PARIS
2 ▶ 7
OCTOBER
2016 ▶ Pullman Bercy Hotel

INTERNATIONAL
RAILWAY SAFETY COUNCIL

Safety Integrity Level allocation shared or divergent practices in the railway domain

▶The transport of the future and the imperatives of safety

K. Abel Ouedraogo, Researcher (IFSTTAR)
Julie Beugin, El-Miloudi El-Koursi (IFSTTAR), Joffrey Clarhaut, Dominique Renaux (UVHC) and Frédéric Lisiecki (EPSF)

Contents

INTERNATIONAL RAILWAY SAFETY COUNCIL

Introduction

Development of a generic methodology for SIL determination and allocation in a railway system (especially TCMS):

- Generic methodology/guide: harmonized? European?
- Linked with: Common Safety Method (CSM), railway standards.

Project: **2 years (From June 2013 to June 2015)**

Funded by: **EPSF**

Research partners: **IFSTTAR and TEMPO (University of Valenciennes)**

Introduction

SIL - used to specify the safety requirements of safety-related functions performed by Electrical/Electronic/Programmable Electronic (E/E/PE) system

- characterized by discrete indicators : a four level scale
- SIL 4 is the most constraining safety level and SIL 1 is the lowest one (sometimes 5 levels are used with SIL 0).

Various methodologies are adopted to perform the SIL allocation : from a rigorous quantitative estimation to a simple qualitative evaluation.

Several issues in the need to harmonize SIL allocation methodology:

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

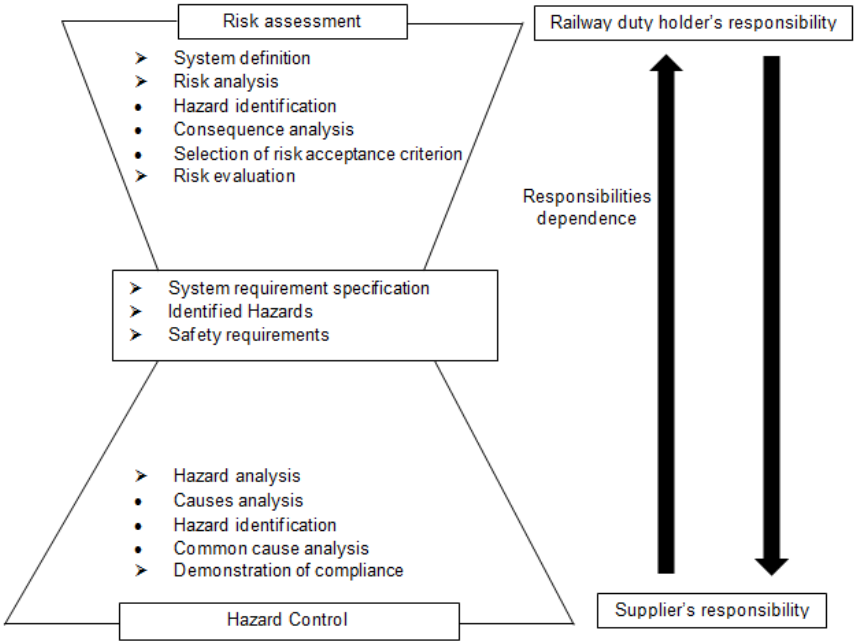
Introduction

- Discussions results stemming from various rail stakeholders' consultations on their SIL use and/or allocation practices.
- Shared and divergent practices in the SIL allocation leading to a homogeneous allocation methodology proposition
- The methodology description and its implementation are presented in detail in [1].

[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.

The hourglass model for risk management 1/2

- The Hourglass Model : overview of the major safety-related activities during the development of a technical system (including the corresponding responsibility).

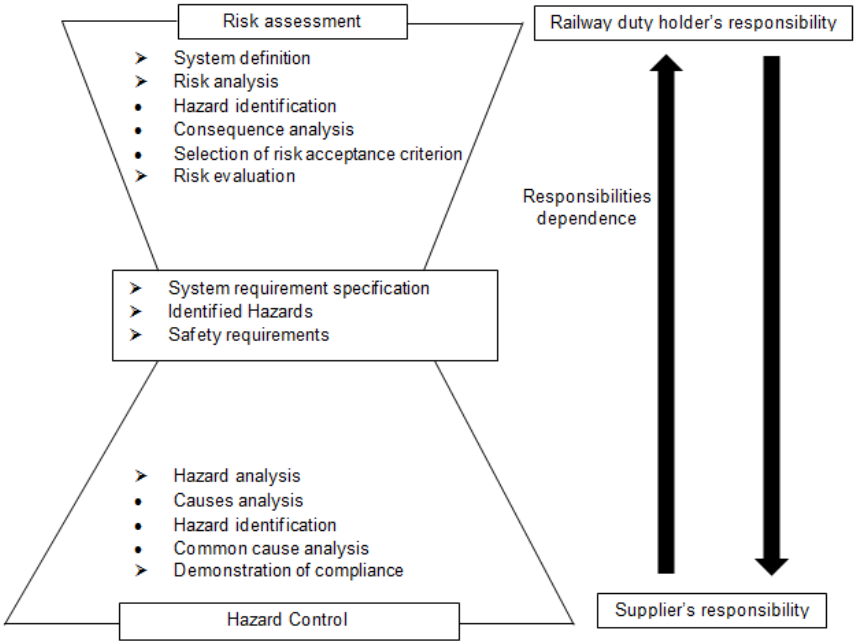


➢ **<u>risk assessment phase :</u>**

specifying the system requirements (list of identified hazards, set of functions, subsystems or operating rules safety requirements)

The hourglass model for risk management 2/2

- The Hourglass Model : overview of the major safety-related activities during the development of a technical system (including the corresponding responsibility).



➢ **<u>hazards control :</u>**
ensuring/demonstrating that the specified system is in compliance with safety requirements (determination and analysis of the system internal causes and the appropriate measures implementation).

SIL use according to railway actors 1/2

- 3 points of views on SIL uses are different and contradictory depending on choices made by involved railway stakeholders (rail duty holder, manufacturers, or notified bodies).

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.

SIL use according to railway actors 2/2

Description of a SIL particular use	Point of view 1	Point of view 2	Remarks
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.

THR (Tolerable Hazard Rate)

SIL allocation practices 1/7

- 4 SIL allocation practices (and associated actor's reactions) are different and contradictory depending on choices made by involved railway stakeholders.

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.

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).		

SIL allocation practices 2/7

- SIL allocation practices

Allocation approach characteristic	Practice 1	Practice 2	Remarks and Examples
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	Identification of each scenario from a given accident in which event combinations from technical, human or operational origin can jointly occur.	- 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.

SIL allocation practices 3/7

- Actor's reactions on this SIL allocation practice

Allocation approach characteristic	Practice 1	Practice 2	Remarks and Examples
2. Level of breakdown of	Identification of all functional failure	Identification of each scenario from a given	- In practice 2, a preliminary step is to use the risk graph as a method for allowing a ive' results), associated constraining

Ref. Table 2	Operators	Notified Bodies	Manufacturers
2.	**Remark:** For the operator, SIL allocations provided by the manufacturers include a large heterogeneity in the details provided. The necessary breakdowns level is the one that ensures the demonstration	**Practice 1:-** There is an activity 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). How to meet this target? - In a functional allocation approach, the requirement is on function (regardless of the system technology in use).	**Practice 2:-** The system actor at the highest level can only allocate functional requirements to lower level actors. ➔Design choices, to perform a safety analysis in order to identify if their system is safe or not (demonstration approach rather than allocation).

SIL allocation practices 4/7

- SIL allocation practices

Allocation approach characteristic	Practice 1	Practice 2	Remarks and Examples
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)	Allocation of a safety target related to hazard (in a specific accident scenario) by apportioning the risk reduction weight on 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 handling a hazard (**practice 2**). Allocating risk reduction weight to the system safety-related functions (to comply with the hazard safety requirements, **practice 1**),(demonstration approach)

SIL allocation practices 5/7

- Actor's reactions on this SIL allocation practice

Allocation approach characteristic	Practice 1	Practice 2	Remarks and Examples

Ref. Table 2	Operators	Notified Bodies	Manufacturers
3.	**Practice 1:** The operator has to control external events (especially risk reduction brought by the system external barriers,): not the same external events according to the operated lines (conventional line, automated line, driverless line with specific procedures).	- **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.	**Practice 2:** THR 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 **Remark:** The SDT has a direct impact on the THR choice: the lower the SDT is, the higher the rate is.

SIL allocation practices 6/7

- SIL allocation practices

Allocation approach characteristic	Practice 1	Practice 2	Remarks and Examples
4. Allocation practices in various accident scenarios involving the same function	If the same function is active in several scenarios, the most constraining requirement from all scenarios is used.		Automatic emergency braking triggered by the train driver or triggered as soon as the train losses its catenary power supply.

SIL allocation practices 7/7

- Actor's reactions on this SIL allocation practice

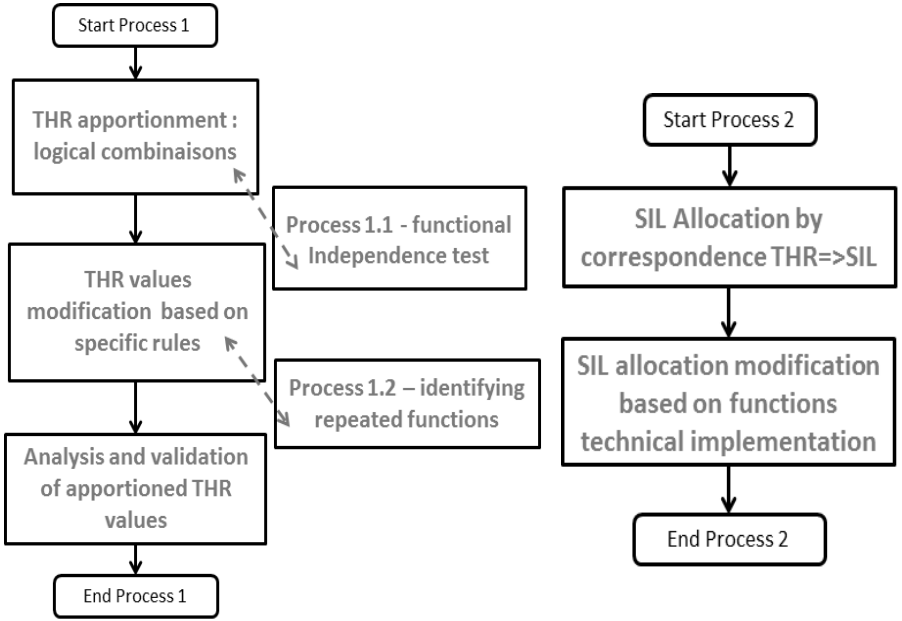
Allocation approach characteristic	Practice 1	Practice 2	Remarks and Examples
4. Allocation practices in various accident scenarios involving the same function	If the same function is active in several scenarios, the most constraining requirement from all scenarios is used.		Automatic emergency braking triggered by the train driver or triggered as soon as the train losses its catenary power supply.

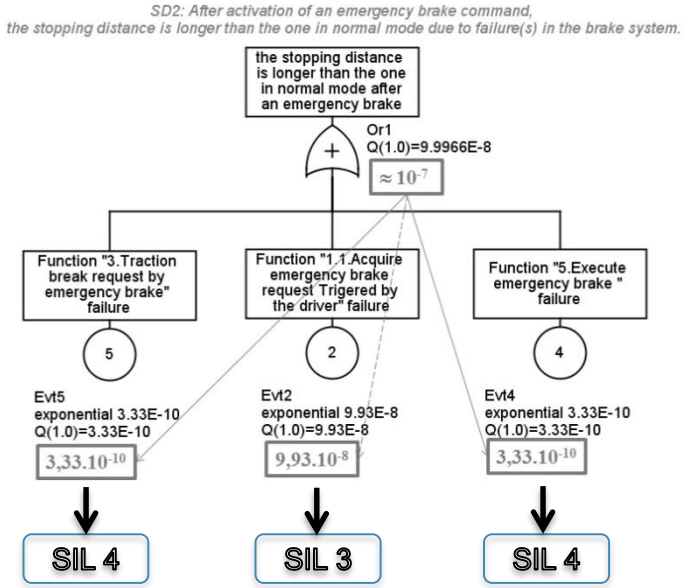
Ref. Table 2	Operators	Notified Bodies	Manufacturers
4.			**Specifications on accident scenarios:** These scenarios are jointly defined between the manufacturer and its suppliers to fix a safety target. At the rolling stock level, the manufacturer receives information on the safety performance of supplier's equipment in order to verify if the proposed equipment performance can be selected or if new more robust equipment should be developed.

INTERNATIONAL RAILWAY SAFETY COUNCIL

Toward a SIL allocation methodology

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





Conclusion

Highlighted and focused on the **SIL allocation shared or divergent practices in railway domain:**

- different points of views related to SIL uses,
- different SIL allocation practices and
- the associated actor's reactions on these allocation practices are described with examples.

The retained practices are included in **a methodology for a harmonized SIL allocation method.**

Possible evolutions according to the changes in regulations

Thank you for your attention

Abel Ouedraogo

IFSTTAR – French institute of science and technology for transport, spatial planning, development and networks

COSYS – Components and Systems

ESTAS – Evaluation and safety of automated transport systems

abel.ouedraogo@ifsttar.fr

INTERNATIONAL RAILWAY SAFETY COUNCIL