One *THR objective* is declined to *apportioned THRs* to functions whose failures lead to a given identified hazardous situation. Even if the initial THR objective is quantitative, it is also recognized to set specifications on the integrity of random and systemic failures and then SIL. The methodology is illustrated by the overview in Figure 1. This is a macro view highlighting two main processes detailed subsequently with examples. In the 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 and that the paper makes explicit, are defined for readjusting some THR values. SIL allocation based on apportioned and validated THR values, are finally established in process 2.

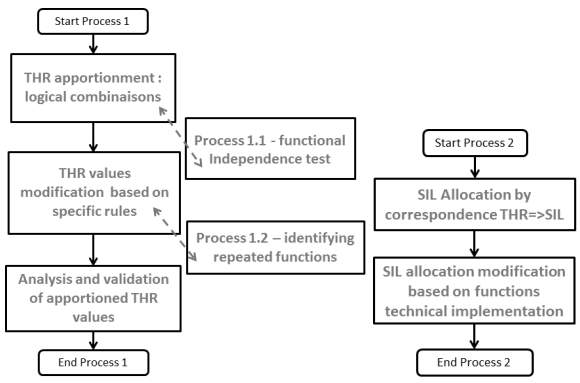


Figure 1. Overview of process 1 & 2: THR apportionment & SIL allocation

The methodology requires the following input data based on a complete functional analysis:

- The list of hazardous situations for the considered system (examples of generic hazards covering standard railway operations are listed in (ERA, 2009 – annex C17);
- The list of safety related-functions directly or indirectly leading to hazards;
- The list of function failure combinations (scenarios) leading to each hazard and functional failures leading directly to a risk of death;

The risk criteria associated to hazards (i.e., maximal THR) or to functions (as CSM-DT).

The *external barriers* to reduce the risk of the system (prevention barriers against accident or protection barriers against damages) are not included in the methodology (*e.g.*, external technical systems, human factors, operational rules). Indeed, the *THR objectives* associated to hazardous situations are considered already taking into account these external barriers. Note that the considered *safety-related functions*, *i.e.* the functions whose failures affect the system safety (*e.g.*, open the doors, maintain the speed), include the *safety functions*, *i.e.* the functions that have for primary role to reduce risks (*e.g.*, control the speed, lock the doors) and contribute to the implementation of *technical safety barriers* (physical or non-physical means reducing the hazard frequency/potential accident caused by the hazard/the severity of potential accidents caused by the hazard).

Figure 2 shows the detailed flowchart of the generic SIL allocation methodology for safety-related functions. Before detailing the application of this flowchart through 2 TCMS examples, the required input data for these examples are defined.

3.1 *The generic rolling stock subsystems considered*

The choice of the "Passenger doors" subsystem as an application study is motivated by its complexity. Generic safety-related functions encountered in the "Passenger doors" subsystem are presented within a Function Analysis System Technique (FAST) diagram in Figure 3 with functions taken from (EN 15380-4 2013, EN 62290-2 2012, TSI LOC&PAS 2013, EN 14752 2006). The subsystem "Emergency brake" is also considered in this study. The main generic safety-related functions are (EN 15380-4 2013):

- Acquire emergency brake request and its tree sub-functions: acquire emergency brake request triggered by the driver, by automatism or by the passengers;
- Operate the emergency brake and its two sub-functions: operate the emergency brake triggered by the driver or by automatism;
- Traction request by emergency brake;
- Isolate emergency devices;
- Execute emergency brake.

The first sub-system, the "Passenger doors" subsystem, is considered without movable step management (to reduce the gap between vehicle and platform) as it is the case for most of metro systems. It has the following functional characteristics:

- Automatic opening/closing;
- Obstacle detection interrupting the closure leading to the doors opening;
- Both visual and acoustic sign/alarm of the door imminent closing and indicating abnormal condition;
- Indication of "doors closed and locked" status allowing the train departure; and during the train route, the doors must remain closed and locked;
- In case of technical incident or accident, the doors unlocking and opening functions are insured by operating on a manual device ("unlocking handle"). An accidental door unlocking during the train route triggers the emergency brake for stopping train.

A list of generic hazardous situations related to "Passenger doors" subsystem or to "Emergency brake" subsystem can be done considering functional failures and taking into account the context (*e.g.*, train in station, off station) and the areas (*e.g.* wrong side of train).

3.2 *Lists of generic hazardous situations*

With the identified generic safety-related functions of "Passenger doors" system (see Fig. 3), some lists of hazardous situations can be established based on functions and associated sub-functions contributing to the considered situation. Table 1 presents a list of generic hazardous situations related to "Emergency brake" subsystem. The combinations of functions and their associated sub-functions (see Fig. 3) whose functional failures lead to each hazardous situation are identified by the fault tree method. Then, the developed methodology describes the way how each safety objective is apportioned in terms of THR to these safety-related functions and their associated sub-functions.

Table 1. Generic hazardous situations related to "Emergency brake" sub-system.

Hazardous situation by type of accident	Safety objective
Collision/derailment (leading to one (critical) or more death (catastrophic)	
Applies to units fitted with a cab (brake command) After activation of an emergency brake command no deceleration of the train due to failure in the brake system (complete and permanent loss of the brake force).	THR≤10^{-9}
Applies to units equipped with traction equipment After activation of an emergency brake command, no deceleration of the train due to failure in the traction system (Traction force ≥ Brake force).	THR≤10^{-9}
After activation of an emergency brake command The stopping distance is longer than the one in normal mode due to failure(s) in the brake system.	THR≤10^{-7}

Table 2 presents a list of generic hazardous situations related to "Passenger doors" subsystem and the associated safety objective in terms of THR values. These values are taken from objectives that are available at the time of this work, *i.e.* objectives taken from French regulations (SAM – Spécifications d'Admission Matériel – approvals specifications for rolling stock) or from European TSI (2013, related to the rolling stock - locomotives and passenger).

Table 2. Generic hazardous situations related to "Passenger doors" subsystem

Hazardous situation by type of accident	Safety objective
Fall of passengers or collision (train fouling the gauge)	
Several doors are opened in inappropriate situations (train running, one or two sides of the train)	THR≤10^{-9}
Several doors are opened in inappropriate situations (train stop at the platform)	THR≤10^{-5}
Traction authorized with several doors not closed but reported erroneously closed secured	THR≤10^{-7}
Possibility to open on request (excluding emergency opening) a door in inappropriate situations (train stop in platform side or in wrong side)	THR≤10^{-7}
Wedging	
Inappropriate closure without imminence phase before closure	THR≤10^{-5}
Closure without obstacle detection	THR≤10^{-5}
Disruption of the passengers flow	
No door opening, train stop, platform side	THR≤10^{-5}
Failure in the internal emergency opening system of two adjacent doors, platform side, train stop	THR≤10^{-7}
Not reporting no disabled accessibility	THR≤10^{-5}

3.3 *Process 1 for THR apportionment*

Given the fault trees associated to each hazardous situation, the process 1 for THR apportionment can start. It comprises 4 phases reiterated for each tree:

- The allocations of the THR objective at the top of the fault tree;
- The apportionment of the THR objective to safety-related functions based on Boolean logical combination rules;
- Then, some "apportioned THR" modifications based on specific rules;
- The "apportioned THR" analysis and quantitative validation.

These 4 phases are described and illustrated by examples related to both TCMS subsystems considered. The "Fault Tree" module of GRIF software is used for the representation and calculation process.

3.3.1 *Allocation of the THR objective*

For each hazardous situation, a safety objective is set in terms of THR. Then these *THR objectives* (Cf. examples in Tables 1-2) are reported to the fault tree top event.

3.3.2 *Apportionment of the THR objective based on Boolean logical combination rules*

A *THR objective* is apportioned to the functions of the fault tree through logic "OR/AND" gates to obtain *apportioned THR*. The use of Boolean logical apportionment rules is conditioned by the fact that the functions are independent and that the THR values are very small compared to 1. The first condition allows the use of elementary probability laws associated to "OR/AND" gates instead of conditional probabilities. The second condition allows the use of rates in the same way as probabilities. The dependent functions are allocated to an identical THR.

An independence test (Cf. process 1.1 in Fig. 1 & 2) must be performed and the associated sub-process applied. "Level *i*" denotes the set of all "OR /AND" gates and the associated functions F_{ij} of the fault tree. The integer variable *j* is used to browse all functions F_{ij} associated to the considered level *i*. For a given level *i*, we define the number of "branches" (set of functions and all sub-elements as gates and associated sub-functions) as equal to the number of functions F_{ij} associated to this level gate. In Figure 4, we have tree functions F11, F12 and F13, and therefore three branches (k = 1, 2 and 3) composed of functions and gates, sub-functions associated with each of these functions.

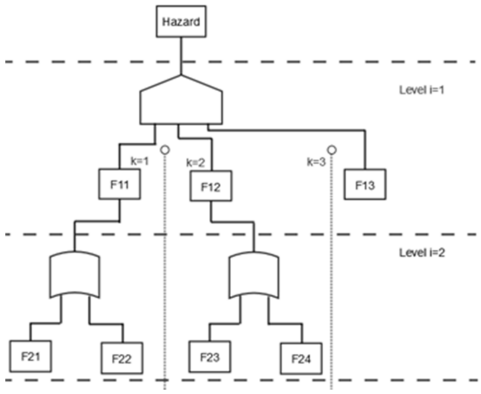


Figure 4. Setting levels and branches for functions independence test

Two safety-related functions are independent if they control the same hazard, but each of them performs its control autonomously, no matter whether the other is present or not (prEN 50126-2 2012).

The independence test verifies that the "basic events" sub-functions associated to each function at a given level *i* are not repeated in the "basic events" sub-functions of the other branches of the same level.

The THR Top/Down apportionment rules are then as follow:

a. If there is only one function at the down level, the immediate top level THR is reported. Example: functions 18 & 18.1 or hazard & function 17 in Figure 5;

b. Dependent functions must have identical THR. If all functions at a given level are dependent

following the independence test, the immediate top THR is reported to each function; however, this THR value can then be further apportioned to sub-functions subject to their independence demonstration. Example: Figure 5, function 14 THR is reported to dependent functions 14.1 & 14.4 as they share repeated functions 14.5 & 14.6 (encircled events);

c. For an "OR" gate, if the sub-functions F_{ij} are independent following the test, the given THR is apportioned equally to each independent sub-functions (prEN50126-2 2012). Example: Figure 5, function 17 THR is apportioned equally to independent sub-functions 14 & 18.

For an "AND" gate, if the sub-functions F_{ij} are independent following the test, the THR apportionment has to take into account functions failures "Safe Down Time" (SDT); the "Safe Down Rate" is equal to SDR=1/SDT. For n independent function, the THR is apportioned based on the following formula:

$$THR_{max} = \prod_{j=1}^{n} THR_j . SDT_j . \sum_{j=1}^{n} \frac{1}{SDT_j}$$

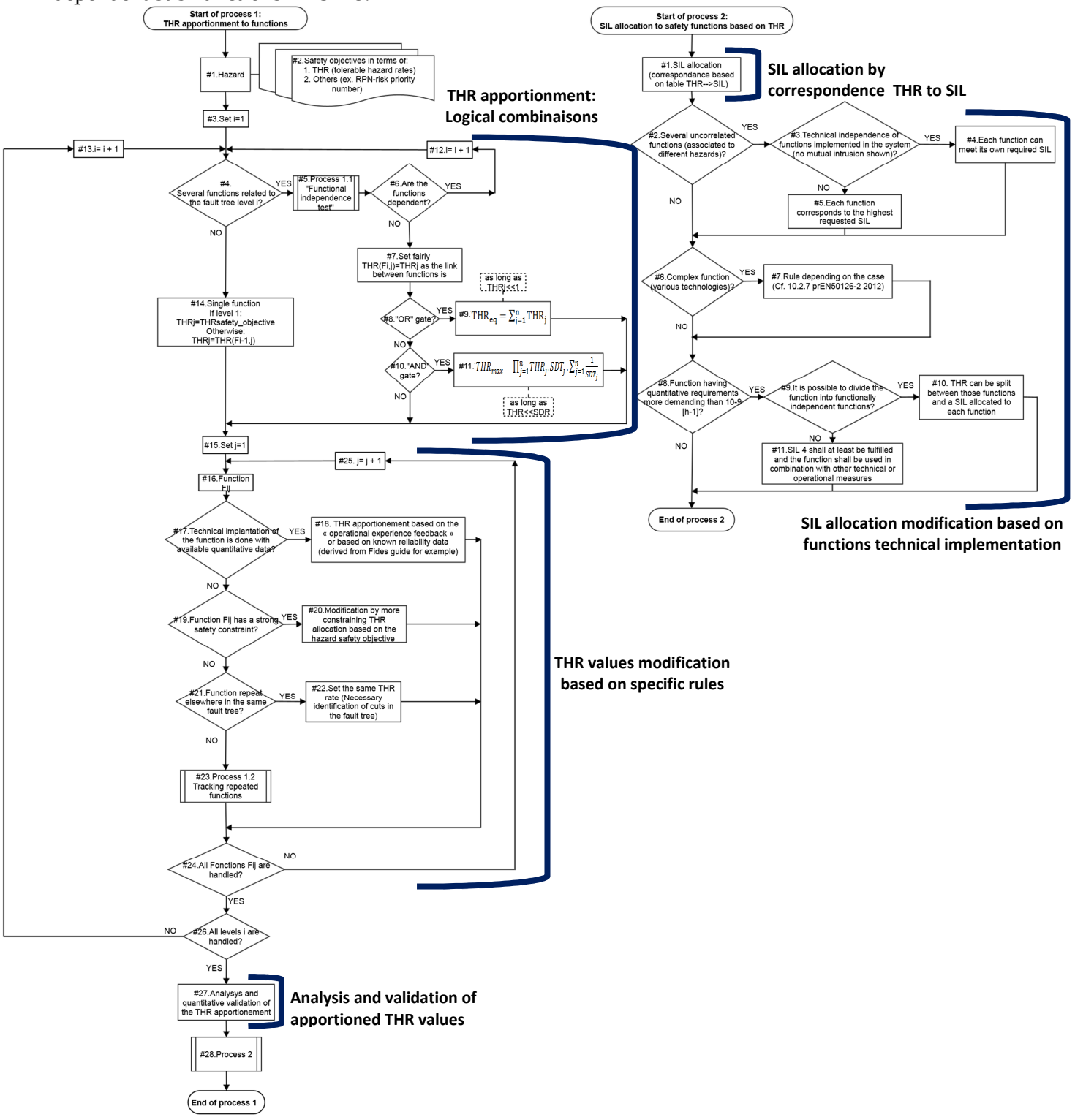


Figure 2. Flowchart of the generic SIL allocation methodology

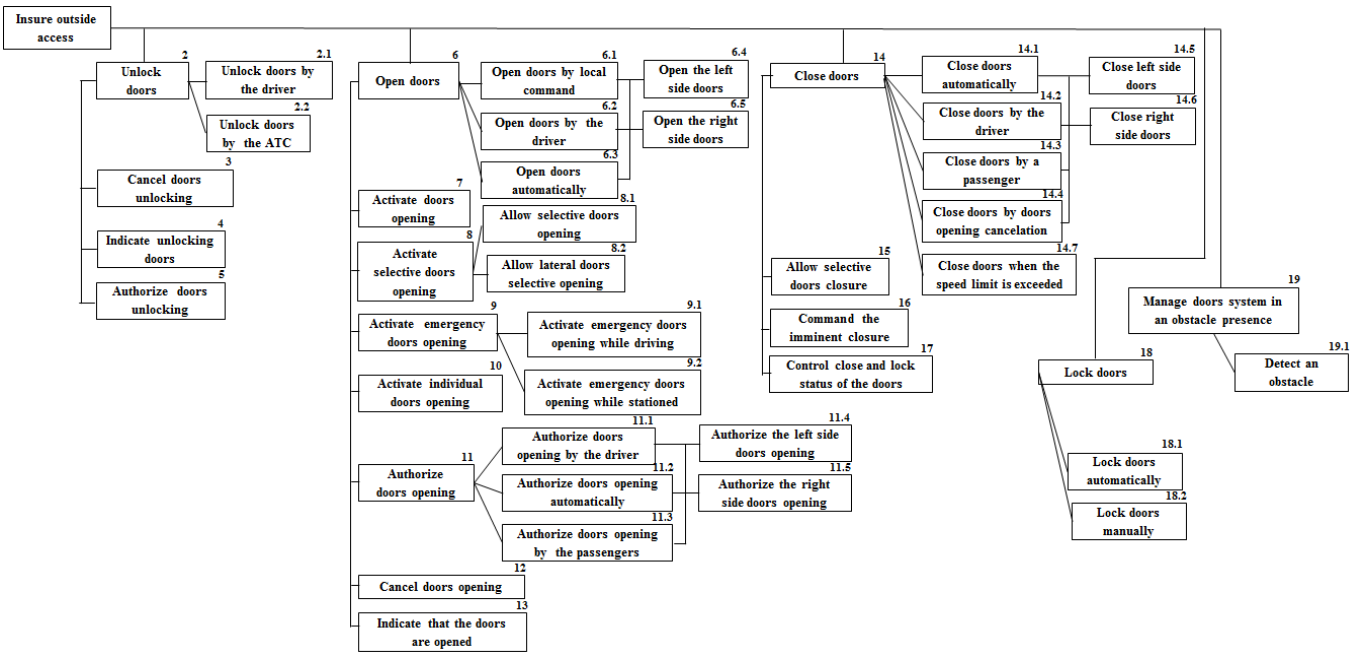


Figure 3. FAST diagram of "Passenger doors" system

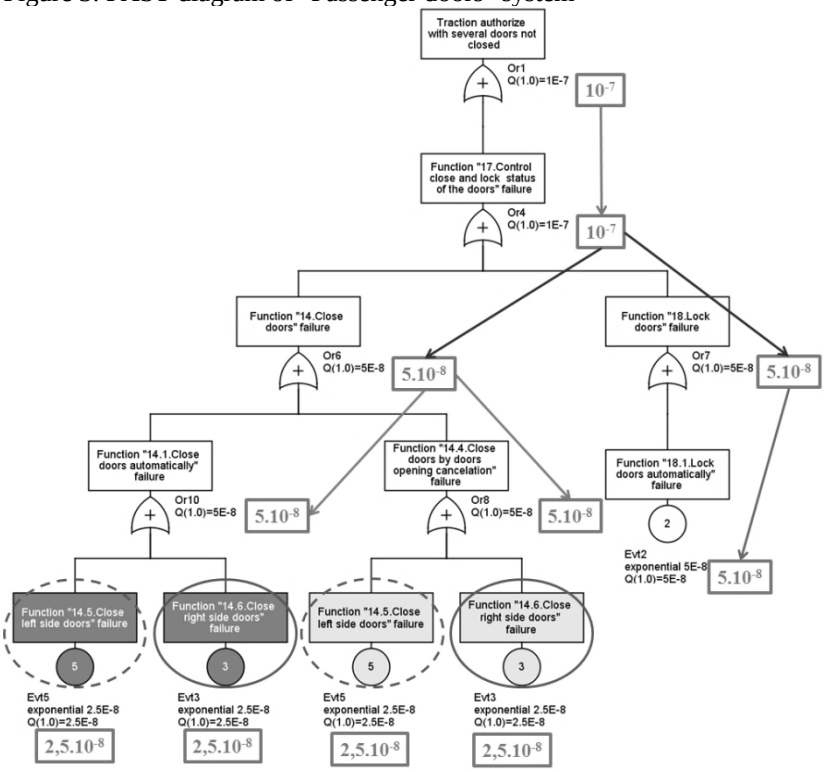


Figure 5. Some THR apportionment illustration

After activation of an emergency brake command, the stopping distance is longer than the one in normal mode due to failure(s) in the brake system.

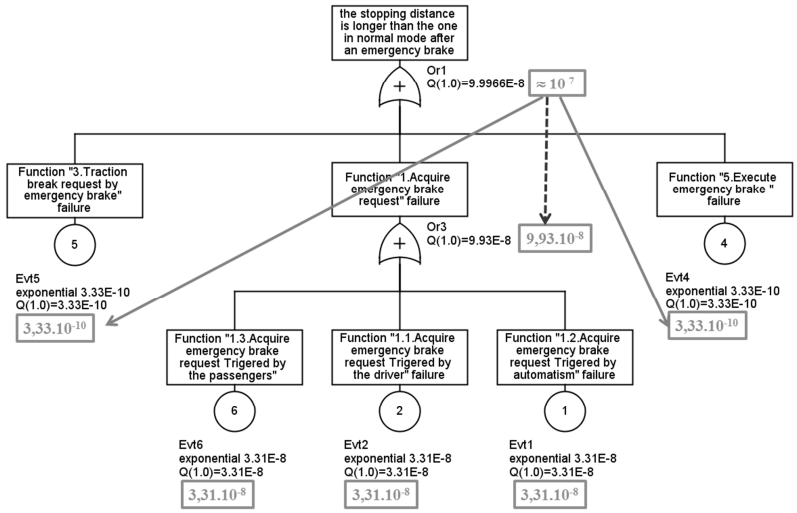


Figure 7. THR apportionment validation

Example: in Figure 6, function 4 *THRmax* is apportioned as product of the two downstream functions (THR_2 & $THR_{2'}$) with $SDT_2=SDT_{2'}=1/2$.

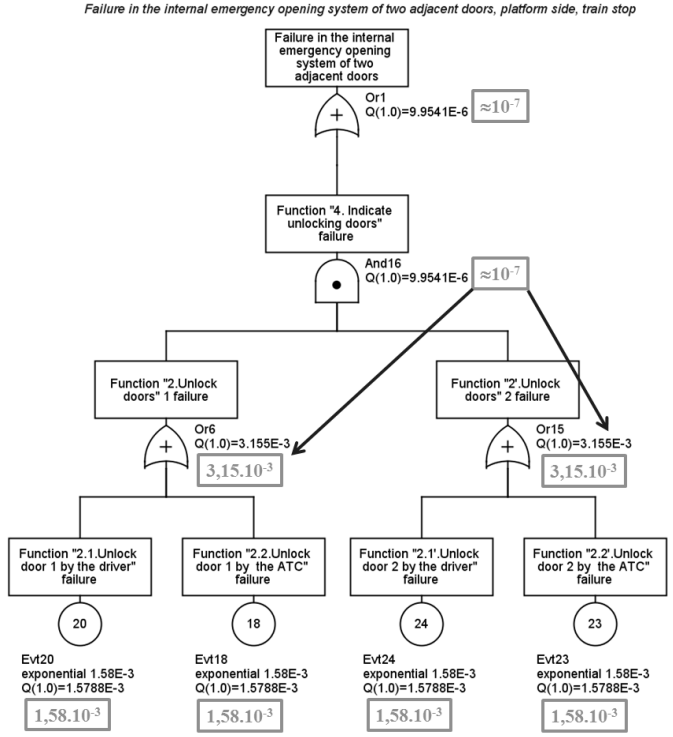


Figure 6. THR apportionment through "AND" gate illustration

After this phase of THR apportionment based on Boolean logical combinations rules, some "apportioned THR" must be modified based on more specific rules.

3.3.3 *Apportioned THR modifications based on specific rules*

Specific rules taken from the standard prEN50126-2 (2012) and from some railway organism consultations involve modifying already apportioned THR. From the fault tree top event, all the functions F_{ij} are examined level by level in order to modify their THR based on the specific rules as follow:

d. For a function whose technical implementation is already fixed (e.g., commercial off-the-shelf COTS, technical conditions in use on a railway network, etc.), the THR is modified based on the available feedback or on reliability data (e.g., from FIDES guide) associated to a given technical solution implementing a safety-related function. The known rate can be reported to the function (Cf. rule at points #17 & 18 on Fig. 1). Example: the compatibility between all rolling stocks and French national railway network requires defining technical implementation conditions in advance.

e. For a function subject to a strong safety constraint (Example: function whose failure leads directly to hazard, signalling functions, braking system functions, etc.), a more constraining THR should be allocated based on safety requirements (Cf. points #19 & 20 on Fig. 1).

f. For functions or sub-functions repeated in different branches of the same fault tree, the apportioned THR must be identical (Cf. points #21 & 22 on Fig. 1). Example: in Figure 5, the two repeated "basic events" sub-functions 14.5 & 14.6 have their THR set to $2{,}5.10^{-8}$/h;

g. For functions appearing in another hazard fault trees, the minimum *THRmin* between the THR is reported to each function; a tracking procedure (process 1.2) based on Breadth-first search algorithm for repeated functions has been defined (Cf. rule at points #23 on Fig. 1).

An analysis needs to be done in order to validate the THR apportionment process.

3.3.4 *THR apportionment analysis and quantitative validation.*

After the apportioned THR modifications based on the specific rules, a quantitative Down-Top analysis is completed to verify compliance with the hazard safety objectives. Example: for the hazardous situation *"After activation of an emergency brake command, the stopping distance is longer than the one in normal mode due to failure(s) in the brake system"*, the safety objective 10^{-7}/h is firstly apportioned equally to the 3 independents sub-functions based on logical combination rules through "OR" gate.

But functions n° 3 & 5 are repeated in the two others hazardous situation related to "Emergency brake" sub-system fault trees with more safety constraints; thus the most restrictive THR ($3{,}33\ 10^{-10}$/h) from the other fault trees is reported to these functions (specific rule d). Therefore the quantitative Down-Top analysis allows function n°1 to be set to $\mathbf{THR_{max}=9{,}93\ 10^{-8}/h}$ for a maximum constraint relaxation on this function and its associated sub-functions with compliance with the hazard safety objectives (Cf. Fig. 7).The constraint relaxation from the THR apportionment validation allows a function to be set at a less restrictive SIL through process 2 for SIL allocation described below.

3.4 *Process 2 for SIL allocation*

The SIL allocation to safety-related functions is set in principle by a THR to SIL correspondence (Cf. table A1, EN50129 2003-appendix A); but for some complex functions including their technical realization, some specific rules must be taken into account in order to modify the allocated SIL (Cf. process 2 presented in Fig. 1) as follow (prEN50126-2 2012):

- If a sub-system implements a number of unrelated functions which require different SIL, two alternative options are possible :
  - every function meets the SIL of the function having the highest SIL;

- if demonstration of mutual non-intrusiveness can be provided, every function can satisfy its own required SIL.

  Example: local door control board deals with several remote functions (open/close doors, detect an obstacle, etc.).

– For a complex function made with various technologies (E/E/PE and others), no general rule can be given.

  Example: Let consider for instance a door locking system. To keep the door locked, safety is guaranteed both by a mechanical lock and an electronic control. The mechanical part will be built according to a code of practice (CoP); therefore the hazards are sufficiently dealt with according to the CoP approach. However, SIL may also be higher if the control is needed for other safety-related functions.

– If a function has quantitative requirements more demanding than 10^{-9} [h^{-1}], the measures and methods for SIL 4 shall at least be fulfilled, as required in standards, and the function shall be used in combination with other technical or operational measures in order to achieve the necessary THR.

  Example: redundancy principle fit in this case, especially when the available technology cannot achieve very low failure rate.

Based on the example of the Figure 7 with validated THR apportionment, the process 2 for SIL allocation application gives the following results summarized in Table 3. Functions 3 & 5 have quantitative requirements more demanding than 10^{-9} [h^{-1}], therefore, SIL 4 will be allocated to these functions in combination with other technical or operational measures.

Table 3. SIL allocation to safety-related functions

Functions/ sub-functions	**THR(/h)**	**SIL**
1. Acquire emergency brake request	$>10^{-8}$	3
1.1 Acquire emergency brake request triggered by the driver	$>10^{-8}$	3
1.2 Acquire emergency brake request triggered by automatism	$>10^{-8}$	3
1.3 Acquire emergency brake request triggered by the passengers	$>10^{-8}$	3
3. Traction break request by emergency brake	$>10^{-10}$	4
5. Execute emergency brake	$>10^{-10}$	4

4 CONCLUSION

Functional safety standards require that SIL has to be allocated to safety-related functions but these standards differ in their derivation of SILs resulting to the misuse of the concept. Based on a state of the art of the SIL use in different domains and some consultations, a SIL allocation methodology is proposed and detailed with examples for an application to a generic TCMS rolling stock. This paper clarifies the specific rules that are implicitly used to guide the THR apportionment (process 1) and then SIL allocation process (process 2). The "Passengers doors" and "Emergency brake" sub-systems are retained as applications studies; the proposed methodology allows the THR apportionment to all fault tree functions and the SIL allocation.

Future research will concentrate on the need for feedback from already consulted organisms for improved guidance in term our generic SIL allocation methodology development.

5 REFERENCES

Draft Regulation LOC&PAS TSI. 2013. Technical Specification for Interoperability relating to the 'rolling stock – locomotives and passenger rolling stock' subsystem of the rail system in the European Union.

EN 14752. 2006. Railway applications – Bodyside entrance systems. CENELEC.

EN 15380. 2013. Railways applications – Classification system for railways vehicles – Part 4: Function groups. CENELEC.

EN 50129. 2003. Railways applications – Communication, signaling and processing systems – Safety related electronic systems for signaling. CENELEC.

EN 62290-2. 2012. Railway applications – Urban guided transport management and command/control systems – Part 2: Functional requirements specification. CENELEC.

ERA, 2009. Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation.

IEC 61508. 2011. Functional safety of E/E/PE safety-related systems. IEC 61508-1 to 7

IEC 61511. 2003. Functional safety - Safety instrumented systems for the process industry sector.

IEC 62061. 2005. Safety of machinery - Functional safety of electrical, electronic and programmable control systems for machinery.

IEEE 1012. 2012. IEEE standard for system and software verification and validation. IEEE-SA Standards Board.

MIL-STD-882 E. 2012. Department of Defense Standard Practice - System Safety.

MODSafe 2010. WP 4 – D4.1 State of the art analysis and review of results from previous projects. Modular Urban Transport Safety and Security Analysis.

MODURBAN 2006. WP23 – D 86. Safety Conceptual Approach for functional and technical prescriptions. Modular Urban guided Rail systems.

Ouedraogo K.A., Beugin J., El-Miloudi E.-K., Clarhaut J., Renaux D., Lisiecki F. 2014. Allocation rules of Safety Integrity Levels in a generic TCMS application. FORMS-FORMAT, Braunschweig, Germany, septembre.

prEN50126. 2012. Railways applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). CENELEC standard project Part 1 to 5.

Regulation 402/2013/EU on the Common safety method for risk evaluation and assessment.

Rouvroye J. L. 2001. Enhanced Markov Analysis as a method to assess safety in the process industry. Beta Research School for Operations Management and Logistics. Technische Universiteit Eindhoven. The Netherlands.

Smith D. J. and Simpson K. G. L. 2004. Functional safety: a straightforward guide to IEC 61508 and related standards.