Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC

Office fédéral des transports OFT
Divisions Infrastructure et Sécurité

Directive

Démonstration de la sécurité des installations de sécurité[1]

Installations de sécurité, applications télématiques et systèmes d'avertissement selon les art. 37 à 41 OCF dans les procédures d'approbation des plans et d'autorisation d'exploiter

(Dir. IS)

Référence : BAV-511.5-36/14/6/4

[1] Le terme « installations de sécurité (IS) » est utilisé dans la Dir. IS au sens large, comme concrétisé dans la deuxième partie du titre et au chap. 1.1.2.

BAV-D-51023501/838

Éditeur Office fédéral des transports, 3003 Berne
Divisions Infrastructure et Sécurité
Section Technique de sécurité

Distributeur Publication sur le site Web de l'OFT
(www.bav.admin.ch)

Langues disponibles Allemand (original)
Français

Entrée en vigueur 1er mai 2026

Office fédéral des transports
Division Infrastructure

Remund Anna Barbara G0BQTG
09.01.2026

Info: admin.ch/esignature | validator.ch

Anna Barbara Remund
Sous-directrice

Division Sécurité

Oberti Stefano 2RC6EK
09.01.2026

Info: admin.ch/esignature | validator.ch

Dr. Stefano Oberti
Sous-directeur

Édition/Historique des modifications

Version	Date	Auteur	Remarques sur les modifications	Statut
V1.0	01.05 2007	moc	Première édition (comme guide IS)	remplacé
V2.0	01.07.2010	moc	Révision et complément après trois ans l'expérience en matière d'applications et adaptation à l'état de la LCdF, de l'OCF et des DE-OCF	remplacé
V2.1_d	01.07.2011	moc	Améliorations aux chap. 4.3.4/fig. 2 et aux chap. 6.3.2, 7.1.1, 7.1.3	remplacé
V3.0_d	23.10.2015	moc	Révision et complément réforme des chemins de fer 2.2 : nouvellement publiée en tant que directive IS	remplacé
V4.0	12.01.2026 01.05.2026	guv	Révision et adaptation à la LCdF à l'OCF et aux DE-OCF du 01.07.2024 et aux PCT du 14.12.2025	publié, en vigueur

Table de matières

Introduction

La Dir. IS concrétise les exigences de la LCdF [1], de l'OCF [4] et des DE-OCF [8] concernant les documents de preuve pour les procédures d'approbation des plans et d'autorisation d'exploiter (PAP et PAE) des IS et décrit la démarche permettant un déroulement fluide de ces procédures.

La Dir. IS contient toutes les exigences relatives aux IS issues des directives : « Exigences relatives aux demandes d'approbation des plans », « Établissement et modification de constructions ou d'installations non soumises à approbation », « Organismes de contrôle indépendants Chemins de fer » et « Exigences IOP imposées aux tronçons du réseau complémentaire ». Par conséquent, il n'est pas nécessaire de consulter lesdites directives. Leur révision éliminera les redondances concernant les exigences relatives aux IS.

La Dir. IS se compose de trois chapitres. Le chap. 1 présente les exigences fondamentales. Le chap. 2 concrétise la démonstration de la sécurité pour un projet standard. Le chap. 3 concrétise la démonstration de la sécurité pour un projet de développement. Les exigences fondamentales du chap. 1 s'appliquent au projet uniquement dans le contexte où il est fait référence au chap. 1 dans les chap. 2 ou 3. La figure 1 donne une vue d'ensemble de la structure et du contenu de la Dir. IS.

Figure 1 : Structure et contenu de la Dir. IS

1 Cadre général

1.1 Généralités

1.1.1 But de la Dir. IS

Le contenu de la Dir. IS sert à satisfaire aux exigences de l'OCF [4] et des DE-OCF ad art. 38, DE 38.1, ch. 1.5 [8] pour la planification et la construction des IS, qui seront approuvées dans la PAP et la PAE. La Dir. IS décrit une démarche uniforme pour la « démonstration de la sécurité des IS »[2] et définit en particulier :

- les spécifications déterminantes ;
- les « documents de preuve pour les IS »[3] à établir ;
- les exigences relatives au contenu auxquelles doivent répondre les documents de preuve ;
- les documents de preuve à soumettre à l'Office fédéral des transports (OFT) et dans quels délais.

1.1.2 Champ d'application de la Dir. IS

Le champ d'application de la Dir. IS comprend les IS au sens large, telles qu'elles sont énumérées aux art. 37 à 41 OCF [4]. Il n'y a pas de démarcation claire entre les IS et les applications télématiques (DE-OCF ad art. 38, DE 38.2, ch. 2 [8]). Le champ d'application de la Dir. IS comprend :

- les IS pour les circulations sur les voies ferrées pour :
  - la commande et la protection de parcours (par ex. enclenchement) ;
  - la signalisation côté infrastructure et le contrôle de la marche des trains ;
  - la manœuvre et la protection des aiguilles ;
  - le contrôle de l'état libre de la voie et la localisation des trains ;
  - la commande et la protection des passages à niveau (installations de passage à niveau).
- les applications télématiques directement[4] liées à la sécurité et à la fiabilité de l'exploitation ferroviaire (art. 38, al. 2, OCF [4]) lors de la saisie, de la transmission, du traitement et de la fourniture d'informations comme :
  - le système de contrôle-commande ferroviaire (dispositifs de commande et d'affichage) ;
  - le système de management du trafic ;
  - le système de transmission à distance (par ex. transmission d'ordres du système de contrôle-commande ferroviaire à l'enclenchement, transmission de messages de l'état de l'enclenchement, de l'installation de passage à niveau, du compteur d'essieux au système de contrôle-commande ferroviaire) ;
  - les réseaux de données[5] ;
  - les systèmes de conduite automatique des trains (relation avec les IS en fonction du degré d'automatisation selon les DE-OCF ad art. 38, DE 38.2, ch. 3 [8]) ;
  - les applications mobiles (par ex. pour les processus d'exploitation).

  Les applications telles que l'information à la clientèle, l'administration (par ex. facturation des prestations), la planification (par ex. planification du trafic) et les dispositifs de contrôle des trains[6] ne sont pas directement liées à la sécurité et à la fiabilité de l'exploitation ferroviaire et ne relèvent

[2] le terme « démonstration de la sécurité » est utilisé ci-après

[3] le terme « documents de preuve » est utilisé ci-après

[4] C.-à-d. que leur défaillance (dysfonctionnement, panne) peut avoir un impact direct sur la sécurité et la fiabilité de l'exploitation ferroviaire.

[5] La démonstration de la sécurité est effectuée conformément à la D RTE 28100 [36].

[6] Les exigences de l'art. 40 OCF [4] s'appliquent aux dispositifs de contrôle des trains.

donc pas du champ d'application de la Dir. IS. Il peut néanmoins s'avérer nécessaire d'effectuer une analyse et évaluation du risque pour ces applications.

En cas de doute, il convient de clarifier avec l'OFT[7] si une application télématique relève du champ d'application de la Dir. IS.

- les systèmes d'avertissement ;
- les passages à niveau sans installations de passage à niveau.

Terme « produit » : les IS peuvent être constituées de différents éléments (y c. logiciel) tels que des systèmes, des sous-systèmes, des composants et des interfaces[8], qui eux-mêmes contiennent des fonctions. De tels éléments sont regroupés dans la Dir. IS sous le terme « produit ».

La Dir. IS est applicable lorsque les IS sont construites ou modifiées, indépendamment du type de signalisation (extérieure ou en cabine). Pour la démonstration de la sécurité dans le domaine de la signalisation en cabine ETCS L2, la Dir. IS doit être appliquée par analogie, en tenant compte des exigences du gestionnaire du système ETCS CH (KGB, EGB) [42]. En cas de première utilisation d'ETCS L2 (construction ou modification d'IS vers ETCS L2) chez un gestionnaire d'infrastructure (GI), la démonstration de la sécurité doit être coordonnée en amont avec l'OFT.

La Dir. IS s'adresse à l'entreprise requérante (en règle générale le GI selon l'art. 2, let. a, LCdF [1]), à l'industrie ferroviaire, aux bureaux d'ingénieurs et aux experts.

La Dir. IS n'a valeur ni de loi ni d'ordonnance. L'application de la Dir. IS doit conduire à des documents de preuve pouvant être approuvés. D'autres démarches sont admissibles, pour autant qu'elles soient conformes aux prescriptions souveraines [1] à [9]. Dans certaines circonstances, elles peuvent entraîner du travail supplémentaire et des coûts plus élevés pour l'ensemble des parties impliquées dans la PAP et la PAE.

Il existe des outils d'aide à l'application de la Dir. IS (par ex. modèles, recommandations et exemples) qui sont mis à disposition par l'Union des transports publics (UTP) dans la D RTE 25100 [33] par le biais de son Webshop RTE.

1.1.3 Exigences formelles relatives aux documents

Les documents :

- doivent être rédigés pour la mise à l'enquête publique dans la langue officielle en vigueur au lieu où les IS sont prévues (à l'exception du romanche). Les documents qui sont mis à l'enquête publique sont colorés en rose dans les tableaux 5 et 12. Les rapports d'examen de l'expert, de tests, de vérification et de validation peuvent également être rédigés dans une autre langue officielle ou en anglais.
- doivent être numérotés avec le numéro de référence 15.xx, s'ils sont requis pour la PAP. Les numéros subordonnés xx doivent être définis par le GI ou l'industrie ferroviaire.
- doivent être désignés conformément à la table des matières et doivent contenir les informations suivantes : titre du document, index ou version, échelle, numéro du plan, date de rédaction. En cas de modification du projet, il faut mettre à jour ces informations. Les contenus modifiés dans les documents doivent être clairement identifiables (par ex. en couleur).
- doivent être rédigés de manière à éviter autant que possible les redondances. Il n'est pas nécessaire de répéter les contenus qui figurent déjà dans d'autres documents. Il suffit de faire référence à ces documents.
- doivent contenir des décisions et des justifications traçables.

[7] Les demandes concernant les clarifications avec l'OFT mentionnées dans la Dir. IS doivent être adressées par courriel à _BAV-Sicherheitstechnik@bav.admin.ch.

[8] c.-à-d. les systèmes/sous-systèmes/éléments/composants/personnes en combinaison les uns avec les autres

- doivent être disponibles en version révisée et libérée.
- doivent être sécurisés en fonction de leur besoin de protection (par ex. en étant cryptés) s'ils sont classés comme critiques[9] pour la sécurité par le GI ou l'industrie ferroviaire. La classification de ces documents comme critiques pour la sécurité doit être claire (par ex. mention de la classification sur la page de titre et dans l'en-tête). De tels documents ne doivent être soumis à l'OFT que s'ils sont nécessaires à l'évaluation de la demande. Ces documents doivent être soumis sous forme cryptée. L'OFT doit être informé de la raison du cryptage (par ex. critique pour la sécurité).
- doivent être signés avec une signature électronique qualifiée conformément à la loi sur la signature électronique[10].
- doivent être soumis sous forme électronique via le site Web de l'OFT.

1.2 Classification du projet

Au début d'un projet, il faut procéder à la classification du projet conformément à la figure 2. Les étapes correspondantes sont expliquées ci-dessous.

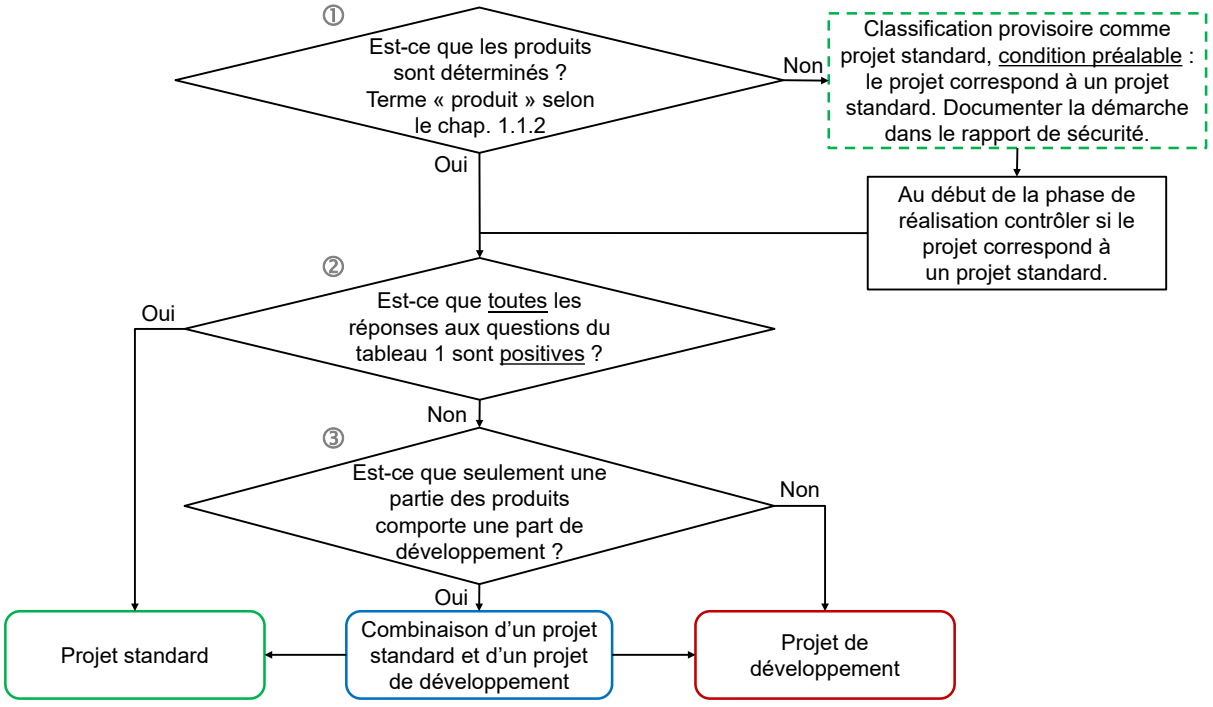

Figure 2 : Arbre de décision pour la classification du projet

① Lorsque les produits ne sont pas encore déterminés dans la phase de planification, il est admis de classer provisoirement le projet comme projet standard. Cette classification reste valable à condition que seuls des produits correspondant à un projet standard selon ② soient utilisés dans la phase de réalisation. Pour la phase de planification, cette démarche doit être documentée dans le rapport de sécurité (RaSe). Pour la phase de réalisation, il faut prouver dans le dossier de sécurité (DoSe) que le projet correspond à un projet standard, conformément au ②.

② Pour que le GI ait la garantie que son projet est un projet standard, il doit répondre aux questions figurant dans le tableau 1. Si toutes les réponses aux questions sont positives, le projet est considéré comme un projet standard et il faut mettre en œuvre les exigences du chap. 2.

[9] Il s'agit par exemple de documents qui pourraient être utilisés par des personnes non autorisées pour provoquer des événements causant la mort de nombreuses personnes.

[10] RS **943.03**

N°	Questions concernant le projet
1	Est-ce que seuls des produits (y c. leurs fonctions) sont utilisés qui : a) disposent d'une homologation de série[11] (HdS) de l'OFT ou b) « sont déjà utilisés par le GI »[12] ou c) sont déjà utilisés spécifiquement pour l'installation par un autre GI disposant d'infrastructure et des conditions d'exploitation comparables (DE-OCF ad art. 39, DE 39.2, ch. 1 à 2 [8]) ? *La première utilisation d'éléments logiques librement programmables (chap. 3.1.3) ou de schémas non conformes aux schémas de principe ou aux principes de construction (chap. 3.1.6) est considérée comme une part de développement.*
2	Est-ce que les produits prévus pour l'utilisation, sont conformes aux versions actuelles des prescriptions souveraines [1] à [9] ? En cas de doute, il est recommandé de coordonner en amont la démarche à suivre avec l'OFT. *On peut partir du principe que les produits disposant d'une HdS de l'OFT sont conformes aux versions actuelles des prescriptions souveraines. Si les prescriptions souveraines déterminantes [1] à [9] d'un objet de l'HdS changent avant l'expiration de la durée de validité de l'HdS (en règle générale dix ans), alors :* *a) l'industrie ferroviaire doit prouver, selon le chap. 3.3.1.2, que l'objet de l'HdS correspond aux prescriptions souveraines actuelles et mettre à disposition du GI et de l'OFT la preuve correspondante ou* *b) l'industrie ferroviaire et le GI doivent traiter les non-conformités aux prescriptions souveraines selon le chap. 1.10.1.*

Tableau 1 : Questions concernant le projet

③ Si seulement une partie des produits comporte une part de développement, le projet est considéré comme une combinaison d'un projet standard et d'un projet de développement.

Les parts de développement peuvent avoir différentes caractéristiques (par ex. d'une nouvelle fonction à un nouvel enclenchement). La part de développement doit être clairement délimitée et traitée selon le chap. 3. Toutes les autres parties relèvent du projet standard et doivent être traitées selon le chap. 2.

Si le projet ne comporte pas de parties relevant du projet standard, il est considéré comme un projet de développement et doit être traité selon le chap. 3.

1.3 Spécifications déterminantes

Les spécifications liées à la sécurité des IS doivent être respectées pour satisfaire à l'art. 2 OCF [4]. Elles sont catégorisées en :

- prescriptions (chap. 1.3.1) ;
- normes techniques appropriées qui permettent de concrétiser les prescriptions (chap. 1.3.2) ;
- règles reconnues de la technique (chap. 1.3.3) ;
- état de la technique (chap. 1.3.4).

Toutes les spécifications déterminantes pour un projet doivent être énumérées et mises en œuvre.

Pour la PAP, les spécifications en vigueur au moment de son ouverture sont déterminantes. Pour les projets de longue durée au cours desquels les spécifications changent, la démarche à suivre doit être coordonnée avec l'OFT.

[11] www.bav.admin.ch → Moyens de transport → Chemin de fer → Informations spécialisées → Homologations de série Eléments des installations ferroviaires → Domaine Technique de sécurité

[12] Il s'agit de produits avec des « grandfather rights » qui possèdent une démonstration de la sécurité éprouvée en pratique.

1.3.1 Prescriptions

Les prescriptions actuelles selon le tableau 2 sont déterminantes pour la démonstration de la sécurité. On distingue :

- Les prescriptions prises en compte dans la Dir. IS : [1], [5]. Il est possible de planifier les IS avec la Dir. IS sans consulter ces prescriptions. Elles sont mentionnées à titre purement informatif dans le tableau 2 et sont colorées en vert.
- Les prescriptions non explicitement prises en compte dans la Dir. IS : [2] à [4], [6] à [13]. Pour la planification et la réalisation des IS, il faut prendre en compte ces prescriptions, si nécessaire, en plus de la Dir. IS.

N°	**N° RS Abréviation**	**Titre** *Lorsque les prescriptions font référence à d'autres documents, il faudra les prendre en compte si nécessaire.* *Les prescriptions souveraines sont les prescriptions [1] à [9].*
[1]	742.101 LCdF	Loi fédérale sur les chemins de fer
[2]	704 LCPR	Loi fédérale sur les chemins pour piétons et les chemins de randonnée pédestre
[3]	741.01 LCR	Loi fédérale sur la circulation routière
[4]	742.141.1 OCF	Ordonnance sur les chemins de fer (y c. les directives de l'UE qui y sont référencées)
[5]	742.142.1 OPAPIF	Ordonnance sur la procédure d'approbation des plans des installations ferroviaires
[6]	741.21 OSR	Ordonnance sur la signalisation routière
[7]	704.1 OCPR	Ordonnance sur les chemins pour piétons et les chemins de randonnée pédestre
[8]	742.141.11 DE-OCF	Ordonnance de l'OFT relative aux dispositions d'exécution de l'ordonnance sur les chemins de fer (y c. DE-OCF ad art. 15b annexe n° 6 ch. 3 Spécification technique d'interopérabilité (STI) concernant le sous-système contrôle-commande et signalisation (CCS) et ch. 4 STI concernant le sous-système exploitation et gestion du trafic)
[9]	742.173.001 PCT	Chemin de fer Prescriptions suisses de circulation des trains PCT (R 300.1-.15)
[10]		Prescriptions d'exploitation (entre autres, dispositions d'exécution des prescriptions de circulation des trains, du GI concerné ou livret de procédures GI IOP)
[11]	Dir. PE-PCT	Directive Promulgation de prescriptions d'exploitation et de circulation des trains
[12]	Dir. CySec-Rail	Directive Cybersécurité chemins de fer[13]
[13]	Dir. HdS	Directive Homologation de série pour éléments d'installations ferroviaires

Tableau 2 : Prescriptions

1.3.2 Normes techniques

Les DE-OCF [8] désignent les normes techniques énumérées dans le tableau 3 comme étant appropriées pour concrétiser les prescriptions. De plus, les DE-OCF [8] prescrivent quand ces normes doivent obligatoirement être appliquées.

Si des enclenchements à relais (RStw) ou des produits utilisant la technologie des relais sont développés ultérieurement ou modifiés alors qu'ils ont été développés à l'origine sans appliquer les normes techniques susmentionnées, il convient de procéder conformément au chap. 3.1.6.

[13] Toutes les spécifications déterminantes (par ex. normes techniques, règles reconnues de la technique) pour la cybersécurité sont énumérées dans la Dir. CySec-Rail [12].

En principe, l'édition actuelle des normes techniques (base DE-OCF) doit servir de base à tout développement. Lorsque des normes techniques n'ont pas été désignées ou si elles font défaut, il y a lieu d'appliquer les règles reconnues de la technique (art. 2, al. 3, OCF [4]). Si les règles reconnues de la technique font également défaut ou sont inadaptées, il convient de se référer à l'état de la technique (DE-OCF ad art. 2, DE 2.4, ch. 1 [8]).

En cas de modification des éditions des normes techniques, il convient de procéder comme suit :

- Lorsqu'au début d'un développement il est déjà connu que de nouvelles éditions des normes techniques existent, que les DE-OCF [8] sont en cours de révision et qu'elles entreront prochainement en vigueur, ces éditions doivent être appliquées en concertation avec l'OFT.
- Lors de la première utilisation de produits ultérieurement développés ou modifiés, il convient de contrôler si les éditions des normes techniques utilisées pour la démonstration de la sécurité d'origine sont toujours valides. Si, entre-temps, de nouvelles éditions de ces normes sont valides, celles-ci doivent être appliquées conformément aux DE-OCF [8] en vigueur.

  Il est toutefois possible d'y déroger, en concertation avec l'OFT, lorsque la prise en compte des éditions actuelles des normes techniques entraîne des frais disproportionnés.
- Lorsqu'une modification strictement technique (par ex. corrections d'erreurs, obsolescence de composants) est effectuée conformément à l'annexe A4.3.1.2 de la Dir. HdS [13], les éditions des normes techniques sur lesquelles s'est fondée la démonstration de la sécurité d'origine peuvent continuer à être appliquées.

N°	**Abréviation**	**Titre** *Lorsque les normes techniques font référence à d'autres documents, il faudra les prendre en compte si nécessaire.*	**DE-OCF ad art.**
[14]	SN EN 50126-1	Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS) Partie 1 : Processus FDMS générique	38, DE 38.1, ch. 1
[15]	SN EN 50126-2	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 *Lorsque la SN EN 50129 [16] est appliquée pour des fonctions plus exigeantes que l'intégrité de base (BI), il n'est pas nécessaire de tenir compte de la SN EN 50126-2 [15], sauf quand celle-ci est explicitement référencée dans la SN EN 50129 [16] (DE-OCF ad art. 38, DE 38.1, ch. 1.3.1 [8]).*	38, DE 38.1, ch. 1
[16]	SN EN 50129	Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Systèmes électroniques de sécurité pour la signalisation	38, DE 38.1, ch. 1.3
[17]	SN EN 50159	Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission	38, DE 38.1, ch. 1.2
[18]	SN EN 12352	Equipements de régulation du trafic - Feux de balisage et d'alerte	37c, DE 37c, ch. 1.2.3
[19]	SN EN 12368	Equipements de régulation du trafic - Signaux	
[20]	SN EN 50121-1 50121-2 50121-4	Applications ferroviaires - Compatibilité électromagnétique Partie 1 : Généralités Partie 2 : Emission du système ferroviaire dans son ensemble vers le monde extérieur Partie 4 : Emission et immunité des appareils de signalisation et de télécommunication	39, DE 39.2, ch. 4.2.2.4
[21]	SN EN 50125-3	Applications ferroviaires - Conditions d'environnement pour le matériel Partie 3 : Equipement pour la signalisation et les télécommunications	39, DE 39.2, ch. 4.2.2.4
[22]	SN EN 50238-1	Applications ferroviaires - Compatibilité entre matériel roulant et systèmes de détection de train Partie 1 : Généralités	39, DE 39.3.e, ch. 1.6

Nº	Abréviation	Titre *Lorsque les normes techniques font référence à d'autres documents, il faudra les prendre en compte si nécessaire.*	DE-OCF ad art.
[23]	VSS 71 253	Rail - Route - Tracés parallèles ou rapprochés - Distance et mesures de protection	23.1, DE 23.1, ch. 1.3, 2.2
[24]	CIE S 004 /E-2001	Couleurs des signaux lumineux	39, DE 39.3.b, ch. 6.1.2

Tableau 3 : Normes techniques

1.3.3 Règles reconnues de la technique

Le tableau 4 énumère les règles reconnues de la technique (liste non exhaustive).

Nº	Abréviation	Titre *Si les règles reconnues de la technique font référence à d'autres documents, il faudra les prendre en compte si nécessaire.*
[25]	R RTE 20012	Profil d'espace libre Voie normale
[26]	R RTE 20100	Sécurité lors de travaux sur et aux abords des voies
[27]	R RTE 20410	Tronçons de ralentissement Voie normale
[28]	R RTE 20510	Tronçons de ralentissement Voie métrique
[29]	R RTE 20512	Profil d'espace libre Voie métrique
[30]	R RTE 24900	Accès au quai par la voie
[31]	R RTE 25000	Compendium Installations de sécurité Collection de règlements
[32]	D RTE 25096	Processus de planification Installations de sécurité
[33]	D RTE 25100	Démonstration de la sécurité Installations de sécurité
[34]	R RTE 25931	Passage à niveau Documentation de base
[35]	D RTE 27900	Manuel des conducteurs de retour de courant et des mises à terre Documentation
[36]	D RTE 28100	Démonstration de la sécurité des réseaux de données Safety et Security
[37]	R RTE 29100	Distances d'implantation des signaux avancés Voie normale
[38]	R RTE 30250	Elektronisches Stellwerk Simis IS (en allemand uniquement)
[39]	SN EN 50716	Applications ferroviaires - Exigences pour le développement de logiciels
[40]	SN EN ISO/IEC 17020	Évaluation de la conformité - Exigences pour le fonctionnement de différents types d'organismes procédant à l'inspection
[41]		Règles de projet Contrôle de la marche des trains pour les entreprises ferroviaires qui emploient un contrôle de la marche des trains conforme au standard ZBMS[14]
[42]		Exigences du gestionnaire du système ETCS CH (KGB, EGB et Level 1 LS en allemand uniquement)[15]
[43]		Prinzipschaltungen bzw. Baugrundsätze (en allemand uniquement)
[44]		Projektierungsgrundsätze HTA 4006 für Relaisstellwerke (en allemand uniquement)

Tableau 4 : Règles reconnues de la technique

[14] www.bav.admin.ch → Moyens de transport → Chemins de fer → Informations spécialisées → Contrôle de la marche des trains → ZBMS

[15] www.bav.admin.ch → Moyens de transport → Chemins de fer → Informations spécialisées → Contrôle de la marche des trains → European Train Control System

1.3.4 État de la technique

Il y a lieu de tenir compte de l'état de la technique si cela permet de réduire davantage un risque sans entraîner de frais disproportionnés (art. 2, al. 4, OCF [4]).

1.4 Parties prenantes et leurs responsabilités

1.4.1 Gestionnaire d'infrastructure

Le GI est responsable, selon le but de la Dir. IS, de la planification et de la construction des IS conformément aux spécifications (art. 2, al. 1 à 4 et art. 10, al. 1 à 2, OCF [4]). Dans ce contexte, il est également responsable de l'intégration au niveau de la technique et de l'exploitation. Le GI peut déléguer une partie des tâches relatives à la planification et à la construction des IS à l'industrie ferroviaire et/ou à des bureaux d'ingénieurs. Il reste toutefois l'interlocuteur de l'OFT pour la PAP et la PAE.

Le GI doit identifier toutes les parties prenantes à la planification et à la construction des IS (par ex. industrie ferroviaire, bureaux d'ingénieurs, experts), définir leurs tâches ou leurs responsabilités et coordonner l'ensemble des travaux. Cela comprend également l'établissement et l'attribution des mandats.

1.4.2 Industrie ferroviaire et bureaux d'ingénieurs

L'industrie ferroviaire et les bureaux d'ingénieurs sont responsables des résultats de leur travail. Dans le cadre des mandats acceptés, ils établissent les documents de preuve exigés et permettent aux experts d'effectuer les examens nécessaires.

1.4.3 Organisme de contrôle indépendant

Dans le champ d'application de la Dir. IS, les experts sont engagés en tant qu'organisme de contrôle indépendant. Pour pouvoir effectuer des examens en tant qu'expert, sur mandat du GI ou de l'industrie ferroviaire, des informations sur les points suivants sont requises, conformément à l'OCF [4] et sur la base de la SN EN ISO/IEC 17020 [40] :

(1) Compétence professionnelle (art. 15*t*, al. 1 à 2, OCF [4], SN EN ISO/IEC 17020 [40]) : l'expert doit confirmer qu'il :

   a) a reçu une formation appropriée (au sens de la SN EN ISO/IEC 17020 [40]) pour effectuer les examens. Celle-ci comprend une période d'initiation, une période de travail sous la supervision d'experts expérimentés et des formations continues (en fonction de l'évolution progressive des techniques et des processus d'examen) ;

   b) dispose des connaissances et d'expérience dans le domaine concerné par l'objet à examiner ;

   c) dispose des connaissances des spécifications déterminantes (chap. 1.3) et comprend en particulier les exigences de la SN EN 50126-1 [14] ;

   d) dispose des connaissances et d'expérience dans le domaine de la gestion du risque ;

   e) dispose des connaissances et d'expérience dans le domaine de l'application des systèmes de gestion de la sécurité et de la qualité ou de l'examen des systèmes de gestion.

   Les points suivants sont pertinents pour la compétence professionnelle en cybersécurité :

   — compréhension générale de la cybersécurité (par ex. Dir. CySec-Rail [12], y c. les règles reconnues de la technique référencées) ;

   — connaissances dans le domaine de l'évaluation et du traitement des risques pour la cybersécurité (Dir. CySec-Rail [12]).

Si un expert est déjà connu de l'OFT sur la base de ses rapports d'examen issus de projets similaires, aucune documentation liée au projet n'est nécessaire pour retracer la confirmation de sa compétence professionnelle. Dans tous les autres cas, l'expert doit mettre cette documentation à la disposition du GI afin qu'elle soit soumise à l'OFT, au plus tard, avec les documents de la PAP.

(2) Indépendance[16] (art. 15*u*, al. 1 à 2, OCF [4]) : l'expert doit confirmer qu'il n'exerce aucune activité susceptible de nuire à l'indépendance de son examen. En particulier, il ne doit pas être impliqué dans le développement, la fabrication, la distribution, la construction, l'acquisition, la possession, l'utilisation ou la maintenance de l'objet à examiner (SN EN ISO/IEC 17020 [40]).

(3) Existence d'une assurance responsabilité civile (art. 15*y* OCF [4]).

(4) Confidentialité (SN EN ISO/IEC 17020 [40]) : l'expert doit confirmer que les documents reçus ou établis pendant l'examen ont été traités de manière confidentielle, sauf accord contractuel contraire.

(5) Sous-traitance correcte (SN EN ISO/IEC 17020 [40]) : si l'expert sous-traite une partie de l'examen, il doit s'assurer que les sous-traitants respectent les exigences indiquées dans le présent chapitre.

1.4.4 Office fédéral des transports

L'OFT est l'autorité chargée de l'approbation des plans (art. 18, al. 2, LCdF [1]).

L'OFT octroie la décision d'approbation des plans (DAP), éventuellement avec des charges (le cas échéant, conditions et limitations dans le temps), après avoir examiné les documents soumis en fonction des risques et par sondages (art. 2*a* OCF [4]). La DAP a valeur d'autorisation de construire (art. 6, al. 6, OCF [4], art. 6 OPAPIF [5]).

L'OFT octroie l'autorisation d'exploiter (AE), éventuellement avec des charges (le cas échéant, conditions et limitations dans le temps), sauf s'il n'y a pas renoncé dans la DAP (art. 8, al. 4, OCF [4]). Au cours de la PAE, il examine les documents soumis en fonction des risques et par sondages. La mise en service (MES) est autorisée avec l'AE.

L'OFT octroie l'HdS selon l'art. 18*x* LCdF [1] éventuellement avec des charges, pour les produits d'IS qui doivent être utilisés de la même manière et dans la même fonction, pour autant qu'ils soient aptes à simplifier la PAP et la PAE selon l'art. 6 resp. l'art. 8 OCF [4].

1.5 Procédure d'approbation des plans

Les IS ne peuvent être construites ou modifiées qu'avec une DAP (art. 18, al. 1, LCdF [1]). Dans certains cas, il est possible d'y renoncer (voir chap. 2.2.1, 2.2.2 et 3.1.3).

Une PAP a lieu dans :

- une procédure ordinaire (art. 18*a* - *h* LCdF [1]), lorsque les intérêts dignes de protection de tiers sont affectés et/ou qu'il existe des effets sur le territoire et l'environnement. Cette procédure nécessite une publication officielle avec mise à l'enquête publique, une consultation des autorités fédérales spécialisées concernées et un avis des cantons concernés.
- une procédure simplifiée (art. 18*i*, al. 1, LCdF [1]) pour :
  - les projets qui affectent un espace limité et ne concernent qu'un ensemble restreint et bien défini de personnes ou
  - les modifications des IS qui n'altèrent pas sensiblement l'aspect extérieur du site, n'affecte pas les intérêts dignes de protection de tiers et n'a que des effets minimes sur l'aménagement du territoire et sur l'environnement ou
  - les IS, qui seront démontées après trois ans au plus.

[16] L'indépendance et l'impartialité au sens de la SN EN ISO/IEC 17020 [40] sont considérées comme équivalentes.

Dans les projets globaux, il peut arriver que les documents de la PAP ne contiennent pas encore suffisamment d'informations sur les IS. Ce cas se présente typiquement lorsque l'autorisation de construire pour le projet global est requise avant celle pour les IS. Dans ce cas, les documents de la PAP pour les IS seront soumis sous forme de plans de détail pour approbation[17]. Les plans de détail qui se fondent sur un projet global déjà approuvé sont approuvés dans le cadre d'une procédure simplifiée (art. 18*i*, al. 2, LCdF [1]). Les plans de détail nécessitent une PAP dans le cadre d'une procédure ordinaire lorsque les intérêts dignes de protection de tiers sont affectés et/ou qu'il existe des effets sur l'aménagement du territoire et sur l'environnement.

En cas de doute, il est recommandé de coordonner le type de PAP et son déroulement avec l'OFT au début du projet.

En règle générale, les délais de traitement suivants s'appliquent (art. 8, al. 1, OPAPIF [5]) :

- 18 mois si des expropriations[18] (art. 3, al. 2, LCdF [1]) sont nécessaires ;
- 12 mois pour la procédure ordinaire (sans expropriations) ;
- 4 mois pour la procédure simplifiée.

Le délai de traitement commence à courir dès que l'OFT a reçu tous les documents de la PAP (art. 8, al. 2, OPAPIF [5]).

Si le projet initial subit des modifications importantes[19] pendant la PAP, elles doivent être soumises à l'OFT pour avis ou, le cas échéant, mises à l'enquête publique (art. 5, al. 1, OPAPIF [5]).

L'OFT indique que si des documents de la PAP sont de mauvaise qualité cela prolonge la durée de la procédure.

1.6 Documents de la PAP et exigences relatives au contenu

Les documents de la PAP se conforment à l'art. 3, al. 2, OPAPIF [5]. Les documents de la PAP suivants doivent satisfaire aux exigences formelles et de contenu selon les chap. 1.1.3 et chap. 1.6.1 - 1.6.4 :

- demande d'approbation des plans ;
- condensé du projet ;
- rapport d'examen de l'expert ;
- prise de position sur la manière avec laquelle les résultats du rapport d'examen de l'expert seront mis en œuvre.

1.6.1 Demande d'approbation des plans

Dans la demande d'approbation des plans (art. 3, al. 1, OPAPIF [5]), les informations suivantes doivent être indiquées :

- l'objet de la demande ;
- le GI avec l'interlocuteur, y compris les coordonnées ;
- les communes et les cantons concernés ;
- la catégorie du réseau où le projet se situe (réseau non IOP, réseau principal IOP ou réseau complémentaire IOP, chap. 1.15) ;
- le type de PAP : procédure ordinaire ou simplifiée (chap. 1.5) ;

[17] Cette démarche est connue sous le nom de procédure de plans de détail. Les plans de détail des IS contiennent les informations nécessaires à leur évaluation au niveau technique et exploitation, selon les tableaux 5 et 12.

[18] C.-à-d. qu'un droit réel d'un tiers (terrain ou servitude) est nécessaire à la réalisation du projet, mais que ce tiers n'est pas d'accord de céder ce droit réel.

[19] Modifications qui sont soumises à la PAP selon les chap. 2.2.1, 3.1.6 ou 3.1.7

- l'état des négociations sur l'acquisition des terrains, des droits et des expropriations nécessaires ;
- les accords avec des tiers (particuliers, organisations, autorités) ;
- les non-conformités aux prescriptions souveraines [1] - [9] (chap. 1.10.1) ;
- les plans de détail (chap. 1.5) ;
- les délais (début des travaux et MES) ;
- les coûts.

1.6.2 Condensé du projet

Le condensé du projet (art. 3, al. 2, OPAPIF [5]) contient les mêmes informations que la demande d'approbation des plans (chap. 1.6.1). Contrairement à cette dernière, il fait partie de la mise à l'enquête publique.

1.6.3 Rapport d'examen de l'expert

Le rapport d'examen de l'expert (art. 3, al. 2, OPAPIF [5]) doit permettre de retracer l'activité d'examen et contenir les informations suivantes :

1) détails du mandat, y compris la date de l'attribution du mandat, les délimitations et les interfaces ;
2) confirmation du respect des exigences applicables à l'expert (1) à (5) selon le chap. 1.4.3 (par ex. au moyen d'une autodéclaration) ;
3) liste des spécifications appliquées lors de l'examen (chap. 1.3) ;
4) identification de l'objet examiné (par ex. versions des logiciels, release, CRC), y compris la liste de tous les documents examinés (avec le numéro, la version et la date) ;
5) degré d'exhaustivité de l'examen (avec justification en cas de sondages) ;
6) liste de tous les documents établis pour l'examen (par ex. check-lists, questionnaire, journal d'examen) ;
7) évaluation de l'examen réalisé ;
8) consignation de tous les constats sous forme de conditions/charges (points à traiter concernant la sécurité), de recommandations (visant à améliorer l'atteinte des objectifs) et d'autres remarques. Tous les constats doivent être assortis d'un délai. Si nécessaire, l'expert doit exiger des réexamens.
9) conclusions de l'examen du point de vue de la sécurité.

1.6.4 Prise de position sur la manière avec laquelle les résultats du rapport d'examen de l'expert seront mis en œuvre

Le GI doit prendre en compte les constats du rapport d'examen de l'expert. Il doit rendre compte à l'OFT de la mise en œuvre de ces constats au moyen des documents des phases de planification et de réalisation. À cet effet, une prise de position du GI (art. 3, al. 2, OPAPIF [5])[20] est requise, par exemple sous la forme d'un document séparé. Si nécessaire, la même exigence s'applique également à l'industrie ferroviaire.

1.7 Procédure d'homologation de série

Une procédure d'HdS selon l'art. 18*x* LCdF [1], cf. Dir. HdS [13], peut être effectuée lorsqu'elle permet de simplifier la PAP et la PAE (art. 7 OCF [4]). En conséquence, la procédure d'HdS allège la PAP et la PAE pour le GI, l'industrie ferroviaire et l'OFT, dans la mesure où la partie générique de l'objet de l'HdS ne doit pas être réexaminée dans le cadre de ces procédures. Dans le cas d'une procédure d'HdS en

[20] Selon cet article, la prise de position du GI est requise pour le rapport d'examen de l'expert de la phase de planification. Par analogie, une prise de position du GI est également requise pour le rapport d'examen de l'expert de la phase de réalisation.

cours pour un produit générique, le PAP peut s'appuyer sur l'autorisation de tests en exploitation issue de la procédure d'HdS. Le déroulement temporel doit être coordonné en conséquence.

Lorsqu'un GI exige par exemple dans le cadre d'un appel d'offres, l'utilisation de produits disposant d'une HdS, cette exigence est plus stricte que celle de la LCdF [1].

1.8 Analyse et évaluation du risque

L'OCF [4] exige la mise en œuvre de la gestion du risque présentée à la figure 3 (art. 5*m*, al. 2, art. 5*l*, al. 1 en tenant compte de l'art. 8*a*, al. 1, OCF [4]). Sur la base de l'analyse et de l'évaluation du risque, il convient de démontrer, lors de la construction ou de la modification des IS, que les risques qui en découlent sont acceptables.

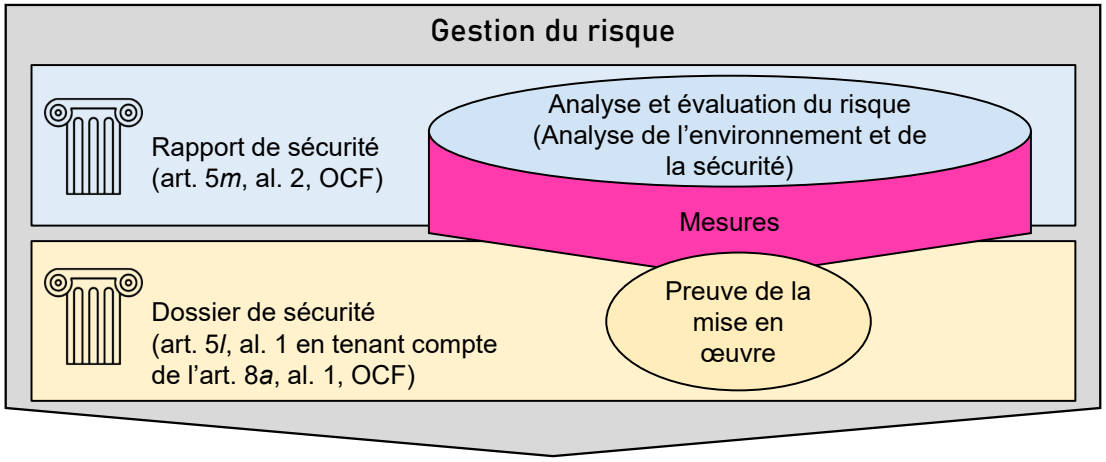

Figure 3 : Gestion du risque

La figure 4 présente le déroulement prévu par la SN EN 50126-1 [14] pour l'analyse et l'évaluation du risque. Les étapes correspondantes sont expliquées ci-après.

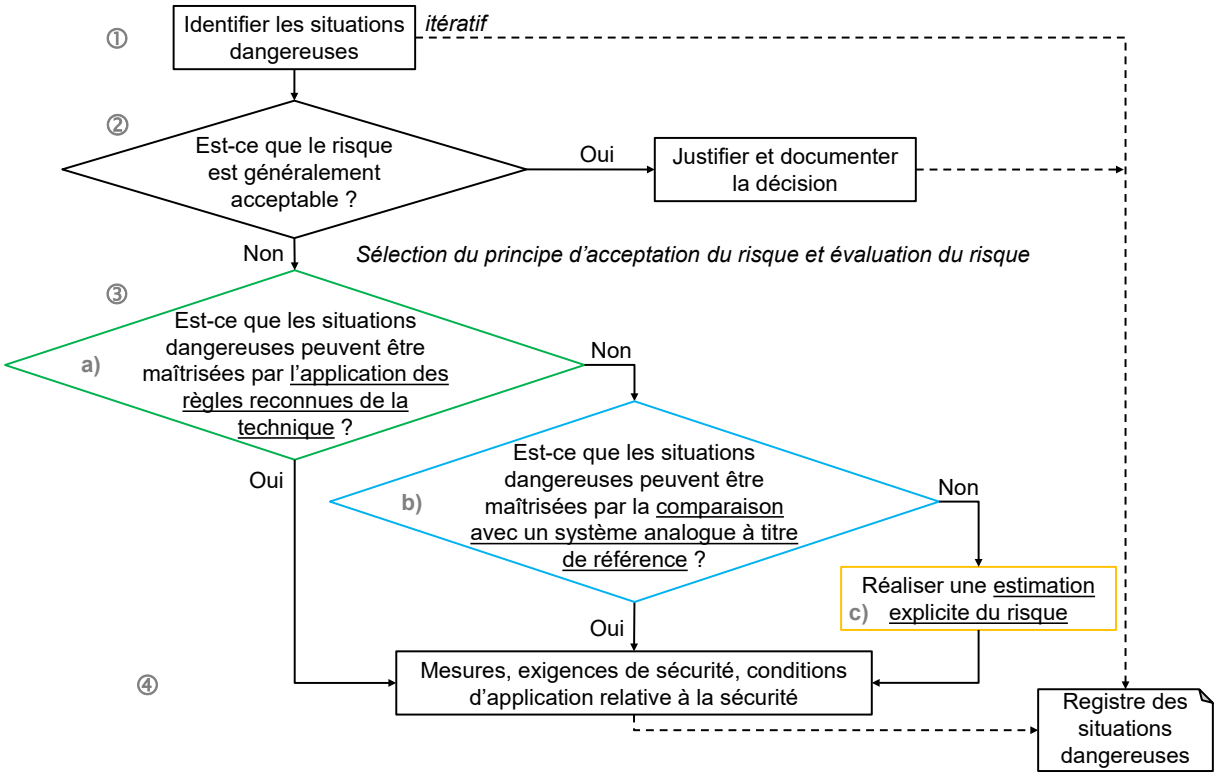

Figure 4 : Déroulement de l'analyse et l'évaluation du risque

① Toutes les situations dangereuses prévisibles, qui en raison de facteurs humains, techniques, organisationnels, de construction, d'exploitation et autres seraient susceptibles d'amener à un événement selon les DE-OCF ad art. 39, DE 39.2, ch. 3.1 [8], doivent être identifiées et consignées dans le registre des situations dangereuses. L'identification des situations dangereuses est une étape itérative, au cours de laquelle toutes les fonctions, interfaces, états de fonctionnement, dérangements et personnes impliquées doivent être pris en compte.

② Pour chaque situation dangereuse identifiée, il faut décider si le risque qui en découle peut être considéré comme « généralement acceptable ». Un tel risque est si faible que des mesures supplémentaires seraient disproportionnées. Une situation dangereuse associée à un risque généralement acceptable ne fait pas l'objet d'un traitement supplémentaire. La décision ayant conduit à la conclusion qu'une situation dangereuse présente un risque généralement acceptable doit être justifiée dans le registre des situations dangereuses.

③ Les situations dangereuses dont le risque n'est pas généralement acceptable doivent être analysées et évaluées quant à leur acceptabilité par le choix et l'application d'un principe et d'un critère d'acceptation du risque. Les principes d'acceptation du risque suivants sont disponibles à cet effet :

a) Application d'un code de bonne pratique (règles reconnues de la technique) : permet de déduire les mesures de maîtrise des situations dangereuses, c.-à-d. des mesures grâce auxquelles les risques liés à ces situations sont éliminés ou au moins réduits à un niveau acceptable. Il peut s'agir de mesures techniques, d'exploitation ou organisationnelles. Les mesures que le produit doit respecter sont appelées exigences de sécurité.

   L'état de la technique prime sur les règles reconnues de la technique. Conformément à l'art. 2, al. 4, OCF [4], il s'applique lorsqu'il permet de réduire davantage un risque à des frais proportionnés. Comme il n'existe pas de démarcation claire entre l'état de la technique et les règles reconnues de la technique, une analyse coûts/bénéfices peut être utile pour déterminer la nécessité d'appliquer les règles reconnues de la technique.

   Si les règles reconnues de la technique ne permettent pas de maîtriser toutes les situations dangereuses, il convient d'appliquer un ou plusieurs autres principes d'acceptation du risque.

b) Comparaison avec un système analogue à titre de référence : à cet effet, il convient de tenir compte des exigences de la SN EN 50126-2 [15].

c) Estimation explicite du risque : à cet effet, l'OFT recommande de suivre la « Methode zur Beurteilung des individuellen Risikos (en allemand uniquement) »[21]. Cette méthode se fonde, d'une part, sur la valeur limite du risque individuel en tant que critère d'acceptation du risque et d'autre part, sur les coûts marginaux harmonisés au sein du DETEC, fixés à 6,5 millions de francs pour la prévention d'un décès, afin de permettre une analyse coûts/bénéfices à partir du risque collectif. L'application de cette méthode présente l'avantage de permettre, avec des ressources limitées disponibles, d'atteindre des solutions optimales du point de vue coûts/bénéfices pour garantir la sécurité. Cette méthode permet également de démontrer qu'en cas de non-conformité aux prescriptions souveraines, il n'en résulte pas de risque inacceptable et que toutes les mesures proportionnées visant à diminuer les risques ont été prises (art. 5, al. 2, let. b, OCF [4]).

④ Pour la définition des exigences de sécurité, il convient de prendre en compte les exigences de la SN EN 50126-2 [15]. Outre les exigences de sécurité, les conditions d'application relatives à la sécurité (SRAC) constituent également des mesures de maîtrise des situations dangereuses. Les hypothèses formulées dans le cadre de l'analyse et l'évaluation du risque sont également définies comme SRAC. Lors de la définition des SRAC, il convient de prendre en compte les exigences de la SN EN 50129 [16].

La relation entre les différentes situations dangereuses et les principes d'acceptation du risque, les critères d'acceptation du risque, les exigences de sécurité et les SRAC nécessaires à leur maîtrise doit être démontrée dans le registre des situations dangereuses conformément à la SN EN 50126-1 [14]. Le registre des situations dangereuses peut être géré à l'aide d'un outil (par ex. base de données).

[21] www.bav.admin.ch → Thèmes généraux → Sécurité → Plus d'informations → Documentation → Méthodes

1.9 Examen de l'expert

Pour démontrer la sécurité et la conformité aux spécifications d'un projet présentant une haute importance pour la sécurité, des examens par un expert sont nécessaires (art. 5*l*, al. 3, OCF [4]).

Il est recommandé de clarifier et d'attribuer le mandat d'examen à l'expert le plus tôt possible dans le projet. L'examen de l'expert peut être effectué par plusieurs experts, qui doivent coordonner leurs examens de manière à éviter toutes lacunes.

Le GI doit soumettre à l'OFT les documents examinés par l'expert ou les versions mises à jour de ces documents dans lesquelles les constats de l'expert ont été traités. Les contenus mis à jour doivent être clairement identifiables dans les documents (par ex. en couleur).

1.10 Non-conformités et exceptions aux spécifications

Les IS doivent en principe être construites conformément aux spécifications déterminantes selon le chap. 1.3. Si, dans un projet, des non-conformités ou des exceptions à ces spécifications s'avèrent nécessaires, elles doivent être traitées dans la PAP selon les chap. 1.10.1 et 1.10.2. Il en va de même lorsqu'une non-conformité ou une exception existante demeure nécessaire malgré une adaptation des IS.

1.10.1 Non-conformités aux prescriptions souveraines

Une non-conformité[22] aux prescriptions souveraines [1] à [9] apparait lorsque les prescriptions souveraines ne sont pas respectées. Cette non-conformité nécessite une demande d'octroi d'une dérogation[23] conformément à l'art. 5, al. 2, OCF [4]. Les informations suivantes sont requises dans la demande :

- la prescription souveraine (désignation exacte) faisant l'objet de la non-conformité ;
- la durée d'application prévue ;
- la ligne, le tronçon de pleine voie, le kilométrage ;
- la justification de la demande, notamment par :
  - la comparaison avec une solution conforme ;
  - l'analyse et l'évaluation du risque (démarche selon le chap. 1.8 recommandée), qui montrent :
    - que le même niveau de sécurité est garanti ou
    - qu'il n'en résulte pas de risque inacceptable et que toutes les mesures proportionnées visant à diminuer les risques sont prises ;
  - les conséquences sur l'exploitation (actuelle et future) ;
  - les conséquences sur les IS dans leur ensemble ;
  - les éventuelles conséquences sur le respect d'autres prescriptions souveraines [1] à [9] ;
  - la preuve que l'interopérabilité n'est compromise ni dans le trafic international ni dans le trafic national ;
  - les coûts de mesures supplémentaires, par exemple d'entretien ou de surveillance.
- les suites en cas de non-octroi de la dérogation :
  - l'estimation des coûts dus aux adaptations afin de respecter les prescriptions souveraines ;
  - difficultés dans les délais et problèmes de coordination avec d'autres projets.
- les documents nécessaires à l'estimation de la situation ;
- les prises de position des domaines concernés par la non-conformité ;

[22] également appelée exception au sens strict

[23] Il s'agit d'une autorisation qui permet de déroger à une prescription souveraine.

- l'évaluation par l'expert.

1.10.2 Non-conformités et exceptions aux règles reconnues de la technique

Les non-conformités aux règles reconnues de la technique (tableau 4) concernent principalement les standards techniques et les exigences d'exploitation chez les GI.

Lorsque les non-conformités aux spécifications RTE sont définies dans les règles du GI ou lorsque des solutions détaillées orientées risques existent dans la R RTE 25000 [31], il est possible de s'y référer sans autres mesures. En l'absence de solutions détaillées orientées risques concrètes, il est recommandé de suivre la démarche selon le chap. 1.8.

Dans les projets ZBMS, des exigences supplémentaires relatives à la gestion des non-conformités aux règles de projet [41] sont consignées directement dans ces règles. Il en va de même pour les projets ETCS : dans ce cas, les exigences relatives à la gestion des non-conformités aux exigences du gestionnaire du système ETCS CH [42] sont consignées directement dans les présents documents et dans les documents auxquels ils font référence. Pour les projets ETCS, les non-conformités selon l'art. 15*e*, al. 2, OCF [4] constituent une exception.

Les non-conformités aux règles reconnues de la technique doivent être déclarées. Pour toutes les non-conformités, il faut apporter la preuve qu'elles n'entraînent pas de risque inacceptable et que toutes les mesures proportionnées de réduction des risques ont été prises. À cet effet, il est recommandé de suivre la démarche selon le chap. 1.8. L'expert doit examiner cette preuve et documenter le résultat de son examen dans son rapport d'examen. Si les non-conformités aux règles reconnues de la technique n'entraînent pas de non-conformités aux prescriptions souveraines [1] à [9], le GI est responsable de leur traitement.

Le traitement des exceptions aux règles reconnues de la technique (tableau 4) est défini dans ces mêmes règles.

1.11 Phases de construction et installations provisoires

Une phase de construction est un état intermédiaire planifié des IS, qui met à disposition des installations de voie utilisables pour l'exploitation. Cet état intermédiaire est communiqué à toutes les parties directement concernées par la construction (notamment les exploitants et les utilisateurs du réseau) sous la forme de plans, de prescriptions d'exploitation et de concepts d'utilisation. Une phase de construction possède une date de début et de fin fixées. Si la phase de construction diffère de l'état final, elle doit être documentée et contrôlée de manière appropriée. Les phases de construction connues lors de la phase de planification doivent être présentées de manière adéquate dans le RaSe ou dans un document séparé. L'attribution des éléments des IS aux phases de construction connues doit être clairement identifiable et fait partie de l'examen de l'expert pour la phase de planification.

L'OFT peut exiger dans la DAP la soumission des preuves de la réalisation de certaines phases de construction.

Une installation provisoire est un état transitoire d'un élément donné ayant la même fonction technique et d'exploitation, ou une fonction comparable (par ex. cales de relais, fiche de remplacement). La réalisation de l'installation provisoire peut influencer l'exploitation des IS. Une installation provisoire peut être planifiée et réalisée à court terme et ne fait pas partie de la PAP. Les installations provisoires doivent être documentées et contrôlées de manière appropriée.

1.12 Intégration au niveau de la technique et de l'exploitation

Pour démontrer l'intégration au niveau de la technique et de l'exploitation, il faut au minimum accomplir les tâches suivantes :

1) Mettre à jour, si nécessaire, l'analyse et l'évaluation du risque (chap. 1.8) ;

2) Définir la configuration des IS (logiciel, matériel, interfaces, documents pour l'utilisateur). En règle générale, la configuration complète des IS est contenue dans les release notes ou dans les documents qui y sont référencés ;

3) Apporter la preuve que les SRAC des produits prévus (phase de planification) ou utilisés (phase de réalisation) et concernés par les modifications ont été mises en œuvre. À cet effet, la check-list ou le protocole de contrôle des SRAC, indiquant le nom du réviseur, la version et la date, peut par exemple servir de preuve ;

4) Tenir compte des charges adressées aux utilisateurs (GI) issues de l'HdS des produits prévus (phase de planification) ou utilisés (phase de réalisation) et concernés par les modifications ;

5) Apporter la preuve de l'absence d'effets rétroactifs : cette preuve est requise en cas de modification du logiciel et/ou du matériel. Les modifications apportées au logiciel et/ou au matériel ne doivent pas avoir d'influence sur les produits non modifiés. Les analyses d'impact des modifications nécessaires doivent être effectuées et évaluées (par ex. par un expert, un contrôleur d'usine ou un chargé de validation). À cet effet, les informations suivantes sont nécessaires :
   - la description et la justification des modifications ;
   - l'effet sur :
     - le niveau fonctionnel ;
     - le niveau non fonctionnel (par ex. vitesse, processus d'exploitation, outils, isolation, mise à la terre, compatibilité électromagnétique) ;
     - les IS dans leur ensemble ;
   - la manière dont ces modifications sont contrôlées.

6) Apporter la preuve que les documents de conception de projet, de montage et les prescriptions d'exploitation déterminants ont été mis à jour et/ou établis ;

7) Apporter la preuve que les formations ou les instructions requises pour le personnel roulant, d'exploitation et de maintenance ont eu lieu ;

8) Apporter la preuve de la mise en œuvre des mesures issues de l'analyse et l'évaluation du risque ;

9) Apporter la preuve que les contrôles requis (revue et libération des documents de construction, contrôle d'usine, vérification, validation, examen de l'expert) ont été effectués.

L'accomplissement des tâches susmentionnées doit être démontré par le GI et examiné par un expert. Si l'OFT a autorisé de manière générique le GI à accomplir les tâches 3) à 8) pour des projets standards au moyen de processus correspondants (par ex. dans le cadre de la PAP), il n'est pas nécessaire de démontrer l'accomplissement de ces tâches pour le projet concerné.

1.13 Changements significatifs

Pour les projets comportant des changements significatifs au sens de l'art. 5*m*, al. 3, OCF [4], le GI doit appliquer le processus de gestion du risque conformément à l'annexe I du règlement d'exécution (UE) n° 402/2013 (art. 5*m*, al. 4, OCF [4]). Cela implique que le GI démontre l'application de ce processus. Un organisme d'évaluation des risques doit ensuite évaluer l'application correcte de ce processus et ses résultats dans un rapport d'évaluation de la sécurité.

Pour les IS, le processus de gestion du risque pour les changements significatifs (art. 5*m*, al. 4, OCF [4]) se fonde sur les mêmes contenus et méthodes que la gestion du risque exigée par l'art. 5*m*, al. 2, et l'art. 8*a*, al. 1, OCF [4] (figure 3). Au chap. 1.4.3 les exigences relatives à l'organisme de contrôle indépendant sont définies indépendamment de l'importance du changement. Celles-ci correspondent aux exigences des art. 15*t* et art. 15*u* OCF [4] en matière de compétence professionnelle et d'indépendance.

Par conséquent, il n'est pas nécessaire de clarifier la question du changement significatif (art. 5*m*, al. 3, OCF [4]) ni de mettre en œuvre l'art. 5*m*, al. 4, OCF [4] pour les IS. Si, en particulier, une modification

des IS nécessite également la reconnaissance d'une autre autorité de surveillance européenne, la démarche à suivre doit être coordonnée avec l'OFT.

1.14 Cybersécurité

« Les IS, qui utilisent ou contiennent des technologies de l'information et de la communication (TIC) »[24], doivent être protégées, de toutes menaces, attaques ou intervention abusive, à l'aide de tous les moyens organisationnels et techniques proportionnés (art. 2, al. 1[bis], OCF [4]).

Étant donné que les TIC sont intégrées dans pratiquement tous les projets, il convient d'accorder une attention particulière à la cybersécurité, indépendamment du type de projet et de la technologie utilisée. Les raisons en sont les suivantes :

- Protection des infrastructures critiques : les IS jouent un rôle central dans le fonctionnement de l'infrastructure et doivent être protégées en fonction de leur besoin de protection.
- Augmentation des cybermenaces : en raison de la progression de la numérisation et de l'interconnexion croissante des IS, celles-ci deviennent de plus en plus des cibles potentielles de cyberattaques. Un système de gestion de la sécurité de l'information efficace protège contre les cybermenaces et réduit la zone d'attaque.
- Prévention des pannes et des dérangements : les cyberattaques peuvent entraîner des pannes des IS, ce qui pourrait affecter la disponibilité. Il est donc essentiel d'intégrer la cybersécurité à un stade précoce de la planification afin de garantir la disponibilité.
- Gestion du risque et prévention : l'intégration des aspects de cybersécurité à la PAP permet d'identifier et de corriger les vulnérabilités potentielles dès la phase de planification. Cela permet d'évaluer plus précisément les risques et de mettre en œuvre des mesures de protection de manière proactive.
- Maintien de la confiance du public : le public et les entreprises comptent sur le fonctionnement sûr et fiable des infrastructures critiques.
- Réduction du risque de sabotage : les IS peuvent être la cible d'attaques visant à provoquer le chaos ou à atteindre des objectifs politiques. Les mesures de protection permettent d'identifier et de contrer ces menaces avant qu'elles ne causent des dommages.

Pour ces raisons, outre l'attention portée à ce thème par la direction du GI, la démarche en matière de cybersécurité selon la figure 5 s'applique au niveau de la PAP. Les étapes correspondantes sont expliquées ci-après.

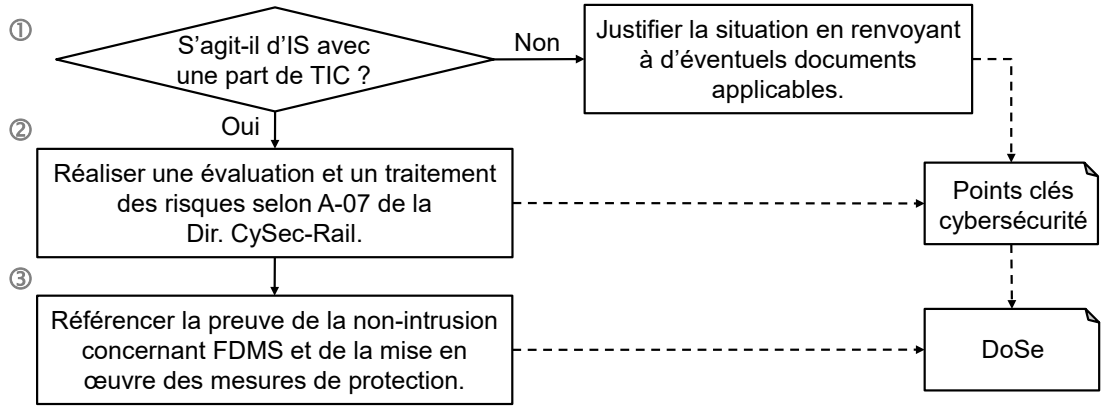

Figure 5 : Cybersécurité

① Clarifier s'il s'agit d'IS avec une part de TIC (par ex. enclenchement, système de contrôle-commande ferroviaire, système de transmission à distance, diagnostic, surveillance et maintenance par réseau). Si les IS n'utilisent pas de TIC ou n'en contiennent pas, cette situation doit être justifiée en

[24] le terme « IS avec une part de TIC » est utilisé ci-après

renvoyant à d'éventuels documents applicables. Dans ce cas, aucune autre mesure de protection n'est nécessaire.

② Pour les IS avec une part de TIC, une évaluation et un traitement des risques doivent être effectués conformément au processus décrit dans l'exigence A-07 de la Dir. CySec-Rail [12]. Les points clés suivants doivent être documentés pour les IS concernées avec une part de TIC, au moyen de documents de référence dans le document « Points clés cybersécurité » :

1) les personnes responsables dans le domaine de la cybersécurité ;
2) la référence aux éventuels documents applicables ;
3) le besoin de protection ;
4) les risques identifiés ;
5) les mesures de protection prévues ;
6) les risques résiduels après la mise en œuvre des mesures de protection prévues.

Des explications concernant les points clés susmentionnés se trouvent dans la Dir. CySec-Rail [12].

③ Lors de la mise en œuvre des mesures de protection, il convient de contrôler si celles-ci ont un impact sur les IS dans leur ensemble. La preuve de la non-intrusion concernant la FDMS et de la mise en œuvre des mesures de protection doit être référencée dans le DoSe.

1.15 Interopérabilité

1.15.1 Généralités

On distingue les catégories de réseaux suivantes (art. 15*a* OCF [4]) :

- Réseau non IOP, composé de :
  - tronçons à voie normale selon l'annexe 5 OCF [4] ;
  - tronçons à écartement métrique ou spécial, y compris les lignes de tramway ;
  - voies de raccordement et infrastructures ferroviaires telles que des installations d'entretien avec leurs faisceaux de voies, des installations de lavage, des hangars de chantier, etc.

  Aucune exigence IOP ne s'applique au réseau non IOP.
- Réseau principal IOP, comprenant les tronçons à voie normale (entièrement interopérables) selon l'annexe 6 OCF [4] ;
- Réseau complémentaire IOP, comprenant tous les tronçons à voie normale (partiellement interopérables) qui n'appartiennent ni au réseau non IOP selon l'annexe 5 OCF [4], ni au réseau principal IOP selon l'annexe 6 OCF [4].

Sur les réseaux principal IOP et complémentaire IOP, la STI CCS doit être respectée conformément à l'annexe n° 6, ch. 3 DE-OCF [8].

Le sous-système CCS au sol (art. 15*b*, al. 1, OCF [4]) présente les caractéristiques ETCS L2 ou ETCS L1 LS sur les réseaux principal IOP ou complémentaire IOP.

1.15.2 Déclaration de conformité

La conformité du sous-système CCS au sol doit être déclarée conformément à la STI CCS (art. 15*k* OCF [4]). La déclaration de conformité de ce sous-système est établie par le GI sur la base du certificat de conformité délivré par un organisme notifié (art. 15k^{bis}, al. 1, art. 15*r* OCF [4]).

Pour l'autorisation d'utilisation spécifiques du sous-système CCS au sol, il faut présenter une déclaration de conformité de ce sous-système (art. 15*j*, al. 2, OCF [4]).

La déclaration de conformité du sous-système CCS au sol est considérée comme remplie si les constituants d'IOP (par ex. Eurobalise, Euroloop, LEU - Eurobalise, LEU - Euroloop, compteur d'essieux, Radio Block Centre) disposant de déclarations de conformité de l'industrie ferroviaire sont utilisés dans le projet et si la preuve de la mise en œuvre des exigences du gestionnaire du système ETCS CH (par ex. règles de conception de projet) [42] a été apportée. Le GI doit disposer des déclarations de conformité des constituants d'IOP (art. 15*i*ter OCF [4]). Lorsque les constituants d'IOP disposent d'une HdS de l'OFT, le GI peut partir du principe que leurs déclarations de conformité sont disponibles.

1.16 Procédure d'autorisation d'exploiter

Conformément à l'art. 8, al. 1 à 2, OCF [4] :

- une AE est requise pour la MES de produits comportant une part de développement et des fonctions relatives à la sécurité avec SIL ≥ 1.
- une AE pour la MES des RStw peut être nécessaire en cas de développement.

La démonstration de la sécurité pour l'obtention de l'AE est régie par l'art. 8, al. 3, OCF [4].

Sur le réseau principal IOP ou complémentaire IOP, une AE est nécessaire pour les premières utilisations spécifiques à l'installation du sous-système CCS au sol (art. 23*c*, al. 1 LCdF [1] ou 15*c* OCF [4]).

Lorsque les modifications des utilisations spécifiques à l'installation du sous-système CCS au sol se basent sur des parts de développement, une AE est nécessaire si l'OFT l'exige (art. 23*c*, al. 2, LCdF [1]).

La démonstration de la sécurité pour l'obtention de l'AE est régie par l'art. 15*j* OCF [4]. En vue de l'octroi de l'AE, le GI doit convenir en amont avec l'OFT de l'étendue et du contenu des documents nécessaires à cet effet.

Une autorisation d'exploiter de l'OFT est également requise pour les systèmes mobiles d'avertissement (art. 41 OCF [4]).

1.17 Programme et libération de mise en service

La sécurité doit être garantie à tout moment. Un programme adapté doit être établi pour la MES. Le niveau de détail requis dépend de l'ampleur du projet. Le programme doit indiquer :

- les travaux à effectuer,
- quand ils doivent être effectués et
- comment et par qui ils doivent être contrôlés.

Avant que les IS puissent être en exploitation, une libération de MES est nécessaire. Cette libération est une déclaration commune de l'expert et du GI confirmant que les exigences nécessaires à l'exploitation des IS sont remplies.

Avant d'accorder la libération de MES, l'expert doit évaluer l'aptitude des IS à être mises en service, en se basant sur les sources suivantes :

- les DoSe requis ;
- le traitement des points en suspens pertinents pour la MES issus des DoSe ;
- les résultats et l'évaluation de ses propres examens ;
- l'évaluation des résultats du contrôle et de la confirmation de l'achèvement complet des travaux par le contrôleur d'usine ou le chargé de validation ;
- la confirmation qu'il n'existe aucun défaut pertinent pour la sécurité ou l'évaluation des défauts et des mesures d'exploitation nécessaires.

Le résultat de l'évaluation de l'expert est consigné dans le document « Libération de mise en service » lors de la MES. En cas d'évaluation positive par l'expert et le GI, ce document doit être signé, ce qui permet la MES des IS et leur transfert à l'exploitation.

2 Projet standard

2.1 Phases et déroulement du projet standard

Le projet standard comprend deux phases. Son déroulement est illustré dans la figure 6.

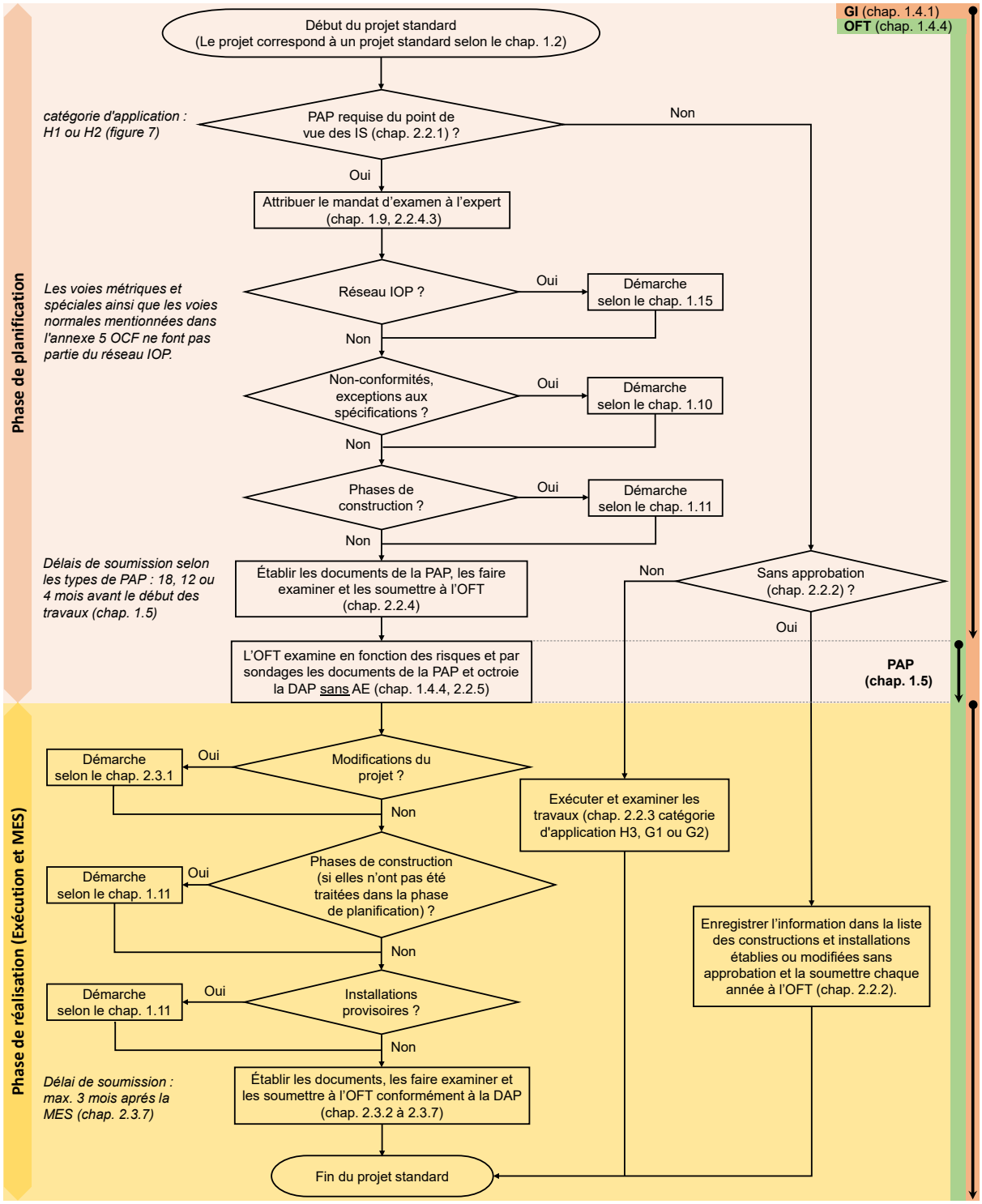

Figure 6 : Déroulement du projet standard

2.2 Phase de planification du projet standard

2.2.1 Attribution de la catégorie d'application du projet standard

Ce chapitre définit les catégories d'application. Le but est de pouvoir attribuer chaque projet standard à une telle catégorie en fonction de sa pertinence en matière de sécurité et de son type. La catégorie d'application détermine si une PAP est nécessaire et quelles exigences sont posées à la démonstration de la sécurité.

Évaluation de l'importance pour la sécurité

- H (haute) : l'importance pour la sécurité est haute si :
  - des fonctions avec une haute importance pour la sécurité (fonctions relatives à la sécurité avec SIL 1 à 4) sont concernées ;
  - des fonctions importantes pour la sécurité, qui ont été développées à l'origine sans attribution d'un SIL, sont concernées (par ex. des fonctions des RStw et des installations de passage à niveau).
- G (faible) : l'importance pour la sécurité est faible, si :
  - des fonctions relatives à la sécurité avec BI (moins exigeantes que SIL 1) sont concernées ;
  - des tronçons de voie en zone pour les chemins de fer routiers (par ex. exploitation des tramways) sont franchis, pour autant qu'aucune commande d'appareil de voie ayant des fonctions SIL ne soit utilisée ;
  - des tronçons de voie sont franchis comme « circulation sans signaux avec assentiment » pour autant qu'aucune commande d'appareil de voie ayant des fonctions SIL ne soit utilisée.

Les informations concernant le SIL ou la BI des fonctions relatives à la sécurité et les SRAC des produits concernés doivent être obtenues auprès de l'industrie ferroviaire.

Évaluation du type du projet standard

(1) Construction ou transformations importantes des IS, première utilisation de produits, par exemple :
  - nouvel enclenchement ou nouvelle installation de passage à niveau ;
  - première utilisation d'un produit disposant d'une HdS de l'OFT ou autorisé d'une autre manière en Suisse sur le réseau du GI.

(2) Modifications avec impact sur les aspects conceptuels et/ou les fonctions des IS existantes, mais d'ampleur limitée, telles que :
  - adaptation de la vitesse ;
  - adaptation des images de signaux ;
  - transformation d'une installation de voie avec adaptation de la signalisation.

(3) Modifications sans impact sur les aspects conceptuels et/ou les fonctions des IS existantes, telles que :
  - correction des erreurs des IS (par ex. conception de projet) ;
  - correction des erreurs du produit générique (par ex. mises à jour strictement logicielles sans nouvelles fonctions) ;
  - « remplacement de produits par une nouvelle génération de produits ayant des fonctions et une technologie identiques »[25] ;
  - démontage et remontage de produits existants (par ex. renouvellement de la superstructure).

[25] Il s'agit d'un remplacement 1:1.

L'attribution à une catégorie d'application résulte de l'évaluation de l'importance pour la sécurité et du type du projet standard selon la figure 7. Il s'agit de la justifier. Dans le cas du déploiement (rollout) d'IS, la démarche décrite au chap. 2.2.2 s'applique.

Un projet standard nécessite une PAP dans le cadre d'une procédure ordinaire lorsque les intérêts dignes de protection de tiers sont affectés et/ou qu'il existe des effets sur l'aménagement du territoire et sur l'environnement. Du point de vue des IS, l'obligation d'une PAP n'existe que si le projet entre dans la catégorie d'application H1 ou H2 (figure 7). Des explications sur les types de PAP et les délais de traitement se trouvent au chap. 1.5.

Type du projet standard	**Importance pour la sécurité**	
	Faible	**Haute**
(1) Construction ou transformations importantes des IS, première utilisation de produits	G1	H1
(2) Modifications avec impact sur les aspects conceptuels et/ou les fonctions	G2	H2
(3) Modifications sans impact sur les aspects conceptuels et/ou les fonctions	Hors du champ d'application de la Dir. IS	H3

Figure 7 : Matrice d'attribution de la catégorie d'application

2.2.2 Projets standard sans approbation

Les modifications suivantes des IS ne nécessitent pas d'approbation, si elles ne touchent aucun intérêt digne de protection de l'aménagement du territoire, de la protection de l'environnement, de la nature et du patrimoine ou de tiers :

- démontage d'appareils de voie avec remplacement des voies, sans modification du tracé, sans toucher aux aiguilles de protection, sans suppression des « dispositifs de dilatation des rails »[26] (annexe à l'art. 1*a*, al. 1, let. e, OPAPIF [5]) ;
- remplacement des dispositifs de déraillement par des aiguilles de protection en respectant la R RTE 25053 [31] ;
- entretien des composants de génie civil de passages à niveau, sans modification notable de la hauteur des rails ni de la route, sans modification de l'installation de passage à niveau sauf si l'on utilise des composants homologués ou déjà approuvés, dans la mesure où il n'en résulte aucune influence négative sur la superstructure (annexe à l'art. 1*a*, al. 1, let. f, OPAPIF [5]) ;
- pose de croix de St-André ou de signaux « tramway » aux passages à niveau (annexe à l'art. 1*a*, al. 1, let. y, OPAPIF [5]) ;
- déploiement (rollout) d'IS approuvé par l'OFT lors d'une ou de plusieurs premières utilisations.

En cas de doute, il est recommandé de coordonner en amont la démarche à suivre avec l'OFT.

Le GI doit soumettre chaque année à l'OFT une liste des constructions et installations construites ou modifiées sans approbation (art. 1*a*, al. 3, OPAPIF [5]). Les IS construites sans approbation doivent y figurer.

2.2.3 Exigences relatives à la démonstration de la sécurité du projet standard

En fonction de la catégorie d'application selon le chap. 2.2.1, les exigences suivantes s'appliquent à la démonstration de la sécurité :

[26] Les dispositifs de dilatation des rails ne font pas partie des IS.

- Catégorie d'application H1 : les exigences des chap. 2.2.4 et 2.3 s'appliquent.
- Catégorie d'application H2 : les exigences des chap. 2.2.4 et 2.3 s'appliquent, mais sont relativisées par les points suivants :
  - Les documents de preuve doivent se focaliser sur la modification et son impact sur les IS dans leur ensemble.
  - Un examen de l'expert est nécessaire pour les phases de planification et de réalisation (chap. 1.9). Il est toutefois possible d'effectuer l'examen de l'expert pour la phase de planification lors de la phase de réalisation. Dans ce cas, les documents de la PAP sont soumis sans le rapport d'examen de l'expert. Le GI assume le risque que des erreurs de la phase de planification ne soient découvertes que tardivement. L'OFT peut toutefois exiger un rapport d'examen de l'expert pour la phase de planification lors de la PAP.

    De plus, il est possible d'effectuer l'examen de l'expert pour les phases de planification et de réalisation et le contrôle d'usine (chap. 2.3.4) en une seule étape lors de la phase de réalisation. Le contrôle d'usine et l'examen de l'expert pour les phases de planification et de réalisation (chap. 2.2.4.3) peuvent être attribués à une seule et même personne dans le cadre du mandat d'examen. Il s'agit de garantir l'indépendance de cette personne, ce qui implique qu'elle ne doit pas assumer d'autres tâches (sauf de nature organisationnelle) en rapport avec l'objet à examiner.
- Catégories d'application H3, G1 et G2 : Il n'est pas nécessaire de distinguer les phases de planification et de réalisation du point de vue de la démonstration de la sécurité. Pour cette dernière, il s'agit de prendre en compte les points suivants, dans le DoSe par exemple :
  - Les modifications apportées aux IS doivent être documentées.
  - L'attribution de la catégorie d'application doit être justifiée.
  - Organisation de la sécurité : les rôles et les responsabilités des personnes impliquées doivent être documentés. L'indépendance des rôles doit apparaître clairement.

    Si l'organisation de la sécurité est garantie par des processus appropriés, une documentation spécifique au projet n'est pas nécessaire.
  - Si les modifications apportées aux IS sont conformes aux spécifications des chap. 1.3.1, 1.3.2[27], 1.3.3 et 1.3.4, aucune analyse et évaluation du risque supplémentaires ne sont nécessaires, car toutes les situations dangereuses sont maîtrisées par l'application des règles reconnues de la technique (tableau 4). Le GI doit consigner les règles reconnues de la technique pertinentes pour le projet standard et prouver leur mise en œuvre.
  - Les éventuelles non-conformités et exceptions aux spécifications doivent être traitées conformément au chap. 1.10.
  - Intégration au niveau de la technique et de l'exploitation (chap. 1.12) :
    - la preuve de la mise en œuvre des SRAC ;
    - les documents de conception de projet, de montage et les prescriptions d'exploitation mis à jour et/ou établis ;
    - l'achèvement des formations ou des instructions du personnel roulant, d'exploitation et de maintenance ;
    - la preuve que les charges issues des HdS sont remplies, y compris la preuve de la mise en œuvre des exigences génériques[28] des produits utilisés ayant une pertinence pour le GI.
  - Pour la catégorie d'application H3, un examen de l'expert est nécessaire pour les phases de planification et de réalisation (chap. 1.9). Il est toutefois possible d'effectuer ces examens et le

[27] Seule la norme technique VSS 71 253 est pertinente [23]. En cas de non-conformités aux prescriptions souveraines, les normes techniques indiquées au chap. 1.8 doivent également être appliquées pour l'analyse et l'évaluation du risque.

[28] www.bav.admin.ch → Droit → Autres bases légales et prescriptions → Directives → Rail → Homologation de série pour éléments d'installations ferroviaires → Hinweise zu den Verfügungen aus den Typenzulassungsverfahren von Sicherungsanlagen und Telematikanwendungen (en allemand uniquement)

contrôle d'usine (chap. 2.3.4) en une seule étape lors de la phase de réalisation. Le contrôle d'usine et l'examen de l'expert pour les phases de planification et de réalisation (chap. 2.2.4.3) peuvent être attribués à une seule et même personne dans le cadre du mandat d'examen. Il s'agit de garantir l'indépendance de cette personne, ce qui implique qu'elle ne doit pas assumer d'autres tâches (sauf de nature organisationnelle) en rapport avec l'objet à examiner. Pour la MES, la démarche selon le chap. 1.17 s'applique.

- Pour les catégories d'application G1 et G2, le contrôle de MES doit être effectué par une personne compétente, sur la base de protocoles de contrôle/check-lists.
- Après la MES :
  - Il s'agit de conserver les protocoles de contrôle/check-lists remplis et signés et
  - de traiter les constats issus du rapport d'examen de l'expert (pour la catégorie d'application H3) ou du contrôle de MES (pour les catégories d'application G1 et G2).

Il faut finaliser les documents de preuve dans un délai de trois mois après la MES. Les documents de preuve pour les catégories d'application H3, G1 et G2 ne doivent pas être soumis à l'OFT. Ils restent en possession du GI et doivent pouvoir être présentés à l'OFT dans le cadre de la surveillance de la sécurité en phase d'exploitation.

2.2.4 Documents de la PAP et exigences relatives au contenu du projet standard

Dans le tableau 5, les documents de la PAP sont énumérés. En complément, il contient des références dans lesquelles on trouve des explications sur les exigences relatives au contenu (art. 3, al. 1 à 2, OPAPIF [5]). Lors de la rédaction des documents de la PAP, il s'agit de respecter les exigences formelles selon le chap. 1.1.3.

Les documents de la PAP énumérés dans le tableau 5 doivent être soumis à l'OFT (art. 18*b* LCdF [1]). Si le GI estime que certains de ces documents ne sont pas pertinents, il peut renoncer à les soumettre en justifiant brièvement sa décision (par ex. « non pertinent »).

Lorsque dans le cadre d'un projet global, des documents comme la table des matières, la demande d'approbation des plans, le condensé du projet, la demande d'octroi d'une dérogation et les plans sont soumis, il convient de prendre en compte les exigences du présent chapitre pour les IS. Il n'est donc pas nécessaire de soumettre à nouveau les documents susmentionnés pour les IS.

Titre du document *Les documents qui sont mis à l'enquête publique sont colorés en rose.* *Pour les trois premiers documents, les numéros de référence sont prédéfinis. Tous les autres documents doivent être numérotés avec le numéro de référence 15.xx. Les numéros subordonnés xx sont à définir par le GI.*	**Explications sur les exigences relatives au contenu**
00 Table des matières	chap. 2.2.4.1
01.01 Demande d'approbation des plans	chap. 1.6.1
01.02 Condensé du projet (requis pour la PAP ordinaire)	chap. 1.6.2
Rapport de sécurité	chap. 2.2.4.2
Demande d'octroi d'une dérogation (requise pour non-conformités aux prescriptions souveraines [1] à [9])	chap. 1.10.1
Tableaux pour : distances de glissement, protection de flancs, distances d'implantation des signaux avancés (peuvent être intégrés dans le rapport de sécurité ou fournis séparément)	[8]
Tableau des parcours (par ex. RADN)	[9]
Plan de signalisation/Concept de signalisation/Plan de situation/S-Plan	chap. 2.2.4.4
Profils d'espace libre/Profils en travers	
Concept de mise à la terre (si modifié ou nouvellement établi)	[35]

Titre du document *Les documents qui sont mis à l'enquête publique sont colorés en rose.* *Pour les trois premiers documents, les numéros de référence sont prédéfinis. Tous les autres documents doivent être numérotés avec le numéro de référence 15.xx. Les numéros subordonnés xx sont à définir par le GI.*	**Explications sur les exigences relatives au contenu**
Plan de détail des passages à niveau	chap. 2.2.4.4
Profils d'espace libre des éléments des passages à niveau	
Profils en travers/Profils d'espace libre de la route	
Diagramme temps-distance des passages à niveau	[34]
Points clés cybersécurité	chap. 1.14
Documentation permettant de retracer la compétence professionnelle de l'expert	chap. 1.4.3, pt. (1)
Rapport d'examen de l'expert phase de planification	chap. 1.6.3
Prise de position du GI sur la manière avec laquelle il mettra en œuvre les résultats du rapport d'examen de l'expert phase de planification	chap. 1.6.4

Tableau 5 : Documents de la PAP du projet standard

2.2.4.1 Table des matières

La table des matières contient la liste des documents avec des informations sur : le numéro de référence, le titre du document, l'index ou la version, l'échelle, le numéro du plan et la date de rédaction. Elle doit être soumise à l'OFT sous forme de document Word modifiable.

2.2.4.2 Rapport de sécurité

Les informations suivantes doivent être consignées dans le RaSe :

1) Définition de l'objet de la demande :
   - l'état actuel des IS (brève description) ;
   - les modifications prévues pour les IS ;
   - les conséquences de ces modifications ;
   - les interfaces ;
   - la dépendance par rapport au projet global ;
   - l'utilisation de la voie ;
   - le concept de manœuvre, en cas de manœuvres régulières, indiquer la fréquence ;
   - les conséquences sur l'exploitation et la sécurité si le projet ne peut pas être réalisé.
2) Hypothèses et délimitation par rapport à d'autres produits et IS voisines sur la ligne ;
3) Spécifications déterminantes (chap. 1.3) ;

   Dans un projet standard conforme aux prescriptions souveraines, la seule norme technique à appliquer est la VSS 71 253 [23]. En cas de non-conformité aux prescriptions souveraines, il s'agit également d'appliquer les normes techniques indiquées au chap. 1.8 pour l'analyse et l'évaluation du risque.
4) Produits prévus, y compris leur release/version et autorisation, pour autant que les produits soient déterminés (chap. 1.2) ;

   L'autorisation a une des caractéristiques suivantes :
   - l'HdS de l'OFT (indiquer le n° d'HdS) ;
   - la démonstration de la sécurité éprouvée en pratique ;
   - la démonstration de la sécurité spécifique à l'installation selon les DE-OCF ad art. 38, DE 38.1, ch. 1.3 [8].

5) Classification du projet (chap. 1.2) ;
6) Catégorie d'application (chap. 2.2.1) ;
7) Sécurisation et signalisation des passages à niveau ainsi que leur commande avec les informations suivantes :
   - les utilisations, la densité de trafic et, le cas échéant, la vitesse maximale autorisée sur la route ;
   - les écoles, les places de jeux, les installations sportives et de loisirs et les autres installations similaires à forte fréquentation situées à proximité ;
   - la preuve d'une visibilité suffisante pour les usagers de la route, qui doivent voir les signaux du passage à niveau et, si nécessaire, les trains (par ex. pour les passages à niveau signalés par une croix de Saint-André ou un signal « Tramway ») ;
   - les signalisations et marquages routiers existants et nouveaux pertinents pour le projet ;
   - la preuve du dégagement des passages à niveau.

   Il est très important d'impliquer en amont les parties prenantes du côté de la route. C'est pourquoi le GI doit fournir des déclarations concernant les accords pertinents.
8) Organisation de la sécurité pour la phase de planification et, si elle est déjà connue, pour la phase de réalisation : documenter les rôles et les responsabilités des personnes impliquées. L'indépendance des rôles doit apparaître clairement.

   Si l'organisation de la sécurité est garantie par des processus appropriés, une documentation spécifique au projet n'est pas nécessaire.
9) Mandat d'examen de l'expert (chap. 1.9 et 2.2.4.3) ;
10) Analyse et évaluation du risque : dans le projet standard, il existe des situations dangereuses typiques qui sont maîtrisées par l'application des règles reconnues de la technique (tableau 4). Cela signifie qu'en cas d'application de ces règles, il n'est pas nécessaire d'analyser les risques liés à ces situations dangereuses de manière plus détaillée. Le GI doit démontrer que les règles reconnues de la technique pertinentes ont été mises en œuvre.
11) Traitement des éventuelles non-conformités et exceptions aux spécifications selon le chap. 1.10 ;
12) Phases de construction (chap. 1.11) ;
13) Intégration au niveau de la technique et de l'exploitation (chap. 1.12) :
    a) la preuve de la mise en œuvre des SRAC, si elles sont pertinentes pour la planification ;
    b) les documents de conception de projet, de montage et les prescriptions d'exploitation qui doivent être mis à jour et/ou établis en raison des modifications prévues ;
    c) le besoin de formation ou d'instruction du personnel roulant, d'exploitation et de maintenance.
14) Conclusion selon laquelle le projet standard planifié correspond aux spécifications déterminantes ou que les dérogations correspondantes ont été demandées et que les IS construites pourront être exploitées en toute sécurité.

Dans le cadre d'un projet global, les informations des pts. 1) et 7) peuvent être reprises dans le rapport technique de niveau supérieur. Le RaSe doit alors faire référence à ce rapport.

2.2.4.3 Mandat d'examen de l'expert

A. Phase de planification : l'expert doit généralement accomplir les tâches suivantes :
   1) Examiner si le projet correspond à un projet standard (chap. 1.2).
   2) Examiner l'attribution correcte de la catégorie d'application[29] (chap. 2.2.1).
   3) Examiner l'exhaustivité des documents et des informations requis (chap. 2.2.4).

[29] Cet examen peut également être effectué par une autre personne compétente.

4) Examiner le respect des prescriptions déterminantes (chap. 1.3). Les éléments suivants, y compris leurs interactions, doivent être pris en compte :
   - les profils d'espace libre ;
   - la désignation des éléments ;
   - les équipements de contrôle de l'état libre de la voie, la longueur des tronçons, les contacts de rail ;
   - les appareils de voie, la protection de flanc ;
   - les signaux principaux et avancés, les distances de freinage, les distances de glissement, la visibilité ;
   - les signaux de manœuvre et complémentaires, les panneaux de signalisation ;
   - les signaux et panneaux dans le domaine de la signalisation en cabine ;
   - la protection des parcours (y c. le bloc de ligne), l'accès aux quais par la voie ;
   - le contrôle de la marche des trains ;
   - les passages à niveau ;
   - les systèmes de télétransmission ;
   - le système de contrôle-commande ferroviaire.
5) Contrôler que les produits sont autorisés pour l'utilisation prévue (chap. 2.2.4.2, pt. 4).
6) Examiner l'organisation de la sécurité (chap. 2.2.4.2, pt. 8).
7) Examiner si les non-conformités aux spécifications et la demande d'octroi d'une dérogation sont entièrement documentées (chap. 1.10). Examen et documentation de l'acceptabilité des non-conformités.
8) Examiner l'analyse et l'évaluation du risque d'éventuelles non-conformités aux prescriptions souveraines [1] à [9].
9) Examiner la plausibilité des points clés pour la cybersécurité (chap. 1.14 et 1.4.3 compétence professionnelle en cybersécurité).
10) Examiner les phases de construction (chap. 1.11).
11) Examiner si les tâches suivantes pour l'intégration au niveau de la technique et de l'exploitation ont été accomplies (chap. 1.12) :
    - la mise en œuvre des SRAC, si elles sont pertinentes pour la phase de planification ;
    - la présence des informations sur la mise à jour ou l'établissement des documents de conception de projet, de montage et des prescriptions d'exploitation ;
    - la présence des informations sur les besoins en formation ou en instruction du personnel roulant, d'exploitation et de maintenance.
12) Documenter l'examen effectué (chap. 1.6.3).

B. Phase de réalisation : en règle générale, l'expert doit accomplir les tâches suivantes pour l'examen théorique et pratique (chap. 2.3.5) :

Examen théorique (concerne les documents)

1) Examiner si le projet correspond à un projet standard, dans la mesure où il a été provisoirement classifié comme tel lors de la phase de planification (chap. 1.2).
2) Examiner l'organisation de la sécurité pour la phase de réalisation, si celle-ci n'a pas déjà été examinée lors de la phase de planification (chap. 2.2.4.2, pt. 8).
3) Examiner si :
   - les modifications du projet sont documentées et conformes aux spécifications (chap. 2.3.1) ;

- les règles reconnues de la technique définies lors de la phase de planification ont été respectées ;
- les charges issues de la DAP ont été exécutées, pour autant qu'elles concernent la sécurité ;
- les constats issus du rapport d'examen de l'expert de la phase de planification ont été mis en œuvre ;
- les documents de construction ont été révisés et libérés (chap. 2.3.2.1) ;
- les documents de construction sont conformes aux spécifications déterminantes. Il convient de sélectionner les spécifications pertinentes pour les documents de construction selon le chap. 1.3.
- les schémas de principe ou les principes de construction, les mesures HTA [44] (RStw, installation de passage à niveau) ont été mis en œuvre ;
- les documents de contrôle pour tous les produits utilisés (y c. les installations extérieures et intérieures) sont disponibles ;
- la mise en œuvre des documents de construction des produits utilisés dans la conception de projet est contrôlée et documentée ;
- les release notes sont disponibles ;
- les IS sont prêtes à être mises en service (chap. 1.17).

4) Examiner si les tâches suivantes pour l'intégration au niveau de la technique et de l'exploitation ont été accomplies (chap. 1.12) :
   - la mise en œuvre des SRAC ;
   - la preuve de l'absence d'effets rétroactifs ;
   - la présence des documents de conception de projet, de montage et des prescriptions d'exploitation mis à jour ;
   - la preuve de la réalisation des formations ou instructions requises.
5) Documenter l'examen effectué (chap. 1.6.3).

Examen pratique (concerne la réalisation technique des IS)

6) Examiner si les produits utilisés correspondent à une autorisation selon le chap. 2.2.4.2, pt. 4).
7) Examiner les fonctions des IS, y compris la réaction en cas de dérangement, ainsi que de l'interaction des différents produits entre eux et avec les IS voisines sur la ligne.
8) Examiner les installations provisoires, si utile (chap. 1.11).
9) Évaluer l'adéquation et l'exhaustivité du contrôle d'usine concernant la sécurité.
10) Documenter l'examen effectué (chap. 1.6.3).

C. ETCS L2 : le mandat attribué à l'expert conformément aux exigences du gestionnaire du système ETCS CH (KGB, EGB) [42] doit être pris en compte lors des phases de planification et de réalisation.

2.2.4.4 Plans

Plans de l'installation extérieure des IS

Dans le projet standard, les informations suivantes doivent idéalement être représentées sur un plan de l'installation extérieure des IS :

- la désignation de tous les éléments, y compris le kilométrage ;
- les tronçons de voie ;
- les appareils de voie (avec la géométrie) ;

- les signaux (avec les images), les panneaux de signalisation, le contrôle de la marche des trains ;
- les passages à niveau (signalisation complète, y c. tous les éléments ferroviaires tels que les éléments de déclenchement et de contrôle) ;
- les vitesses ;
- les déclivités ;
- les quais, les bâtiments techniques et d'exploitation.

Les informations susmentionnées peuvent par exemple être fournies avec un ou plusieurs des plans suivants, utilisés dans la pratique :

- Plan de signalisation, en règle générale à l'échelle 1:500 ou 1:1000 avec la représentation de la voie par un trait simple ;
- Concept de signalisation : s'étend sur la zone pertinente (par ex. ligne entière) et est par exemple représenté sous forme schématique ;
- Plan de situation : plan de signalisation, complété par des informations sur l'infrastructure adjacente (par ex. passages à niveau, quais, routes, ponts, immeubles) ;
- S-Plan : plus détaillé que le plan de signalisation et à l'échelle 1:500 ou 1:250 avec la représentation de la voie par un double trait. Ce plan est déterminant pour la phase de réalisation.

Profils d'espace libre, s'ils concernent les signaux et les panneaux

- Type du profil d'espace libre
- Axe de la voie, dévers de la voie, surlargeur en courbe
- Cotes (par ex. hauteurs, distances par rapport à l'axe de la voie)
- Dégagement d'évacuation, dégagement de service

Pour les signaux et les panneaux, le profil d'espace libre est généralement représenté dans les profils en travers.

Plans des passages à niveau

- Plan de détail des passages à niveau à l'échelle 1:200 ou 1:100 avec la représentation de la voie par un double trait. Les informations suivantes doivent être représentées ou indiquées :
  - les éléments routiers (par ex. signaux, barrières, rideaux) ;
  - les limites et marquages de la route ;
  - les cotes (distances par rapport aux limites de la route et à l'axe de la voie) ;
  - les signalisations et les marquages routiers existants pertinents pour le projet.
- Profils d'espace libre des éléments des passages à niveau (y c. cotes)
- Profils en travers/Profils d'espace libre de la route (y c. cotes)

Représentation dans les plans

- Il faut utiliser le code de couleur standardisé (D RTE 25100 [33]) afin de montrer clairement quelles sont les parties d'IS existantes, nouvelles ou à supprimer. De même, il faut représenter les projets de tiers dans le même périmètre afin de pouvoir évaluer les éventuelles influences sur le projet standard à soumettre.
- Il faut dessiner tous les nouveaux éléments dans leur position prévue.
- Il faut représenter à l'échelle les dimensions et distances pertinentes pour le projet.
- Les désignations, abréviations, couleurs et symboles utilisés doivent figurer dans une légende, accompagnée des explications correspondantes. Il est également possible d'utiliser une légende indépendante du plan pour les documents de la PAP.

- Tous les plans doivent être mis à jour au plus tard lors de la phase de réalisation afin de correspondre aux IS construites.

2.2.5 Décision d'approbation des plans de l'OFT pour le projet standard

L'OFT octroie la DAP sans AE (chap. 1.4.4) pour les IS nouvelles ou modifiées.

2.3 Phase de réalisation du projet standard

Dans la phase de réalisation, il doit être prouvé que les IS ont été construites conformément aux spécifications et à l'approbation des plans et qu'elles peuvent être exploitées en toute sécurité (art. 5*l*, al. 1, OCF [4]).

2.3.1 Modifications du projet standard

Après l'octroi de la DAP, si des modifications sont apportées aux documents approuvés dans la PAP, il convient de procéder selon la figure 8. Les étapes correspondantes sont expliquées ci-après.

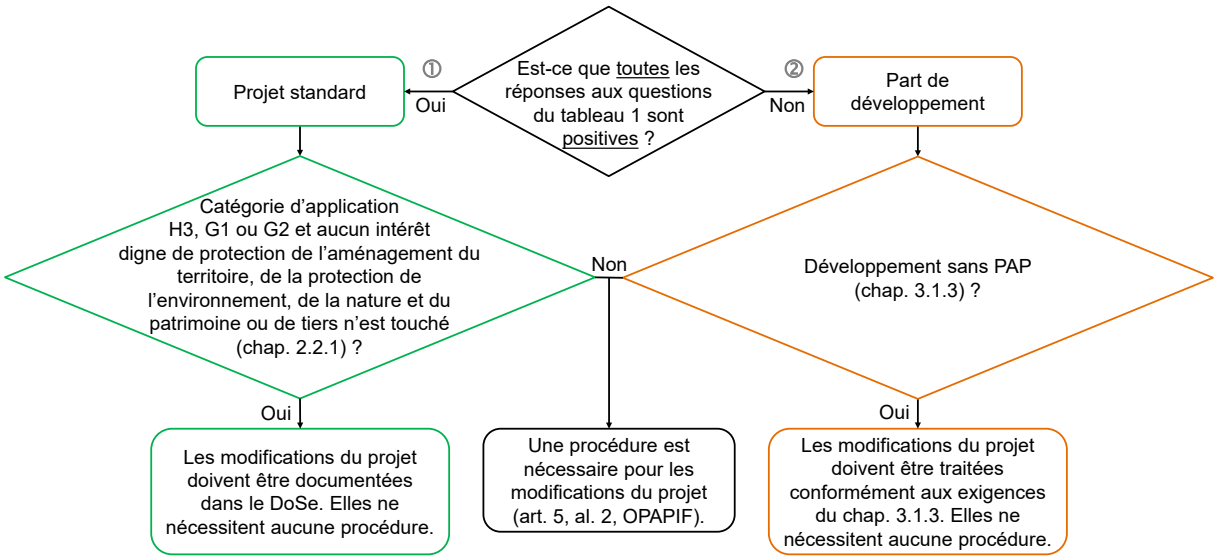

Figure 8 : Modifications du projet standard

Pour déterminer si les modifications du projet correspondent à un projet standard, il faut répondre aux questions figurant dans le tableau 1 (chap. 1.2).

① Lorsque toutes les réponses aux questions sont positives, les modifications du projet sont considérées comme un projet standard.

Lorsque les modifications du projet entrent dans la catégorie d'application H3, G1 ou G2 selon le chap. 2.2.1 et qu'elles ne touchent aucun intérêt digne de protection de l'aménagement du territoire, de la protection de l'environnement, de la nature et du patrimoine ou de tiers, elles doivent être documentées dans le DoSe et examinées par l'expert (pour la catégorie d'application H3).

Dans le cas contraire, une procédure est requise pour les modifications du projet (art. 5, al. 2, OPAPIF [5]). Les exigences du chap. 2 doivent être mises en œuvre pour les documents concernés par les modifications du projet.

② Lorsque toutes les réponses aux questions ne sont pas positives, les modifications du projet sont considérées comme part de développement.

Lorsque les modifications du projet selon le chap. 3.1.3 ne nécessitent pas de PAP, les exigences correspondantes doivent être mises en œuvre.

Dans le cas contraire, une procédure est requise pour les modifications du projet (art. 5, al. 2, OPAPIF [5]). Les exigences du chap. 3 doivent être mises en œuvre pour les documents concernés par les modifications du projet.

Sauf ordre contraire de l'OFT, les travaux non concernés par les modifications du projet peuvent se poursuivre si les IS sont déjà en construction (art. 5, al. 3, OPAPIF [5]).

2.3.2 Documents et exigences relatives au contenu du projet standard

Dans le tableau 6, les documents de la phase de réalisation sont énumérés. En complément, il contient des références dans lesquelles on trouve des explications sur les exigences relatives au contenu. Lors de la rédaction de ces documents, les exigences formelles selon le chap. 1.1.3 doivent être respectées.

Titre du document	Explications sur les exigences relatives au contenu
S-Plan (si pas fourni dans les documents de la PAP)	chap. 2.2.4.4
Documents de construction et de contrôle, y compris révision et libération des documents de construction	chap. 2.3.2.1
Dossier de sécurité	chap. 2.3.2.2
Programme de mise en service	chap. 1.17
Libération de mise en service	chap. 1.17
Rapports de contrôle d'usine	chap. 2.3.4
Rapport d'examen de l'expert phase de réalisation	chap. 1.6.3
Prise de position du GI sur la manière avec laquelle il mettra en œuvre les résultats du rapport d'examen de l'expert phase de réalisation	chap. 1.6.4

Tableau 6 : Documents de la phase de réalisation du projet standard

2.3.2.1 Documents de construction et de contrôle

Documents de construction

Les documents détaillés relatifs aux produits qui décrivent l'utilisation spécifique du produit dans une installation sont nommés documents de construction. Chaque document de construction établi ou modifié doit être contrôlé comme suit :

- Révision par l'auteur (généralement l'industrie ferroviaire) concernant :
  - le respect des règles de conception de projet ;
  - la mise en œuvre des schémas de principe ou des principes de construction ;
  - la mise en œuvre des SRAC ;
  - l'exhaustivité.
- Libération par le GI : le GI contrôle notamment que les exigences fonctionnelles et d'exploitation soient respectées. Il doit également s'assurer que les documents de construction sont conformes à la DAP, y compris aux documents approuvés dans la PAP.

Documents de contrôle

En règle générale, les documents de contrôle doivent également être établis avec les documents de construction. Ils indiquent les cas de contrôle et la manière dont le contrôleur d'usine doit procéder. Ils doivent être établis selon les modèles et les originaux de l'industrie ferroviaire. Il convient de prendre en compte tous les produits utilisés pour l'installation intérieure et extérieure, ainsi que l'interaction entre ces différents produits.

Implication de l'expert

Les documents de construction et de contrôle doivent être examinés par l'expert (chap. 2.3.5).

2.3.2.2 Dossier de sécurité

Le DoSe doit être établi et signé par des spécialistes parallèlement aux travaux du projet standard (art. 5*l*, al. 2, OCF [4]). Il se base sur le RaSe et doit donner une vue exhaustive sur les IS dans leur ensemble, même si le DoSe ne traite qu'une partie d'entre elles. Il faut veiller à ce que tous les produits utilisés y soient pris en compte.

Le DoSe est établi en deux étapes :

- Version initiale avant la MES (DoSe initial) : l'aptitude à la MES des IS y est démontrée. Les pts. 1) à 16) mentionnés ci-dessous doivent être traités, pour autant que les informations soient disponibles. Cette version du DoSe doit être présentée à temps à l'expert avant la MES. Il faut évaluer la pertinence des points en suspens en vue de la MES et documenter les étapes nécessaires pour leur traitement.
- Version finale après la MES (DoSe final) : complète la version initiale afin d'apporter la preuve du traitement des points initialement déclarés en suspens.

Le DoSe doit contenir les informations suivantes. Si certaines de ces informations figurent intégralement dans le RaSe, il est judicieux d'y faire référence.

1) Définition des IS considérées : si elle est identique à celle du rapport technique de niveau supérieur, il est possible d'y faire référence.
2) Documents de référence : par exemple spécifications, DAP, S-Plan, documents de construction, de contrôle, de conception de projet, de montage, prescriptions d'exploitation, release notes, analyses d'impact des modifications, révision et libération des documents de construction, protocoles de contrôle/check-lists, libération de MES, rapports de contrôle d'usine et d'examen de l'expert.
3) Produits utilisés, y compris leur version et leur autorisation, conformément au chap. 2.2.4.2, pt. 4).
4) Preuve que le projet correspond à un projet standard, dans la mesure où il a été provisoirement classifié comme tel lors de la phase de planification (chap. 1.2).
5) Organisation de la sécurité pour la phase de réalisation : documenter les rôles et les responsabilités des personnes impliquées. L'indépendance des rôles doit apparaître clairement.

   Si l'organisation de la sécurité est garantie par des processus appropriés, une documentation spécifique au projet n'est pas nécessaire.
6) Mandat d'examen de l'expert pour la phase de réalisation (chap. 2.2.4.3, let. B et C).
7) Modifications du projet (chap. 2.3.1).
8) Documentation expliquant comment il a été garanti que les règles reconnues de la technique définies lors de la phase de planification ont été respectées.
9) Preuve de la mise en œuvre des mesures issues de l'analyse et de l'évaluation du risque en cas de non-conformités aux prescriptions (chap. 2.2.4.2, pt. 11).
10) Charges, constats et points en suspens :
    - l'exécution des charges figurant dans la DAP ;
    - la mise en œuvre des constats issus des rapports d'examen d'expert des phases de planification et de réalisation ;
    - le traitement des points en suspens issus de la révision des documents de construction ;
    - le traitement des points en suspens issus de tous les rapports de contrôle d'usine.
11) Preuve du contrôle fonctionnel complet, spécifique aux installations : cette preuve peut par exemple être apportée par les rapports et les documents de contrôle d'usine correspondants.

12) Référence à la preuve de la non-intrusion et de la mise en œuvre des mesures de protection concernant la cybersécurité (chap. 1.14).
13) Installations provisoires (chap. 1.11).
14) Intégration au niveau de la technique et de l'exploitation (chap. 1.12) :
    a) la preuve de la mise en œuvre des SRAC ;
    b) la preuve de l'absence d'effets rétroactifs, si elle n'est pas fournie à un niveau supérieur ;
    c) les documents de conception de projet, de montage et les prescriptions d'exploitation mis à jour et/ou établis ;
    d) l'achèvement des formations ou des instructions du personnel roulant, d'exploitation et de maintenance ;
    e) la preuve de l'exécution des charges figurant dans les HdS des produits utilisés, y compris la preuve de la mise en œuvre des exigences génériques[28], pertinentes pour le GI.
15) Le cas échéant, liste des travaux restants :
    — l'évaluation de la pertinence pour la MES ;
    — les responsabilités et les délais.
16) Conclusion selon laquelle les IS :
    — sont construites conformément à la DAP ou sont conformes à cette dernière à l'exception des modifications du projet notées au pt. 7),
    — respectent les prescriptions déterminantes ou que les dérogations correspondantes ont été octroyées et
    — peuvent être exploitées en toute sécurité.

Le DoSe (y c. tous les documents de référence) doit être conservé et doit pouvoir être présenté à l'OFT dans le cadre de la surveillance de la sécurité en phase d'exploitation.

2.3.3 Conception de projet

Par la conception de projet, on entend la mise en œuvre spécifique, sur l'installation, des fonctions exigées au niveau de la technique et de l'exploitation en tenant compte des règles de conception de projet, des schémas de principe ou des principes de construction spécifiques aux produits. La mise en œuvre des documents de construction des produits utilisés dans la conception de projet doit être contrôlée et documentée.

2.3.4 Contrôle d'usine

Le contrôle d'usine est un contrôle spécifique à l'installation, fonctionnel et complet des IS. Il a pour objectif de contrôler les fonctions des produits utilisés ainsi que l'interaction entre les différents produits au niveau des interfaces.

L'exécution du contrôle d'usine s'effectue sur la base des documents de contrôle d'usine. Ces documents comprennent par exemple les documents de construction et de contrôle, les schémas ainsi que les analyses d'impact des modifications selon le chap. 1.12, pt. 5), nécessaires pour les modifications apportées au logiciel et/ou au matériel. Le contrôle d'usine peut être effectué par plusieurs contrôleurs d'usine en fonction du produit. Ils doivent coordonner leurs contrôles de manière à éviter toute lacune.

Le contrôleur d'usine doit être indépendant. Cela signifie qu'il ne doit pas assumer d'autres tâches (sauf de nature organisationnelle) en rapport avec l'objet à contrôler.

Les constats effectués lors du contrôle d'usine doivent être documentés. Les défauts identifiés doivent être évalués avec le GI dans le cadre de ce contrôle. Le cas échéant, il faut décider s'ils peuvent être compensés par des mesures d'exploitation afin de garantir un fonctionnement sûr.

Après le contrôle d'usine, l'expert et le GI reçoivent la confirmation que le contrôle d'usine a été entièrement effectué et que les IS sont soit sans défaut, ou présentent encore des points en suspens. Cette confirmation est nécessaire pour l'évaluation de l'aptitude des IS à être mises en service (chap. 1.17).

Les constats issus du contrôle d'usine doivent être corrigés sans délais et ensuite contrôlés par le contrôleur d'usine.

Les résultats du contrôle d'usine doivent être consignés dans le rapport de contrôle d'usine. Les informations suivantes doivent y figurer :

- la liste des documents du contrôle d'usine ;
- l'identification univoque de l'objet contrôlé (par ex. versions des logiciels, release, CRC) ;
- l'environnement du contrôle d'usine : laboratoire et/ou sur site (IS réelles) ;
- les résultats du contrôle d'usine.

2.3.5 Examen de l'expert phase de réalisation

L'examen de l'expert de la phase de réalisation doit être effectué conformément au mandat d'examen (chap. 2.2.4.3, let. B et C). Ce mandat est établi et attribué par le GI. Les exigences du chap. 1.9 doivent être respectées.

Dans le cadre de la préparation de l'examen de l'expert de la phase de réalisation, l'expert doit définir son déroulement et établir les documents nécessaires (par ex. protocoles d'examen, check-lists). Cette préparation fait partie de son travail d'examen et devrait commencer en amont.

L'examen de l'expert de la phase de réalisation comprend deux parties :

- Examen théorique des documents, notamment pour évaluer si les documents établis lors de la réalisation (par ex. documents de construction et de contrôle, DoSe) correspondent aux documents approuvés dans PAP et si les charges figurant dans la DAP sont remplies, dans la mesure où elles concernent la sécurité.
- Examen pratique de la réalisation technique des IS, notamment de leur bon fonctionnement. Cette partie de l'examen nécessite la desserte des IS construites.

Les détails concernant les tâches à accomplir dans le cadre des examens théorique et pratique figurent au chap. 2.2.4.3, let. B et C.

Lorsque l'examen de l'expert de la phase de planification est effectué en même temps que celui de la phase de réalisation, les documents de la PAP doivent également être examinés.

2.3.6 Travaux de finalisation sur les IS

En règle générale, les travaux suivants sont à réaliser après la MES :

- le traitement des points en suspens figurant dans le DoSe initial ;
- le traitement des points en suspens issus de tous les rapports de contrôle d'usine et, le cas échéant, la levée des mesures d'exploitation ;
- la mise en œuvre des constats issus du rapport d'examen de l'expert de la phase de réalisation ;
- la mise à jour de la documentation comme plans, documents de construction, release notes ;
- l'établissement du DoSe final.

2.3.7 Documents à soumettre et délais

Les documents suivants doivent être finalisés dans les trois mois suivant la MES :

- DoSe final ;

- rapport d'examen de l'expert phase de réalisation ;
- prise de position du GI sur la manière dont il mettra en œuvre les résultats du rapport d'examen de l'expert phase de réalisation.

La DAP définit les documents que le GI doit soumettre à l'OFT après la MES ainsi que les délais.

2.3.8 Aperçu des catégories d'application, de la documentation, de la PAP et des délais

La figure 9 présente un aperçu des catégories d'application, de la documentation, de la PAP et des délais du projet standard. Des détails à ces sujets se trouvent aux chap. 2.2.1, 2.2.3, 2.2.4, 2.3.2, 1.5 et 2.3.7.

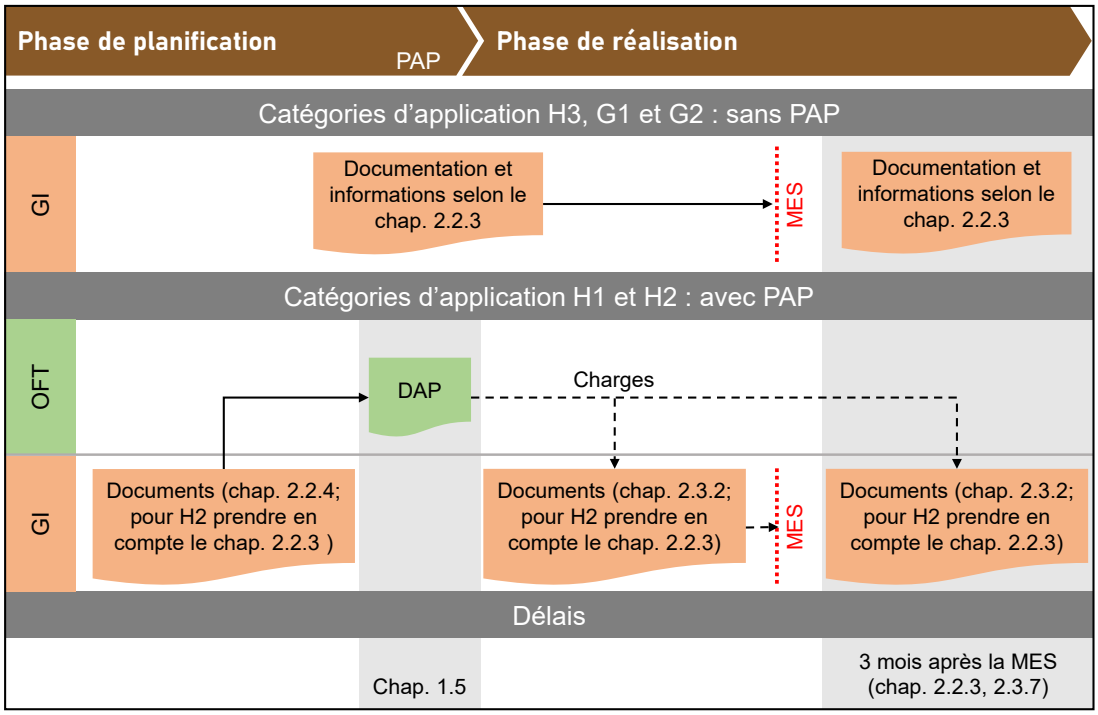

Figure 9 : Aperçu des catégories d'application, de la documentation, de la PAP et des délais

3 Projet de développement

3.1 Principes du projet de développement

Pour les développements, les phases du cycle de vie conformément à la SN EN 50126-1 [14] doivent être exécutées (DE-OCF ad art. 38, DE 38.1, ch. 1 [8]). Il est défini ci-après quand et par qui les exigences des SN EN 50126-1 [14] et SN EN 50129 [16] doivent être respectées (DE-OCF ad art. 38, DE 38.1, ch. 1.5 [8]). Une bonne compréhension de ces normes est nécessaire pour mettre en œuvre les contenus du chap. 3.

3.1.1 Phases et déroulement du projet de développement

Le projet de développement comprend trois phases. Son déroulement est illustré dans la figure 10.

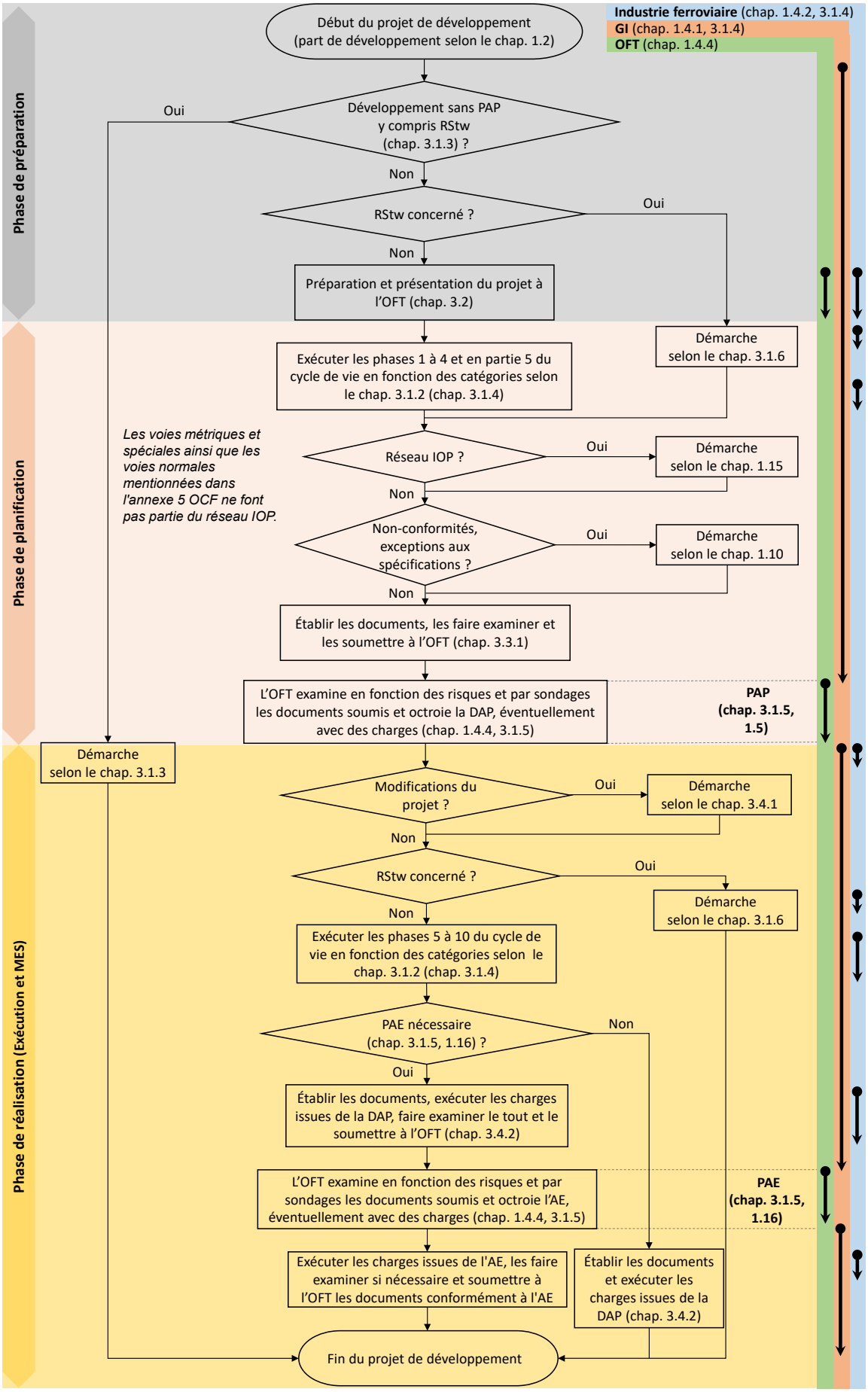

Figure 10 : Déroulement du projet de développement

3.1.2 Catégories d'objets du développement et exigences relatives à la démonstration de la sécurité

L'on distingue trois catégories d'objets du développement :

- Première utilisation de produits nouvellement développés (le produit n'existait pas auparavant) :
  - Dans la phase de planification, les exigences selon les chap. 3.1.4, 3.1.5, 3.1.7 et 3.3 doivent être mises en œuvre.
  - Dans la phase de réalisation, les exigences selon les chap. 3.1.4, 3.1.5, 3.1.7 et 3.4 doivent être mises en œuvre.
- Première utilisation de produits ultérieurement développés ou modifiés (un produit utilisé en Suisse est ultérieurement développé ou modifié) :
  - Il convient de déterminer, au moyen d'une analyse d'impact selon la SN EN 50126-1 [14], quelles phases du cycle de vie doivent être répétées en raison du développement ultérieur ou de la modification et quels documents doivent être établis ou mis à jour. Les résultats de l'analyse d'impact doivent être mis en œuvre au cours des phases de planification et de réalisation.

    Si des fonctions SIL sont concernées, l'examen de l'analyse d'impact est effectué par un expert. En fonction des résultats de l'analyse d'impact, il est défini quel expert (phases 1 à 4 ou 5 à 10 du cycle de vie ou première utilisation) effectue cet examen.

    Si seules des fonctions BI sont concernées, l'examen de l'analyse d'impact est effectué par le chargé de validation de la phase 9 du cycle de vie.
  - Pour les RStw ou les produits utilisant la technologie des relais, les exigences du chap. 3.1.6 s'appliquent.
- Première utilisation de produits dont le développement a été mené à terme (produit non utilisé en Suisse jusqu'à présent) :
  - Dans la phase de planification, il faut démontrer que les produits dont le développement a été mené à terme satisfont aux exigences du GI et que les tâches d'intégration au niveau de la technique et de l'exploitation ont été accomplies au stade de la planification. À cet effet, les phases 1 à 4 du cycle de vie selon les chap. 3.1.4, 3.1.5, 3.1.7 et 3.3 doivent être exécutées.
  - Dans la phase de réalisation, il faut démontrer que les spécifications des produits dont le développement a été mené à terme sont mises en œuvre et que l'intégration au niveau de la technique et de l'exploitation est achevée. À cet effet, les exigences selon les chap. 3.1.4, 3.1.5, 3.1.7 et 3.4.3 doivent être mises en œuvre.
  - Dans le cas d'une procédure d'HdS en cours pour un produit générique, l'autorisation de tests en exploitation issue de cette procédure peut être prise en compte (chap. 1.7).
  - Les autorisations de pays étrangers peuvent être prises en compte par l'OFT. Dans ce cas, au moins les documents ou informations suivants sont requis :
    - les autorisations de pays étrangers, y compris les documents qui y sont référencés. Les charges qui en découlent doivent être remplies et leur mise en œuvre doit être documentée.
    - la preuve de la conformité des objets du développement avec les objets des autorisations de pays étrangers, y compris les SRAC ;
    - la preuve de la mise en œuvre des prescriptions souveraines [1] à [9] pour les objets des autorisations de pays étrangers selon le chap. 3.3.1.2.
  - Les certificats de conformité aux exigences des normes techniques (chap. 1.3.2) ne sont pas exigés par les prescriptions souveraines [1] à [9], mais peuvent être pris en compte par l'OFT. Dans ce cas, les documents et informations suivants sont au minimum requis :
    - les certificats, y compris les documents qui y sont référencés. Les charges qui en découlent doivent être remplies et leur mise en œuvre doit être documentée.

- la preuve de la mise en œuvre des prescriptions souveraines [1] à [9] pour les objets du certificat selon le chap. 3.3.1.2.

3.1.3 Projets de développement sans PAP

La première utilisation de produits ultérieurement développés ou modifiés (chap. 3.1.2) concerne toujours le développement ultérieur ou la modification de produits déjà utilisés. Dans ce cas, aucune PAP n'est nécessaire si aucun intérêt digne de protection de l'aménagement du territoire, de la protection de l'environnement, de la nature et du patrimoine ou de tiers n'est affecté et si l'un des critères suivants est rempli :

(1) Il s'agit de modifications strictement techniques (par ex. correction des erreurs, obsolescence de composants, modifications du processus de fabrication).

(2) Le développement de fonctions, p. ex. au moyen d'éléments logiques librement programmables, est effectué par l'industrie ferroviaire conformément aux spécifications de processus correspondantes satisfaisant aux exigences des SN EN 50126-1 [14], SN EN 50129 [16] et SN EN 50716 [39], pour autant que ces spécifications aient été approuvées par l'OFT au moyen de l'HdS.

Les informations suivantes sont nécessaires pour la démonstration de la sécurité, le cas échéant avec référence à des documents adaptés :

a) la confirmation du GI qu'aucun intérêt digne de protection de l'aménagement du territoire, de la protection de l'environnement, de la nature et du patrimoine ou de tiers n'est affecté ;

b) pour le critère (1) : la mise en œuvre des critères pour les modifications strictement techniques selon l'annexe A4.3.1.2 de la Dir. HdS [13] par l'industrie ferroviaire et évaluation par l'expert des phases 5 à 10 du cycle de vie ou, pour les fonctions BI, par le chargé de validation de la phase 9 du cycle de vie ;

c) pour le critère (2) : la mise en œuvre des spécifications de processus applicables à la fonction développée par l'industrie ferroviaire et évaluation par l'expert des phases 5 à 10 du cycle de vie ou, pour les fonctions BI, par le chargé de validation de la phase 9 du cycle de vie ;

d) la preuve de la mise en œuvre des prescriptions souveraines [1] à [9] pertinentes pour le développement par le GI avec l'industrie ferroviaire (chap. 3.3.1.2) ;

e) pour la MES des fonctions SIL, la démarche selon le chap. 1.17 s'applique. Pour les fonctions BI, le contrôle de MES doit être effectué par une personne compétente, sur la base de protocoles de contrôle/check-lists.

Lorsqu'il s'agit d'une combinaison d'un projet standard et d'un projet de développement, la mise en œuvre des pts. a) à e) peut être démontrée dans un chapitre distinct du DoSe du projet standard. Dans le cas contraire, la mise en œuvre de ces points doit être démontrée dans le DoSe pour la première utilisation (chap. 3.4.2.2).

Lorsque des RStw ou des produits utilisant la technologie des relais sont concernés, il est défini au chap. 3.1.6 quand aucune PAP n'est requise et quelles exigences s'appliquent à la démonstration de la sécurité.

3.1.4 Processus de développement : cycle de vie et activités de sécurité

Pour l'objet de développement[30], les phases 1 à 10 du cycle de vie selon la SN EN 50126-1 [14] doivent en général être exécutées dans les phases de planification et de réalisation du projet de développement.

L'exécution des phases 11 à 12 du cycle de vie ne fait pas partie du projet de développement. Ces phases sont mentionnées, car le projet de développement fournit pour elles des informations concernant l'exploitation, la maintenance, le suivi des performances et le retrait du service.

[30] système au sens de la SN EN 50126-1 [14] et de la SN EN 50126-2 [15]

La figure 11 présente le cycle de vie de l'objet du développement selon la SN EN 50126-1 [14]. La phase de planification comprend les phases 1 à 4 et en partie 5 du cycle de vie. La phase de réalisation comprend les phases 5 à 10 du cycle de vie. Les trois flèches indiquent la coordination entre le GI et l'industrie ferroviaire.

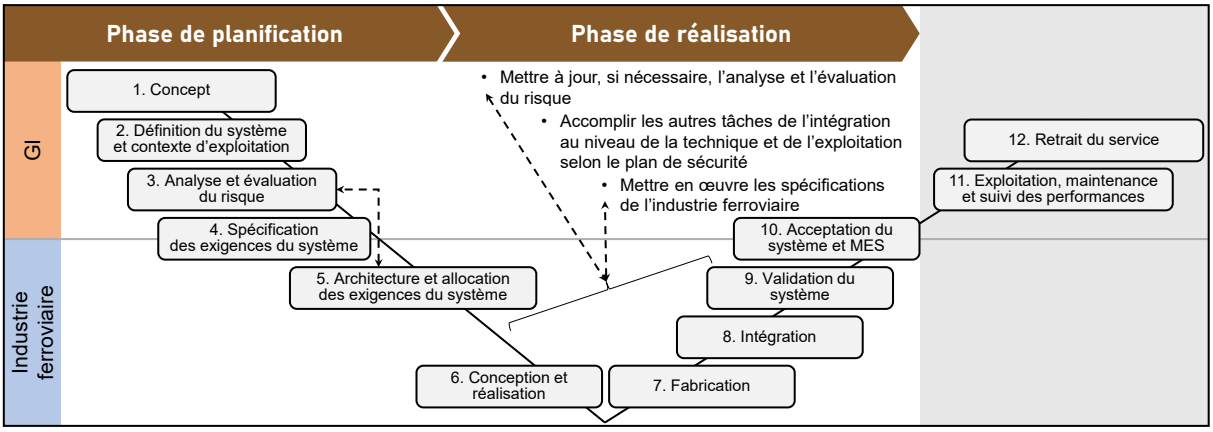

Figure 11 : Cycle de vie de l'objet du développement

Les phases 1 à 10 du cycle de vie doivent être documentées conformément à la SN EN 50126-1 [14]. Il faut démontrer que les activités de sécurité requises ont été réalisées, que les livrables nécessaires sont disponibles et que les objectifs des phases du cycle de vie correspondants ont été atteints. Les exigences de la SN EN 50126-1 [14] s'appliquent à cet effet, avec les concrétisations et compléments suivants :

1) Le GI doit réaliser les activités de sécurité conformément à la SN EN 50126-1 [14] pour les phases 1 à 4 du cycle de vie. Idéalement, l'industrie ferroviaire est déjà impliquée dans ces phases.

2) Les spécifications déterminantes doivent être prises en compte (chap. 1.3).

3) Les exigences relatives à l'indépendance et à la compétence professionnelle des rôles selon la SN EN 50126-2 [15] s'appliquent. Dans ce contexte, les experts doivent satisfaire aux exigences selon le chap. 1.4.3.

4) Le plan de sécurité doit être établi dans la phase 2 du cycle de vie. Il doit indiquer les activités de sécurité à réaliser pour satisfaire aux spécifications déterminantes. Des informations doivent être fournies pour chaque exigence du plan de sécurité de la SN EN 50126-1 [14]. Pour certaines exigences, des concrétisations et des compléments sont apportés ci-après.

   — Planification des activités de sécurité : la forme tabulaire selon la SN EN 50126-1 [14] peut être utilisée comme base. Le tableau 7 présente des exemples de compléments.

ID	Phase du cycle de vie	Activité de sécurité	À réaliser par	Document d'entrée	Livrable
x	3	Effectuer l'analyse et l'évaluation du risque conformément à la Dir. IS.	Prénom Nom	- Concept - Définition du système et contexte d'exploitation	- Analyse et évaluation du risque - Registre des situations dangereuses
x+1	3	Etablir un plan d'examen de l'expert des phases 1 à 4 du cycle de vie.	Prénom Nom	Mandat d'examen des phases 1 à 4 du cycle de vie	Plan d'examen de l'expert des phases 1 à 4 du cycle de vie
x+2	4	Prouver la mise en œuvre des prescriptions souveraines conformément à la Dir. IS.	Prénom Nom	Liste des articles et chapitres pertinents des prescriptions souveraines et la preuve de leur mise en œuvre.	Preuve de la mise en œuvre des prescriptions souveraines

ID	Phase du cycle de vie	Activité de sécurité	À réaliser par	Document d'entrée	Livrable
x+3	4	Etablir un concept de tests de qualification de sécurité conformément à la Dir. IS.	Prénom Nom	- Concept - Définition du système et contexte d'exploitation - Analyse et évaluation du risque - Registre des situations dangereuses	Concept de tests de qualification de sécurité

Tableau 7 : Exemple de planification des activités de sécurité

— Le cycle de vie de l'objet du développement est représenté sur la figure 11. En fonction des catégories d'objets du développement mentionnées au chap. 3.1.2, il faut définir les phases du cycle de vie à exécuter.

— Vérification : démarche selon le pt. 12) ;

— Validation : démarche selon le pt. 13) ;

— Processus pour l'autorisation de sécurité : procédure selon le chap. 3.1.5.

Outre ces concrétisations des exigences de la SN EN 50126-1 [14], la planification des points suivants doit être définie dans le plan de sécurité :

— la preuve de la mise en œuvre des prescriptions souveraines [1] à [9] (chap. 3.3.1.2) ;

— les autres tâches d'intégration au niveau de la technique et de l'exploitation (chap. 1.12) ;

— les points clés concernant la cybersécurité (chap. 1.14) ;

— l'établissement du DoSe pour la première utilisation (chap. 3.4.2.2).

5) Dans la phase 2 du cycle de vie, le plan FDM doit être établi. Au moment de la rédaction, l'accent est mis sur la formulation des exigences FDM selon la SN EN 50126-1 [14]. Il est possible d'établir séparément le plan FDM ou de le regrouper avec le plan de sécurité dans un plan FDMS.

   D'autres contenus du plan FDM, selon les exigences normatives, se rapportent à la mise en œuvre technique et ne peuvent être définis par l'industrie ferroviaire que dans les phases ultérieures du cycle de vie, selon le pt. 8).

6) Dans la phase 3 du cycle de vie, l'analyse et l'évaluation du risque doivent être effectuées selon le chap. 1.8. Elles se réfèrent à l'objet du développement défini dans les phases 1 à 2 du cycle de vie.

7) Dans la phase 4 du cycle de vie, les activités de sécurité du GI et de l'industrie ferroviaire se chevauchent, ce qui nécessite une étroite collaboration.

8) Dans la phase 5 du cycle de vie, l'industrie ferroviaire doit :

   — informer le GI lorsque de nouvelles situations dangereuses sont identifiées dans le cadre du processus de maîtrise des situations dangereuses (SN EN 50126-2 [15]). Les mesures de maîtrise des situations dangereuses ou les contraintes définies pour l'utilisation des fonctions de l'objet du développement peuvent donner lieu à des SRAC adressés au GI.

   — mettre à jour le plan de sécurité et le plan FDM ou le plan FDMS pour les phases 6 à 10 du cycle de vie ou les compléter avec ses propres documents. Il convient également de définir comment garantir que les spécifications déterminantes issues du développement selon la SN EN 50126-1 [14] soient transmises aux phases 11 à 12 du cycle de vie (concernant l'exploitation, la maintenance, le suivi des performances et le retrait du service).

   — établir la documentation relative à la planification du logiciel conformément au tableau A.1 de la SN EN 50716 [39].

9) Dans les phases 6 à 9 du cycle de vie, l'industrie ferroviaire doit :

   — prouver la maîtrise des situations dangereuses conformément à la SN EN 50129 [16] ;

- prouver le développement du logiciel conformément à la SN EN 50716 [39]. Les spécifications relatives aux outils de développement de logiciel se trouvent également dans la SN EN 50716 [39]. Pour tous les autres outils, il faut tenir compte des spécifications de la SN EN 50129 [16].
- établir et mettre à jour le DoSe pour l'application spécifique (pas nécessaire pour BI). Ce DoSe peut se fonder sur des DoSe de produits génériques et/ou d'applications génériques. Tous ces DoSe doivent être conformes aux exigences de la SN EN 50129 [16] en termes de structure et de contenu.
- faire référence à la preuve de la non-intrusion concernant les FDMS et de la mise en œuvre des mesures de protection de la cybersécurité dans le DoSe pour l'application spécifique ;
- transmettre au GI toutes les spécifications nécessaires à l'exécution des phases 11 à 12 du cycle de vie (concernant l'exploitation, la maintenance, le suivi des performances et le retrait du service selon la SN EN 50126-1 [14]).

10) Dans les phases 6 à 9 du cycle de vie, le GI doit :
    - mettre à jour l'analyse et l'évaluation du risque (SN EN 50126-2 [15]) lorsque :
        - des situations dangereuses supplémentaires sont identifiées pour l'objet du développement ;
        - de nouvelles prescriptions d'exploitation sont nécessaires ;
        - des mesures supplémentaires sont exigées pour atteindre les objectifs de sécurité selon le concept de la phase 1 du cycle de vie.
    - accomplir d'autres tâches d'intégration au niveau de la technique et de l'exploitation conformément au plan de sécurité du pt. 4) ;
    - établir et mettre à jour le DoSe pour la première utilisation selon le chap. 3.4.2.2 (pas exigé pour BI, mais judicieux).
11) Au cours de la phase 10 du cycle de vie, les activités de sécurité du GI et de l'industrie ferroviaire se chevauchent, ce qui nécessite une étroite collaboration. Pour la MES, la démarche selon le chap. 1.17 s'applique.
12) Vérification :
    - À la fin de chaque phase du cycle de vie, la vérification doit être effectuée et documentée conformément à la SN EN 50126-1 [14]. Idéalement, les activités de vérification à effectuer sont définies dans le plan de vérification et les résultats sont documentés dans le rapport de vérification. L'établissement et l'attribution du mandat de vérification sont effectués par le GI, ou par l'industrie ferroviaire. Les informations contenues dans les pts. 1) à 11) de ce chapitre indiquent qui doit établir et attribuer ce mandat. Dans ledit mandat, il faut tenir compte des exigences selon le tableau 8, issues des SN EN 50126-1 [14] et SN EN 50126-2 [15].

Exigences pour le chargé de vérification
1. Confirmer l'indépendance selon la SN EN 50126-2 [15].
2. Confirmer la compétence professionnelle selon la SN EN 50126-2 [15].
3. Établir un plan de vérification précisant ce qui doit être vérifié, ainsi que le type de processus (par ex. analyse) et les examens nécessaires.
4. Effectuer la vérification selon le plan de vérification. Dans les phases du cycle de vie, les éléments suivants doivent être vérifiés : – le respect des exigences définies dans la SN EN 50126-1 [14] pour chaque phase du cycle de vie, concernant les activités et les livrables requis ; – l'exactitude et l'adéquation de l'analyse de la FDMS, si elle est définie ; – la conformité des livrables requis de la phase du cycle de vie en cours avec ceux des phases de cycle de vie précédentes ; – l'adéquation des procédures, des outils et des techniques utilisés au cours de la phase du cycle de vie, si ceux-ci sont définis ; – l'exactitude, la cohérence et l'adéquation des spécifications de tests et des tests effectués, si approprié ;

– les tâches de vérification spécifiques aux phases 6 et 8 du cycle de vie conformément à la SN EN 50126-1 [14].
5. Consigner les non-conformités à la SN EN 50126-1 [14] constatées lors de la vérification, les classer en fonction du risque et les transmettre aux responsables de la gestion des modifications et de la prise de décision.
6. Établir le rapport de vérification. Idéalement, la vérification est documentée dans un rapport de vérification comprenant un chapitre distinct pour chaque phase du cycle de vie.

Tableau 8 : Exigences pour le chargé de vérification

— Les constats issus de la vérification doivent être traités et réexaminés par le chargé de vérification, ou, le cas échéant, par le chargé de validation.

— La vérification peut être effectuée par plus d'un chargé de vérification.

13) Validation :

— Dans la phase 4 du cycle de vie, la validation des phases 1 à 4 du cycle de vie doit être effectuée conformément au plan de validation et documentée dans le rapport de validation. Il est possible d'établir séparément le plan de validation de la sécurité ou de le regrouper avec le plan de validation FDM dans un plan de validation FDMS. L'établissement et l'attribution du mandat de validation sont effectués par le GI. Dans le mandat de validation, il faut tenir compte des exigences selon le tableau 9, issues des SN EN 50126-1 [14] et SN EN 50126-2 [15]. Elles sont harmonisées avec les exigences pour l'expert (chap. 3.3.1.3, let. A) afin d'éviter les examens doubles.

Exigences pour le chargé de validation des phases 1 à 4 du cycle de vie
1. Confirmer l'indépendance selon la SN EN 50126-2 [15].
2. Confirmer la compétence professionnelle selon la SN EN 50126-2 [15].
3. Établir un plan de validation conformément à la SN EN 50126-1 [14] et le coordonner avec l'expert.
4. Effectuer la validation selon le plan de validation et justifier les éventuelles non-conformités à ce dernier.
5. Examiner la conformité du processus et des résultats du développement par rapport aux exigences de la SN EN 50126-1 [14].
6. Prendre en compte les concrétisations et les compléments aux pts. 4), 5) et 13) de ce chapitre.
7. Examiner l'exactitude, la cohérence et l'adéquation de la vérification.
8. Examiner les exigences du système en fonction de l'environnement/usage prévu.
9. Examiner la conformité des SRAC par rapport aux exigences de la SN EN 50129 [16].
10. Consigner les non-conformités à la SN EN 50126-1 [14] constatées lors de la validation, les classer en fonction du risque et les transmettre aux responsables de gestion des modifications et de prise de décision.
11. Établir le rapport de validation conformément à la SN EN 50126-1 [14].

Tableau 9 : Exigences pour le chargé de validation des phases 1 à 4 du cycle de vie

— Dans la phase 9 du cycle de vie, la validation doit être effectuée selon le plan de validation et documentée dans le rapport de validation. Il appartient à l'industrie ferroviaire d'établir et d'attribuer le mandat de validation.

— Les constats issus des rapports de validation doivent être traités et réexaminés par le chargé de validation, ou, le cas échéant, par l'expert concerné.

— La validation peut être effectuée par plus d'un chargé de validation.

14) Examen de l'expert :

— Les explications concernant l'examen de l'expert se trouvent au chap. 1.9.

— L'examen de l'expert des phases 1 à 4 du cycle de vie doit être effectué. L'établissement et l'attribution du mandat d'examen sont effectués par le GI selon le chap. 3.3.1.3, let. A. L'expert doit établir un plan d'examen[31] pour la mise en œuvre du mandat d'examen. L'examen d'expert

[31] plan d'évaluation indépendante de la sécurité selon la SN EN 50126-1 [14]

doit être effectué conformément au plan d'examen et documenté dans le rapport d'examen de l'expert des phases 1 à 4 du cycle de vie selon le chap. 1.6.3.

— Si aucune exigence de sécurité n'a été imposée à une fonction de l'objet du développement ou si exclusivement un taux d'occurrence maximal acceptable de danger $10^{-5}h^{-1}$ a été défini, l'expert confirme l'affectation BI (SN EN 50126-2 [15]) dans le rapport d'examen de l'expert des phases 1 à 4 du cycle de vie. Si nécessaire, l'expert peut consulter l'architecture prévue dans la phase 5 du cycle de vie ou formuler des charges concernant l'architecture ou la réalisation technique.

  Si l'expert confirme exclusivement l'affectation BI pour toutes les fonctions de l'objet de développement, aucun autre examen de l'expert n'est exigé dans les phases suivantes du cycle de vie (SN EN 50126-2 [15]).

— Si un examen de l'expert des phases 5 à 10 du cycle de vie est nécessaire, il est effectué avant la MES. L'établissement et l'attribution du mandat d'examen de l'expert sont effectués par l'industrie ferroviaire selon le chap. 3.3.1.3, let. B. L'expert doit établir un plan d'examen pour la mise en œuvre du mandat d'examen. L'examen de l'expert doit être réalisé selon le plan d'examen et documenté dans le rapport d'examen de l'expert des phases 5 à 10 du cycle de vie selon le chap. 1.6.3.

— L'examen de l'expert pour la première utilisation doit prendre en compte les résultats de l'examen de l'expert des phases 5 à 10 du cycle de vie ayant une pertinence pour la première utilisation. L'établissement et l'attribution du mandat d'examen sont effectués par le GI selon le chap. 3.3.1.3, let. C. L'expert doit établir un plan d'examen pour la mise en œuvre du mandat d'examen. L'examen de l'expert doit être réalisé selon le plan d'examen et documenté dans le rapport d'examen de l'expert pour la première utilisation selon le chap. 1.6.3.

— Dès lors que l'OFT exige une AE pour la MES, les experts des phases 5 à 10 du cycle de vie et de la première utilisation doivent documenter les résultats de leur examen dans leurs rapports d'examen de l'expert respectifs avant la MES.

15) Pour l'objet du développement comprenant exclusivement des fonctions BI, au minimum, les informations suivantes sont requises dans les phases 5 à 10 du cycle de vie, conformément aux exigences des SN EN 50126-2 [15], SN EN 50129 [16] et SN EN 50716 [39] :

— Exigences organisationnelles : il faut démontrer que l'organisation définie dans le plan de sécurité satisfait aux exigences de la SN EN 50129 [16] concernant l'indépendance des rôles pour BI.

— Preuve de la qualité : il faut démontrer que :

  – les mesures de qualité ont été mises en œuvre conformément au processus de gestion de la qualité ;

  – les formations ou les instructions nécessaires du personnel roulant, d'exploitation de maintenance ont eu lieu ;

  – les manuels de maintenance nécessaires sont disponibles.

— Preuve de la sécurité : le GI doit prouver la mise en œuvre des activités de sécurité selon le plan de sécurité du pt. 4).

— Preuve de la sécurité : l'industrie ferroviaire doit :

  – démontrer le respect des exigences du système et de sécurité (par ex. en faisant référence à un rapport de validation) ;

  – justifier le respect du taux de défaillance fonctionnelle tolérable ;

  – définir les conditions d'environnement et les SRAC. Les hypothèses formulées lors du processus d'allocation des exigences de sécurité doivent être consignées comme SRAC ;

  – définir des mesures adéquates de gestion des pannes comme les diagnostics, la maintenance, la formation du GI ;

  – démontrer l'absence d'effets rétroactifs (chap. 1.12, pt. 5) ;

- énumérer les techniques/mesures choisies selon la SN EN 50716 [39], décrire et prouver leur mise en œuvre (chap. 3.4.2.4) ;
- démontrer la réussite des tests de qualification de sécurité (chap. 3.4.3.1).

— Reference à la preuve de la non-intrusion concernant la FDMS et de la mise en œuvre des mesures de protection concernant la cybersécurité.

— Le contrôle de MES doit être effectué par une personne compétente, sur la base de protocoles de contrôle/check-lists.

— Si nécessaire, l'industrie ferroviaire soutient le GI lors des tests en exploitation (chap. 3.4.3.2).

3.1.5 Types de procédure

Les types de procédure possibles sont présentés à la figure 12. Le type de procédure est déterminé sur la base des trois étapes suivantes.

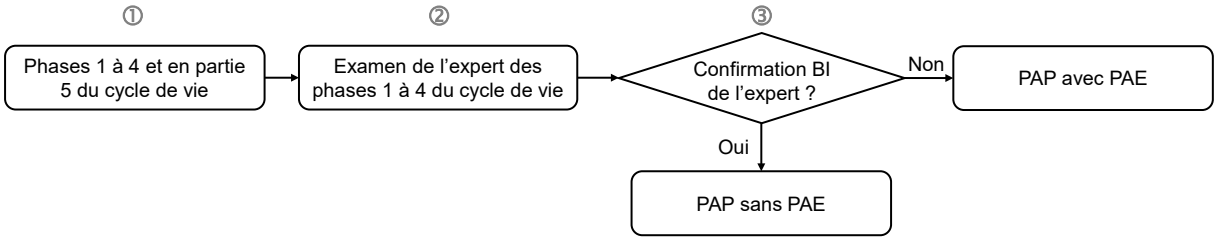

Figure 12 : Types de procédure

① L'exécution des phases 1 à 4 et en partie 5 du cycle de vie doit être documentée selon les chap. 3.1.4 et 3.3.1.

Si des RStw sont concernés, il convient de procéder selon le chap. 3.1.6.

② L'expert des phases 1 à 4 du cycle de vie doit examiner les documents selon ① conformément au chap. 3.1.4, pt. 14).

③ Si la BI est confirmée pour toutes les fonctions de l'objet du développement par l'expert des phases 1 à 4 du cycle de vie, une PAP sans PAE est requise. Dans le cas contraire, une PAP avec PAE est requise.

Les explications relatives à la PAP et à la PAE se trouvent aux chap. 1.5 et 1.16.

3.1.6 Développements des RStw et exigences relatives à la démonstration de la sécurité

Pour les développements des RStw, la démarche selon la figure 13 s'applique. Pour les autres produits utilisant la technologie des relais, cette démarche doit être appliquée par analogie. Les étapes correspondantes sont expliquées ci-dessous.

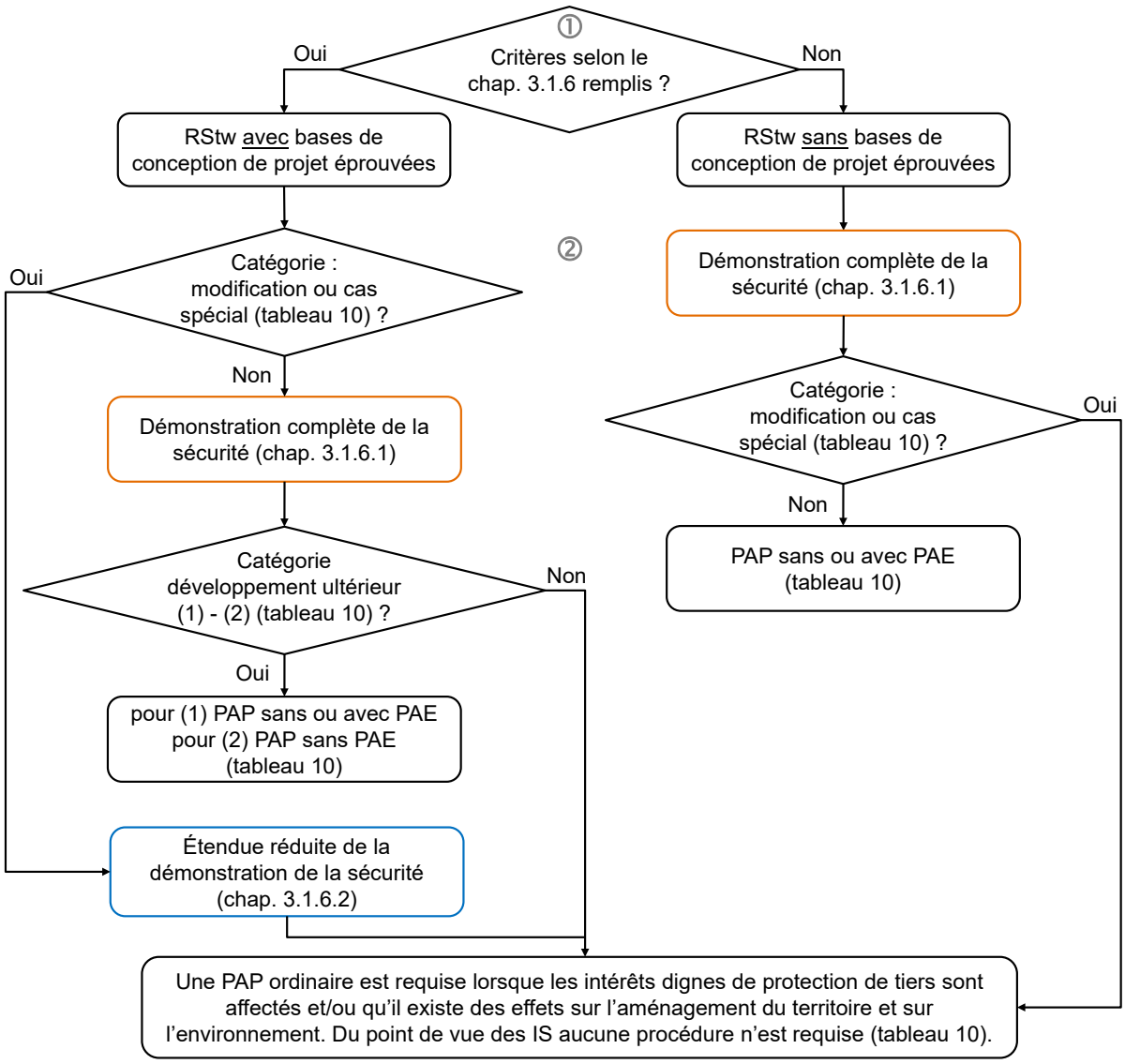

Figure 13 : Démarche pour les développements des RStw

① Déterminer s'il s'agit d'un RStw avec ou sans bases de conception de projet éprouvées. À cet effet, le GI doit contrôler que les critères suivants sont remplis :

a) Le RStw se fonde sur des bases de conception de projet éprouvées, c. -à-d. sur des schémas de principe ou des principes de construction avec des cas et des fonctions de base définis.

b) Le RStw est par exemple entretenu et développé par l'industrie ferroviaire ou le centre de compétence du GI. Les bases de conception de projet actuelles sont par exemple consignées dans un répertoire.

Si les critères a) et b) sont remplis, il s'agit d'un RStw avec bases de conception de projet éprouvées. Dans le cas contraire, il s'agit d'un RStw sans bases de conception de projet éprouvées.

② Les développements des RStw sont classés en trois catégories : modification, cas spécial et développement ultérieur.

Les conditions préalables pour les catégories modification et cas spécial sont les suivantes :

— aucun impact sur les processus d'exploitation n'est constaté ;

— aucun développement au niveau des interfaces (par ex. système de contrôle-commande ferroviaire) n'est permis ;

— aucune non-conformité aux fonctions de base n'est permise ;

- les contrôles des contacts de travail et de repos sont installés aux endroits prévus à cet effet ;
- enclenchement à câblage systématique (Spurplan) : les fonctions ne peuvent être intégrées que dans des schémas déjà prévus à cet effet ;
- enclenchement à câblage libre (Verschlussplan) : les nouveaux verrouillages ne peuvent être intégrés que dans la logique de verrouillage déjà existante ;
- les principes de commande et de verrouillage mutuel concernant les différentes possibilités de commande doivent être maintenus.

Un schéma électrique qui est déjà utilisé dans une installation spécifique chez un GI et qui dispose d'un DoSe et d'un rapport d'examen de l'expert peut être utilisé comme base de conception de projet.

Dans le cas contraire, il s'agit de la catégorie développement ultérieur.

Les exigences pour la démonstration de la sécurité sont définies en fonction de la distinction selon ① et des catégories mentionnées ci-dessous. Des informations complémentaires se trouvent dans le tableau 10.

<table>
<tr><th>Catégorie</th><th>RStw <u>avec</u> bases de conception de projet éprouvées</th><th>RStw <u>sans</u> bases de conception de projet éprouvées</th></tr>
<tr><td rowspan="5">Modification</td><td colspan="2">Souvent, des modifications non fonctionnelles doivent être apportées aux IS existantes, car, par exemple, aucun contact libre du relais n'est disponible. Sur la base du schéma électrique existant, il est décidé à quel endroit les insertions peuvent être réalisées sans modifier la fonction. Si le schéma de principe ne couvre pas exactement la topologie des voies, il doit être adapté spécifiquement pour l'installation.</td></tr>
<tr><td colspan="2">Démonstration de la sécurité</td></tr>
<tr><td>à étendue réduite selon le chap. 3.1.6.2</td><td>complète selon le chap. 3.1.6.1</td></tr>
<tr><td colspan="2">PAP</td></tr>
<tr><td colspan="2">Une PAP ordinaire est requise lorsque les intérêts dignes de protection de tiers sont affectés et/ou qu'il existe des effets sur l'aménagement du territoire et sur l'environnement. Aucune procédure n'est requise du point de vue des IS.</td></tr>
<tr><td rowspan="5">Cas spécial</td><td colspan="2">Sont considérées comme cas spécial, les fonctions d'un RStw déjà en service et pouvant être utilisées dans d'autres RStw du même type.</td></tr>
<tr><td colspan="2">Démonstration de la sécurité</td></tr>
<tr><td>à étendue réduite selon le chap. 3.1.6.2</td><td>complète selon le chap. 3.1.6.1</td></tr>
<tr><td colspan="2">PAP</td></tr>
<tr><td colspan="2">Une PAP ordinaire est requise lorsque les intérêts dignes de protection de tiers sont affectés et/ou qu'il existe des effets sur l'aménagement du territoire et sur l'environnement. Aucune procédure n'est requise du point de vue des IS.</td></tr>
<tr><td rowspan="6">Développement ultérieur</td><td colspan="2">Le développement ultérieur comprend par exemple :
(1) le développement de nouvelles fonctions et/ou de nouvelles interfaces ;
(2) la reproduction d'une fonction connue (par ex. reproduction d'un signal de répétition avec des tronçons de contrôle de l'état libre de la voie séparés), qui est déjà mise en œuvre dans d'autres types d'enclenchements et doit être utilisée pour la première fois dans un RStw.</td></tr>
<tr><td>(3) l'intégration d'une fonction utilisée à plusieurs reprises dans un schéma de principe.</td><td></td></tr>
<tr><td colspan="2">Démonstration de la sécurité</td></tr>
<tr><td colspan="2">complète selon le chap. 3.1.6.1</td></tr>
<tr><td colspan="2">PAP, PAE</td></tr>
<tr><td>– Pour (1), une PAP est requise (chap. 1.5). Une PAE peut être requise (chap. 1.16) ;</td><td>Une PAP est requise (chap. 1.5). Une PAE peut être requise (chap. 1.16).</td></tr>
</table>

Catégorie	RStw avec bases de conception de projet éprouvées	RStw sans bases de conception de projet éprouvées
	– Pour (2), une PAP sans PAE est requise ; – Pour (3) ou pour les cas non couverts ici, une PAP ordinaire est requise lorsque les intérêts dignes de protection de tiers sont affectés et/ou qu'il existe des effets sur l'aménagement du territoire et sur l'environnement. Aucune procédure n'est requise du point de vue des IS.	

Tableau 10 : Détails concernant les développements des RStw

Il est possible d'attester le respect des exigences pour la démonstration de la sécurité des RStw lors des phases de planification et de réalisation dans un chapitre distinct des documents du projet standard (RaSe, DoSe, rapport de contrôle d'usine, rapport d'examen de l'expert), ou dans des documents séparés. Les exigences formelles du chap. 1.1.3 doivent être prises en compte.

3.1.6.1 Démonstration complète de la sécurité

Selon le tableau 10, la démonstration complète de la sécurité est requise dans les phases de planification et de réalisation pour :

- les RStw avec bases de conception de projet éprouvées en cas de développement ultérieur ;
- les RStw sans bases de conception de projet éprouvées en cas de modification, de cas spécial ou de développement ultérieur.

Phase de planification

1) Le GI doit :
   - décrire le développement ultérieur, la modification ou le cas spécial susmentionné ;
   - démontrer la mise en œuvre des prescriptions souveraines selon le chap. 3.3.1.2 ;
   - effectuer l'analyse et l'évaluation du risque conformément au chap. 1.8 ;
   - définir toutes les exigences ;
   - documenter les rôles, les responsabilités et les compétences professionnelles des personnes impliquées ;
   - coordonner le mandat pour développement ultérieur, la modification ou le cas spécial avec l'industrie ferroviaire ou le centre de compétence du GI ;
   - établir et attribuer le mandat d'examen de l'expert pour les phases de planification et de réalisation. En règle générale, l'expert doit accomplir les tâches indiquées dans le tableau 11.

Tâches de l'expert pour la phase de planification	
A1.	Examiner la description du développement ultérieur, de la modification ou du cas spécial.
A2.	Examiner l'analyse et l'évaluation du risque ainsi que toutes les exigences définies.
A3.	Examiner si les bases de conception de projet référencées sont adaptées au développement ultérieur, à la modification ou au cas spécial.
A4.	Examiner la preuve de la mise en œuvre des prescriptions souveraines [1] à [9] (chap. 3.3.1.2).
A5.	Examiner si les non-conformités aux spécifications et la demande d'octroi de dérogation sont entièrement documentées (chap. 1.10). Examiner et documenter l'acceptation des non-conformités.
A6.	Examiner l'analyse et l'évaluation du risque d'éventuelles non-conformités aux prescriptions souveraines [1] à [9].
A7.	Examiner les rôles, les responsabilités et les compétences professionnelles des personnes impliquées.
A8.	Documenter l'examen effectué (chap. 1.6.3).

Tâches de l'expert pour la phase de réalisation
B1. Examiner si les tâches de l'intégration au niveau de la technique et de l'exploitation sont accomplies (chap. 1.12).
B2. Examiner si les charges figurant dans la DAP sont remplies, pour autant qu'elles concernent la sécurité.
B3. Examiner si les constats issus du rapport d'examen de l'expert de la phase de planification sont mis en œuvre.
B4. Examiner si les modifications du projet sont documentées et conformes aux spécifications (chap. 3.4.1).
B5. Examiner les fonctions des IS, y compris la réaction en cas de dérangement ainsi que l'interaction des différents produits entre eux et avec les IS voisines sur la ligne.
B6. Examiner les schémas électriques.
B7. Examiner si : – les exigences de la phase de planification sont mises en œuvre ; – la sécurité de chaque schéma électrique concerné est démontrée en cas de défaillance, de dérangement ou de dysfonctionnement ; – les impacts sur les prescriptions d'exploitation sont indiqués ; – les impacts sur les interfaces sont indiqués ; – les éventuelles SRAC sont conformes aux exigences de la SN EN 50129 [16] ; – les documents de contrôle sont disponibles pour le contrôle d'usine ; – les constats figurant dans le rapport de contrôle d'usine sont traités.
B8. Évaluer l'adéquation et l'exhaustivité du contrôle d'usine concernant la sécurité.
B9. Documenter l'examen effectué (chap. 1.6.3). Dès lors que l'OFT exige une AE pour la MES, l'expert doit documenter les résultats de son examen dans le rapport d'examen de l'expert avant la MES.

Tableau 11 : Tâches de l'expert dans les phases de planification et de réalisation

2) L'industrie ferroviaire ou le centre de compétence du GI doit :
   - référencer toutes les bases de conception de projet, le cas échéant le DoSe et le rapport d'examen de l'expert des schémas électriques ;
   - établir et attribuer le mandat de contrôle au contrôleur d'usine.
3) L'expert doit effectuer l'examen de la phase de planification conformément au mandat d'examen et documenter les résultats de son examen selon le chap. 1.6.3.

Phase de réalisation

1) Le GI doit :
   - démontrer l'achèvement de l'intégration au niveau de la technique et de l'exploitation (chap. 1.12) ;
   - prouver l'exécution des charges figurant dans la DAP ;
   - prouver le traitement des points en suspens issus du rapport de contrôle d'usine ;
   - prouver le traitement des points en suspens issus du rapport d'examen de l'expert de la phase de planification ;
   - documenter les modifications du projet (chap. 3.4.1) ;
   - évaluer les points en suspens concernant leur pertinence pour la MES, définir les responsabilités et les délais pour leur traitement.
2) L'industrie ferroviaire ou le centre de compétence du GI doit :
   - mettre en œuvre les exigences de la phase de planification ;
   - indiquer les endroits où l'adaptation des schémas électriques a été effectuée par rapport aux bases de conception de projet ;

- démontrer la sécurité de chaque schéma électrique concerné en cas de défaillance, de dérangement et dysfonctionnement[32] ;
- indiquer les impacts sur les prescriptions d'exploitation. Il faut d'indiquer les clarifications avec l'exploitation et la maintenance ;
- indiquer les impacts sur les interfaces ;
- définir les SRAC (si nécessaire). Les exigences de la SN EN 50129 [16] doivent être prises en compte ;
- démontrer l'absence d'effets rétroactifs selon le chap. 1.12, pt. 5) ;
- établir des documents de contrôle pour le contrôle d'usine.

3) Le contrôleur d'usine doit effectuer le contrôle d'usine conformément au mandat et documenter les résultats de son contrôle dans le rapport de contrôle d'usine selon le chap. 2.3.4.
4) Les constats issus du rapport de contrôle d'usine doivent être réexaminés soit par le contrôleur d'usine, soit, le cas échéant, par l'expert.
5) L'expert doit effectuer l'examen d'expert de la phase de réalisation conformément au mandat d'examen et documenter les résultats de son examen selon le chap. 1.6.3.
6) Tests de qualification de sécurité : la démarche au sens du chap. 3.4.3.1 s'applique.
7) MES : la démarche selon le chap. 1.17 s'applique.

3.1.6.2 Étendue réduite de la démonstration de la sécurité

Selon le tableau 10, une étendue réduite de la démonstration de la sécurité dans les phases de planification et de réalisation est nécessaire pour les RStw dont les bases de conception de projet sont éprouvées, en cas de modification ou de cas spécial. Pour ces derniers, il n'est pas nécessaire de distinguer entre les phases de planification et de réalisation du point de vue de la démonstration de la sécurité. Pour cette dernière, les points suivants doivent être pris en compte :

1) Le GI doit décrire la modification ou le cas spécial. Il doit être clairement indiqué à quels endroits l'adaptation du schéma électrique a été effectuée par rapport aux bases de conception de projet.
2) Si nécessaire, l'industrie ferroviaire ou le centre de compétence du GI soutient le GI pour la modification ou le cas spécial.
3) L'expert doit examiner l'adaptation du schéma électrique par rapport aux bases de conception de projet et documenter les résultats de son examen selon le chap. 1.6.3.
4) MES : la démarche selon le chap. 1.17 s'applique.

3.1.7 Aperçu des phases du cycle de vie, des types de procédure, de la documentation et des délais

Les dépendances entre les phases du cycle de vie, les types de procédure, la documentation et les délais de l'objet du développement sont représentées dans la figure 14. Pour plus de détails sur les phases du cycle de vie, les types de procédure et la documentation, voir les chap. 3.1.4, 3.1.5, 3.3.1 et 0. Des informations complémentaires concernant les types de procédure et les délais sont fournies ci-après.

[32] par exemple l'attraction ou la chute intempestive d'un contact de relais

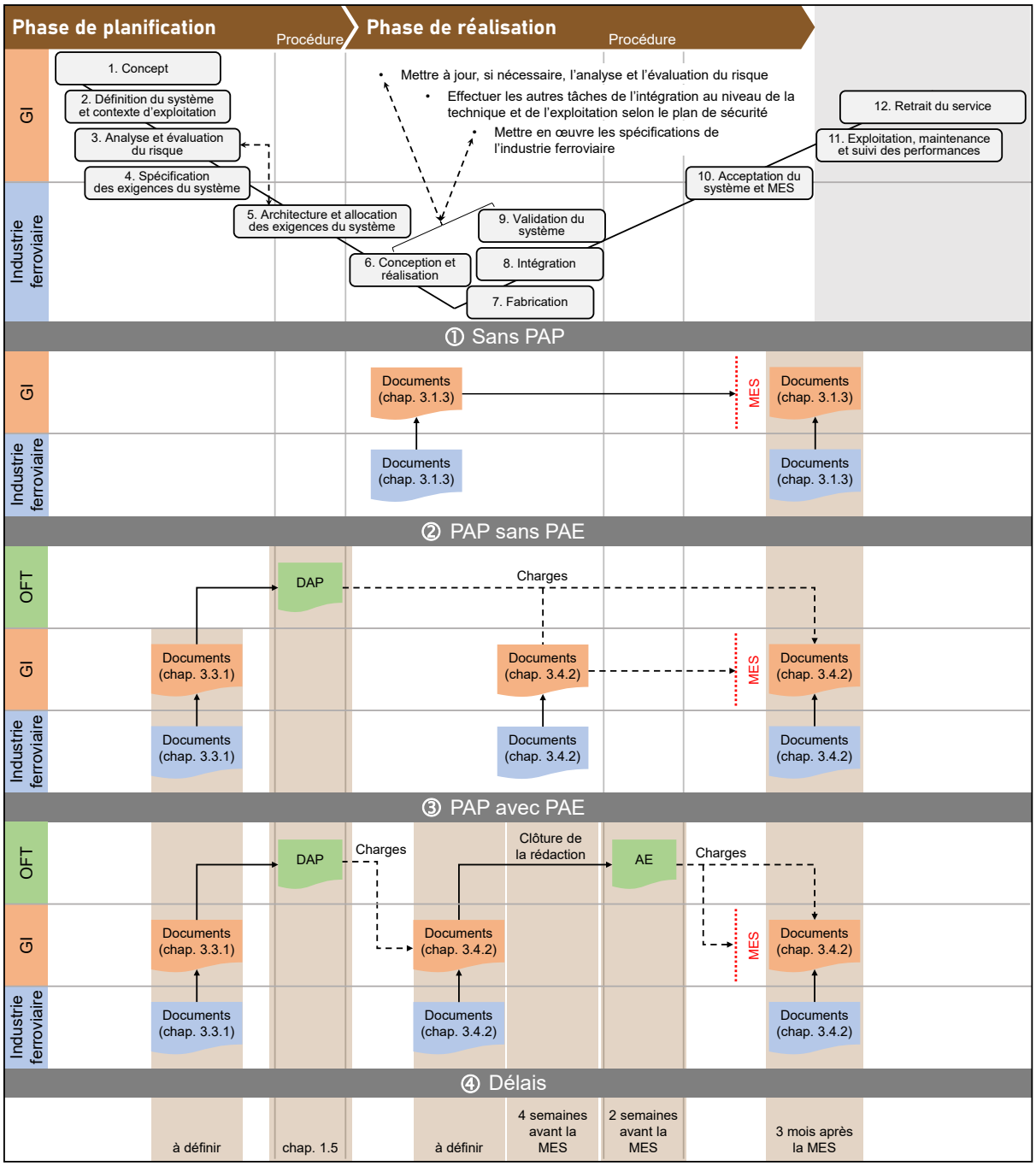

Figure 14 : Aperçu des phases du cycle de vie, des types de procédure, de la documentation et des délais

① Les développements sans PAP sont réalisés lorsque les critères selon le chap. 3.1.3 sont remplis.

② Selon le chap. 3.1.5, la PAP sans PAE s'applique aux développements comportant exclusivement des fonctions BI. L'OFT octroie la DAP dans la phase 5 du cycle de vie.

③ Selon le chap. 3.1.5, la PAP avec PAE s'applique aux développements comportant des fonctions SIL. L'OFT octroie la DAP et exige l'AE dans la phase 5 du cycle de vie.

④ Il appartient au GI de définir la date de soumission des documents de la PAP. Le GI doit également définir la date de soumission des documents pour la PAE en coordination avec l'OFT. Il en va de même pour les éventuelles soumissions ultérieures. En règle générale, l'OFT accepte la dernière soumission quatre semaines avant la MES (clôture de la rédaction pour le GI). Deux semaines avant la MES, l'OFT octroie l'AE. Le GI peut ainsi utiliser les deux semaines restantes jusqu'à la MES pour exécuter les charges résiduelles.

Le GI est responsable de la planification de la procédure. Elle doit être coordonnées avec les livrables de l'industrie ferroviaire.

La finalisation des documents de preuve doit être effectuée dans un délai de trois mois après la MES.

Pour les développements sans PAP, il n'est pas nécessaire de soumettre les documents de preuve à l'OFT. Ils restent en possession du GI et doivent pouvoir être présentés à l'OFT dans le cadre de la surveillance de la sécurité en phase d'exploitation.

3.2 Phase de préparation du projet de développement

La phase de préparation est exécutée lorsque le projet de développement nécessite une PAP et ne concerne pas les RStw. L'OFT soutient le GI dans cette phase avec la « coordination des projets innovants » (KIP). Il est recommandé au GI de prendre contact avec la KIP[33] avant la phase de planification. La KIP organise ensuite une concertation commune et s'assure que les sections spécialisées concernées de l'OFT soient consultées. Dans l'idéal, les parties prenantes de l'industrie ferroviaire y participent également.

Les exigences générales de l'OFT s'appliquent à cette concertation : les développements ne doivent pas être évalués uniquement en fonction de la technique, mais en tenant compte également de critères généraux comme le rapport coût/bénéfice et/ou la conformité à la stratégie de l'OFT.

La concertation a pour but d'assurer un début du développement dans les règles de l'art. Il s'agit notamment d'évoquer les points suivants, qui font partie du plan de sécurité :

- les spécifications déterminantes (chap. 1.3) et les éventuelles non-conformités (chap. 1.10) ;
- l'analyse et l'évaluation du risque (chap. 1.8) ;
- les points clés concernant la cybersécurité (chap. 1.14) ;
- l'aptitude et les mandats d'examen des experts (chap. 3.3.1.3) ;
- la définition du type de procédure (chap. 3.1.5) ;
- la démarche pour établir le DoSe pour la première utilisation (chap. 3.4.2.2) ;
- les tests de qualification de sécurité et les tests en exploitation (chap. 3.4.3) ;
- le déploiement (rollout) des IS ;
- Selon le chap. 1.1.2, lorsque, d'autres démarches sont appliquées, il est exigé pour la PAP que le développement de l'objet soit suffisamment avancé pour que les informations spécifiques à l'installation soient prises en compte dans les documents de la phase de planification (tableau 12).

3.3 Phase de planification du projet de développement

3.3.1 Documents et exigences relatives au contenu

Dans le tableau 12, les documents pour la phase de planification sont énumérés et attribués aux phases du cycle de vie. En complément, il contient des références dans lesquelles figurent des explications sur les exigences relatives au contenu des documents (art. 3, al. 1 à 2, OPAPIF [5]). Lors de la rédaction de ces documents, les exigences formelles selon le chap. 1.1.3 et les exigences relatives à la documentation de FDMS de la SN EN 50126-1 [14] doivent être mises en œuvre.

[33] KIP@bav.admin.ch

Les documents énumérés dans le tableau 12 doivent être soumis à l'OFT (art. 18*b* LdCF [1]). Si le GI estime que certains de ces documents ne sont pas pertinents pour le développement concret, il peut renoncer à les soumettre en justifiant brièvement sa décision (par ex. « non pertinent »).

Lorsque, dans le cadre d'un projet global ou d'un projet standard, des documents comme la table des matières[34], la demande d'approbation des plans et le condensé du projet sont soumis, ces documents ne doivent alors pas être soumis à nouveau pour l'objet du développement.

Les exigences relatives au contenu du RaSe selon l'art. 5*m*, al. 2, OCF [4] et du rapport technique selon l'art. 3 OPAPIF [5] sont couvertes par les documents des phases 1 à 4 du cycle de vie. Par conséquent, il n'est pas nécessaire de fournir le RaSe et le rapport technique en tant que documents séparés.

Titre du document *Les documents qui sont mis à l'enquête publique sont colorés en rose.* *Pour les trois premiers documents, les numéros de référence sont prédéfinis. Tous les autres documents doivent être numérotés avec le numéro de référence 15.xx. Les numéros subordonnés xx sont à définir par le GI ou l'industrie ferroviaire.*	**Auteur (mandant)**	**Explications sur les exigences relatives au contenu**
Documents généraux		
00 Table des matières	GI	chap. 3.3.1.1
01.01 Demande d'approbation des plans	GI	chap. 1.6.1
01.02 Condensé du projet (requis pour la PAP ordinaire)	GI	chap. 1.6.2
Demande d'octroi d'une dérogation (requise pour non-conformités aux prescriptions souveraines [1] à [9])	GI industrie ferroviaire	chap. 1.10.1
Analyse d'impact (si nécessaire)	GI industrie ferroviaire	chap. 3.1.2, [14]
Documents pour RStw (s'ils ne sont pas déjà couverts par les documents du projet standard)	GI	chap. 3.1.6
Documentation permettant de retracer les compétences professionnelles de l'expert phases 1 à 4 du cycle de vie	expert (GI)	chap. 1.4.3, pt. (1)
Documentation permettant de retracer les compétences professionnelles de l'expert pour la première utilisation (non requise pour BI)	expert (GI)	chap. 1.4.3, pt. (1)
Mandat d'examen de l'expert pour la première utilisation (non requis pour BI)	GI	chap. 3.3.1.3, let. C
Plan d'examen de l'expert pour la première utilisation (non requis pour BI)	expert (GI)	chap. 3.1.4, pt. 14)
Démarche pour le déploiement (requise lors du déploiement, rollout)	GI	
Documents de la phase 1 du cycle de vie		
Concept	GI	[14]
Plan de vérification	VER (GI, industrie ferroviaire)	chap. 3.1.4, pt. 12), [14]
Mandat d'examen de l'expert phases 1 à 4 du cycle de vie	GI	chap. 3.3.1.3, let. A
Documents de la phase 2 du cycle de vie		
Définition du système	GI	[14]
Plan de sécurité	GI	chap. 3.1.4, pt. 4), [14]
Plan de FDM	GI	chap. 3.1.4, pt. 5), [14]
Documents de la phase 3 du cycle de vie		
Analyse et évaluation du risque	GI	chap. 3.1.4, pt. 6)

[34] La table des matières doit être complétée par les informations selon le chap. 3.3.1.1.

Titre du document *Les documents qui sont mis à l'enquête publique sont colorés en rose.* *Pour les trois premiers documents, les numéros de référence sont prédéfinis. Tous les autres documents doivent être numérotés avec le numéro de référence 15.xx. Les numéros subordonnés xx sont à définir par le GI ou l'industrie ferroviaire.*	**Auteur (mandant)**	**Explications sur les exigences relatives au contenu**
Registre des situations dangereuses	GI	chap. 1.8, [14]
Plan d'examen de l'expert phases 1 à 4 du cycle de vie	expert (GI)	chap. 3.1.4, pt. 14)
Documents de la phase 4 du cycle de vie		
Spécification des exigences	GI	[14]
Conditions d'utilisation relatives à la sécurité	GI	[14], [16]
Plan de validation	VAL (GI)	chap. 3.1.4, pt. 13), [14]
Rapport de vérification phases 1 à 4 du cycle de vie	VER (GI)	chap. 3.1.4, pt. 12), [14]
Rapport de validation phases 1 à 4 du cycle de vie	VAL (GI)	chap. 3.1.4, pt. 13), [14]
Points clés cybersécurité	GI	chap. 1.14
Preuve de la mise en œuvre des prescriptions souveraines	GI industrie ferroviaire	chap. 3.3.1.2
Rapport d'examen de l'expert phases 1 à 4 du cycle de vie y compris confirmation BI de l'expert en cas de BI)	expert (GI)	chap. 3.1.4, pt. 14), [14]
Prise de position du GI sur la manière avec laquelle il mettra en œuvre des résultats de l'examen de l'expert phases 1 à 4 du cycle de vie	GI	chap. 1.6.4
Documents de la phase 5 du cycle de vie		
Plan de sécurité mis à jour	industrie ferroviaire	chap. 3.1.4, pt. 8), [14]
Plan de FDM mis à jour	industrie ferroviaire	chap. 3.1.4, pt. 8), [14]
Concept de tests de qualification de sécurité et de tests d'exploitation (si nécessaire)	GI	chap. 3.4.3
Documentation sur la planification du logiciel	industrie ferroviaire	tableau A.1 [39]
Mandat d'examen de l'expert phases 5 à 10 du cycle de vie (non requis pour BI)	industrie ferroviaire	chap. 3.3.1.3, let. B
Documentation permettant de retracer la compétence professionnelle de l'expert phases 5 à 10 du cycle de vie (non requise pour BI)	expert (industrie ferroviaire)	chap. 1.4.3, pt. (1)
Plan d'examen de l'expert phases 5 à 10 du cycle de vie (non requis pour BI)	expert (industrie ferroviaire)	chap. 3.1.4, pt. 14)

Tableau 12 : Documents de la phase de planification

3.3.1.1 Table des matières

La table des matières contient la liste des documents et les informations sur : le numéro de référence, le titre du document, l'index ou la version, la date de rédaction et l'attribution aux phases du cycle de vie selon les tableaux 12, 14 et la SN EN 50716 [39]. Elle doit être soumise à l'OFT sous forme de document Word modifiable.

3.3.1.2 Preuve de la mise en œuvre des prescriptions souveraines

Les articles ou chapitres pertinents issus des prescriptions souveraines [1] à [9] doivent être énumérés et leur mise en œuvre doit être prouvée, comme cela est illustré dans le tableau 13 pour les DE-OCF [8].

DE-OCF ad l'art.	Preuve de la mise en œuvre
39, DE 39.2, ch. 3 à 3.1	Couvert par l'analyse et l'évaluation du risque [réf.].
39, DE 39.3.a, ch. 7.1	Formulée comme exigence AF-007 dans la spécification des exigences [réf.]. La mise en œuvre de la AF-007 sera confirmée dans le rapport de validation de la phase 9 du cycle de vie [réf.].

Tableau 13 : Exemple de preuve de la mise en œuvre des prescriptions souveraines

3.3.1.3 Mandats d'examen de l'expert

A. Phase de planification (phases 1 à 4 du cycle de vie) : en règle générale, l'expert doit accomplir les tâches suivantes :

1) Établir le plan d'examen[31] conformément à la SN EN 50126-1 [14] pour la mise en œuvre du mandat d'examen, le mettre à disposition du mandant et de l'OFT.
2) Effectuer l'examen selon le plan d'examen et justifier les éventuelles non-conformités au plan d'examen.
3) Examiner l'analyse et l'évaluation du risque.
4) S'il n'existe que des fonctions BI, confirmer l'affectation BI conformément à la SN EN 50126-2 [15] (chap. 3.1.4, pt. 14).
5) Prendre en compte les concrétisations et les compléments selon le chap. 3.1.4.
6) Examiner la preuve de la mise en œuvre des prescriptions souveraines [1] à [9] (chap. 3.3.1.2).
7) Examiner si les non-conformités aux spécifications et la demande d'octroi d'une dérogation sont entièrement documentées (chap. 1.10). Examen et documentation de l'acceptabilité des non-conformités.
8) Examiner l'analyse et l'évaluation du risque d'éventuelles non-conformités aux prescriptions souveraines [1] à [9].
9) Évaluer l'adéquation et l'exhaustivité du plan de validation FDMS en termes de sécurité.
10) Évaluer les compétences professionnelles au sein de l'organisation de développement.
11) Évaluer le système de gestion de la qualité.
12) Évaluer le système de gestion de la configuration et des modifications.
13) Si nécessaire, effectuer un audit pour les phases 1 à 4 du cycle de vie.
14) Examiner la plausibilité des points clés concernant la cybersécurité du GI (chap. 1.14 et 1.4.3 compétence professionnelle en cybersécurité).
15) Examiner si les constats issus du rapport de validation des phases 1 à 4 du cycle de vie sont traités.
16) Consigner les non-conformités à la SN EN 50126-1 [14] constatées lors de l'examen de l'expert, les classer en fonction du risque et les transmettre aux responsables de gestion des modifications et de prise de décision.
17) Documenter l'examen effectué (chap. 1.6.3).

B. Phase de réalisation (phases 5 à 10 du cycle de vie) : en règle générale, l'expert doit accomplir les tâches suivantes :

1) Examiner la preuve de la mise en œuvre des prescriptions souveraines [1] à [9] (chap. 3.3.1.2).

2) Examiner si les exigences des phases 5 à 10 du cycle de vie sont respectées conformément à la SN EN 50126-1 [14], en tenant compte des vérifications et de la validation effectuées. Il convient d'examiner si les activités de sécurité requises ont été réalisées, si les livrables nécessaires sont disponibles et si les objectifs des phases du cycle de vie correspondantes ont été atteints.
3) Prendre en compte les concrétisations et les compléments selon le chap. 3.1.4.
4) Examiner le respect des exigences de la SN EN 50129 [16].
5) Examiner le respect des exigences de la SN EN 50716 [39].
6) Évaluer la mise en œuvre des techniques/mesures conformément aux SN EN 50129 [16] et SN EN 50716 [39].
7) Évaluer si des audits de sécurité ont été effectués et documentés de manière appropriée.
8) Examiner si les constats issus du rapport de validation de la phase 9 du cycle de vie sont traités.
9) Indiquer les éventuelles non-conformités aux exigences des SN EN 50126-1 [14], SN EN 50129 [16] et SN EN 50716 [39] constatées lors de l'examen et justifier leur acceptabilité.
10) Examiner si les constats pertinents pour les phases 5 à 10 du cycle de vie issus du rapport d'examen de l'expert des phases 1 à 4 du cycle de vie sont traités.
11) Examiner la plausibilité des points clés, la non-intrusion concernant la FDMS et de la mise en œuvre des mesures de protection pour la cybersécurité de l'industrie ferroviaire (chap. 1.14 et 1.4.3 compétence professionnelle en cybersécurité).
12) Examiner si la release note contient les informations requises (chap. 3.4.2.3).
13) Documenter l'examen effectué (chap. 1.6.3).

C. Phase de réalisation (première utilisation) : en règle générale, l'expert doit accomplir les tâches suivantes :
   1) Examiner si :
      a) les activités de sécurité ont été effectuées conformément au plan de sécurité ;
      b) les tâches d'intégration au niveau de la technique et de l'exploitation sont accomplies (chap. 1.12) ;
      c) les constats du rapport d'examen de l'expert des phases 1 à 4 du cycle de vie sont traités ;
      d) les constats pertinents pour la première utilisation issus du rapport d'examen de l'expert des phases 5 à 10 de cycle de vie sont traités ;
      e) les charges issues de la DAP sont remplies, pour autant qu'elles concernent la sécurité ;
      f) les points pertinents pour la première utilisation issus du DoSe pour l'application spécifique et, le cas échéant, du DoSe pour le produit et/ou l'application générique (chap. 3.1.4, pt. 9) sont traités ;
      g) les modifications du projet sont documentées et conformes aux spécifications (chap. 3.4.1) ;
      h) la release note est disponible.
   2) Examiner les fonctions des IS, y compris la réaction en cas de dérangement, ainsi que l'interaction des différents produits entre eux et avec les IS voisines sur la ligne.
   3) Prendre en compte les concrétisations et les compléments selon le chap. 3.1.4.
   4) Examiner les critères d'acceptation ainsi que les processus de preuve et d'acceptation.
   5) Examiner les tests de qualification de sécurité et les tests en exploitation (chap. 3.4.3).
   6) Examiner la non-intrusion concernant la FDMS et la mise en œuvre des mesures de protection pour la cybersécurité du GI (chap. 1.14 et 1.4.3 compétence professionnelle en cybersécurité).
   7) Examiner le respect des conditions pour l'acceptation de l'objet du développement conformément à la SN EN 50126-2 [15].

8) Examiner l'aptitude de la première utilisation à être MES (chap. 1.17).

9) Documenter l'examen effectué (chap. 1.6.3).

3.4 Phase de réalisation du projet de développement

3.4.1 Modifications du projet de développement

Dès lors que des modifications sont apportées aux documents approuvés dans la PAP après l'octroi de la DAP, il convient de procéder comme suit :

- Les modifications du projet répondant aux critères du chap. 3.1.3 doivent être documentées dans le DoSe pour la première utilisation et examinées par l'expert pour la première utilisation ou, pour les fonctions BI, par le chargé de validation de la phase 9 du cycle de vie.
- Les modifications du projet pour les RStw ou les produits utilisant la technologie des relais ne requérant pas de PAP selon le tableau 10 doivent être documentées dans le DoSe et examinées par l'expert (chap. 3.1.6).
- Dans le cas contraire, une procédure est requise pour les modifications du projet (art. 5, al. 2, OPAPIF [5]). Les exigences du chap. 3 doivent être mises en œuvre pour les documents concernés par les modifications du projet. Les exigences du chap. 3.1.6 doivent être mises en œuvre pour les RStw ou les produits utilisant la technologie des relais.

Sauf ordre contraire de l'OFT, les travaux non concernés par les modifications du projet peuvent se poursuivre si les IS sont déjà en construction (art. 5, al. 3, OPAPIF [5]).

3.4.2 Documents et exigences relatives au contenu du projet de développement

Dans le tableau 14, les documents nécessaires pour la phase de réalisation sont énumérés et attribués aux phases du cycle de vie. En complément, il contient des références dans lesquelles on trouve des explications sur les exigences relatives au contenu des documents. Lors de la rédaction de ces documents, il faut prendre en compte les exigences formelles selon le chap. 1.1.3 et les exigences relatives à la documentation de FDMS de la SN EN 50126-1 [14].

Titre du document	Auteur (mandant)	Explications sur les exigences relatives au contenu
Documents généraux		
Table des matières	GI industrie ferroviaire	chap. 3.3.1.1
Demande d'AE (requise pour la PAE)	GI	
Échéancier PAE (requis pour la PAE)	GI	chap. 3.4.2.1
Documents pour RStw (s'ils ne sont pas déjà couverts par les documents du projet standard)	GI industrie ferroviaire	chap. 3.1.6
Concept de mise à la terre (si modifié ou nouvellement établi)	GI industrie ferroviaire	[35]
Documentation des informations sur BI (si elle ne figure pas déjà dans d'autres documents de ce tableau	GI industrie ferroviaire	chap. 3.1.4, pt. 15)
Points clés cybersécurité	industrie ferroviaire	chap. 1.14
Preuves d'interopérabilité (si nécessaire)	GI	chap. 1.15, 1.16

Titre du document	Auteur (mandant)	Explications sur les exigences relatives au contenu
Déclarations de conformité des constituants d'interopérabilité (s'ils ont été co-développés)	industrie ferroviaire	art. 15*l*[ter] OCF [4]
Preuve de la mise en œuvre des prescriptions souveraines (si elle n'a pas été entièrement fournie dans les phases 1 à 4 du cycle de vie)	GI industrie ferroviaire	chap. 3.3.1.2
Documents de la phase 5 du cycle de vie		
Architecture du système	industrie ferroviaire	[14]
Analyse des situations dangereuses, y compris le registre des situations dangereuses	industrie ferroviaire	[14]
Attribution des exigences de sécurité	industrie ferroviaire	[14]
Critères d'acceptation, ainsi que les processus de preuve et d'acceptation	GI	[14]
Documents de la phase 6 du cycle de vie		
Analyse de la FDM	industrie ferroviaire	[14]
Analyse des situations dangereuses	industrie ferroviaire	[14]
Processus d'installation et de mise en service	industrie ferroviaire	[14]
Processus d'exploitation et de maintenance	industrie ferroviaire	[14]
Processus de fabrication	industrie ferroviaire	[14]
Mesures de formation	industrie ferroviaire	[14]
Dossier de sécurité pour l'application spécifique (pas nécessaire pour BI)	industrie ferroviaire	chap. 3.1.4, pt. 9), [16]
Dossier de sécurité pour la première utilisation (pas exigé pour BI, mais judicieux)	GI	chap. 3.4.2.2
Documents de la phase 7 du cycle de vie		
Rapports d'assurance qualité (concernant le processus de fabrication et les mesures relatives à la FDMS)	industrie ferroviaire	[14]
Rapports d'inspection et d'examen	industrie ferroviaire	[14]
Dispositions pour la manipulation du matériel et la logistique	industrie ferroviaire	[14]
Documents de la phase 8 du cycle de vie		
Documentation d'installation	industrie ferroviaire	[14]
Rapport d'intégration (si nécessaire)	industrie ferroviaire	[14]
Mesures prises pour résoudre les problèmes de défaillances et d'incompatibilités	industrie ferroviaire	[14]
Analyse d'impact (si nécessaire)	industrie ferroviaire	[14]
Dispositions logistiques du système	industrie ferroviaire	[14]
Documents de la phase 9 du cycle de vie		
Rapport de validation	VAL (industrie	chap. 3.1.4, pt. 13), [14]

Titre du document	Auteur (mandant)	Explications sur les exigences relatives au contenu
	ferroviaire)	
Documents de la phase 10 du cycle de vie		
Rapport d'examen de l'expert phases 5 à 10 du cycle de vie (non requis pour BI)	expert (industrie ferroviaire)	chap. 3.1.4, pt. 14), [14]
Acceptation des SRAC (si nécessaire)	GI	[14]
Rapport d'acceptation	GI	[14]
Rapport de vérification des phases 5 à 10 du cycle de vie	VER (industrie ferroviaire)	chap. 3.1.4, pt. 12), [14]
Rapport d'examen de l'expert pour la première utilisation (non requis pour BI)	expert (GI)	chap. 3.1.4, pt. 14), [14]
Documentation du logiciel	industrie ferroviaire	chap. 3.1.4, pt. 9), [39]
Release note	industrie ferroviaire	chap. 3.4.2.3
Preuve de la mise en œuvre des techniques/mesures selon les SN EN 50129 [17] et SN EN 50716 [39]	industrie ferroviaire	chap. 3.4.2.4
Programme de mise en service[35]	GI	chap. 1.17
Libération de mise en service[35]	GI, expert	chap. 1.17
Prise de position du GI sur la manière avec laquelle il mettra en œuvre des résultats de l'examen de l'expert pour la première utilisation (non requise pour BI)	GI	chap. 1.6.4
Prise de position de l'industrie ferroviaire sur la manière avec laquelle elle mettra en œuvre des résultats de l'examen de l'expert phases 5 à 10 du cycle de vie (non requise pour BI)	industrie ferroviaire	chap. 1.6.4

Tableau 14 : Documents de la phase de réalisation

3.4.2.1 Échéancier PAE

Dans l'échéancier pour l'obtention de l'AE, il faut présenter la planification des activités de sécurité. Il convient de prendre en compte les interdépendances avec la planification des activités de sécurité des phases 5 à 10 du cycle de vie, ainsi que les délais selon le chap. 3.1.7, pt. ④.

3.4.2.2 Dossier de sécurité pour la première utilisation

Le DoSe pour la première utilisation correspond au DoSe selon l'art. 5*l*, al. 1, OCF [4]. Il est requis pour la première utilisation de l'objet du développement (chap. 3.1.2) en Suisse chez un GI.

Aucun DoSe n'est exigé pour les fonctions exclusivement BI. Toutefois, il est judicieux de démontrer la mise en œuvre des exigences applicables au GI selon le chap. 3.1.4, pt. 15) dans le DoSe pour la première utilisation.

Le DoSe pour la première utilisation doit être établi et signé par des spécialistes parallèlement aux travaux du projet de développement (art. 5*l*, al. 2, OCF [4]). Lors de sa rédaction, il faut prendre en compte les exigences selon le chap. 1.1.3 et la SN EN 50126-1 [14]. La figure 15 présente le contenu du DoSe pour la première utilisation. La structure peut être adaptée aux conditions du GI et aux exigences de l'objet du développement.

[35] Dans le cas d'une combinaison d'un projet standard et d'un projet de développement, les informations du projet standard doivent être complétées par les informations de la part de développement.

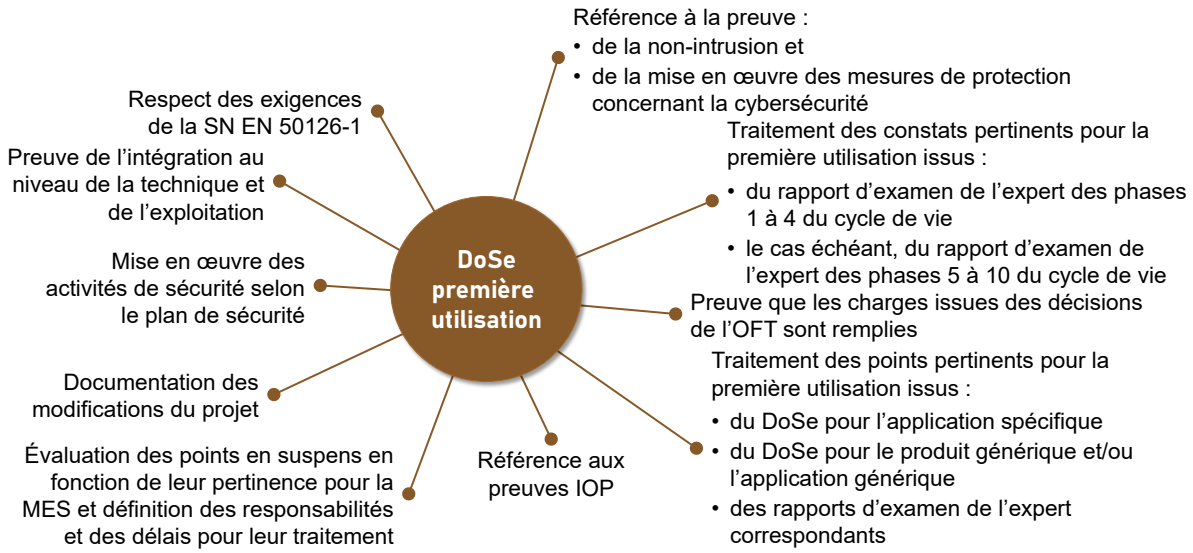

Figure 15 : Contenu du DoSe pour la première utilisation

3.4.2.3 Release note

L'objet du développement doit être identifiable au moyen d'une release note. À cet effet, les informations suivantes sont requises :

- l'identification univoque du matériel : désignation, numéro de référence, version ;
- l'identification univoque du logiciel, y compris de ses fonctions : version du logiciel, release, par exemple CRC ;
- l'identification univoque des interfaces ;
- les documents pour l'utilisateur : ils comprennent essentiellement les SRAC et les documents pour la conception de projet, le montage, la MES, l'exploitation et la maintenance ;
- les erreurs et limitations connues ;
- les modifications par rapport aux versions/releases précédentes ;
- la compatibilité avec les versions/releases précédentes.

3.4.2.4 Preuve de la mise en œuvre des techniques/mesures

Les techniques/mesures choisies pour le développement du produit, conformément aux SN EN 50129 [16] et SN EN 50716 [39], doivent être énumérées et leur mise en œuvre doit être décrite et prouvée. L'énumération et la description de la mise en œuvre sont présentées à titre d'exemple dans le tableau 15. La preuve de la mise en œuvre des techniques/mesures est généralement apportée dans le rapport de vérification ou de validation. Tout cela fait partie du DoSe pour l'application spécifique ou pour les produits génériques et/ou les applications génériques.

Tableau SN EN 50129	Techniques/Mesures	SIL 3	Description de la mise en œuvre
E.3	Indépendance des rôles	HR	Les détails sont donnés dans le plan de sécurité [réf.] et le plan d'assurance qualité du logiciel [réf.].
E.4	Séparation des fonctions relatives à la sécurité et des fonctions non relatives à la sécurité pour empêcher les influences imprévues	HR	La séparation requise est définie dans le document [réf.].

Tableau 15 : Exemple d'énumération et de description des techniques/mesures

3.4.3 Tests de qualification de sécurité et tests en exploitation

3.4.3.1 Tests de qualification de sécurité

La nécessité d'effectuer des tests de qualification de sécurité doit être déterminée et justifiée entre les parties concernées (GI, industrie ferroviaire), par exemple en fonction de la nouveauté et de la complexité de l'objet du développement (SN EN 50129 [16]). Les tests de qualification de sécurité doivent être effectués chez le GI.

Lorsque les tests de qualification de sécurité sont effectués lors de l'exploitation opérationnelle et que l'objet du développement « exécute des fonctions relatives à la sécurité »[36], une autorisation de l'OFT est requise. Le GI doit définir des mesures appropriées pour garantir la sécurité de l'exploitation pendant ces tests.

Pour obtenir l'autorisation d'effectuer des tests de qualification de sécurité, le GI doit soumettre à l'OFT un concept de tests de qualification de sécurité au plus tard deux mois avant le début des tests de qualification de sécurité. Les contenus typiques de ce concept sont les suivants :

1) l'objet du développement, y compris la release note ;
2) le lieu, l'étendue et la durée ;
3) les responsabilités ;
4) les dépendances ;
5) les tests à effectuer, les résultats attendus et les critères d'évaluation de l'achèvement des tests ;
6) le traitement des défaillances, des dérangements et des dysfonctionnements ;
7) les mesures permettant de garantir une sécurité suffisante pendant les tests de qualification de sécurité. À cet effet, il convient d'identifier les situations dangereuses et d'analyser et d'évaluer les risques associés. Lors de l'identification des situations dangereuses, il convient de prendre en compte à la fois l'environnement de test et les interfaces avec l'exploitation opérationnelle. Ensuite, il convient de définir les mesures permettant d'éliminer les risques ou du moins de les réduire à un niveau acceptable. Il peut s'agir de mesures techniques, d'exploitation ou organisationnelles.
8) les prescriptions d'exploitation pour le personnel roulant, d'exploitation et éventuellement de maintenance ;
9) le traitement des modifications de l'objet du développement : si des modifications s'avèrent nécessaires pendant les tests de qualification de sécurité, il convient d'examiner dans quelle mesure ces tests doivent être entièrement ou partiellement répétés ;
10) le traitement des résultats (notamment en cas d'échec des tests) ;
11) la preuve que les charges de la DAP sont remplies.

Lorsque les tests de qualification de sécurité sont effectués dans des zones sécurisées (PTC [9]), aucune autorisation de l'OFT n'est requise, indépendamment du fait que l'objet du développement exécute ou non des fonctions relatives à la sécurité. Il en va de même si les tests de qualification de sécurité sont effectués lors de l'exploitation opérationnelle et que l'objet du développement n'exécute aucune fonction relative à la sécurité. Le GI est responsable de l'établissement du concept de tests de qualification de sécurité selon les pts. 1) à 10) et de sa mise en œuvre.

Si les contenus susmentionnés figurent déjà dans le DoSe du produit générique et/ou de l'application générique, il est possible d'y faire référence.

Après les tests de qualification de sécurité, les tests effectués et leurs résultats doivent être documentés dans le rapport technique de sécurité du DoSe de l'application spécifique ou du produit générique et/ou de l'application générique (SN EN 50129 [16]).

[36] assure la responsabilité en matière de sécurité au sens de la SN EN 50129 [16]

3.4.3.2 Tests en exploitation

Si les tests de qualification de sécurité de l'objet du développement (chap. 3.4.3.1) ont été effectués, ils couvrent en général les tests en exploitation.

Néanmoins, l'OFT peut, au cas par cas, exiger des tests en exploitation dans la PAP ou la PAE. Il s'agit de renforcer la confiance que l'objet du développement, par exemple :

- satisfait aux exigences d'exploitation définies et/ou
- atteint les objectifs de fiabilité requis.

Pour l'autorisation des tests en exploitation, le GI doit soumettre à l'OFT un concept de tests en exploitation. Ce concept comprend typiquement le contenu selon le chap. 3.4.3.1, pts. 1) - 6), 9) et 10).

L'OFT peut autoriser les tests en exploitation dans le cadre des procédures suivantes :

- PAP, si l'objet du développement comporte exclusivement des fonctions BI ;
- PAE, si le développement de l'objet du développement n'est pas encore achevé au moment de la planification ;
- procédure d'HdS, si le développement de l'objet du développement est achevé au moment de la planification et si l'exigence selon l'art. 7, al. 1, OCF [4] est respectée. Le déroulement de cette procédure est décrit dans la Dir. HdS [13].

Après l'achèvement des tests en exploitation, le GI doit soumettre à l'OFT le rapport de tests en exploitation avec les contenus suivants :

- la description des tests effectués et de leurs résultats ;
- l'évaluation des constats, y compris les mesures à prendre ;
- les documents de preuve et les documents pour l'utilisateur mis à jour, y compris le rapport d'examen de l'expert.

Termes et abréviations

Terme	Abréviation	Explication	Source
Absence d'effets rétroactifs y compris analyse d'impact des modifications		selon le chap. 1.12, pt. 5)	
Acceptation		selon la source	[14]
Analyse et évaluation du risque		selon la source L'appréciation du risque inclut l'analyse et l'évaluation du risque.	[14]
Analyse d'impact		selon la source	[14]
Audit		selon la source	[14]
Autorisation		Terme généralement utilisé pour désigner le processus de contrôle ou la décision qui en résulte.	
Autorisation d'exploiter	AE		
Autorisé d'une autre manière		C.-à-d. déjà utilisé spécifiquement pour l'installation par le GI ou par un autre GI disposant d'infrastructure et des conditions d'exploitation comparables (DE-OCF ad art. 39, DE 39.2, ch. 1 à 2 [8]).	
Besoin de protection		selon la source	[12]
Catégories de réseaux : - Réseau non IOP - Réseau principal IOP et - Réseau complémentaire IOP		selon le chap. 1.15.1	
Chargé de validation	VAL	selon la source	[14]
Chargé de vérification	VER	selon la source	[14]
Circulation sans signaux avec assentiment		selon la source	[9]
Compétence professionnelle		selon le chap. 1.4.3, pt. (1)	
Conditions d'application relatives à la sécurité (de l'anglais Safety-related Application Conditions)	SRAC	selon la source	[14]
Contrôle de la marche des trains voie métrique et voie spéciale	ZBMS	selon la source	[41]
Cyclic Redundancy Check (anglais)	CRC		
Défaillance/Panne		selon la source	[14]
Décision d'approbation des plans	DAP		
Démonstration de la sécurité		Ensemble des activités ayant pour but de confirmer la sécurité, y compris la documentation. Elle comprend par exemple les tests, la validation, l'établissement des preuves et les éventuels examens de l'expert.	

Terme	Abréviation	Explication	Source
Démonstration de la sécurité éprouvée en pratique		Sont également considérées comme des bases suffisantes les preuves de sécurité et les rapports d'examen de l'expert selon des méthodes antérieures ou l'épreuve de la pratique, pour autant que la traçabilité soit garantie.	
Documents pour l'utilisateur		selon le chap. 3.4.2.3	
Dossier de sécurité	DoSe	selon le chap. 3.4.2.2 et sources	[14] [16]
Enclenchement à relais (de l'allemand Relaisstellwerk)	RStw		
Enquête publique		Il s'agit notamment des documents qui peuvent entraîner des répercussions sur des tiers (particuliers, organisations, autorités).	
Expert		Personne qui effectue des examens indépendants et qui remplit les exigences du chap. 1.4.3.	
(de l'anglais Independent Safety Assessor, ISA)		selon la source	[16]
Expropriation		selon la note de bas de page[18]	
Examen de l'expert		Le terme « Examen de l'expert » est synonyme du terme « évaluation indépendante de la sécurité » utilisé dans les sources.	[14] [16]
État de la technique		Décrit les possibilités techniques existantes qui ont fait leurs preuves dans la pratique, mais qui ne se sont pas encore imposées.	
Faible importance pour la sécurité		selon le chap. 2.2.1	
Fonction relative à la sécurité		selon la source	[14]
Gestionnaire d'infrastructure	GI	Entreprise ferroviaire qui construit et exploite l'infrastructure.	[1]
Gestion du risque		selon le chap. 1.8 et la source	[14]
Haute importance pour sécurité		selon le chap. 2.2.1	
Hautement recommandée	HR	selon la source	[16]
Homologation de série	HdS	selon la source	[13]
Installation de passage à niveau		selon la source	[9]
Installations de sécurité	IS	selon le chap. 1.1.2	
Intégration au niveau de la technique et de l'exploitation		Intégration des produits utilisés dans les IS dans leur ensemble, en tenant compte de toutes les spécifications techniques et d'exploitation pertinentes.	
IS dans leur ensemble		Les IS supérieures d'un point de vue de la technique et d'exploitation, lorsque le projet traité ne concerne qu'une partie des IS.	
Intégrité basique (de l'allemand Basisintegrität)	BI	selon les sources	[14] [16]
Interopérabilité	IOP		
Level 1 Limited Supervision (en anglais)	L1 LS		[42]

Terme	Abréviation	Explication	Source
Level 2 (en anglais)	L2		[42]
Logiciel		selon la source	[14]
Mise en service	MES		
Modifications du projet		Les modifications apportées pendant la PAP ainsi qu'après l'octroi de la DAP.	[13]
Modification strictement technique		Modifications répondant à tous les critères de l'annexe A4.3.1.2 de la Dir. HdS [13]. Le terme « modification strictement technique » est utilisé comme synonyme de « modification de l'état technique de l'appareil » selon la Dir. HdS [13].	[13]
Non-conformités et exceptions aux spécifications		selon le chap. 1.10	
Norme européenne	EU		
Norme Suisse	SN		
Organisme d'évaluation des risques		selon la source (également connu sous le nom de RBS, en allemand)	[4]
Part de développement		Il s'agit par exemple de nouvelles fonctions, d'un nouveau type d'enclenchement, de nouvelles interfaces, d'une modification de l'utilisation prévue de fonctions existantes, de schémas non-conforme aux schémas de principe ou des principes de construction.	
Prescriptions		selon le tableau 2	
Prescriptions d'exploitation		Elles sont définies dans les DE-OCF ad art. 12, DE 12.1, ch. 1 [8]. Il s'agit par exemple du tableau des parcours, des instructions de service, des check-lists, de la gestion des interventions et des pannes, des manuels de maintenance.	[8]
Prescriptions souveraines		Les prescriptions souveraines sont les prescriptions [1] à [9].	
Procédure d'approbation des plans	PAP		
Procédure d'autorisation d'exploiter	PAE		
Processus de gestion du risque		selon l'art. 5*m*, al. 4, OCF [4]	[4]
Projet		Le terme « projet » est utilisé comme synonyme du terme « projet » (Vorhaben en allemand) dans l'OCF [4].	
Projet global		Il s'agit d'un projet supérieur comprenant divers domaines spécialisés comme les installations techniques de construction et électriques.	

Terme	Abréviation	Explication	Source
Proportionné (rapport coût/bénéfice)		Les principes suivants s'appliquent : - Les mesures sont proportionnées lorsque leur utilité est supérieure à leur coût. La zone de dispersion doit être considérée et prise en compte dans la pesée des intérêts. - Un montant uniforme de 6,5 millions de francs est utilisé comme coût marginal pour éviter un mort pour les groupes de personnes que sont les riverains, les voyageurs dans le train et les collaborateurs (DE-OCF [8]). Les coûts d'une mesure sont les coûts totaux du cycle de vie pendant la durée d'utilisation prévue.	Gestion de la sécurité[37]
Rapport de sécurité	RaSe		
Ouvrage de référence en matière de technique ferroviaire (de l'allemand Regelwerk Technik Eisenbahn)	RTE		
Règles reconnues de la technique		Elles ont fait leurs preuves et se sont imposés dans la pratique. Les DE-OCF ad art. 2, DE 2.3 [8] contiennent des informations sur la manière dont elles sont identifiées.	[8]
Registre des situations dangereuses		selon la source	[14]
Relatif à la sécurité		selon la source	[14]
Release note (anglais)		selon le chap. 3.4.2.3	
Risque		selon la source	[14]
Niveau d'intégrité de sécurité (de l'allemand Sicherheits-Integritätslevel)	SIL	selon la source	[14]
Situation dangereuse		selon la source	[14]
Sous-traitant		selon la source	[40]
Spécification technique d'interopérabilité concernant le sous-système « contrôle-commande et signalisation »	STI CCS		[8]
Système européen de contrôle de la marche des trains (de l'anglais European Train Control System)	ETCS		[42]
Taux de défaillance fonctionnel tolérable		selon la source	[14]
Taux d'occurrence maximal acceptable de danger		selon la source	[14]
Tests de qualification de sécurité		selon le chap. 3.4.3.1	
Tests en exploitation		selon le chap. 3.4.3.2	
Technologies de l'information et de la communication	TIC	selon la source	[12]
Zone pour les chemins de fer routiers		selon la source	[9]

[37] www.bav.admin.ch → Thèmes généraux → Sécurité → Aperçu → Plus d'informations → Documentation → Concepts