PRATIQUES PARTAGÉES OU DIVERGENTES D'ALLOCATION DE NIVEAUX D'INTÉGRITÉ DE SÉCURITÉ DANS LE DOMAINE FERROVIAIRE

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

Beugin J., Ouedraogo K. A., El-Koursi E.M.
Univ Lille Nord de France, IFSTTAR
20 rue Élisée Reclus
59650 Villeneuve d'Ascq

Clarhaut J., Renaux D.
Univ Lille Nord de France, LAMIH
Le Mont Houy
59313 Valenciennes, Cedex 9

Lisiecki F.
EPSF
60 rue de la Vallée
80000 Amiens

Résumé

Les conditions de conception et d'exploitation des systèmes ferroviaires au sein de l'U.E sont régies par des directives, des règlements, des décrets, normes qui permettent, notamment, d'assurer la sécurité du système global de transport. Cependant, chaque état membre de l'U.E. a développé ses propres règles de sécurité en se basant sur ses propres concepts techniques et opérationnels. Les pratiques divergentes qui résultent de ce constat suscitent aujourd'hui une volonté d'harmoniser les méthodes et les objectifs de sécurité ferroviaire via l'adoption de Spécifications Techniques d'Interopérabilité (STI), la définition d'Objectifs de Sécurité Communs (OSC) et la définition d'une Méthode de Sécurité Commune (MSC). Ainsi, la maîtrise du risque résiduel du système ferroviaire implique, au travers d'un processus de gestion des risques, d'allouer des objectifs de sécurité aux différentes parties du système, dont certains sont liés à des niveaux de sécurité, les SIL (Safety Integrity Level – niveau d'intégrité de la sécurité). Après avoir identifié les particularités de l'utilisation des SIL, les auteurs présentent les résultats de discussions issus de consultations avec différents acteurs ferroviaires (exploitants, organismes notifiés et constructeurs) sur les pratiques d'allocation des SIL. L'objectif est de mettre en avant les points qui font consensus et ceux, au contraire, qui font débat et de proposer au final, une méthodologie homogène d'allocation de SIL pour le domaine ferroviaire. Détaillée dans [Ouedraogo *et al.* 2015], la mise en œuvre de cette méthodologie sous la forme d'un guide d'application pratique permettra aux différents acteurs concernés par l'allocation des SIL (donneurs d'ordre, constructeurs, systémiers, etc.) de répondre à cette problématique.

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, 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 point of a SIL allocation and to propose an harmonized SIL allocation methodology in the railway domain. More detailed in [Ouedraogo *et al.* 2015], a 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

Les conditions de conception et d'exploitation des systèmes ferroviaires sont aujourd'hui régies, en Europe, par des règles décrites dans des textes juridiques (directives, règlements, décrets, etc.) et un référentiel normatif. Ces conditions permettent notamment d'assurer la sécurité des circulations en imposant l'apport de preuves de gestion des risques des sous-systèmes impliqués. Jusqu'à présent, les états membres de l'U.E ont mis au point leurs règles de sécurité principalement sur la base de concepts techniques et opérationnels nationaux. De ce fait, des différences existent et peuvent affecter le fonctionnement optimal des transports ferroviaires dans l'U.E. Pour répondre aux objectifs d'harmonisation, des étapes ont été franchies avec l'adoption de Spécifications Techniques d'Interopérabilité (STI), la définition d'Objectifs de Sécurité Communs (OSC) et la définition d'une Méthode de Sécurité Commune (MSC). Cette dernière fait l'objet du règlement 402/2013/UE mis en place par l'Agence Ferroviaire de Sécurité. L'unification des méthodes et des objectifs de sécurité ferroviaire se poursuit, en lien avec le référentiel normatif initial composé des normes EN 50126, EN 50128 et EN 50129 (leur révision étant en cours). Ces normes de sécurité ferroviaire décrivent les aspects sécuritaires à appliquer aux différents niveaux du cycle de vie d'un système ferroviaire. Elles s'appuient, de la même manière que la MSC sur un processus de gestion des risques qui implique d'allouer des objectifs de sécurité aux différentes parties du système, dont certains sont liés à des niveaux de sécurité, les SIL (Safety Integrity Level – niveau d'intégrité de la sécurité), afin de maîtriser le risque résiduel du système complet (La MSC n'intègre pas le concept de SIL pour le moment).

Le concept de SIL a été introduit, de manière générique, pour la sécurité des systèmes E/E/PE (Électrique / Électronique / Électronique Programmable). Il permet de tenir compte, dans la spécification d'exigences de tels systèmes, à la fois :

- du côté aléatoire des défaillances pouvant survenir suite à des problèmes au sein de ses équipements matériels,
- du côté déterministe lié aux problèmes de conception globaux du système, les problèmes de fautes systématiques en conception logicielle étant les plus surveillés et analysés.

Néanmoins, différentes méthodes sont utilisées pour réaliser l'allocation des SIL aux « fonctions relatives à la sécurité » d'un système. Les différences fondamentales dans ces méthodes proviennent souvent de l'approche initiale adoptée pour mener

l'évaluation du ou des risques, cette approche pouvant varier d'une estimation quantitative rigoureuse à une simple évaluation qualitative avec entre-deux, la possibilité d'une approche semi-quantitative [Blanquart *et al.* 2012].

De plus, plusieurs difficultés rencontrées pour construire une méthodologie harmonisée d'allocation des SIL, sont inhérentes à l'utilisation des niveaux d'intégrité de sécurité comme :

- le faible niveau d'harmonisation des définitions au travers des différentes normes sectorielles qui utilisent le concept de SIL (ex. l'IEC 61511 pour l'industrie des processus, l'IEC 62061 pour la sécurité des machines, l'ISO 26262 pour l'industrie automobile) ;
- les différents critères associés qui sont soit relatifs à la défaillance d'un équipement unique de sécurité (probabilité de défaillance dangereuse par heure – PFH, probabilité moyenne de défaillance à la demande – PFDavg), soit liés aux dangers en sortie du système global compte tenu de plusieurs défaillances dans le système (ex. taux de danger tolérable – THR) ;
- La prise en compte de la complexité du système dès lors que l'obtention des SIL est obtenue à partir d'estimations de fiabilité/disponibilité sur ce système.

Cet article a pour but de présenter les résultats de discussions issus de consultations avec différents acteurs ferroviaires sur leurs pratiques d'allocation/utilisation des SIL (Satey Integrity Level). En particulier seront mis en avant les points qui font consensus ou ceux, au contraire, qui font débat et qui ont servi au final, à élaborer une méthodologie d'allocation de SIL. La méthodologie obtenue a pour but de servir de démarche homogène d'allocation des SIL dans le domaine ferroviaire. La description de sa mise en œuvre, présentée plus en détails dans [Ouedraogo *et al.* 2015], vise à constituer un guide que l'EPSF proposera aux différents acteurs concernés par la problématique d'allocation des SIL dans les systèmes de sécurité ferroviaire (donneurs d'ordre, constructeurs, systémiers, etc). Les principes de la méthodologie seront rappelés brièvement dans cet article pour se focaliser en priorité sur les pratiques partagées d'allocation et celles qui restent divergentes. Par rapport à ces dernières, le choix retenu dans la méthodologie sera argumenté. Au préalable sera rappelé le vocabulaire précis lié à la gestion des risques et les acteurs intervenants.

Depuis l'allocation d'objectifs de sécurité vers l'allocation de niveaux d'intégrité de sécurité au sein d'une démarche de gestion des risques ferroviaire

La démarche de mise en sécurité d'un système ferroviaire global ou d'un sous-système défini inclut une phase d'analyse des risques et une phase de maitrise des situations dangereuses [Blas *et al.* 2008]. Pour tout système technique ferroviaire, un niveau de sécurité acceptable doit être assuré et le modèle du sablier présenté sur la figure ci-dessous, fournit une vue générale des principales activités nécessaires relatives à la sécurité. L'analyse des risques dans le domaine des transports ferroviaires s'appuie communément sur les rôles distincts des acteurs tenus de mettre en œuvre ce processus : l'autorité de transport qui va exploiter le système, et le constructeur ou le fournisseur concevant et réalisant le système. Ceci permet le partage des responsabilités entre les entités. Dans la pratique et en fonction du contexte de chaque projet, plusieurs entités interviennent d'une part ; et d'autre part, le partage des responsabilités entre les entités n'est pas aussi clair et définitif, ceci afin d'avoir une certaine latitude de conception (certaines orientations, objectifs, règles d'exploitation différentes en fonction des Matériels Roulants, etc.) et ainsi faciliter l'innovation. De manière générale, les entités qui interviennent sont classées en 2 groupes, le premier étant le client de l'autre et cette réciprocité se retrouvant à différents niveaux de définition du système :

- le **maître d'ouvrage** (**MOA**) est l'entité porteuse du besoin. Elle définit l'objectif du projet, son calendrier et le budget consacré à ce projet.
- Le **maître d'œuvre** (**MOE**) est la personne ou l'entité choisie par le maître d'ouvrage pour la réalisation d'un projet dans les conditions de délais, de qualité ainsi que de coûts fixés par ledit projet, le tout conformément à un contrat.

Deux aspects principaux se dégagent du modèle de gestion des risques : l'appréciation du risque et la maîtrise des situations dangereuses [prEN 50126 2015] [Braband 1999].

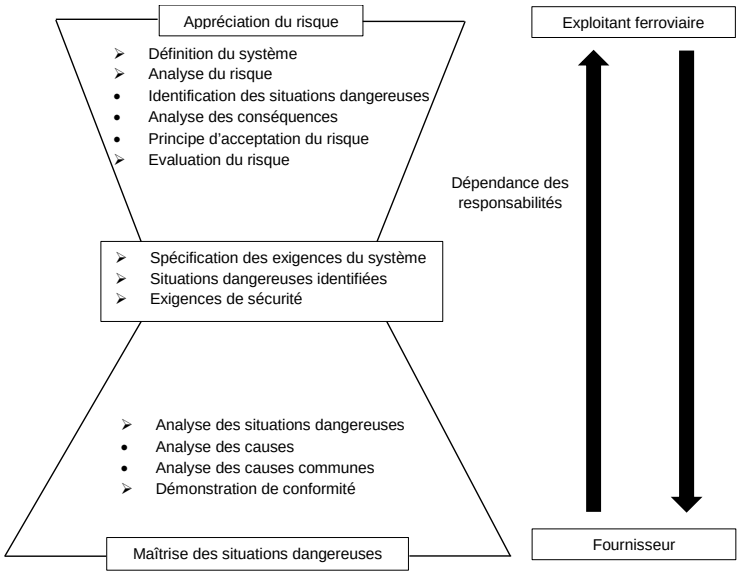

Figure 1. Gestion des risques dans le domaine des transports guidés, adaptée de [prEN 50126 2015]

1 L'appréciation du risque

L'appréciation du risque est un processus couvrant une analyse de risque et une évaluation des risques [Règlement 402/2013] à partir de la définition du système. L'analyse du risque comprend l'identification des situations dangereuses (conditions pouvant conduire à un accident) ainsi que les contextes opérationnels associés, l'analyse des conséquences et la sélection des principes d'acceptation du risque et les critères associés. L'accident est défini comme un événement ou série d'événements inattendus conduisant au décès, à des blessures, à des dommages aux biens ou à l'environnement [prEN 50126 2012]. L'analyse des conséquences permet d'identifier les liens entre les situations dangereuses et les accidents, pour chaque scénario d'accident (à l'aide de diagrammes causes-conséquences et d'arbres d'événements par exemple). L'acceptabilité des risques pour le système étudié est évaluée sur la base de l'un ou de plusieurs des principes suivants d'acceptation des risques :

- l'application de règles de l'art (appelées aussi codes de pratique) et/ou
- la comparaison avec des systèmes similaires (appelés aussi systèmes de référence) et/ou
- une estimation explicite des risques.

On procède généralement à l'estimation explicite des risques [ERA 2009] :

- lorsque les codes de pratique (CoP) ou les systèmes de référence ne peuvent pas être appliqués pour maîtriser entièrement les risques à un niveau acceptable. Cette situation se présente typiquement lorsque le système évalué est entièrement nouveau ou lorsqu'il y a des déviations par rapport à un code de pratique ou à un système de référence similaire;
- lorsque la stratégie de conception choisie ne permet pas d'utiliser des codes de pratique ni des systèmes de référence similaires, par souhait notamment de concevoir un système plus économique mais n'ayant jamais été utilisé (exemple, localisation des trains non plus par le biais de balises distribuées le long des voies mais à l'aide d'un système de localisation satellitaire embarqué dans les trains moins coûteux à maintenir).

Cette phase d'appréciation du risque permet de spécifier les exigences du système en constituant la liste des situations dangereuses identifiées et un ensemble d'exigences de sécurités liées à des fonctions, des sous-systèmes ou des règles d'exploitation.

2 La maîtrise des situations dangereuses

Le second aspect du processus de gestion des risques est la maîtrise des situations dangereuses et consiste à s'assurer/démontrer que le système défini est conforme aux exigences de sécurité par la détermination et l'analyse des causes internes au système ainsi que la mise en œuvre des mesures adéquates.

Les risques liés au dysfonctionnement des fonctions relatives à la sécurité et aux systèmes qui réalisent ces fonctions, sont maitrisables en respectant un ensemble de mesures techniques imposées par la réglementation ou par les normes. Seuls les risques induits par les systèmes E/E/PE sont traités par une évaluation des risques suivie d'une allocation d'objectifs de sécurité (souvent associés à des catégories de fréquence). Ceux liés aux systèmes mécaniques ou pneumatiques sont traités par des CoP ou des systèmes de référence. La notion de niveau d'acceptabilité des risques a été développée dans la norme IEC 61508 et les normes ferroviaires EN 50126. Une combinaison matricielle de la gravité et de la fréquence d'occurrence de l'accident permet de fixer les niveaux d'acceptabilité. Une fréquence ou taux maximal d'occurrence acceptable pour la situation dangereuse considérée notée THR (Tolerable Hazard Rate) est déterminé en nombre d'évènements dangereux par heure [Blas *et al.* 2008].

En principe, il convient que la société d'exploitation ferroviaire spécifie/alloue l'objectif de sécurité THR de sorte que le concepteur du système soit en mesure de déterminer si la conception du système est capable de satisfaire aux critères. Dans la pratique, la société d'exploitation ferroviaire détermine les objectifs au niveau du système ferroviaire et peut avoir besoin de collaborer avec l'industrie ferroviaire pour définir le THR au niveau de la situation dangereuse technique [prEN 50126 2015]. L'étape suivante consiste à déterminer les niveaux d'intégrité de la sécurité (SIL) des fonctions à partir des objectifs de sécurité alloués initialement dans la plupart des cas sous forme de THR associés à chaque situation dangereuse (certains SIL peuvent être alloués directement par l'exploitant).

3 Le concept de SIL

Les SIL (*Safety Integrity Levels*, niveaux d'intégrité de sécurité) sont des niveaux discrets définis pour spécifier le niveau cible d'exigences en matière d'intégrité de sécurité de fonctions relatives à la sécurité, celles-ci étant réalisées par des systèmes E/E/PE (cf. norme IEC 61508-partie 4 2011). La propriété d' « intégrité de sécurité » caractérise la manière dont sont contrôlées les défaillances aléatoires[1] et les défaillances systématiques[2] liées à un mode de défaillance dangereux d'une fonction relative à la sécurité[3]. Cette propriété est donc associée, pour définir un SIL, à un objectif chiffré de défaillance dangereuse et à des exigences concernant l'évitement et la maîtrise d'anomalies systématiques (cf. « capabilité systématique » dans la norme IEC 61508).

[1] Les **défaillances aléatoires** résultent de mécanismes de dégradation aléatoires du matériel ; leurs occurrences peuvent être quantifiées à l'aide de mesures telles que la fréquence moyenne de défaillance.

[2] Les **défaillances systématiques** sont des défaillances latentes liées de façon déterministe à des causes données ; elles se révèlent durant la phase d'exploitation du système opérant sous certaines conditions.

[3] Le langage courant emploie fréquemment le raccourci de **fonctions de sécurité**. L'ensemble des **fonctions relatives à la sécurité** incluent le sous-ensemble des fonctions de sécurité. La distinction entre les deux a été explicitée dans la norme [prEN50126 2015], les fonctions relatives à la sécurité étant les *fonctions dont la défaillance affecte la sécurité*, et les fonctions de sécurité étant les *fonctions dont le seul objectif est d'assurer la sécurité*. En fait, les premières n'ont pas pour rôle premier de réduire le risque mais leur défaillance génère néanmoins des risques (ex. : maintenir la vitesse, ouvrir les portes). Les secondes ont ce rôle premier de réduction des risques (ex. : contrôler la vitesse, verrouiller les portes) et contribuent à la mise en œuvre de **barrières de sécurité techniques** (une barrière étant définie dans cette même norme, au sens général, comme un moyen physique ou non physique qui réduit la fréquence d'une SD et/ou d'un accident potentiel causé par la SD et/ou qui réduit la gravité des accidents potentiels causés par la SD).

Les SIL sont caractérisés par des indicateurs discrets positionnés sur une échelle à quatre niveaux. Sur cette échelle, le SIL 4 désigne le plus haut degré d'intégrité de sécurité et est associé aux exigences de sécurité les plus contraignantes, le SIL 1 possède le plus bas degré d'intégrité de sécurité (parfois 5 niveaux sont utilisés avec le SIL 0).

La partie suivante présente les pratiques d'utilisation / d'allocation des SIL issues de consultations avec différents acteurs ferroviaires dans le cadre de la mise en place d'une méthodologie harmonisée d'allocation des SIL. Il s'agit d'une proposition émanant de travaux de projet qui n'a pas valeur de règle nationale. Ces travaux ne visaient pas à développer une méthode supplémentaire (de nombreuses méthodes étant déjà disponibles) mais à proposer une méthodologie tenant compte de plusieurs pratiques existantes et largement employées tout en formalisant des principes implicitement utilisés.

Pratiques d'utilisation / d'allocation des SIL selon les acteurs ferroviaires

Le tableau 1 présente, sur chaque ligne, deux points vue principaux (parmi d'autres) rencontrés lors d'une utilisation particulière du SIL. Le tableau 2 présente, sur chaque ligne, des pratiques qui orientent les démarches d'allocation (les colonnes sont fusionnées lorsqu'il y consensus sur la pratique). Ces points de vue et pratiques sont le plus souvent différents et parfois contradictoires car dépendent de choix adoptés par les acteurs ferroviaires rencontrés, qu'ils soient exploitant ferroviaires, constructeurs, organismes notifiés pour la certification ferroviaire (cf. Table 3 présentant les pratiques préconisées selon les acteurs).

Les normes actuelles tentent d'harmoniser les démarches d'analyse de risques et leurs processus associés (identification des dangers, des scénarios d'accidents, des causes de dangers, allocation des objectifs de sécurité, etc.) pour renforcer les faiblesses des méthodes existantes, notamment vis-à-vis des mutations que subissent le secteur ferroviaire (ex. nouvelle distribution des responsabilités, essor des nouvelles technologies à bord des trains, ou sur voie ou au niveau des postes de contrôle). Ces mutations visent à obtenir des systèmes plus performants mais les rendent en revanche beaucoup plus complexes, en particulier pour l'analyse de leur sécurité [Blas *et al.* 2008]. Il en résulte de nombreux débats pour l'évolution des démarches à retenir dans les normes révisées, notamment beaucoup de discussions sur ces aspects se tiennent dans le cadre de la dernière version du projet de norme prEN50126 qui est mis actuellement à l'enquête et ceci depuis plusieurs mois.

À noter que la norme EN50126 initialement dédiée au système de signalisation ferroviaire évolue pour toucher un plus grand nombre de systèmes (les systèmes de signalisation, le matériel roulant, le système d'alimentation électrique pour les installations fixes). La norme EN50129 est également en cours de maintenance. La version 2001 de la norme EN50128 peut encore être considérée dans certains cahiers des charges alors qu'il existe une version plus récente de 2011. Enfin, dans le droit européen, les normes EN ne sont pas obligatoires pour le domaine suburbain (mais leur utilisation et souvent spécifiée dans les cahiers des charges) sauf si les systèmes concernés sont des systèmes de contrôle/commande et de signalisation dans le cadre de contrats européens, ou alors, des systèmes mixtes exploités en partie sur un réseau urbain, en partie sur un réseau national (exemple : tram-train).

Description d'une utilisation particulière du SIL	Point de vue 1	Point de vue 2	Remarque / exemple
1. Utilisation du SIL 0 adjointe aux autres niveaux SIL1 à SIL4	Le SIL 0 est alloué aux fonctions non liées à la sécurité, ces fonctions constituant toutefois une première marche pour réduire le risque. Ce type de fonction, bien que développé avec un faible niveau de confiance, apporte une réduction de risque minimum mais non négligeable (par exemple : réduction de l'occurrence d'un accident inférieure ou égale à un facteur 10).	Les fonctions qui ont un impact sur la sécurité doivent être allouées à minima à un SIL1.	- Ce point vient du fait que la norme EN 50128 de 2001 utilise le SIL 0 pour les fonctions non liées à la sécurité et réalisées par un logiciel alors que celle de 2011 utilise le SIL 0 pour les fonctions qui ont un impact sur la sécurité, même si cet impact est faible. - La prEN50126 introduit la notion de *basic integrity* (pas encore adoptée). Cette notion repose sur le 1er point de vue.
2. SIL d'une fonction combinant deux sous-fonctions dépendantes ou indépendantes entre-elles	Seules les règles logiques combinant des taux liés aux sous-fonctions (THR) sont considérées pour obtenir le SIL de la fonction. Les SIL sont alloués selon la plage de THR associée à la fonction et selon indépendance des sous-fonctions.	Des fonctions avec un SIL de bas niveau peuvent être combinées pour obtenir une fonction avec un SIL de plus haut niveau. (ex. une fonction SIL 4 peut être obtenue par 2 sous-fonctions indépendantes de SIL2)	La notion d'indépendance n'est pas encore arrêtée dans la prEN 50126 car s'il y a dépendance, il faut trouver la modélisation qui convienne. L'approche de l'EN50126 est encore en discussion et va évoluer.
3. Fonction qui peut faire intervenir en partie un opérateur humain	L'opérateur humain est pris en compte dans les études en le considérant comme fiable (résilient) ou, à l'opposé, non fiable. Dans ce cas, il joue sur l'allocation.	L'opérateur humain est exclu.	Dans l'exemple de la fonction « acquérir une demande de FU » un ensemble de solutions est possible pour la mise en sécurité comme, faire remonter une alarme en cabine pour que le conducteur soit à l'origine de la demande ou, un mécanisme de détection automatique peut être à l'origine de la demande. Le SIL reste le même quelle que soit la solution.

Table 1. Points de vue différents identifiés sur des utilisations liées au SIL

Caractéristique d'une démarche d'allocation	Pratique 1	Pratique 2	Remarques et exemples
1. Degré de gravité des conséquences suite à la défaillance d'une fonction pour allouer les SIL	Des démarches d'allocation font apparaître un lien direct entre SIL et le degré de gravité de la défaillance fonctionnelle.	Le taux de sollicitation de la fonction (selon l'occurrence du danger) associé au degré de gravité si elle défaille, permettent de déterminer un SIL.	- La **pratique 1** tend à être proscrite. - La **pratique 2** peut être illustrée par l'exemple suivant : la défaillance de la protection contre une survitesse n'est pas critique s'il n'y a pas de survitesse.
2. Niveau de décomposition des causes d'un accident en causes fonctionnelles pour allouer des SIL (i.e. à quel niveau s'arrêter)	Identification de toutes les causes de défaillances **fonctionnelles** menant jusqu'à la situation dangereuse (causes **en amont** du danger, i.e. évènements qui se combinent pour mener au danger)	Identification de chaque scénario issu d'un accident donné (causes **en aval** du danger, i.e. évènements faisant suite à l'occurrence du danger jusqu'à obtenir un accident) dans lesquels des combinaisons d'évènements d'origine technique, humaine ou opérationnelle peuvent intervenir conjointement.	- Dans la **pratique 2**, une démarche préliminaire consiste à utiliser le graphe de risque[4] comme une méthode permettant de faire une allocation préalable de SIL car ses résultats sont reconnus comme étant 'conservateurs', i.e. ils mènent à des niveaux dont les exigences de sécurité associées sont plus contraignantes que réellement nécessaires. Dans cette démarche, si le résultat issu du graphe de risque identifie le besoin de mettre en œuvre une fonction de sécurité de niveau très élevé, un autre outil pour une décomposition plus fine sera employé (comme un graphe d'évènements ou un arbre de défaillances). De plus, le graphe de risque est limité car il ne tient compte que d'une seule possibilité d'évitement du danger même si plusieurs existent.
3. L'élément concerné par une allocation d'objectif de sécurité (préalable au SIL)	Allocation d'un objectif sur les fonctions identifiées au niveau du système à l'étude (ex. matériel roulant), i.e. répartition du poids qu'on alloue au dys-fonctionnement des fonctions au départ prévues pour réduire le risque ; du fait de leur défaillance, elles n'apportent plus cette réduction.	Allocation d'un objectif de sécurité lié à un danger (dans un scénario d'accident spécifique) en répartissant le poids de réduction du risque sur les composantes humaine, opérationnelle ou technique qui réalisent une fonction liée à la sécurité.	- Exemple illustrant la **pratique 2** : pour le danger survitesse, il y aura une partie du risque qui sera prise en charge par l'infrastructure, une autre par l'exploitant et une autre sera supportée par le matériel roulant. - **Remarque associant démonstration à allocation** : l'allocation peut se voir comme allant uniquement jusqu'à la définition d'exigences de sécurité liées aux barrières (techniques/humaines/organisationnels) contrant un danger, ces barrières étant définies suite à l'analyse de scénarios d'accident (**pratique 2**). Allouer des poids de réduction du risque aux fonctions de sécurité du système (pour répondre aux exigences de sécurité liées au danger, **pratique 1**), peut se voir comme relevant d'une démarche de démonstration plutôt que d'allocation du fait qu'on cherche à montrer si le système est conforme aux exigences. La frontière n'apparait pas aussi clairement dans les pratiques. - **Remarque sur le SSIL** : La notion de 'software SIL' a disparue dans la 50128-2011 et la prEN50126 car le SIL est alloué à une fonction.
4. Pratique d'allocations au sein de différents scénarios d'accident faisant intervenir une même fonction	Pour un scénario d'accident spécifique (lorsqu'un événement déclencheur comme une survitesse pouvant conduire à un accident avec un risque inacceptable si une composante de sécurité n'intervient pas), une composante technique mise en place parmi d'autres face au risque généré par l'événement déclencheur, permet de tenir un risque final résiduel toléré. Si une même fonction intervient dans plusieurs scénarios, l'exigence la plus forte venant de l'ensemble des scénarios est retenue.		Pour illustrer 2 scénarios d'accident (l'accident étant par exemple un heurt d'obstacle) ayant un contexte différent mais faisant intervenir la même fonction (freinage automatique d'urgence) pour une même situation dangereuse (présence d'obstacle) : dans un 1er cas, le conducteur du train peut déclencher le freinage d'urgence dès qu'il aperçoit l'obstacle. Dans un 2nd cas, le freinage peut être déclenché dès que le train n'a plus d'alimentation caténaire coupée par le centre de contrôle par exemple. Les poids de sécurité reportés sur les composantes techniques et humaines seront différents d'un cas à l'autre (le conducteur pouvant supporter un poids de réduction du risque). Chaque cas mènera vis-à-vis des poids retenus, à une allocation d'exigence de sécurité différente sur la fonction, l'objectif le plus contraignant est alors retenu.

Table 2. Principales pratiques rencontrées pour allouer les SIL

[4] Pour rappel, la méthode du graphe de risque permet une représentation simplifiée de scénarios. Pour cela, une fonction de sécurité empêchant l'occurrence de l'accident lie directement une situation dangereuse et l'accident. Pour allouer un SIL à cette fonction, le scénario est qualifié à l'aide 4 critères chacun ayant une échelle associée : le taux de sollicitation, le taux d'exposition, la fréquence du danger et le degré de gravité des conséquences. Selon la valeur des critères pour le scénario analysé, la méthode mènera à un SIL spécifique pour la fonction.

Réf. Table 2	Exploitants	Organismes notifiés	Constructeurs
1.	**Pratique 2** : En fonction du degré de gravité lié aux conséquences d'un danger, on définit quel est l'objectif de sécurité associé au danger en termes d'occurrence. Si l'accident est catastrophique, de par le règlement européen 402/2013 sur la méthode de sécurité commune, l'occurrence à respecter pour une défaillance de fonction menant directement à l'accident est de 10^{E}-9 par heure, s'il est critique l'occurrence est de 10^{E}-7 par heure (ces valeurs se rapportent aux CSM-DT – *CSM-Design Targets*, qui excluent les facteurs humains et règles d'exploitation agissant comme mesures de sécurité).		
2.	**Remarque :** Au niveau exploitant, les allocations fournies par les constructeurs comprennent une grande hétérogénéité dans les niveaux de détails. Peu importe la modélisation arborescente utilisée dès lors que les interlocuteurs se comprennent. Le niveau de décomposition nécessaire est celui qui permet d'assurer la démonstration, le niveau suffisant dépend du constructeur (il peut descendre ou non jusqu'aux sous-systèmes détaillés, avec par exemple des mécanismes d'actionneur liés à la commande de frein).	**Pratique 1** - Il existe une activité préalable pour la détermination des THR qui est faite par le gestionnaire d'infrastructure ou l'entreprise ferroviaire pour un mode de défaillance donné d'une fonction (certains THR sont aussi définis au niveau des décisions Européennes dans des STI). À partir d'un THR, le constructeur va analyser comment concevoir son système / sélectionner son produit pour répondre à cet objectif. - Dans une démarche d'allocation fonctionnelle, l'exigence est sur la fonction. Avant de définir un SIL, l'exigence est définie quel que soit le type de technologie sur laquelle le système repose. L'exigence sur la fonction est commune et peut être vue comme étant atteinte par une 'boîte'. Si on utilise de l'électronique programmable pour réaliser cette 'boîte', l'exigence prend le qualificatif de SIL. Dans ce cas, cela implique des démarches particulières pour la mise sous contrôle des défaillances systématiques.	**Pratique 2** - Le donneur d'ordre de plus haut niveau d'un système ne peut qu'allouer des exigences fonctionnelles aux acteurs de plus bas niveau. Ensuite, il est de la responsabilité ces derniers, de par les choix de conception qu'ils mettent en œuvre, de faire une analyse de sécurité pour identifier si leur système est sûr. Les fonctions que le système met en œuvre peuvent induire un risque ou non (ex. : énergie par stockage d'hydrogène ou énergie électrique). Le constructeur, à partir de son produit, démontre un objectif. Il est alors dans une démarche de démonstration et non plus d'allocation. - Le donneur d'ordre qui gère le système au niveau système ferroviaire global définit en fait quel est le poids, d'un point de vue sécurité, sur la fonction de sécurité, ce poids pouvant être réparti sur des aspects techniques, humains ou opérationnels (pas uniquement techniques) - Un cas particulier est que, s'il est par exemple décidé de mettre des balises sur la voie pour réaliser une fonction SIL 4, il faut aussi que la partie embarquée au niveau du matériel roulant puisse récupérer cette information et réagir en cas de défaillance avec le même niveau de sécurité. Dans ce cas, le donneur d'ordre n'a pas besoin d'allouer le poids sur la fonction bord puisque l'exigence est déjà déduite.
3.	**Pratique 1 et remarque** Il est du ressort de l'exploitant ou du gestionnaire d'infrastructure de pouvoir maîtriser les événements extérieurs (en particulier le poids de réduction du risque apporté par les barrières extérieures au système). En effet, le matériel roulant ne sera pas soumis aux mêmes événements extérieurs selon les lignes exploitées (ligne conventionnelle, ligne automatisée, ligne sans conducteur avec des procédures spécifiques). La possibilité de relâcher un objectif de THR vis-à-vis d'événements extérieurs est donc de la responsabilité de l'exploitant ou du gestionnaire d'infrastructure.	- **Pratique 1 et 2** : D'après des observations de dossiers au niveau européen : un objectif de sécurité peut être alloué à une situation dangereuse ou, un exploitant peut aussi parfois réclamer directement une fonction SILx. C'est ce qui est notamment observé dans les transports guidés urbains lorsque le réseau est d'une certaine taille et selon la maturité de l'exploitant dans les démarches. Sur d'autres réseaux, d'autres n'ont pas cette capacité et spécifient uniquement, au niveau le plus haut d'accident un risque individuel toléré (ex. nombre de blessés par an). Dans ce cas, le constructeur qui est impliqué dans l'étude préalable de sécurité, peut dérouler un arbre défaillance en partant du risque individuel jusqu'à spécifier un poids dans l'arbre de défaillance des SIL. - la démarche SIRF en Allemagne (*Sicherheitsrichtlinie Fahrzeug* – Règlement de sécurité du matériel roulant) s'intéresse à l'allocation de THR au danger à partir de l'analyse d'un accident.	**Pratique 2** : on devrait allouer des objectifs de sécurité THR au niveau du nœud de danger dans la vue en nœud papillon de la norme EN50129 (en partant de l'accident pour établir un scénario d'accident), charge ensuite aux différents acteurs, de traiter cet objectif. De ce fait, il faudrait s'arrêter au niveau système, i.e. au niveau du système ferroviaire global. Ensuite, il s'agira pour les acteurs de démontrer que les THR sont atteints. **Autre remarque** : - le SDT (Safe Down Time) intervient dès qu'on a une porte ET dans un arbre. Il fait partie des éléments qui doivent être alloués (ceci est cependant difficile voire impossible dans une phase descendante du cycle en V, toutefois les phases du cycle sont itératives pour pouvoir reboucler et ajuster les valeurs). Le SDT a un impact direct sur le choix du taux : plus le SDT est court plus le taux peut être élevé.

4.			**Précision sur les scénarios d'accident :** Ces scénarios sont tracés conjointement entre le constructeur et ses fournisseurs pour fixer ensemble un objectif de sécurité. Au niveau matériel roulant, le constructeur reçoit des informations sur les performances de sécurité des équipements des fournisseurs afin de statuer si les performances des équipements proposés permettent de les sélectionner ou si un nouvel équipement plus robuste doit être développé.

Table 3. Réactions des différents acteurs sur les pratiques d'allocation mentionnées dans la Table 2

Compte tenu de ces utilisations et pratiques liées au SIL, la partie suivante présente les choix retenus dans la méthodologie d'allocation des SIL proposée et présentée plus en détails dans [Ouedraogo *et al.* 2015].

Choix retenus dans la méthodologie

1 Aspects généraux sur la méthodologie

La méthodologie proposée est déclinée en deux processus et leurs différentes étapes sont fondées sur des règles pratiques et des hypothèses à vérifier. Sa mise en œuvre débute par l'utilisation d'objectifs de sécurité quantitatifs, les THR. Le fait de partir de ces objectifs quantitatifs permet de tenir compte des valeurs des objectifs MSC liés à la conception de systèmes techniques (CSM-DT) récemment définies par l'ERA. Même si les THR sont des critères quantitatifs, ils sont utilisés pour spécifier des exigences quantitatives (sur l'intégrité de sécurité vis-à-vis des défaillances aléatoires) et sont liés aux exigences qualitatives (sur l'intégrité de sécurité vis-à-vis des défaillances systématiques) (cf. norme EN50129 et prEN50126).

Les arbres de défaillances, outils connus et communément employés en fiabilité et sécurité des systèmes, sont employés pour représenter les liens causes/conséquences entre l'occurrence d'une situation dangereuse et les défaillances des fonctions relatives à la sécurité associées ; d'autres formalismes pourraient tout aussi bien être utilisés comme celui des arbres d'événements ou des diagrammes de causes/conséquences.

2 1er Processus s'appuyant sur le THR

Le taux de danger tolérable (THR) est associé à un danger particulier. Il apparaît comme étant un critère qui joue beaucoup sur l'allocation des SIL dans le domaine ferroviaire. Un danger avec un taux toléré résulte de combinaisons ou d'enchaînements de défaillances maîtrisées au sein du système placé dans un contexte opérationnel particulier. On parle alors de situation dangereuse dans un scénario d'accident plutôt qu'uniquement de danger.

Dans ce processus, les éléments du système sont considérés d'un point de vue fonctionnel étant donné que plusieurs architectures matérielles/logicielles sont possibles. À noter qu'il n'y a pas d'indications explicites dans les normes ferroviaires actuelles sur la façon de réduire l'allocation des SIL à la considération d'architectures techniques particulières comme c'est le cas dans les autres normes dérivées de la norme générique IEC 61508.

Des règles de répartition du THR objectif de sécurité associé à l'occurrence d'une situation dangereuse dans un scénario d'accident considéré sont déclinées sur des fonctions et sous-fonctions relatives à la sécurité. D'une part, ces règles sont liées aux combinaisons logiques (conjonction ou disjonction) des fonctions relatives à la sécurité empêchant l'occurrence d'une situation dangereuse. Ce sont les défaillances des fonctions relatives à la sécurité en lien avec les situations dangereuses qui sont plutôt manipulées compte tenu des combinaisons entre causes dangereuses et conséquences identifiées. D'autre part, pour tenir compte des conditions techniques (dernier maillon de sécurité, indépendance fonctionnelle, solution technique complexe), des règles spécifiques de répartition/modification des THR sont définies.

Après les modifications des THR basées sur les règles spécifiques, une analyse et une validation quantitative « Down-Top » est effectuée pour vérifier la conformité de la répartition du THR objectif de sécurité de chaque situation dangereuse correspondante. Cette validation a pour but d'apporter éventuellement des réductions/modifications explicites de l'allocation des SIL en considérant des architectures techniques particulières.

À noter que lorsque l'objectif de sécurité THR n'est pas atteint, il faudra alors démontrer l'acceptabilité du risque (argumentaire à dire d'expert, raisonnement basé sur GAME, etc.).

3 2nd Processus d'allocation des SIL

L'objectif de sécurité se rapporte à une défaillance de fonction, tandis que le SIL se rapporte à une fonction : à chaque mode de défaillance d'une fonction donnée on peut attribuer un objectif de sécurité comme un THR, puis on attribue un SIL à cette fonction, à partir du THR le plus exigeant la concernant. L'allocation des SIL aux fonctions relatives à la sécurité sur la base des THR répartis et validés dans le processus précédent est alors mise en place. Dans un premier temps, l'allocation des SIL aux fonctions relatives à la sécurité se fait par la correspondance THR=>SIL (Cf. tableau A.1 de la norme EN 50129);

La manière dont sont implémentées les fonctions sur les sous-systèmes d'un train (projection des fonctions sur l'architecture matérielle/logicielle) a également un impact sur l'allocation des SIL. Des règles d'allocation spécifiques tenant compte de ces conditions d'implémentation (solutions techniques complexes, intrusion mutuelle des fonctions à implémentées, exigences de sécurité très fortes/faibles) sont également définies dans ce dernier processus; notamment pour une fonction présentant des exigences quantitatives plus sévères que 10^{-9}/h, le besoin d'y associer des méthodes et des mesures techniques ou

opérationnelles applicables au SIL 4 ; ou d'allouer au moins un SIL 1 à une fonction présentant des exigences quantitatives relative à la sécurité faibles THR≥ 10^{-5}/h.

4 Évolutions possibles de la méthodologie selon les évolutions des textes réglementaires

Le projet de norme prEN50126 (en cours de révision et sujet à des évolutions) préconise l'utilisation du concept de TFFR pour les fonctions (Tolerable Functional Failure Rate, taux de défaillance fonctionnelle tolérable) et celui de THR pour les situations dangereuses, la couche des dangers est ainsi séparée de la couche des fonctions. Pour adapter la méthodologie générique proposée, il faudra alors définir un THR (non modifiable) pour chaque situation dangereuse identifiée et une répartition en termes de TFFR aux fonctions et sous-fonctions relatives à la sécurité du système.

Conclusions

Cet article a permis de se focaliser et d'apporter un éclairage sur les pratiques utilisées pour l'allocation des SIL dans le domaine ferroviaire compte tenu de l'expérience des acteurs rencontrés, de la littérature sur ce sujet, et de travaux dans des projets de recherche passés comme MODUrban ou MODTRAIN. Celles-ci sont reprises dans un guide décrivant une méthodologie visant à harmoniser l'allocation des SIL proposé prochainement par l'EPSF.

Remerciements

Les auteurs remercient les différents exploitants, constructeurs et organismes notifiés qui ont acceptés de relire le guide méthodologique proposé, pour leurs échanges, et pour leurs remarques pertinentes et détaillées. Elles ont permis d'améliorer la méthodologie proposée compte tenu de leur expérience métier et de montrer que le débat est encore ouvert sur divers points.

Références

Braband J. (1999). 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.

Blanquart, J. P., Astruc, J. M., Baufreton, P., Boulanger, et al., 2012, Criticality categories across safety standards in different domains. 6th conference on Embedded Real Time Software and Systems.

Blas A., Boulanger J.-L, 2008, Comment améliorer les méthodes d'analyse de risques et d'allocation des THR, SIL et autres objectifs de sécurité. Lambda-Mu 16, Avignon 6-10 Octobre 2008.

ERA (2009). Guide d'application du règlement de la commission concernant l'adoption d'une méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques visée à l'article 6, paragraphe 3 de la directive sur la sécurité ferroviaire, ERA/GUI/01-2008/SAF, Agence Ferroviaire Européenne, Valenciennes.

Ouedraogo K.-A., Beugin J., El-Koursi E.-M., Clarhaut J., Renaux D., Lisiecki F, 2015, 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.

prEN 50126 (2015). Applications ferroviaires: spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS). Projet de norme du CENELEC à l'enquête, Comité Européen de Normalisation Électrotechnique.

Règlement d'exécution 402/2013/UE, 2013, Méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques d'un système ferroviaire. Commission Européenne, modifications apportées dans le règlement d'exécution 2015/1136 au 13 juillet.