SLOVENSKI STANDARD
SIST EN 50126-2:2018

01-januar-2018

Nadomešča:
SIST-TP CLC/TR 50126-2:2007

Železniške naprave - Specifikacija in prikaz zanesljivosti, razpoložljivosti, vzdrževalnosti in varnosti (RAMS) - 2. del: Sistemski pristop k varnosti

Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 2: Systembezogene Sicherheitsmethodik

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 2: Approche systématique pour la sécurité

Ta slovenski standard je istoveten z: **EN 50126-2:2017**

ICS:

03.120.01	Kakovost na splošno	Quality in general
45.020	Železniška tehnika na splošno	Railway engineering in general

SIST EN 50126-2:2018 **en,fr**

NORME EUROPÉENNE

EUROPÄISCHE NORM

EUROPEAN STANDARD

EN 50126-2

Octobre 2017

ICS 45.020

Remplace CLC/TR 50126-2:2007

Version française

Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) - Partie 2: Approche systématique pour la sécurité

Bahnanwendungen - Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) - Teil 2: Systembezogene Sicherheitsmethodik

Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

La présente Norme Européenne a été adoptée par le CENELEC le 2017-07-03. Les membres du CENELEC sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à cette Norme Européenne.

Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du CEN-CENELEC Management Centre ou auprès des membres du CENELEC.

La présente Norme Européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CENELEC dans sa langue nationale, et notifiée au CEN-CENELEC Management Centre, a le même statut que les versions officielles.

Les membres du CENELEC sont les comités électrotechniques nationaux des pays suivants: Allemagne, Ancienne République yougoslave de Macédoine, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.

Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Bruxelles

Sommaire

Page

Avant-propos européen

Le présent document (EN 50126-2:2017) a été élaboré par le Comité Technique CLC/TC 9X « Applications électriques et électroniques dans le domaine ferroviaire ».

Les dates suivantes sont fixées :

- date limite à laquelle ce document doit être mis en application au niveau national par publication d'une norme nationale identique ou par entérinement (dop) 2018-07-03
- date limite à laquelle les normes nationales en contradiction avec ce document doivent être annulées (dow) 2020-07-03

Le présent document remplace le CLC/TR 50126-2:2007.

La précédente édition du CLC/TR 50126-2:2007 est rendue obsolète par les nouvelles éditions EN 50126-1:2017 et EN 50126-2:2017 ; la raison en est que le domaine d'application de la présente partie a été modifiée comparée à la version remplacée.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits attachés à des brevets. Le CENELEC ne saurai(en)t être tenu(s) pour responsable(s) de ne pas avoir identifié tout ou partie de tels droits attachés à des brevets.

L'EN 50126 « *Applications ferroviaires — Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)* » comprend les parties suivantes :

— Partie 1 : Processus FDMS générique ;

— Partie 2 : Approche systématique pour la sécurité.

Le présent document a été préparé dans le cadre d'un mandat confié au CENELEC par la Commission européenne et l'Association européenne de libre-échange et couvre les exigences essentielles de la (des) directive(s) UE.

Pour la relation avec la (les) Directive(s) UE, voir l'Annexe ZZ, informative, qui fait partie intégrante du présent document.

Introduction

L'EN 50126-1:1999 visait à introduire l'application d'un processus systématique de management de la FDMS dans le domaine ferroviaire. L'application de cette norme et l'expérience acquise au cours de ces dernières années ont révélé la nécessité de mettre en œuvre une démarche de révision et de restructuration avec la volonté d'établir une approche systématique et cohérente de la FDMS, applicable à tous les domaines d'application ferroviaire : Contrôle-commande et Signalisation, Matériel Roulant et installations Fixes.

Le travail de révision a permis d'améliorer la cohérence et l'homogénéité de la norme, du concept de management de la sécurité et de la mise en application de l'EN 50126 en tenant également compte des Rapports techniques associés existants.

La présente Norme européenne fournit aux sociétés d'exploitation ferroviaire et aux industries ferroviaires de l'ensemble de l'Union européenne un processus permettant de mettre en œuvre une démarche cohérente de management de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité, désignée par l'acronyme FDMS.

Les processus relatifs à la spécification et à la démonstration des exigences de FDMS sont les pierres angulaires de la présente norme. La présente Norme européenne encourage une vision et une démarche communes de management de la FDMS.

L'EN 50126 représente une partie de l'application spécifique au domaine ferroviaire de l'IEC 61508. La satisfaction aux exigences de la présente Norme européenne ainsi qu'aux exigences d'autres normes pertinentes suffit ; il n'est pas nécessaire de démontrer en plus la conformité à l'IEC 61508.

En ce qui concerne la sécurité, l'EN 50126-1 fournit un processus de management de la sécurité étayé par les lignes directrices et les méthodes décrites dans l'EN 50126-2.

L'EN 50126-1 et l'EN 50126-2 ne sont pas liés à la technologie utilisée. En ce qui concerne la sécurité, l'EN 50126 adopte la perspective de la sécurité avec une approche fonctionnelle.

Il convient d'adapter l'application de la présente norme aux exigences spécifiques pour le système en cours d'examen.

La présente Norme européenne peut être systématiquement appliquée par les sociétés d'exploitation et les industries ferroviaires tout au long des phases du cycle de vie d'une application ferroviaire afin de développer des exigences de FDMS spécifiques au domaine ferroviaire et de satisfaire à ces exigences. L'approche système définie par la présente Norme européenne facilite l'appréciation des interactions relatives à la FDMS entre les éléments des applications ferroviaires, même si elles sont complexes.

La présente Norme européenne promeut la synergie entre les parties prenantes du domaine ferroviaire afin de parvenir au meilleur compromis entre les performances de FDMS et les coûts des applications ferroviaires. L'adoption de la présente Norme européenne s'inscrit dans le cadre du Marché unique européen et facilite l'interopérabilité du réseau ferroviaire européen.

Conformément aux règles de rédaction du CENELEC [1)], les exigences à caractère obligatoire stipulées dans la présente norme sont indiquées par la forme verbale « doit ». Sous réserve de justification, la norme autorise l'adaptation des processus.

Des lignes directrices spécifiques à l'application de la présente norme en matière de sécurité sont données dans l'EN 50126-2. L'EN 50126-2 spécifie différentes méthodes à utiliser dans le cadre du processus de management de la sécurité. Lorsqu'une méthode particulière est retenue pour le système en cours d'examen, les exigences obligatoires pour cette méthode sont par voie de conséquence obligatoires pour le management de la sécurité du système en cours d'examen.

1) CEN/CENELEC « Règlement intérieur — Partie 3 : Règles de structure et de rédaction des publications CEN/CENELEC (2017-02), Annexe H ».

La présente Norme européenne comprend un corps principal (Articles 1 à 11) et les Annexes A, B, C, D, E, F, G et ZZ. Les exigences définies dans le corps principal de la norme sont normatives, tandis que les annexes sont informatives.

1 Domaine d'application

La présente Partie 2 de l'EN 50126 :

- prend en considération les aspects génériques relatifs à la sécurité du cycle de vie FDMS ;
- définit les méthodes et les outils qui sont indépendants de la technologie des systèmes et sous-systèmes ;
- fournit :
  - — une présentation de l'approche systématique pour la sécurité, un concept clé de l'EN 50126 ;
  - — les méthodes pour déterminer les exigences de sécurité et leurs exigences d'intégrité de sécurité concernant le système et pour les allouer aux différents sous-systèmes ;
  - — les méthodes pour déterminer les niveaux d'intégrité de sécurité (SIL) pour les fonctions électroniques relatives à la sécurité.

NOTE La présente norme ne permet pas l'allocation de niveaux d'intégrité de sécurité aux fonctions non électroniques.

- fournit des lignes directrices et des méthodes concernant :
  - — le processus de sécurité ;
  - — la démonstration et l'acceptation de la sécurité ;
  - — l'organisation et l'indépendance des rôles ;

  - — l'appréciation du risque ;
  - — la spécification des exigences de sécurité ;
  - — l'allocation des exigences de sécurité fonctionnelle ;
  - — la conception et la réalisation.
- fournit à l'utilisateur de la présente norme les méthodes permettant d'assurer la sécurité à l'égard du système en cours d'examen et de ses interactions ;
- fournit des lignes directrices sur la définition du système en cours d'examen, y compris l'identification des interfaces et interactions du système avec ses sous-systèmes ou d'autres systèmes afin de réaliser l'analyse du risque ;
- ne définit pas :
  - — les objectifs de FDMS ni les grandeurs, les exigences ou les solutions pour des applications ferroviaires spécifiques ;
  - — les règles ou les processus de certification des produits ferroviaires vis-à-vis des exigences de la présente norme ;
  - — un processus d'homologation par l'autorité de tutelle en matière de sécurité.

La présente Partie 2 de l'EN 50126 s'applique aux domaines d'application ferroviaire, à savoir Contrôle-commande et Signalisation, Matériel Roulant et Installations Fixes, et spécifiquement :

- à la spécification et à la démonstration des exigences de sécurité pour toute application ferroviaire et à tout niveau d'une telle application, selon le cas, allant des systèmes ferroviaires complets aux grands systèmes et aux sous-systèmes et équipements (individuels et combinés) de ces grands systèmes, y compris ceux qui comportent des logiciels. Elle est notamment applicable :

  — aux nouveaux systèmes ;

  — aux nouveaux systèmes intégrés dans des systèmes préexistants acceptés, mais seulement dans la mesure où, et dans la façon dont le nouveau système comprenant la nouvelle fonctionnalité y est intégré. Elle n'est sinon pas applicable aux parties inchangées du système existant ;

  — dans toute la mesure du possible, aux modifications et extensions des systèmes préexistants qui ont été acceptés avant la création de la présente norme, mais seulement dans la mesure où et si les systèmes existants ont été modifiés. Elle n'est sinon pas applicable aux parties inchangées du système existant ;

- à toutes les phases concernées du cycle de vie d'une application donnée ;

- à l'utilisation des sociétés d'exploitation ferroviaire et des industries ferroviaires.

Il n'est pas nécessaire d'appliquer la présente norme aux systèmes existants qui ne sont pas modifiés, y compris ceux déjà conformes à toute version antérieure de l'EN 50126.

Le processus défini par la présente Norme européenne part du principe que les sociétés d'exploitation et les industries ferroviaires ont développé au niveau de l'entreprise des politiques de Qualité, Performances et Sécurité. L'approche définie dans la présente norme est en accord avec l'application des exigences de management de la qualité de l'EN ISO 9001.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

EN 50126-1:2017, *Applications ferroviaires — Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) — Partie 1: Processus FDMS générique*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans le EN 501261 ainsi que les suivants s'appliquent.

4 Abréviations

ALARP (As Low As Reasonable Practicable)	Aussi bas que cela est raisonnablement possible
ACA	Analyse coûts - avantages
CCF (Common Cause Failure)	Défaillance de cause commune (analyse)
CBP	Code de bonne pratique
COTS (Commercial Off-The-Shelf)	Disponible dans le commerce
DRA (Differential Risk Aversion)	Aversion différentielle du risque
ERE	Estimation du risque explicite
CEM	Compatibilité électromagnétique
AAE	Analyse par arbre d'événement
AMDEC	Analyse des modes de défaillance, de leurs effets et de leur criticité
AAP	Analyse par arbre de panne
GA (Generic Application)	Application générique
GASC (Generic Application Safety Case)	Dossier de sécurité pour une application générique
GP (Generic Product)	Produit générique
GPSC (Generic Product Safety Case)	Dossier de sécurité pour un produit générique
GAME	Globalement Au Moins Equivalent
HAZOP (Hazard and Operability Study)	Etude de danger et d'exploitabilité
IM (Infrastructure Manager)	Gestionnaire d'infrastructure
URL	Unité remplaçable de ligne
MEM (Minimum Endogenous Mortality)	Mortalité endogène minimale
CAR	Critère d'acceptation du risque
FDMS	Fiabilité, disponibilité, maintenabilité et sécurité
RAP (Risk Acceptance Principle)	Principe d'acceptation du risque
RBD (Reliability Block Diagram)	Bloc-diagramme de fiabilité
RRA (Rapid Ranking Analysis)	Analyse par classement hiérarchique rapide
RU (Railway undertaking)	Entreprise ferroviaire
SA (Specific Application)	Application spécifique
SASC (Specific Application Safety Case)	Dossier de sécurité pour une application spécifique
SDR (Safe Down Rate)	Taux de passivation
SDT (Safe Down Time)	Temps de mise en sécurité
SIL (Safety Integrity Level)	Niveau d'intégrité de sécurité
SRAC (Safety-related Application Conditions)	Conditions d'application relatives à la sécurité
TFFR (Tolerable Functional Failure Rate)	Taux de défaillance fonctionnelle acceptable
THR (Tolerable Hazard Rate)	Taux d'occurrence maximal acceptable de danger
VPF (Value of Preventing a Fatality)	Coût de prévention de décès

5 Processus de sécurité

5.1 Appréciation du risque et maîtrise des situations dangereuses

Le présent paragraphe décrit le Modèle du sablier : il propose une approche simplifiée qui, même si elle ne comporte pas tous les aspects liés au modèle de cycle de vie, permet de clarifier certaines questions.

Le Modèle du sablier offre un aperçu général des principales activités relatives à la sécurité qui sont nécessaires pour assurer un niveau de sécurité acceptable pour un système technique, y compris les domaines de responsabilité correspondants.

Un système technique signifie un produit ou un ensemble de produits comprenant la conception, la réalisation et la documentation de soutien. Le développement d'un système technique commence par la spécification de ses exigences et s'achève par son acceptation. La conception des interfaces tient compte des interactions avec les opérateurs humains et leur comportement, bien que le système technique n'inclue pas les opérateurs humains eux-mêmes et leurs actions. Le processus de maintenance (décrit dans les manuels de maintenance) et le fonctionnement sont spécifiés, mais ne sont pas considérés comme faisant partie du système technique proprement dit. Ils peuvent être restreints par les « conditions d'application ».

L'objectif de ce modèle est de mettre en évidence la distinction à faire entre l'analyse du risque dans le cadre de l'appréciation du risque (au niveau du système ferroviaire) et l'analyse des dangers dans le cadre de la maîtrise des situations dangereuses (au niveau du système en cours d'examen).

Cela permet d'améliorer la coopération entre les parties prenantes concernées, en clarifiant les responsabilités et les interfaces, et présente l'avantage de réduire la complexité et de faciliter la modularité.

Le Modèle du sablier décrit deux aspects principaux :

- l'appréciation du risque, la détermination des exigences de sécurité sur le plan opérationnel et technique (y compris la maintenance) ; et
- la maîtrise des situations dangereuses et le respect des exigences de sécurité fonctionnelle résultant des niveaux supérieurs en déterminant et analysant les causes et en concevant et réalisant des mesures de contrôle.

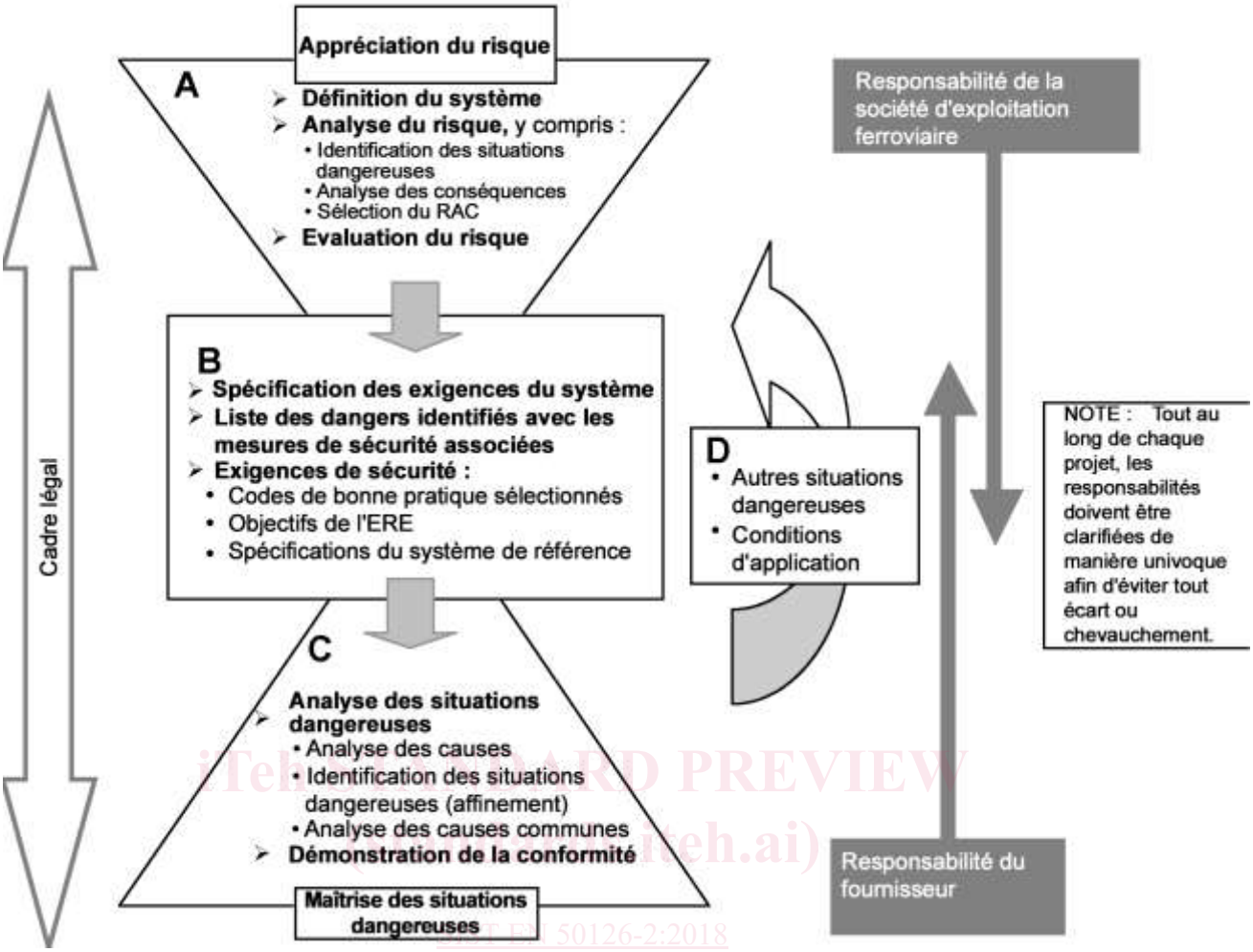

Figure 1 — Le Modèle du sablier

NOTE La partie A (Appréciation du risque) est associée aux phases 1 à 3 du cycle de vie représenté sur la Figure 4 du EN 50126-1:2017. La partie B correspond à la phase 4, tandis que la partie C correspond aux phases 5 à 9. La partie D montre la « prise en compte de l'identification des dangers ultérieurs dans l'analyse du risque » (voir Figure 4 du EN 50126-1:2017).

5.2 A. Appréciation du risque

5.2.1 Généralités

L'appréciation du risque est assurée au niveau du système ferroviaire.

Elle s'appuie sur une définition du système, et inclut l'analyse du risque et l'évaluation du risque.

Elle définit les exigences de sécurité du système de haut niveau, notamment les exigences de sécurité applicables au système en cours d'examen du point de vue de la société d'exploitation ferroviaire et de l'exploitant. Elle tient compte des aspects opérationnels relatifs à la sécurité, de l'expérience antérieure et des exigences réglementaires pour l'application ferroviaire.

La principale tâche de cette activité est la réalisation de l'analyse du risque, qui est déterminée à partir de la définition du système. L'analyse du risque comprend l'identification des dangers, l'analyse des conséquences et le choix des principes d'acceptation du risque (PAR).

La spécification des exigences de sécurité est le résultat final de l'appréciation du risque. A la Figure 1, elle se trouve dans la zone B, car elle constitue une interface (tout comme les spécifications des exigences du système et la liste des dangers identifiés) entre les différentes responsabilités.

5.2.2 Réalisation de l'appréciation du risque

Il convient de choisir un niveau de détail convenable pour l'appréciation du risque afin d'étudier le risque de manière adéquate. Il ne s'agit pas de répertorier tous les dangers triviaux ni de croire qu'il sera toujours possible d'identifier les dangers au-delà des limites des connaissances actuelles. Il convient que l'appréciation du risque reflète une analyse raisonnable des dangers et de leurs risques associés dans le cadre des activités d'exploitation ferroviaire et de la technologie appliquée proprement dite. Lorsque cela est jugé utile, il convient de corréler les appréciations du risque aux registres des accidents enregistrés et de leurs causes.

Si possible, au cours de cette première étape, il convient d'éviter toute considération relative à la réalisation technique/architecturale, c'est-à-dire qu'il convient de considérer le système à développer comme une boîte noire dont les fonctions et les dangers sont évalués uniquement à ses frontières. Ces frontières sont des interfaces bien définies entre l'environnement opérationnel et le système en cours d'examen.

Par exemple, un « mouvement intempestif de train » représente un danger pour un train. Il peut être considéré comme une abstraction à la limite du « système train » et est susceptible de provoquer différents accidents selon le contexte opérationnel (collision faisant suite à une survitesse du train lorsqu'il est en marche, chute de personnes consécutive à un mouvement du train qui est censé être à l'arrêt, etc.).

Les hypothèses définies au cours de l'appréciation du risque doivent être vérifiées et mises à jour tout au long des phases du cycle de vie.

5.3 B. Résultats de l'appréciation du risque

Les résultats de l'appréciation du risque sont un ensemble d'exigences de sécurité liées à des fonctions, des systèmes ou des règles d'exploitation clairement identifiés. Ils font partie intégrante de la spécification des exigences du système qui établit l'interface technique entre les parties prenantes.

NOTE La structure organisationnelle et les responsabilités du projet sont d'autres facteurs à prendre en compte pour la compréhension et la maîtrise du risque. Pour les exigences et les aspects organisationnels, il est conseillé de se référer à l'Article 7.

Sur la base des principes d'acceptation du risque choisis, les exigences de sécurité peuvent faire référence à des codes de bonne pratique (CBP), à des systèmes de référence ou spécifier des objectifs explicites déterminés à partir d'une estimation du risque explicite (ERE).

Les exigences de sécurité comprennent les fonctions de sécurité exigées qu'il est possible d'apprécier de manière quantitative (taux d'occurrence maximal de dangers, par exemple), semi-quantitative ou qualitative (recours à des conducteurs formés pour maîtriser le risque d'erreurs humaines, par exemple).

Il convient d'apprécier les exigences de sécurité selon une approche holistique du système en cours d'examen, c'est-à-dire qu'il convient d'évaluer le risque résiduel de l'ensemble du système après introduction des exigences de sécurité en tenant compte de tous les dangers identifiés.

5.4 C. Maîtrise des situations dangereuses

L'étape Maîtrise des situations dangereuses dans le modèle du sablier permet de s'assurer que le système en cours d'examen satisfait aux exigences de sécurité. La maîtrise des situations dangereuses est réalisée pour une architecture système spécifique.

Les principaux effets des facteurs humains, des règles d'exploitation et de maintenance générale, ainsi que des procédures, sont l'objet de l'analyse du risque citée ci-dessus. Il convient donc que ces effets aient déjà été pris en compte dans les exigences de sécurité. Par conséquent, au cours de l'étape de maîtrise des situations dangereuses, le concepteur du système en cours d'examen peut se concentrer sur les causes internes des dangers identifiés.

La principale tâche de cette activité est l'« analyse des dangers », qui comprend :

– une identification des dangers concernant le système en cours d'examen (affinement) ;

– une analyse des causes ;

– une analyse des causes communes (voir 11.4).

L'identification des dangers est une tâche qui se répète sur plusieurs niveaux pendant le développement du système en cours d'examen. Afin de distinguer ces différentes tâches (et les documents associés), l'identification des dangers apparaît deux fois sur la Figure 1 :

1. au cours de l'appréciation du risque, l'identification des dangers concerne les dangers de haut niveau engendrés par les fonctions du système (boîte noire) et par l'exploitation associée du système ainsi que par son environnement ;

2. dans le cadre de la maîtrise des situations dangereuses, une identification affinée/répétée des dangers concerne les dangers et leurs causes, engendrés par les solutions techniques, c'est-à-dire par l'architecture qui a été définie et les interfaces internes du système en cours d'examen, ainsi que les nouveaux dangers potentiels induits par le système proprement dit.

Ces deux types de situations dangereuses identifiées doivent être traités dans le cadre de la maîtrise des situations dangereuses. La Figure 2 représente le cas général, où la cause d'un danger au niveau du système ferroviaire est un danger au niveau du système en cours d'examen, vis-à-vis de sa frontière. La frontière d'une identification des dangers est toujours fixée par la définition du système, qui détermine le périmètre de la tâche. Cela implique une structure hiérarchique des dangers. Par conséquent, il convient d'appliquer une approche hiérarchique à l'analyse des dangers et à l'enregistrement des situations dangereuses.

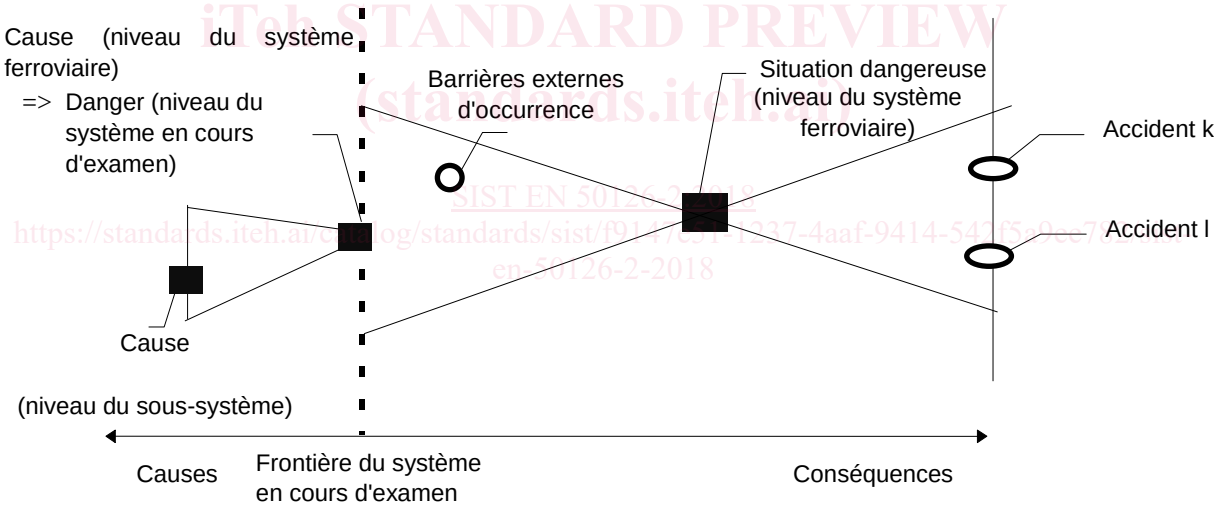

Figure 2 — Représentation des dangers par rapport aux frontières du système

La figure est orientée danger et présente une forme en « nœud de papillon », ce qui signifie que plusieurs causes peuvent engendrer le même danger et qu'un danger peut engendrer plusieurs accidents différents.

EXEMPLE Le danger au niveau du système ferroviaire est un train qui franchit un signal de danger et emprunte l'itinéraire d'un autre train, entraînant potentiellement une collision (l'accident). La cause au niveau du système ferroviaire (le danger au niveau du système en cours d'examen) est une distance de freinage trop importante. L'absence de freinage (ou le freinage tardif) par le conducteur est la cause au niveau du sous-système. La barrière externe d'occurrence est assurée par l'équipement de sécurité qui commande un frein d'urgence.

La démonstration du respect des exigences de sécurité pour le système en cours d'examen peut être vérifiée sous différentes formes. Ces formes dépendent de la nature des exigences sous-jacentes au début de la maîtrise des situations dangereuses.