



xx.xx.2025

Directive

Démonstration de la sécurité Installations de sécurité ¹

Installations de sécurité, applications téléma-
tiques et systèmes d'avertissement selon art.
37 - 41 OCF dans les procédures d'approba-
tion des plans et d'autorisation d'exploiter

(Dir. IS)

numéro de dossier : OFT -412.00-00075/00006

| Conventions | Signification |
|-------------------|----------------|
| marqué en couleur | points ouverts |

¹ La notion "installations de sécurité (IS)" est utilisée dans la Dir. IS au sens large, comme concrétisé dans la deuxième partie du titre et au chap. 1.2.1.

Éditeur

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

Distributeur

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

Langues disponibles

Allemand (original)
Le français sera publié dès que la traduction sera disponible

Entrée en vigueur

xx.xx.2025

Office fédéral des transports

Anna Barbara Remund, sous-directrice
Divisions Infrastructure

xx, sous-directeur
Divisions Sécurité

Editions / Historique des changements

| Version | Date | Auteur | Remarques sur les modifications | Statut |
|---------|------------------|--------|---|----------|
| V 1.0 | 1er mai 2007 | moc | Première édition (comme guide IS) | remplacé |
| V 2.0 | 1er juillet 2010 | moc | Révision et complément après 3 ans l'expérience en matière d'applications et adaptation à l'état de la LCdF, de l'OCF et des DE-OCF | remplacé |
| V 2.1_d | 1er juillet 2011 | moc | Améliorations aux chap. 4.3.4 / fig. 2 et chap. 6.3.2, 7.1.1, 7.1.3 | remplacé |
| V 3.0_d | 23 oct. 2015 | moc | Révision et complément réforme des chemins de fer 2.2 : nouvellement publiée en tant que directive IS | remplacé |
| V4.0 | | | - | |

Remarque : le tableau suivant sera supprimé après la révision de la Dir.

| Version | Date | Créateur | Remarques sur les modifications | Statut |
|---------|------------|----------|--|----------|
| x1.0_d | 18.10.2023 | guv | - Partie du document faitier corrigée - Partie du projet standard mentionnée et partiellement corrigée après la révision du GPr | remplacé |
| x1.1_f | 20.12.2023 | guv | Partie du projet standard ajustée après la révision du GPr | remplacé |
| x2.0_d | 12.02.2024 | guv | Partie Document faitier partiellement corrigé après la révision du GPr. <i>Cette version peut être utilisée comme base pour la création d'outils pour les projets standard.</i> | remplacé |

| | | | | |
|---------|--------------------------|-----|--|----------|
| x3.0_d | 28.03.2024 | guv | <ul style="list-style-type: none"> - Partie du document faitier mise au point après la révision du GPr - Partie Projet standard adaptée si nécessaire <i>Les modifications par rapport à la version x1.0_f sont visibles dans le document Delta x1.0_f__ x3.0_f du 28.03.2024.</i> | remplacé |
| x3.1_f | 05.04.2024 | guv | Ajustements formels ; st Review | remplacé |
| x3.2_d | 19.09.2024 | guv | <ul style="list-style-type: none"> - st Commentaires de révision partiellement corrigés - Clarifications selon la "Dir. IS Réouverture de la discussion Projet standard" prises en compte à l'exception des modifications du projet - projet de développement (x1.4_d) et a pris en compte les retours des réunions sur le projet de développement. - Divers compléments/adaptations apportés au projet de développement | remplacé |
| x3.3_d | 31.10.2024 | guv | <ul style="list-style-type: none"> - st Commentaires d'examen corrigés - Clarifications et réactions prises en compte selon les discussions avec les CFF "Dir. IS Réouverture de la discussion sur le projet standard". - Le chapitre RStw a été intégré ; diverses adaptations et compléments ont été apportés. - Ch. cybersécurité adapté <i>Cette version a été utilisée comme base pour la création des outils du projet standard.</i> | remplacé |
| x3.4_d | 30.11.2024 | guv | <ul style="list-style-type: none"> - PGr Commentaires de révision corrigés - Diverses adaptations | remplacé |
| x3.5_d | 03.02.2025 | guv | <ul style="list-style-type: none"> - PGr Commentaires de révision corrigés - st Commentaires d'examen corrigés - Diverses adaptations | remplacé |
| x3.6a_d | 11.04.2025 | guv | <ul style="list-style-type: none"> - PGr Commentaires de révision partiellement corrigés - st Commentaires de révision partiellement corrigés - Diverses adaptations | remplacé |
| x3.6_d | 15.05.2025 | guv | <ul style="list-style-type: none"> - PGr Commentaires de révision corrigés - OFT Commentaires de révision corrigés - Diverses adaptations | remplacé |
| x3.7_d | 30.05.2025 12.06.2025 | guv | Diverses adaptations (par ex. IOP) <i>Branchenreview</i> | en cours |

Table de matières

| | |
|---|-----------|
| Introduction | 7 |
| 1 Cadre global..... | 8 |
| 1.1 Généralités | 8 |
| 1.1.1 Objectif de la Dir. IS | 8 |
| 1.1.2 Champ d'application de la Dir. IS | 8 |
| 1.1.3 Exigences formelles pour les documents | 9 |
| 1.2 Classification du projet | 10 |
| 1.3 Spécifications déterminantes | 11 |
| 1.3.1 Prescriptions | 12 |
| 1.3.2 Normes techniques | 13 |
| 1.3.3 Règles reconnues de la technique | 14 |
| 1.3.4 État de la technique | 15 |
| 1.4 Parties prenantes et leurs responsabilités | 15 |
| 1.4.1 Gestionnaire d'infrastructure | 15 |
| 1.4.2 Industrie ferroviaire et bureaux d'ingénieurs | 15 |
| 1.4.3 Organisme de contrôle indépendant | 15 |
| 1.4.4 Office fédéral des transports | 16 |
| 1.5 Procédure d'approbation des plans | 16 |
| 1.6 Documents PAP et exigences relatives au contenu | 17 |
| 1.6.1 Demande d'approbation des plans | 18 |
| 1.6.2 Condensé du projet | 18 |
| 1.6.3 Rapport d'examen de l'expert | 18 |
| 1.6.4 Prise de position sur la mise en œuvre des résultats de l'examen l'expert | 19 |
| 1.7 Procédure d'homologation de série | 19 |
| 1.8 Analyse et évaluation du risque | 19 |
| 1.9 Examen de l'expert | 21 |
| 1.10 Dérogations et exceptions aux spécifications | 21 |
| 1.10.1 Dérogations et exceptions aux prescriptions souveraines | 21 |
| 1.10.2 Dérogations et exceptions aux règles techniques reconnues | 22 |
| 1.11 Phases de construction et installations provisoires | 23 |
| 1.12 Intégration technique et d'exploitation | 23 |
| 1.13 Changements significatifs | 24 |
| 1.14 Cybersécurité | 24 |
| 1.15 Interopérabilité | 26 |
| 1.15.1 Généralités | 26 |
| 1.15.2 Déclaration de conformité | 26 |
| 1.16 Procédure d'autorisation d'exploiter | 26 |

| | | |
|------------|---|-----------|
| 2 | Projet standard | 28 |
| 2.1 | Phases et déroulement du projet standard | 28 |
| 2.2 | Phase planification du projet standard | 29 |
| 2.2.1 | Attribution de la catégorie d'application du projet standard | 29 |
| 2.2.2 | Projets standard sans PAP | 30 |
| 2.2.3 | Exigences relatives à la démonstration de la sécurité du projet standard | 30 |
| 2.2.4 | Documents PAP et exigences relatives au contenu du projet standard | 32 |
| 2.2.4.1 | Table des matières | 33 |
| 2.2.4.2 | Rapport de sécurité | 33 |
| 2.2.4.3 | Mandat d'examen d'expert | 34 |
| 2.2.4.4 | Plans | 36 |
| 2.2.5 | Décision d'approbation des plans de l'OFT pour le projet standard | 37 |
| 2.3 | Phase de réalisation du projet standard | 37 |
| 2.3.1 | Modifications d'un projet standard | 38 |
| 2.3.2 | Documents et exigences relatives du contenu du projet standard | 38 |
| 2.3.2.1 | Dossiers de construction et documents de contrôle | 39 |
| 2.3.2.2 | Dossier de sécurité | 39 |
| 2.3.2.3 | Programme et autorisation de mise en service | 41 |
| 2.3.3 | Étude de projet | 41 |
| 2.3.4 | Contrôle d'usine | 42 |
| 2.3.5 | Examen d'expert phase de réalisation | 42 |
| 2.3.6 | Travaux finaux | 43 |
| 2.3.7 | Documents à fournir et délais | 43 |
| 3 | Projet de développement | 44 |
| 3.1 | Principes du projet de développement | 44 |
| 3.1.1 | Phases et déroulement du projet de développement | 44 |
| 3.1.2 | Catégories d'objets de développement et exigences relatives à la démonstration de la sécurité | 46 |
| 3.1.3 | Projets de développement sans PAP | 46 |
| 3.1.4 | Processus de développement : cycle de vie et activités de sécurité | 47 |
| 3.1.5 | Types de procédures | 53 |
| 3.1.6 | Développements sur RStw et exigences pour la démonstration de la sécurité | 54 |
| 3.1.6.1 | Démonstration complète de la sécurité | 56 |
| 3.1.6.2 | Etendue réduite de la démonstration de la sécurité | 58 |
| 3.1.7 | Aperçu des phases du cycle de vie, des types de procédures, de la documentation et des délais | 59 |
| 3.2 | Phase de préparation du projet de développement | 60 |
| 3.3 | Phase de planification du projet de développement | 60 |
| 3.3.1 | Documents et exigences relatives au contenu | 60 |
| 3.3.1.1 | Table des matières | 62 |

| | | |
|-------------------------------------|--|-----------|
| 3.3.1.2 | Preuve de la mise en œuvre des prescriptions souveraines | 63 |
| 3.3.1.3 | Mandats d'examen d'expert aux experts | 63 |
| 3.4 | Phase de réalisation du projet de développement | 64 |
| 3.4.1 | Modifications du projet de développement | 64 |
| 3.4.2 | Documents et exigences relatives au contenu du projet de développement | 65 |
| 3.4.2.1 | Échéancier PAE | 67 |
| 3.4.2.2 | Dossier de sécurité première application..... | 67 |
| 3.4.2.3 | Release note | 67 |
| 3.4.2.4 | Preuve de la mise en œuvre des techniques/mesures | 67 |
| 3.4.3 | Essais de qualification de sécurité et tests en exploitation..... | 68 |
| 3.4.3.1 | Essais de qualification de sécurité..... | 68 |
| 3.4.3.2 | Tests en exploitation | 69 |
| Termes et abréviations | | 70 |

Introduction

La directive Démonstration de la sécurité des installations de sécurité (Dir. IS) V4.0 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 procédure à suivre pour que la PAP et la PAE des IS se déroulent sans accroc.

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, ces directives ne doivent pas être consultées. La révision de ces directives permet d'éliminer les redondances concernant les exigences relatives aux IS.

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

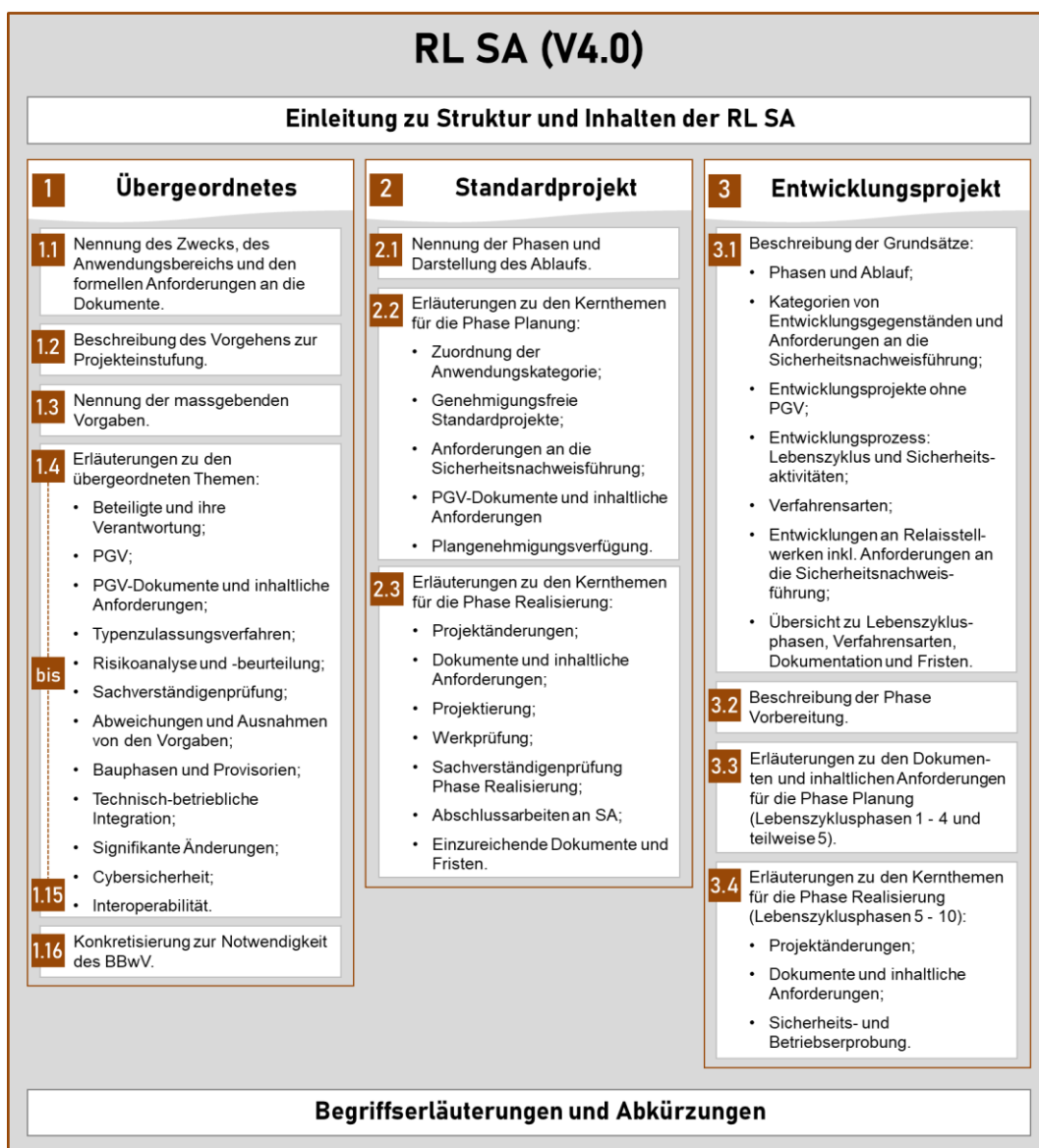


Figure 1: Structure et contenus de la Dir. IS

1 Cadre global

1.1 Généralités

1.1.1 Objectif de la Dir. IS

Les contenus de la Dir. IS servent à satisfaire aux exigences de l'OCF [4] pour la planification et la construction des IS et aux DE-OCF ad art. 38, DE 38.1, ch. 1.5 [8], qui sont approuvées dans la PAP et la PAE. La Dir. IS décrit un procédé uniforme pour la "démonstration de la sécurité des IS"² qui définit les :

- spécifications déterminantes ;
- "documents de preuve pour l'IS"³ à établir ;
- exigences relatives au contenu auxquelles les documents de preuve doivent répondre ;
- documents de preuve à remettre à l'Office fédéral des transports (OFT) et à quel moment.

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 - 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 :

- IS pour la circulation sur les voies ferrées pour la :
 - commande et la protection de parcours (par ex. poste d'enclenchement) ;
 - signalisation côté infrastructure et contrôle de la marche des trains ;
 - manoeuvre et la protection des aiguilles ;
 - le contrôle de l'état libre de la voie et la localisation des convois ;
 - la commande et la protection des passages à niveau (installations de passages à niveau).
- Applications télématiques qui, lors de la saisie, de la transmission, du traitement et de l'émission d'informations, ont un rapport direct avec la sécurité et la fiabilité de l'exploitation ferroviaire (art. 38 al. 2 OCF [4]), comme :
 - système de contrôle-commande ferroviaire (dispositifs de commande, d'affichage) ;
 - système de gestion du trafic ;
 - système de transmission à distance (par exemple, transmission d'ordres du système de contrôle-commande ferroviaire au poste d'enclenchement; transmission de messages d'état du poste d'enclenchement, de l'installation de passage à niveau, des compteurs d'essieux au système de contrôle ferroviaire) ;
 - systèmes de conduite automatique des trains (relation avec l'IS en fonction du degré d'automatisation) ;
 - réseaux de données⁴ (p. ex. dans l'environnement des postes d'enclenchement, des systèmes de contrôle-commande ferroviaire, du contrôle de la marche des trains) ;
 - applications mobiles (par ex. pour soutenir les processus d'exploitation ou de maintenance) ;
 - les dispositifs de contrôle des trains pour contrôler si les véhicules satisfont aux exigences d'une exploitation sûre, dans la mesure où ils agissent automatiquement sur les processus d'exploitation.

² le terme "gestion des preuves de sécurité" est utilisé dans la suite du texte

³ le terme "documents justificatifs" est utilisé dans la suite du texte

⁴ La preuve est apportée conformément à la norme D RTE 28100 [36].

Les applications telles que l'information à la clientèle, l'administration (p. ex. facturation de services), la planification (p. ex. planification du trafic) ne sont pas directement liées à la sécurité et à la fiabilité de l'exploitation ferroviaire et ne sont donc pas soumises à la Dir. IS. Il peut être nécessaire d'effectuer une analyse et une évaluation du risque pour eux aussi. En cas de doute, il est possible de clarifier avec l'OFT⁵ si une telle application entre dans le champ d'application de la Dir IS.

- Systèmes d'avertissement ;
- Passages à niveau sans installations de passage à niveau.

Terme de "produit" : les IS peuvent être constituées de différents éléments (y compris les logiciels) tels que des systèmes, des sous-systèmes, des composants et des interfaces ⁶, qui contiennent à leur tour des fonctions. De tels éléments (y compris les fonctions) sont regroupés dans la Dir. IS sous le terme de "produit".

La Dir IS est applicable lorsqu'une IS est construite ou modifiée, indépendamment de la 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 chef de système ETCS CH"⁷. Une telle démonstration de la sécurité doit être convenue suffisamment tôt avec l'OFT en cas de construction ou de modification d'une IS sur ETCS L2.

La Dir. IS s'adresse au requérant (en règle générale le gestionnaire d'infrastructure (GI) selon l'art. 2 let. a LCdF [1]), à l'industrie ferroviaire, aux bureaux d'ingénieurs et aux experts⁸.

La Dir. IS n'a pas le rang d'une loi ou d'une ordonnance. L'application de la Dir. IS doit conduire à des documents de preuve pouvant être approuvés. D'autres procédures sont également autorisées, pour autant qu'elles soient conformes aux prescriptions souveraines [1] - [10]. Dans certaines circonstances, elles peuvent entraîner un surcroît de travail et une augmentation des coûts pour tous les participants à la PAP et à la PAE.

Il existe des outils d'aide à la Dir. IS (p. ex. modèles, recommandations et exemples) qui sont mis à disposition par l'Union des transports publics (UTP) auprès du D RTE 25100 [33] dans la boutique en ligne de RTE.

1.1.3 Exigences formelles pour les documents

Les documents :

- doivent être rédigés dans la langue officielle de mise à disposition du public en vigueur sur le lieu de l'IS prévue (à l'exception du romanche) ; les documents mis à disposition du public sont colorés en rose dans les tableaux 6 et 12. Les rapports d'examen de l'expert ou les rapports de test, de vérification et de validation peuvent également être rédigés dans une autre langue officielle ou en anglais.
- qui sont nécessaires pour les PAP doivent être numérotés avec le chiffre de référence 15.xx; Les chiffres subordonnés xx doivent être définis par le GI ou l'industrie ferroviaire.
- doivent être désignés de la même manière que dans la table des matières et doivent contenir les informations suivantes : Titre du document, index ou version, échelle, numéro du plan, date d'élaboration, auteur et vérificateur. En cas de modification du projet, ces informations doivent être mises à jour. Les contenus modifiés dans les documents doivent être identifiés de manière compréhensible (p. ex. par des couleurs) ;

⁵ Les demandes de clarification avec l'OFT mentionnées dans la Dir. IS doivent être adressées par e-mail à BAV-Sicherheitstechnik@bav.admin.ch.

⁶ c'est-à-dire les systèmes/sous-systèmes/éléments/composants/personnes combinés entre eux

⁷ www.bav.admin.ch (Moyens de transport → Chemins de fer → Informations spécialisées → Contrôle de la marche des trains → European Train Control System)

⁸ dans les normes techniques, par exemple, évaluateur de sécurité indépendant [15] - [16] ou expert en sécurité indépendant [17]

- doivent être rédigés de manière aussi peu redondante que possible. Il n'est pas nécessaire de répéter les contenus qui figurent déjà dans d'autres documents. Il suffit de faire référence à ces documents, à condition de s'assurer qu'ils contiennent les informations demandées.
- doivent contenir des décisions et des justifications compréhensibles ;
- doivent être disponibles en version validée ;
- classés comme critiques pour la sécurité par le GI ou l'industrie ferroviaire⁹ doivent être protégés en fonction de leur besoin de protection, par ex. en étant cryptés. La classification de ces documents comme critiques pour la sécurité doit être claire (p. ex. mention de classification sur la page de titre et dans l'en-tête). De tels documents ne doivent être remis à l'OFT que s'ils sont nécessaires à l'évaluation de la demande. La remise de ces documents doit se faire sous forme codée. L'OFT doit être informé de la raison du cryptage (par ex. critique pour la sécurité).
- doivent être signés au moyen d'une signature électronique qualifiée conformément à la SCSE¹⁰ ;
- doivent être soumises sous forme électronique via le site Internet 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.

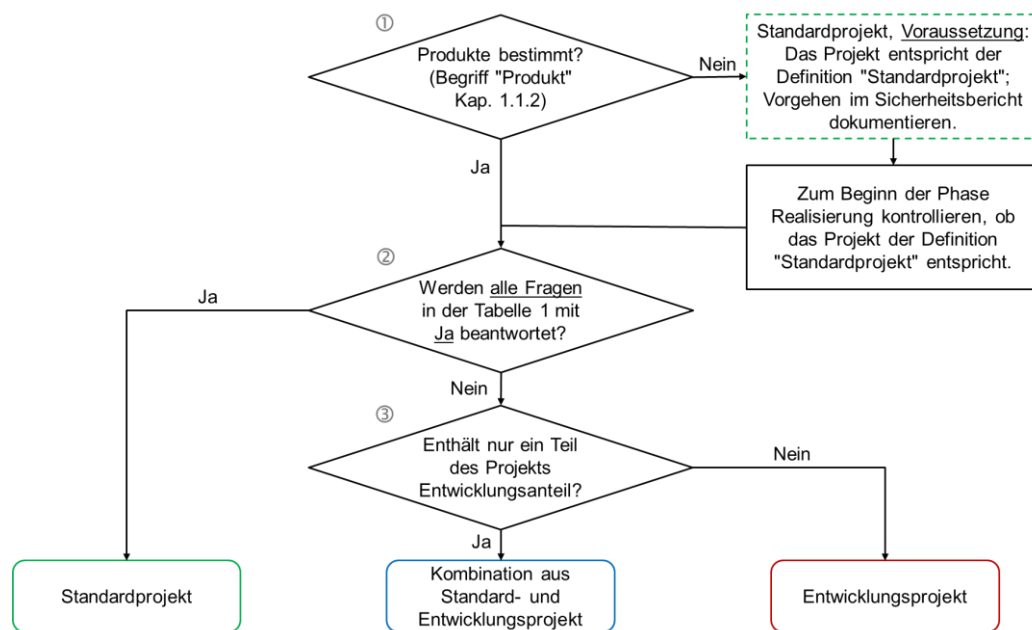


Figure 2 : Arbre de décision pour la classification du projet

- ① Si les produits ne sont pas encore définis dans la phase de planification, il est permis de classer provisoirement le projet comme projet standard. Cette classification reste valable à condition que seuls des produits correspondant à la définition de "projet standard" selon ② soient utilisés dans la phase de réalisation. Pour la phase de planification, cette procédure doit être documentée dans le rapport de sécurité. Pour la phase de réalisation, selon ②, il faut prouver dans le dossier de sécurité (DoSe) que le projet correspond à la définition de "projet standard".
- ② Clarifier si le projet correspond à la définition de "projet standard".

⁹ Il s'agit par ex. de documents qui pourraient être utilisés par des personnes non autorisées pour provoquer des événements entraînant de nombreuses victimes.

¹⁰ RS 943.03 Loi fédérale sur les services de certification dans le domaine de la signature électronique et autres applications de certificats numériques (Loi sur la signature électronique, SCSE)

Définition de "projet standard" : un projet d'un GI est un projet standard lorsque seuls sont utilisés des produits conformes aux versions actuelles des prescriptions souveraines [1] - [10] et disposant d'une homologation de série de l'OFT ou autorisés d'une autre manière en Suisse, c.-à-d. déjà utilisés spécifiquement pour l'installation par le GI ou par d'autres GI comparables.

Pour que le GI ait la garantie que son projet est un projet standard selon la définition ci-dessus, il doit répondre aux questions contenues dans le tableau 1. Si les réponses à toutes les questions sont oui, le projet est considéré comme un projet standard et les exigences du chap. 2 doivent être mises en œuvre.

| No. | Questions sur le projet |
|-----|--|
| 1 | N'utilise-t-on que des produits qui : a) sont homologués par l'OFT, ou b) "sont déjà en service chez le GI" ¹¹ , ou c) sont déjà en service, de manière spécifique à l'installation, auprès d'un autre GI disposant d'infrastructures et de conditions d'exploitation comparables (DE-OCF ad art. 39, DE 39.2, ch. 1 – 2 [8])? |
| 2 | Est-ce que seules les fonctions de produits dont l'application dispose d'une HdS de l'OFT ou d'une autre autorisation en Suisse sont utilisées? <i>La première utilisation d'éléments logiques librement programmables (chap. 3.1.3) ou de schémas qui s'écartent des circuits de principe ou des principes de construction (chap. 3.1.6) est considérée comme un projet de développement.</i> |
| 3 | Les produits prévus pour être utilisés, sont-ils conformes aux versions actuelles des prescriptions souveraines [1] - [10]? En cas de doute, il est recommandé de se mettre d'accord suffisamment tôt avec l'OFT sur la procédure à suivre. <i>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 pour un objet de l'HdS changent [1] - [10] avant l'expiration de la durée de validité (en règle générale 10 ans) de l'HdS alors:</i> a) <i>l'industrie ferroviaire doit prouver, conformément au 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</i> b) <i>l'industrie ferroviaire et le GI doivent traiter les dérogations par rapport aux prescriptions souveraines selon le chap. 1.10.1.</i> |

Tableau 1 : Questions sur le projet

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

Les parties de développement peuvent prendre différentes formes (par ex. d'une nouvelle fonction à un nouveau poste d'enclenchement). La part de développement doit être clairement régularisée et traitée conformément au chap. 3. Toutes les autres parties relèvent du projet standard et doivent être traitées conformément au chap. 2.

Si le projet ne comporte pas de parties relevant du projet standard, le projet est considéré comme un projet de développement et doit être traité conformément au 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 susceptibles de concrétiser les prescriptions (chap. 1.3.2) ;
- règles reconnues de la technique (chap. 1.3.3) ;

¹¹ Il s'agit de produits avec des "droits acquis" qui possèdent une démonstration de la sécurité par la pratique.

- 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 prescriptions en vigueur au moment de l'ouverture de la PAP sont déterminantes. Pour les projets de longue durée au cours desquels les prescriptions changent, la procédure doit être coordonnée avec l'OFT.

1.3.1 Prescriptions

Les prescriptions actuelles selon le tableau 2 sont déterminantes pour la démonstration de la sécurité. On y fait la distinction entre :

- Les prescriptions prises en compte dans la Dir. IS : [1], [5]. La planification des IS est possible avec la Dir. IS sans la consultation de 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] - [4], [6] - [14]. Pour la planification et la réalisation des IS, ces prescriptions doivent être prises en compte, si nécessaire, en plus de la Dir. IS.

| No. | CS No. Abréviation | Titre <i>Lorsque les prescriptions font référence à d'autres documents, ceux-ci doivent être pris en compte si nécessaire. Les prescriptions souveraines sont les prescriptions [1] - [10].</i> |
|------|-----------------------|--|
| [1] | 742.101 LCdF | Loi 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 sur la circulation routière |
| [4] | 742.141.1 OCF | Ordonnance sur la construction et l'exploitation des chemins de fer (Ordonnance sur les chemins de fer) (y compris les directives de l'UE) |
| [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 | Dispositions d'exécution de l'ordonnance sur les chemins de fer (y compris annexe no 6 ch. 3 Spécification technique d'interopérabilité (STI) des sous-systèmes de contrôle-commande et de signalisation (CCS)) |
| [9] | 742.173.001 PCT | Chemins de fer suisses Prescriptions de circulation des trains suisses (R 300.1-15) |
| [10] | Standard ZBMS | Standard national Contrôle de la marche des trains pour les chemins de fer qui ne migrent pas vers l'ETCS |
| [11] | | Prescriptions d'exploitation (entre autres, dispositions d'exécution des Prescriptions de circulation des trains de l'GI concernée) <i>La conformité avec les prescriptions souveraines [1] - [10] doit être assurée (DE-OCF ad art. 2, DE 2.3, ch. 2 [8].</i> |
| [12] | Dir. PE-PCT | Directive Promulgation de Prescriptions d'exploitation et circulation des trains |
| [13] | Dir. Rail CySec | Directive sur la cybersécurité ferroviaire ¹² |

¹² Toutes les prescriptions pertinentes (par ex. normes techniques, règles de l'art reconnues) en matière de cybersécurité sont énumérées dans la présente directive.

| No. | CS No. Abréviation | Titre <i>Lorsque les prescriptions font référence à d'autres documents, ceux-ci doivent être pris en compte si nécessaire. Les prescriptions souveraines sont les prescriptions [1] - [10].</i> |
|------|-----------------------|--|
| [14] | 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. En outre, les DE-OCF [8] prescrivent quand ces normes techniques doivent être obligatoirement appliquées. A l'exception de la norme VSS 71 253 [24], elles ne doivent être appliquées que pour les projets de développement.

Si des postes d'enclenchement à relais (RStw) sont développés ultérieurement ou modifiés alors qu'ils ont été conçus à l'origine sans l'application des normes techniques susmentionnées, il convient de procéder conformément au chapitre 3.1.6 .

En principe, l'état actuel des normes (base DE-OCF) doit servir de base à tout développement nouveau, développement ultérieur ou modification d'un produit. Si aucune norme technique n'a été désignée ou si elles manquent, les règles reconnues de la technique doivent être appliquées (art. 2 al. 3 OCF [4]). Si les règles d'art font également défaut ou sont inadaptées, il convient de consulter l'état de la technique (DE-OCF ad art. 2, DE 2.4, ch. 1 [8]).

Si les états des normes changent, il faut procéder comme suit :

- Si, au début d'un projet de développement, de développement ou de modification d'un produit, on sait déjà qu'il existe de nouvelles versions de normes techniques, que les DE-OCF [8] sont donc en cours de révision et qu'elles entreront en vigueur dans un avenir proche, les nouvelles versions de normes techniques doivent être appliquées pour le développement.
- En cas de développement ou de modification d'un produit, il convient de vérifier si les états des normes techniques utilisés dans la gestion initiale du justificatif de sécurité sont toujours valables. Si des états de normes plus récents sont valables entre-temps, ils doivent être appliqués pour le développement ou la modification conformément aux DE-OCF actuelles [8].

En accord avec l'OFT, il est possible de s'écarter de cette procédure dans les cas suivants :

- Lorsque la prise en compte de l'état actuel des normes lors d'un développement ou d'une modification d'un produit est liée à des dépenses disproportionnées.
- Si une modification strictement technique (par ex. élimination de défauts, obsolescence de composants) est effectuée, les normes techniques sur lesquelles se base la démonstration de sécurité initiale peuvent continuer à être appliquées. Le fait qu'il s'agisse d'une modification strictement technique doit être prouvé par le respect des critères de l'annexe A4.3.1.2 de la directive HdS [14].

| No. | Abréviation | Titre <i>Lorsque les normes techniques font référence à d'autres documents, ceux-ci doivent être pris en compte si nécessaire.</i> | DE-OCF Ad art. |
|------|---------------|--|--------------------------|
| [15] | 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 générique FDMS | 38, DE 38.1, ch. 1 |
| [16] | 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 : Méthodologie de sécurité relative au système <i>En cas d'application de la SN EN 50129 [17] 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 [16], sauf en cas de renvois explicites dans la SN EN 50129 [17] (DE-OCF ad art. 38, DE 38.1, ch. 1.3.1 [8].</i> | 38, DE 38.1, ch. 1 |

| No. | Abréviation | Titre <i>Lorsque les normes techniques font référence à d'autres documents, ceux-ci doivent être pris en compte si nécessaire.</i> | DE-OCF Ad art. |
|------|-------------------------------------|---|-----------------------------------|
| [17] | 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 |
| [18] | SN EN 50159 | Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité dans les systèmes de transmission | 38, DE 38.1, ch. 1.2 |
| [19] | SN EN 12352 | Installations de contrôle du trafic - Feux d'avertissement et de sécurité | 37c, DE 37c, ch. 1.2.3 |
| [20] | SN EN 12368 | Installations de contrôle du trafic Lampes de signalisation | |
| [21] | SN EN 50121-1 50121-2 50121-4 | Applications ferroviaires - Compatibilité électromagnétique Partie 1 : Généralités Partie 2 : émissions parasites de l'ensemble du système ferroviaire vers le monde extérieur Partie 4 : Émissions et immunité des appareils de signalisation et de télécommunication | 39, DE 39.2, ch. 4.2.2.4 |
| [22] | SN EN 50125-3 | Applications ferroviaires - Conditions d'environnement pour le matériel - Partie 3 : Conditions d'environnement pour les équipements de signalisation et de télécommunication | 39, DE 39.2, ch. 4.2.2.4 |
| [23] | 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 |
| [24] | VSS 71 253 | Rail - Route - Tracé parallèle et rapprochement - Distance et mesures de protection | 23.1, DE 23.1, ch. 1.3, 2.2 |
| [25] | CIE S 004 /E-2001 | Couleurs des feux de signalisation | 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 <i>Si les règles reconnues de la technique font référence à d'autres documents, il convient de les prendre en compte si nécessaire.</i> |
|------|-------------|--|
| [26] | R RTE 20012 | Profil d'espace libre Voie normale |
| [27] | R RTE 20100 | Sécurité lors de travaux sur les voies |
| [28] | R RTE 20410 | Postes à vitesse réduite voie métrique |
| [29] | R RTE 20512 | Profil d'espace libre de la voie métrique |
| [30] | R RTE 24900 | Accès au quai par la voie ferrée |
| [31] | R RTE 25000 | Compendium des installations de sécurité |
| [32] | D RTE 25096 | Processus de planification des installations de sécurité |
| [33] | D RTE 25100 | Preuve des installations de sécurité |
| [34] | R RTE 25931 | Passage à niveau documentation de base |
| [35] | R RTE 27900 | Manuel de retour et de mise à la terre |
| [36] | D RTE 28100 | Preuve des réseaux de données - Safety et Security |
| [37] | R RTE 29100 | Distances de pré-signalisation voie normale |

| No. | Abréviation | Titre |
|------|---------------------|---|
| | | <i>Si les règles reconnues de la technique font référence à d'autres documents, il convient de les prendre en compte si nécessaire.</i> |
| [38] | R RTE 30250 | Elektronisches Stellwerk Simis IS |
| [39] | SN EN 50716 | Applications ferroviaires - Exigences pour le développement de logiciels |
| [40] | SN EN ISO/IEC 17020 | Évaluation de la conformité - Exigences relatives au fonctionnement de différents types d'organismes procédant à des inspections |
| [41] | | Bases d'étude du contrôle de la marche des trains pour les entreprises ferroviaires qui utilisent un contrôle de la marche des trains selon le ZBMS ¹³ |
| [42] | | Exigences du chef de système ETCS CH (KGB, EGB et Level 1 LS) ⁷ |
| [43] | | Circuits de principe ou principes de construction |
| [44] | | Principes d'étude HTA 4006 pour les postes d'enclenchement à relais |

Tableau 4 : Règles reconnues de la technique

1.3.4 État de la technique

L'état de la technique doit être pris en compte s'il permet de réduire encore un risque avec un effort proportionné (art. 2 OCF [4]).

1.4 Parties prenantes et leurs responsabilités

1.4.1 Gestionnaire d'infrastructure

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

Le GI doit identifier tous les participants 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 requis et permettent aux experts d'effectuer les examens nécessaires.

1.4.3 Organisme de contrôle indépendant

Pour pouvoir effectuer des examens en tant qu'expert sur mandat du GI ou de l'industrie ferroviaire, il est nécessaire, selon l'OCF [4] et en référence à la SN EN ISO/IEC 17020 [40], de disposer d'informations sur les points suivants :

- (1) Compétence spécialisée (art. 15t al. 1 - 2 OCF [4], SN EN ISO/IEC 17020 [40]) : L'expert doit confirmer qu'il ;
 - a) a reçu une formation appropriée (formation au sens de la norme SN EN ISO/IEC 17020 [40]) pour effectuer les essais. Elle comprend une période d'initiation, une période de travail sous la

¹³ www.bav.admin.ch (Moyens de transport→ Chemins de fer→ Informations spécialisées→ Contrôle de la marche des trains→ ZBMS

supervision d'examineurs expérimentés et une formation continue (en fonction de l'évolution progressive des techniques et des méthodes d'essai).

- b) possède des connaissances spécialisées et de l'expérience dans le domaine concerné par l'objet d'examen.
- c) a connaissance des spécifications déterminantes (chap.1.3) et comprend en particulier les exigences de la norme SN EN 50126-1 [15] ;
- d) a des connaissances et de l'expérience dans le domaine de la gestion du risque
- e) a des connaissances et de l'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.

Si un expert est déjà connu de l'OFT sur la base de ses expertises issues de projets similaires, aucune documentation liée au projet n'est nécessaire pour vérifier la confirmation de la compétence technique. Dans tous les autres cas, l'expert doit remettre cette documentation à l'OFT au plus tard avec les documents PAP.

- (2) Indépendance¹⁴ (art. 15u al. 1 - 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 l'entretien de l'objet d'essai (SN EN ISO/IEC 17020 [40]) ;
- (3) Existence d'une assurance responsabilité civile (art. 15y OCF [4]);
- (4) Confidentialité (SN EN ISO/IEC 17020 [40]) : L'expert doit confirmer que les documents reçus ou créés pendant l'audit ont été traités de manière confidentielle, sauf disposition contractuelle contraire.
- (5) une sous-traitance correcte (SN EN ISO/IEC 17020 [40]) : Si l'expert sous-traite une partie de l'essai, il doit s'assurer que les sous-traitants remplissent les exigences mentionnées dans ce chapitre.

1.4.4 Office fédéral des transports

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

L'OFT délivre la décision d'approbation des plans (DAP), éventuellement assortie de charges (le cas échéant, de conditions et de délais), après avoir examiné les documents présentés en fonction des risques et par échantillonnage (art. 2a OCF [4]). La DAP équivaut à une autorisation de construire (art. 6 al. 6 OCF [4]).

L'OFT délivre éventuellement la décision de l'AE avec des conditions (éventuellement des conditions et des limitations de durée), pour autant qu'il n'y ait pas renoncé dans la DAP (art. 8 OCF [4]). Pendant l'HdS, il examine les documents remis en fonction des risques et par échantillonnage . La mise en service (MES) est autorisée avec l'AE.

L'OFT octroie l'HdS selon l'art. 18x LCdF [1] éventuellement avec des conditions pour les produits 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]). Des exceptions sont néanmoins admises pour les projets standard et de développement (chap. 2.2.1, 2.2.2 et 3.1.3).

Une PAP a lieu dans le cas: :

¹⁴ L'indépendance et l'impartialité au sens de la norme SN EN ISO/IEC 17020 [43] sont considérées comme équivalentes.

- D'une procédure ordinaire (art. 18a - h LCdF [1]), lorsque des intérêts de tiers dignes de protection sont touchés et qu'il y a des répercussions 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.
- D'une procédure simplifiée (art. 18i al. 1 LCdF [1]) :
 - des projets localisés avec peu de personnes concernées clairement identifiables ou
 - les modifications de l'IS qui ne modifient pas sensiblement l'aspect extérieur, qui n'affectent pas les intérêts de tiers dignes de protection et qui n'ont qu'un impact négligeable sur le territoire et l'environnement ou
 - IS, qui seront retirées au plus tard au bout de trois ans.

De projets globaux, il peut arriver que les documents PAP ne contiennent pas encore suffisamment d'informations sur les IS. Ce cas se présente typiquement lorsque le permis de construire pour un projet global est requis plus tôt que les DAP pour les IS. Dans ce cas, les documents PAP pour les IS sont soumis sous forme de plans détaillés pour approbation¹⁵. Les plans détaillés qui se fondent sur un projet global déjà approuvé sont approuvés selon une procédure simplifiée (art. 18i al. 2 LCdF [1]). Si des intérêts de tiers dignes de protection sont touchés par les plans de détail et qu'il y a des répercussions sur le territoire et l'environnement, une procédure ordinaire est nécessaire pour leur approbation.

En cas de doute, il est recommandé de se mettre d'accord avec l'OFT sur le type de PAP et son déroulement au début du projet.

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

- 18 mois si des expropriations¹⁶ sont nécessaires ;
- 12 mois pour la procédure ordinaire (sans expropriations) ;
- 4 mois pour la procédure simplifiée.

Ces délais sont des délais dits d'ordre qui doivent garantir un déroulement ordonné de la PAP. Leur non-respect n'entraîne aucune conséquence juridique et ne confère à la GI aucun droit d'exécution.

Le délai de traitement commence à courir dès que l'OFT a reçu les documents PAP complets (art. 8, al. 2, OPAPIF [5]). Font exception à cette règle les plans détaillés.

Si des modifications importantes¹⁷ par rapport au projet initial interviennent pendant le 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 fait remarquer que des documents PAP lacunaires prolongent la durée de la procédure.

1.6 Documents PAP et exigences relatives au contenu

Les documents PAP sont régis par l'art. 3 al. 2 OPAPIF [5]. Les documents PAP suivants sont d'application générale et doivent satisfaire aux exigences de forme et de contenu énoncées au chap. 1.1.3 et aux chap. 1.6.1 - 1.6.4 :

- Demande d'approbation des plans ;
- Condensé du projet ;
- Rapport d'examen de l'expert ;

¹⁵ Cette procédure est connue sous le nom de procédure des plans détaillés. Les plans détaillés de l'IS contiennent les informations nécessaires à leur évaluation technique et opérationnelle, conformément aux tableaux 6 et 13.

¹⁶ c'est-à-dire qu'un droit réel (terrain ou servitude) est nécessaire à la réalisation du projet par un tiers, mais que le tiers n'est pas d'accord pour céder ce droit réel.

¹⁷ Il s'agit de modifications qui sont soumises à la PAP conformément au chap.2.2 ou0.

- Prise de position sur la mise en œuvre des résultats de l'examen l'expert

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 mentionnées :

- Objet de la demande ;
- GI avec personne de contact, y compris les coordonnées ;
- Communes et cantons concernés ;
- où se situe le projet (réseau non IOP, réseau principal IOP ou réseau complémentaire) (chap. 1.15);
- Type de PAP : procédure ordinaire ou simplifiée (chap. 1.5) ;
- État des négociations sur l'acquisition de terres et de droits et expropriations nécessaires ;
- Concertation avec des tiers (particuliers, organisations, autorités) ;
- Dérogations aux prescriptions souveraines [1] - [10] (chap.1.10.1) ;
- Plans détaillés (chap. 1.5) ;
- Délais (début des travaux et MES) ;
- Coûts.

1.6.2 Condensé du projet

Le condensé du projet contient les mêmes informations que la demande d'approbation des plans (chap.1.6.1). Contrairement à la demande d'approbation des plans, elle 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'audit et contenir les informations suivantes :

- 1) Détails du mandat, y compris la date d'attribution du mandat, la régularisation et les interfaces ;
- 2) Confirmation du respect des exigences de l'expert (1) - (5) selon le chap. 1.4.3.1 (par ex. au moyen d'une auto-déclaration) ;
- 3) Mentionner les objectifs par rapport auxquels l'examen a été réalisé (chap. 1.3) ;
- 4) Identification de l'objet du contrôle, y compris la mention de tous les documents contrôlés (avec le numéro/la version/la date du document).
- 5) Détails de l'audit (complet ou, en cas d'échantillonnage, justification incluse) ;
- 6) Mention de tous les documents de contrôle établis (p. ex. listes de contrôle, questionnaires, journal de contrôle) ;
- 7) Évaluation de l'audit réalisé ;
- 8) Consigner toutes les constatations sous forme de conditions/obligations (erreurs à corriger du point de vue de la sécurité), de recommandations (pour améliorer la réalisation des objectifs), d'autres remarques. Toutes les constatations doivent être datées. Si nécessaire, le responsable de la sécurité doit exiger des contrôles supplémentaires ;
- 9) Conclusion sur l'examen du point de vue de la sécurité.

1.6.4 Prise de position sur la mise en œuvre des résultats de l'examen l'expert

Le GI doit tenir compte des conclusions du rapport d'examen de l'expert. Elle doit rendre compte à l'OFT de la mise en œuvre de ces conclusions avec les documents des phases de planification et de réalisation. Pour ce faire, une prise de position (art. 3 al. 2 OPAPIF [5])¹⁸ de le GI est nécessaire, par ex. sous la forme d'un document indépendant. Le cas échéant, la même chose s'applique également à l'industrie ferroviaire.

1.7 Procédure d'homologation de série

Une procédure d'homologation de série selon l'art. 18x LCdF [1], cf. Directive HdS [14], peut être mise en œuvre si elle est de nature à simplifier la PAP et la PAE (art. 7 OCF [4]). En conséquence, la procédure d'homologation de série 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'homologation de série ne doit pas être examinée une nouvelle fois dans le cadre de ces procédures. Dans le cas d'une procédure d'homologation de série en cours pour un produit générique, le PAP peut s'appuyer sur l'autorisation d'essai en exploitation issue de la procédure d'homologation de série. Le déroulement temporel doit être coordonné en conséquence.

Si un GI exige des produits homologués, par ex. dans le cadre d'une procédure d'appel d'offres, cette exigence est plus stricte que les exigences du LCdF [1].

1.8 Analyse et évaluation du risque

L'OCF [4] exige la mise en œuvre de la gestion du risque présentée dans Figure 3 : la figure 3 (art. 5m al. 2, art. 5l al. 1 en tenant compte de l'art. 8a al. 1 de l'OCF [4]). Sur la base de l'analyse et de l'évaluation du risque, il est démontré, en cas de nouvelle construction ou de modification de l'IS, que les risques qui en découlent sont acceptables.

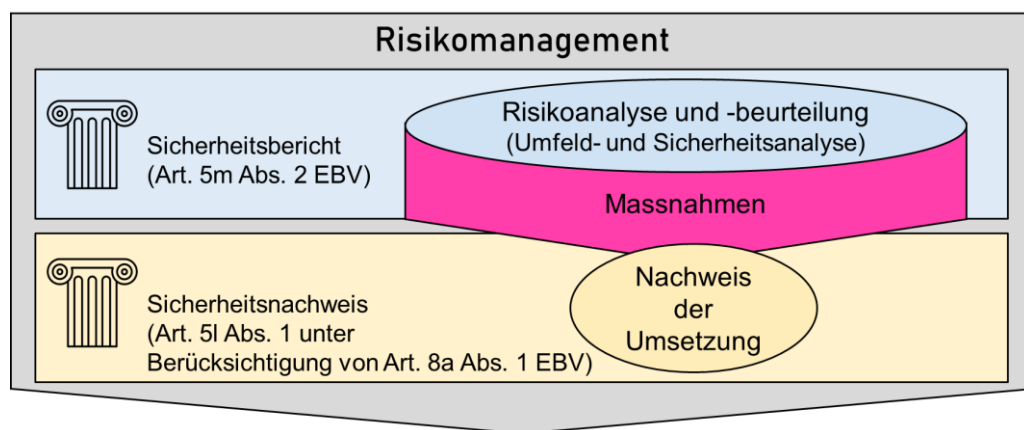


Figure 3 : Gestion du risque

La figure 4 montre le déroulement prévu par la norme SN EN 50126-1 [15] pour l'analyse et l'évaluation du risque. Les étapes correspondantes sont expliquées ci-après.

¹⁸ Selon cet article, l'avis du GI est requis pour le rapport d'audit de l'IS de la phase de planification. Il en découle qu'une prise de position du GI est également requise pour le rapport d'audit AS de la phase de réalisation.

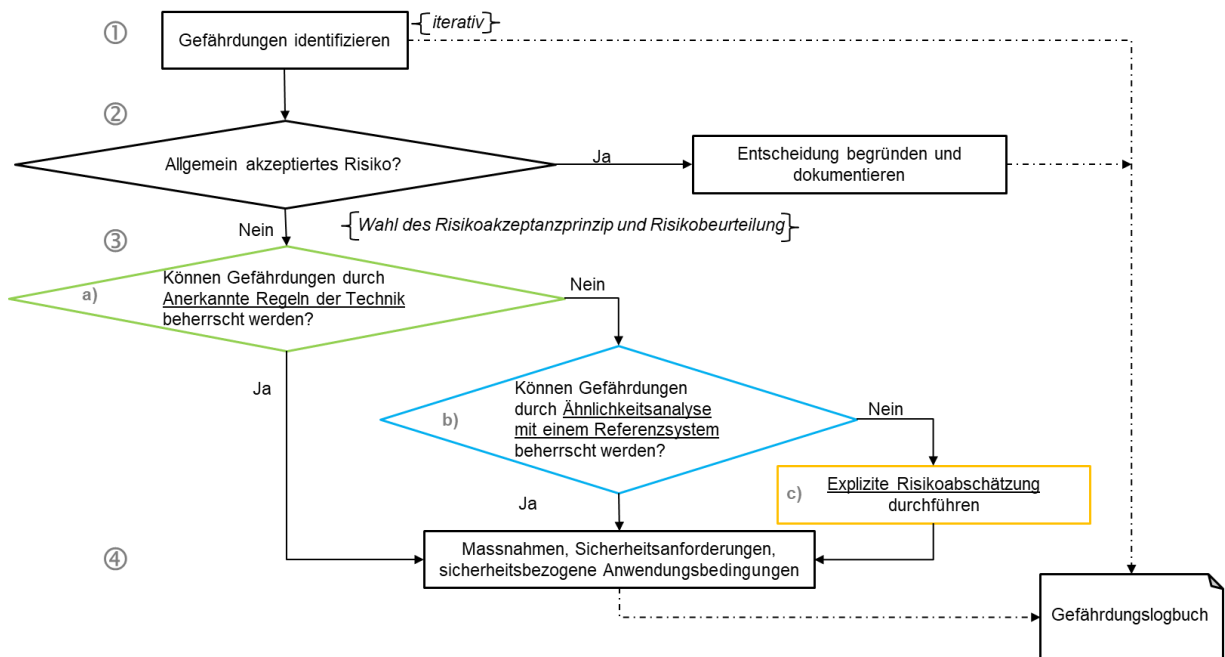


Abbildung 1: Ablauf der Risikoanalyse und -beurteilung

- ① Tous les dangers prévisibles qui peuvent conduire à un événement selon les DE-OCF ad art. 39, DE 39.2, ch. 3.1 [8] en raison de la construction, de l'exploitation, des personnes - de la technique - de l'organisation ou d'autres conditions, doivent être identifiés et enregistrés dans le registre des dangers). L'identification des dangers est une étape itérative. Toutes les fonctions, interfaces, états de fonctionnement, incidents et groupes de personnes doivent être pris en compte.
- ② Pour chaque danger identifié, il faut décider si le niveau de risque est "généralement accepté". Un tel risque est si faible que des mesures supplémentaires sont disproportionnées. Un danger associé à un risque généralement accepté n'est plus traité. La décision qui a conduit au risque généralement accepté doit être justifiée dans le registre des dangers.

Les dangers liés à un risque qui n'est pas généralement accepté doivent être analysés et évalués en termes d'acceptation par le choix et l'application d'un principe et d'un critère d'acceptation des risques. Les principes d'acceptation des risques suivants sont disponibles à cet effet :

- a) Application de l'ouvrage de référence (règles de l'art) : Ce principe s'appuie sur l'application des règles concrètes reconnues de la technique. Celles-ci permettent de déduire des mesures de maîtrise des dangers , c'est-à-dire avec lesquelles les risques liés au danger sont éliminés ou du moins réduits à un niveau acceptable. Il peut s'agir de mesures techniques, opérationnelles ou organisationnelles . Les mesures à respecter par le produit sont appelées exigences de sécurité.

Si les règles de l'art ne permettent pas de maîtriser tous les phénomènes dangereux, il convient d'appliquer une combinaison ou un autre principe d'acceptation des risques.
- b) Analyse de similarité avec un système de référence : lors de l'application de ce principe, les exigences de la norme SN EN 50126-2 [16] doivent être prises en compte.
- c) évaluation explicite du risque : lors de l'application de ce principe, l'OFT recommande de procéder selon la "méthode d'évaluation du risque individuel"¹⁹ . Cette méthode utilise d'une part la valeur limite du risque individuel comme critère d'acceptation du risque. D'autre part, elle utilise les coûts marginaux de 6,5 millions de francs harmonisés à l'échelle du DETEC pour éviter les pertes de vies humaines, afin d'effectuer les analyses coûts/bénéfices sur la base du risque collectif. L'application de cette méthode a l'avantage de permettre de trouver des solutions optimales en termes de coûts/bénéfices pour garantir la sécurité avec les moyens limités

¹⁹ www.bav.admin.ch (Thèmes généraux → Sécurité)

à disposition. Cette méthode convient également pour prouver qu'il n'y a pas de risque inacceptable en cas de dérogation par rapport aux prescriptions et que toutes les mesures proportionnées de réduction des risques ont été prises (art. 5 al. 2 let. b OCF [4]).

Pour la définition des exigences de sécurité, il convient de tenir compte des prescriptions selon la norme SN EN 50126-2 [16]. Outre les exigences de sécurité, les conditions d'application relatives à la sécurité (SBAWB²⁰) peuvent également être des mesures de maîtrise des dangers. Les hypothèses formulées dans le cadre de l'analyse et de l'évaluation des risques sont également définies en tant que conditions d'applications relatives à la sécurité. Lors de la définition des conditions d'applications relatives à la sécurité, il convient de tenir compte des prescriptions selon la norme SN EN 50129 [17].

Le lien entre les différents dangers et les principes d'acceptation des risques, les critères d'acceptation des risques, les exigences de sécurité et les conditions d'applications relatives à la sécurité nécessaires pour les maîtriser doit être établi dans le registre des dangers selon SN EN 50126-1 [15].

1.9 Examen de l'expert

Pour prouver la sécurité et la conformité aux prescriptions, des examens de l'expert sont nécessaires pour les projets ayant une grande importance pour la sécurité (art. 5l 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. Ils doivent coordonner leurs examens de manière à éviter toute lacune.

Le GI doit remettre à l'OFT les documents examinés par l'expert ou les versions actualisées de ces documents, dans lesquelles les constats de l'expert ont été intégrées. Les contenus actualisés des documents doivent être identifiés de manière compréhensible (p. ex. par des couleurs).

1.10 Dérogations et exceptions aux spécifications

Les IS doivent en principe être construites en conformité avec les prescriptions déterminantes selon le chap.1.3. Si, dans un projet, des dérogations ou des exceptions à ces prescriptions sont nécessaires, elles doivent être traitées dans le PAP conformément au chap. 1.10.1 - 1.10.2. Il en va de même, si une dérogation ou une exception déjà existante reste nécessaire malgré une adaptation de l'IS.

1.10.1 Dérogations et exceptions aux prescriptions souveraines

Il y a dérogation²¹ aux prescriptions souveraines [1]- [10] lorsque les prescriptions souveraines ne peuvent pas être respectées. Cette dérogation nécessite une demande d'octroi d'une autorisation exceptionnelle conformément à l'art. 5 al. 2 OCF [4]. Les informations suivantes sont requises dans la demande :

- prescription souveraine (désignation précise) dont il faut déroger ;
- la durée prévue de l'intervention ;
- Ligne, section de ligne, kilométrage de la voie ;
- Justification de la demande, notamment par
 - Comparaison avec une solution sans dérogation ;
 - Analyse et évaluation du risque (procédure recommandée au chap. 1.8), qui montrent que
 - le même niveau de sécurité est garanti ;

²⁰ appelé SRAC dans la norme SN EN 50129 [18]

²¹ également appelée exception réelle

- ou qu'il n'a pas de risques inacceptables et que toutes les mesures, en proportion gardées pour réduire le risque ont été prises.
 - les conséquences sur le fonctionnement (actuel et futur) ;
 - Conséquences sur l'ensemble de l'IS ;
 - les éventuelles répercussions sur le respect d'autres exigences découlant des prescriptions souveraines [1] - [10] ;
 - la preuve que l'interopérabilité en trafic transfrontalier et national n'est pas compromise ;
 - Coûts des mesures supplémentaires pour, par exemple, l'entretien, la surveillance.
- Conséquences en cas de non-octroi de la dérogation :
 - Conséquences sur la sécurité au début de la construction ;
 - Estimation des coûts pour les adaptations nécessaires au respect des prescriptions souveraines ;
 - Difficultés à respecter les délais, problèmes de coordination avec d'autres projets.
- Documents nécessaires à l'évaluation de la situation ;
- Avis des secteurs concernés par la dérogation ;
- Évaluation par l'expert.

Une exception²² des prescriptions souveraines [1] - [10] existe lorsque les prescriptions souveraines permettent une exception selon des critères clairs tels que

- Dérogations pour équiper les passages à niveau de barrières ou de demi-barrières selon l'art. 37c al. 3 OCF [4] ;
- Disposition des signaux lumineux clignotants selon les DE-OCF ad l'art. 37c, DE 37c, ch. 1.5.2.1 - 1.5.2.2 [8].

Dans ce cas, aucune demande d'autorisation exceptionnelle n'est nécessaire.

1.10.2 Dérogations et exceptions aux règles techniques reconnues

Les dérogations par rapport aux règles techniques reconnues (tableau 4) concernent surtout les standards techniques et les exigences d'exploitation chez les GI.

Si les dérogations par rapport aux prescriptions RTE sont fixés dans les règles du GI ou s'il existe des solutions détaillées axées sur les risques dans le R RTE 25000 [31] , il est possible de s'y référer sans autre mesure. S'il n'existe pas de solutions concrètes détaillées, il est recommandé de suivre la procédure décrite au chap. 1.8.

Dans les projets de contrôle de la marche des trains voie métrique, des exigences supplémentaires concernant la gestion des dérogations par rapport aux bases de planification [41] sont directement consignées dans ce document. Il en va de même pour les projets ETCS. Dans ce cas, les exigences relatives à la gestion des dérogations par rapport aux exigences du chef de projet ETCS CH [42] sont directement consignées dans le présent document et dans les documents qui y sont référencés. Dans les projets ETCS, les dérogations selon l'art. 15e al. 2 OCF [4] font exception à cette règle.

Les dérogations par rapport aux règles techniques reconnues doivent être indiqués dans le rapport de sécurité. Pour toutes les dérogations il faut apporter la preuve qu'ils n'entraînent pas de risque inacceptable et que toutes les mesures proportionnées de réduction des risques ont été prises. Pour cela, il est recommandé de suivre la procédure décrite au chap. 1.8. L'expert doit vérifier cette preuve et documenter le résultat de son contrôle dans le rapport de l'expert. Si les dérogations par rapport aux règles

²² également appelée fausse exception

techniques reconnues n'entraînent pas de divergences par rapport aux prescriptions souveraines [1] - [10], le GI est responsable de la gestion de ces dérogations.

Le traitement des exceptions aux règles de l'art (tableau 4) est défini dans les règles techniques reconnues.

1.11 Phases de construction et installations provisoires

Une phase de construction est un état intermédiaire planifié de l'IS, qui met à disposition des voies 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 règles d'exploitation et de concepts d'utilisation. Une phase de construction a une date de début et une date de fin déterminées. Dans la mesure où la phase de construction diffère de l'état final, elle doit être documentée et contrôlée sous une forme appropriée. Les phases de construction connues dans la phase de planification doivent être présentées sous une forme appropriée dans le rapport de sécurité ou dans un document séparé. L'affectation des éléments de l'IS aux phases de construction connues doit être évidente et fait l'objet de l'examen de l'expert phase planification.

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

Une installation provisoire est un état temporaire d'un élément donné ayant la même fonction technique et opérationnelle ou une fonction comparable (p. ex. cales de relais, fiche de remplacement). La réalisation du provisoire peut influencer l'utilisation opérationnelle de l'IS. Un aménagement provisoire peut être planifié et réalisé à court terme et ne fait pas l'objet du PAP. Les solutions provisoires doivent être documentées et contrôlées de manière appropriée.

1.12 Intégration technique et d'exploitation

Pour prouver l'intégration technique et d'exploitation, il faut au moins effectuer les tâches suivantes :

- 1) Mettre à jour, si nécessaire, l'analyse et l'évaluation du risque (chap. 1.8) ;
- 2) Définir la configuration IS (logiciel (SW), matériel (HW), interfaces, documents utilisateur). En règle générale, la configuration -IS complète est contenue dans les Release notes ou dans les documents qui y sont référencés ;
- 3) Apporter la preuve que les conditions d'applications relatives à la sécurité des produits prévus (phase de planification) ou utilisés (phase de réalisation) et concernés par les modifications (selon la Release note) ont été mis en œuvre. La liste de contrôle ou le procès-verbal de contrôle des conditions d'applications relatives à la sécurité avec le nom du contrôleur, la version et la date peuvent par ex. servir de preuve à cet égard ;
- 4) Tenir compte des charge imposées aux utilisateurs (GI) par 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 de rétroactivité : Cette preuve doit être apportée 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 nécessaires des effets des modifications doivent être réalisées et évaluées (p. ex. par un expert, un contrôleur d'usine, un validateur). Pour ce faire, les informations suivantes sont nécessaires :
 - Description et justification des modifications ;
 - Effet sur :
 - Le niveau fonctionnel ;
 - Le niveau non fonctionnel (par ex. vitesse, processus d'exploitation, outils, isolation, mise à la terre, compatibilité électromagnétique) ;
 - l'IS globale ;

— comment ces modifications sont contrôlées.

- 6) les documents d'étude de projet, de montage et les prescriptions d'exploitation déterminants ont été mis à jour et/ou rédigés ;
- 7) Apporter la preuve que les formations ou instructions nécessaires du personnel d'exploitation, de conduite et de maintenance ont eu lieu.
- 8) Apporter la preuve de la mise en œuvre des mesures issues de l'analyse et de l'évaluation des risques ;
- 9) Fournir la preuve que les contrôles requis (revue et validation des dossiers de construction, contrôle d'usine, vérification, validation, examen de l'expert) ont été effectués.

L'exécution des tâches susmentionnées doit être prouvée par le GI et vérifiée par un expert. Si l'OFT a autorisé de manière générique le GI à remplir les tâches 3) - 8) pour des projets standard via des processus correspondants (par ex. dans le cadre de PAP), il n'est pas nécessaire de prouver l'accomplissement de ces tâches pour chaque projet.

1.13 Changements significatifs

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

Pour les IS, la procédure de gestion des risques pour les modifications significatives (art. 5m, al. 4, OCF [4]) repose sur les mêmes contenus et méthodes que la gestion des risques exigée par l'art. 5m, al. 2, et l'art. 8a, al. 1, OCF [4] (figure 3). Au chap. 1.4.3 les exigences relatives aux organismes de contrôle indépendants sont définies indépendamment de l'importance de la modification. Elles correspondent aux exigences de l'art. 15t et de l'art. 15u OCF [4] en ce qui concerne la compétence professionnelle et l'indépendance.

Par conséquent, pour l'IS, il n'est pas nécessaire de clarifier la question de la modification significative (art. 5m al. 3 OCF [4]) ni de mettre en œuvre l'art. 5m al. 4 OCF [4]. Si, en particulier, il devait y avoir une modification de l'IS nécessitant également la reconnaissance d'une autre autorité de surveillance européenne, la manière de procéder doit être déterminée au cas par cas avec l'OFT.

1.14 Cybersécurité

" IS, qui utilisent ou contiennent des technologies de l'information et de la communication (TIC) " ²³ , doivent être protégés par tous les moyens organisationnels et techniques proportionnés contre les menaces, les attaques ainsi que les interventions abusives (art. 2 al. 1 ^(bis) OCF [4]).

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

- Protection des infrastructures plus 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 l'avancée 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 management de la sécurité de l'information (SMSI) efficace protège contre les cybermenaces et minimise la surface d'attaque.

²³ le terme "IS avec composante TIC" est utilisé dans la suite du texte

Prévention des pannes et des dysfonctionnements : Les cyberattaques peuvent entraîner des pannes de l'IS, ce qui pourrait avoir un impact sur la disponibilité. Il est donc important d'intégrer la cybersécurité à un stade précoce de la planification afin de garantir la disponibilité.

- identifier les vulnérabilités potentielles dès la planification et d'y remédier. Les risques peuvent ainsi être mieux évalués et des mesures de protection peuvent être prises de manière proactive.
- Maintenir la confiance du public : le public et les entreprises comptent sur le fonctionnement sûr et fiable des infrastructures critiques.
- Réduction du sabotage : les IS peuvent être attaquées. De telles attaques visent souvent à provoquer le chaos ou à poursuivre des objectifs politiques. Les mesures de protection servent à identifier et à contrer de telles menaces avant qu'elles ne causent des dommages.

C'est pourquoi, outre l'attention portée à ce thème au niveau de la direction du GI, la procédure décrite sur la figure 5, s'applique au niveau du PAP en matière de cybersécurité. Les étapes correspondantes sont expliquées ci-après.

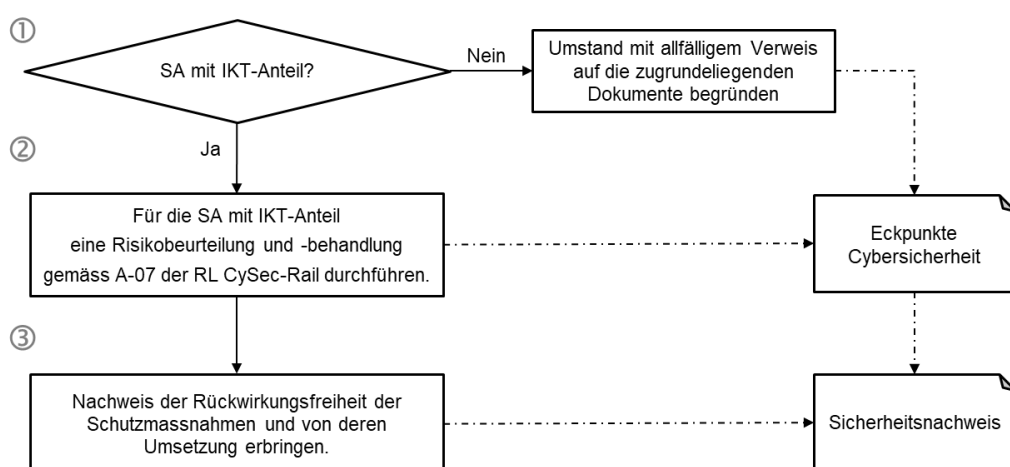


Figure 5: Arbre décisionnel sur la cybersécurité

- ① Clarifier s'il s'agit d'une IS avec une part de TIC (p. ex. poste d'enclenchement, système de commande ferroviaire, système de télétransmission, diagnostic, surveillance et maintenance basés sur le réseau). Si l' IS n'utilise ni ne contient les TIC, cette circonstance doit être justifiée par un renvoi éventuel aux documents sur lesquels elle se fonde. Dans ce cas, aucune autre mesure de protection n'est nécessaire.

Pour les IS ayant une composante 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 [13] . Les points clés suivants doivent être documentés pour les IS concernées ayant une composante TIC au moyen de documents de référence dans le document "Points clés Cybersécurité" :

- 1) Personnes compétentes dans le domaine de la cybersécurité ;
- 2) Renvoi à d'éventuels documents annexes ;
- 3) Besoin de protection ;
- 4) les risques identifiés ;
- 5) les mesures de protection prévues ;
- 6) Risques résiduels après les mesures de protection prévues.

Des explications sur les points clés susmentionnés sont disponibles dans la Dir. CySec-Rail [13] .

- ③ Lors de la mise en œuvre des mesures de protection, il convient de vérifier si elles ont un impact sur l'ensemble de l'IS. La preuve de la non-rétroactivité des mesures de protection et de la mise en œuvre des mesures de protection doit être référencée dans la preuve de sécurité.

1.15 Interopérabilité

1.15.1 Généralités

On distingue les catégories de réseaux suivantes (art. 15a 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 tramways ;
 - les voies de raccordement et les infrastructures ferroviaires telles que les installations d'entretien avec leurs champs de voies, les installations de lavage, les ateliers, etc.

Aucune exigence IOP ne s'applique sur le réseau non IOP.

- Réseau principal IOP avec les tronçons à voie normale (entièrement interoperables) selon l'annexe 6 OCF [4] ;
- Réseau complémentaire IOP comprenant toutes les tronçons à voie normales (partiellement interoperables) 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 le réseau principal 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. 15b al. 1 OCF [4]) a les caractéristiques ETCS L2 et ETCS L1 LS sur le réseau principal 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. 15k OCF [4]). La déclaration de conformité de ce sous-système est délivrée par le GI sur la base du certificat de conformité délivré par un organisme notifié (art. 15k^{bis} al. 1 OCF [4]).

Pour l'autorisation de projets du sous-système CCS au sol, une déclaration de conformité de ce sous-système doit être présentée (art. 15j OCF [4]).

Für die Bewilligung anlagenspezifischer Anwendungen des streckenseitigen Teilsystems ZZS muss eine Konformitätserklärung dieses Teilsystems vorgelegt werden (Art. 15j OCF [4]).

Actuellement, la déclaration de conformité du sous-système CCS au sol est considérée comme établie si les constituants d'IOP (par ex. Eurobalise, Euroloop, LEU - Eurobalise, LEU - Euroloop, compteur d'essieux, Radio Block Centre) avec des déclarations de conformité de l'industrie ferroviaire sont utilisés dans le projet et que la preuve de la conformité aux exigences du gestionnaire du système ETCS CH (par exemple, règles de conception) [42] a été fournie.

Le GI doit disposer des déclarations de conformité des constituants d'IOP (art. 15i^{er} OCF [4]). Si les constituants d'IOP sont homologués par l'OFT, le GI peut partir du principe que leurs déclarations de conformité sont disponibles.

En collaboration avec le gestionnaire du système ETCS, des travaux sont actuellement menés afin d'aligner davantage la déclaration de conformité actuelle du sous-système CCS au sol sur les exigences de l'OCF [4].

1.16 Procédure d'autorisation d'exploiter

Sur la base de l'art. 8 al. 1 - 2 OCF [4], les dispositions suivantes s'appliquent dans le champ d'application de la Dir. IS :

- une AE est requise pour la MES de produits comportant une part de développement et des fonctions liées à la sécurité selon $SIL \geq 1$.
- 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 ou complémentaire IOP, une AE est nécessaire pour les nouvelles applications spécifiques à l'installation du sous-système CCS au sol (art. 23c al. 1 LCdF [1] ou 15c OCF [4]).

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

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

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

2 Projet standard

2.1 Phases et déroulement du projet standard

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

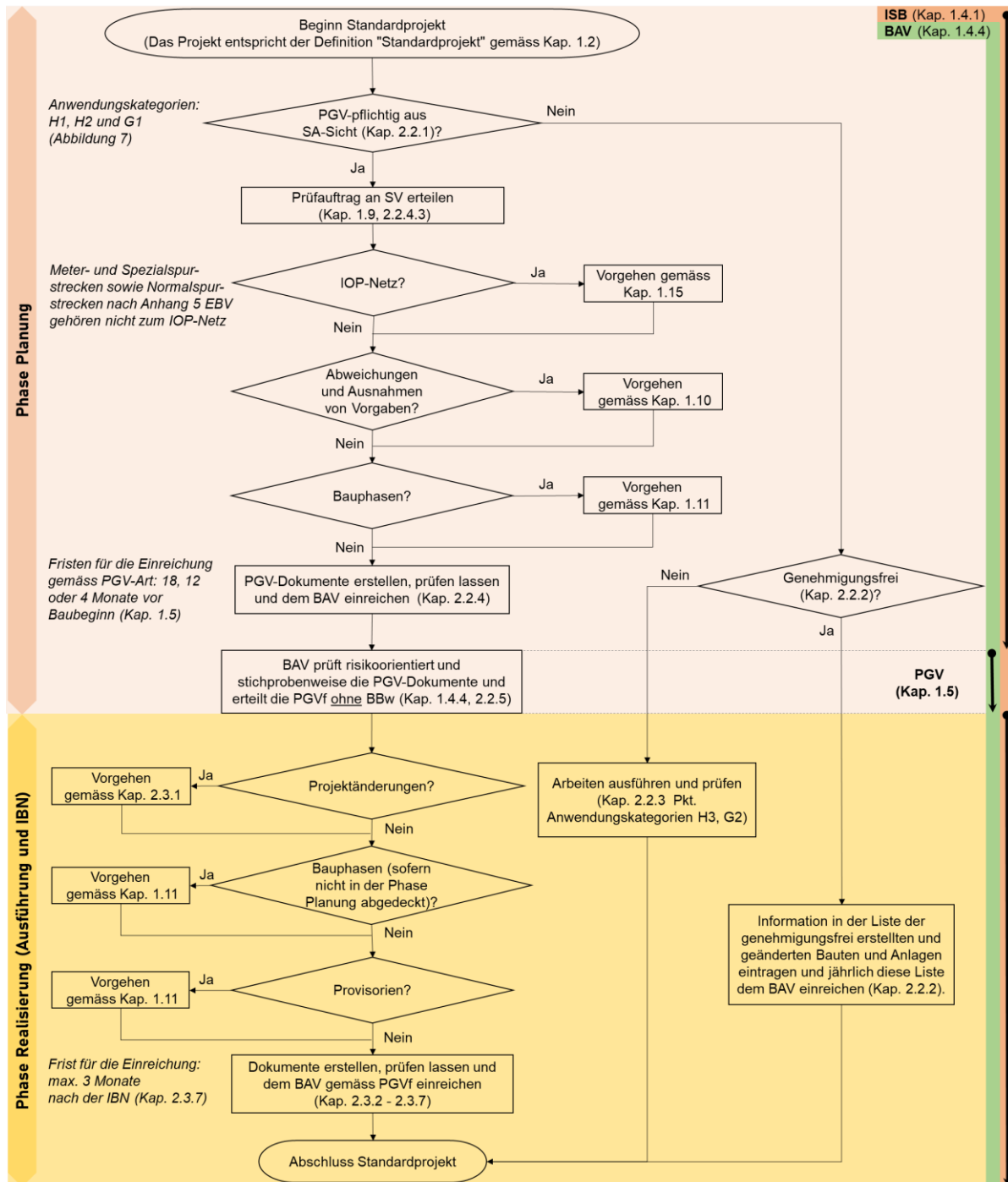


Figure 6: Déroulement du projet standard

2.2 Phase planification du projet standard

2.2.1 Attribution de la catégorie d'application du projet standard

Ce chapitre définit ce que l'on appelle la catégorie d'applications. L'objectif 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 un PAP est nécessaire et quelles exigences sont posées à la gestion des preuves de sécurité.

Évaluation de l'importance de la sécurité

- H (élevé) : L'importance de la sécurité est élevée si :
 - les fonctions ayant une importance élevée pour la sécurité (fonctions liées à la sécurité selon SIL 1 - 4) sont concernées ;
 - des fonctions importantes pour la sécurité, par ex. des postes d'enclenchement à relais et électroniques, des commandes de passages à niveau et d'aiguillages, qui ont été développées à l'origine sans attribution d'un SIL, sont concernées.

Une importance élevée pour la sécurité est également présente lorsque seules certaines fonctions (par ex. commande, affichage ou automatisation) ont une importance élevée pour la sécurité.

- G (faible) : L'importance pour la sécurité est faible, si :
 - des fonctions liées à la sécurité avec BI (moins exigeantes que SIL 1) sont concernées ;
 - des tronçons de voie peuvent être empruntés en mode tramway, pour autant qu'aucune commande d'aiguillage ne soit utilisée.

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

Évaluation du type du projet standard

- (1) Construction d'une nouvelle IS, transformations importantes d'IS existantes, première utilisation de produits tels que :
 - Construction d'un nouveau poste d'enclenchement ou d'un passage à niveau ;
 - Première utilisation de produits homologués par l'OFT ou autorisés d'une autre manière en Suisse sur le réseau du GI .
- (2) Modifications ayant une incidence sur les aspects conceptuels et/ou fonctionnels des IS existantes, mais d'ampleur limitée, telles que
 - Ajustement de la vitesse ;
 - Ajustement des images de signaux ;
 - Transformation d'une voie ferrée avec adaptation de la signalisation.
- (3) Modifications sans influence sur les aspects conceptuels et/ou la fonction des IS existantes telles que
 - Correction d'erreurs aux IS (par ex. à l'étude de projet) ;
 - Correction d'erreurs sur le produit générique (par ex. simples mises à jour logicielles sans nouvelles fonctions) ;
 - "Remplacement de produits par une nouvelle génération de produits de fonction identique et de même technologie" ;²⁴
 - Démontage et remontage de produits existants au même endroit (par ex. rénovation de la superstructure).

²⁴ 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 de projet standard conformément à la figure 7. Elle doit être justifiée dans le rapport de sécurité.

Un projet standard est soumis à la PAP lorsque des intérêts de tiers dignes de protection sont touchés et qu'il y a des répercussions sur le territoire et l'environnement. Du point de vue des IS, l'obligation de PAP n'existe que s'il entre dans la catégorie d'application **H1**, **H2** ou **G1** (figure 7). Des explications sur les types de PAP et les délais de traitement se trouvent au chap.1.5.

| Art des Standardprojekts | Sicherheitsrelevanz | |
|--|--------------------------------|------|
| | Gering | Hoch |
| (1) Neubau, umfangreiche Umbauten, erstmaliger Einsatz von Produkten | G1 | H1 |
| (2) Änderungen <u>mit</u> Einfluss auf konzeptionelle Aspekte und/oder Funktion | G2 | H2 |
| (3) Änderungen <u>ohne</u> Einfluss auf konzeptionelle Aspekte und/oder Funktion | Ausserhalb des Fokus der RL SA | H3 |

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

2.2.2 Projets standard sans PAP

Les modifications suivantes des IS ne nécessitent pas d'autorisation, si elles n'affectent pas les intérêts dignes de protection de tiers et n'ont qu'un impact négligeable sur l'espace et l'environnement :

- Démantèlement d'aiguillages avec remplacement de la voie, sans modification du tracé, sans rétroaction sur des aiguillages de protection, sans démantèlement des dispositifs de dilatation des rails²⁵ (annexe à l'art. 1a al. 1 let. e OPAPIF [5]);
- Le remplacement des dispositifs de déraillement par des aiguillages de protection en respectant la R RTE 25053 [31]
- Entretien des composants techniques de construction des installations de passages à niveau (annexe à l'art. 1a al. 1 let. f OPAPIF [5]);
- Pose de croix de Saint-André ou de signaux "tramway" aux passages à niveau (annexe à l'art. 1a al. 1 let. y OPAPIF [5]);

En cas de doute, il est recommandé de se mettre d'accord suffisamment tôt avec l'OFT sur la procédure à suivre.

Le GI doit soumettre chaque année à l'OFT une liste des constructions et installations construites ou modifiées sans approbation (art. 1a 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 la figure 7, les exigences suivantes s'appliquent à la démonstration de la sécurité :

- Catégorie d'utilisation **H1** : Les exigences selon chap. 2.2.4 et 2.3 s'appliquent.
- Catégories d'utilisation **H2** et **G1** : les exigences du chap. 2.2.4 et 2.3 s'appliquent, mais sont relativisées par les points suivants :

²⁵ Les dispositifs de dilatation des rails ne font pas partie de l'IS.

- Les documents justificatifs doivent, dans la mesure du possible, se concentrer sur la modification et son impact sur l'ensemble de l'IS ;

- Pour la catégorie d'application **H2**, un rapport d'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 Planification lors de la phase Réalisation. Dans ce cas, les documents PAP sont remis rapport d'expert. Dans ce cas, le GI assume le risque que, le cas échéant, des erreurs de la phase Planification ne soient découvertes qu'à un stade tardif. L'OFT peut demander un rapport d'expert pour la phase planification dans la PAP.

En outre, 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 mandat d'examen permet de confier à une seule et même personne le contrôle d'usine et d'examen de l'expert pour les phases de planification et de réalisation (chap. 2.2.4.3). L'indépendance de cette personne doit être garantie, c'est-à-dire que cette personne ne doit pas assumer d'autres tâches (sauf de nature organisationnelle) en rapport avec l'objet de l'examen.

- Pour la catégorie d'application **G1**, il est possible de renoncer à l'examen de l'expert.

- Catégories d'application **H3** et **G2**: une distinction entre les phases de planification et de réalisation n'est pas nécessaire du point de vue de la démonstration de la sécurité. Pour la démonstration de la sécurité, les points suivants doivent être pris en compte :

- Les modifications apportées aux IS doivent être documentées ;
- Les rôles et les responsabilités du personnel impliqué doivent être documentés (chap. 2.2.4.2 pt. 8).
- Si les modifications apportées à l'IS sont conformes aux prescriptions du chap. 1.3.1, 1.3.2²⁶, 1.3.3, 1.3.4 , il n'est pas nécessaire de procéder à une analyse et à une évaluation des risques supplémentaires, car tous les dangers sont maîtrisés par l'application des règles techniques reconnues (tableau 4). Le GI doit consigner les règles techniques reconnues pertinentes dans le projet standard et prouver leur mise en œuvre ;
- Les éventuelles dérogations et exceptions aux directives doivent être traitées conformément au chap. 1.10 ;
- Intégration technique et opérationnelle (chap. 1.12) :
 - Preuve de la mise en œuvre du SBAWB ;
 - Documents d'étude de projet, de montage et prescriptions d'exploitation mis à jour et/ou nouvellement élaborés
 - Preuve du respect des obligations découlant des HdS, y compris preuve de la mise en œuvre des exigences génériques²⁷ des produits utilisés ayant une pertinence pour le GI.
- Pour la catégorie d'utilisation **H3**, l'examen de l'expert est nécessaire pour les phases de planification et de réalisation (chap. 1.9). 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 dans la phase de réalisation. Le mandat d'examen permet de confier à une seule et même personne le contrôle d'usine et l'examen de l'expert pour les phases de planification et de réalisation (chap. 2.2.4.3). L'indépendance de cette personne doit être garantie, c'est-à-dire que cette personne ne doit pas assumer d'autres tâches (sauf de nature organisationnelle) en rapport avec l'objet de l'examen. Pour la mise en service, la procédure au sens du chap. 2.3.2.3 s'applique.
- Pour la catégorie d'utilisation **G2**, l'examen pour la mise en service doit être effectué par une personne compétente sur la base de protocoles de contrôle/de check-lists.

²⁶ seule la norme VSS 71 253 est pertinente [24]

²⁷ www.bav.admin.ch → Informations juridiques → Autres bases légales et prescriptions → Directives → Chemin de fer → Homologation de type pour les éléments des installations ferroviaires → Indications concernant les décisions issues des procédures d'homologation de série des installations de sécurité et des applications télématiques

— A l'issue de la mise en service:

- les protocoles de contrôle/listes de contrôle remplis et signés sont à conserver, et
- les résultats de l'examen de la mise en service sont à actualiser.

Les documents justificatifs ne doivent pas être remis à l'OFT. Ils restent auprès de la GI et doivent pouvoir être présentés à l'OFT dans le cadre de la surveillance de la sécurité pendant la phase d'exploitation.

2.2.4 Documents PAP et exigences relatives au contenu du projet standard

Le tableau 5 présente un aperçu des documents PAP du projet standard. En complément, il contient des renvois où l'on peut trouver des explications sur les exigences relatives au contenu des documents PAP (art. 3 al. 1 - 2 OPAPIF [5]). Lors de l'élaboration de ces documents, les exigences formelles selon le chap. 1.1.3 doivent être prises en compte.

Les documents PAP mentionnés dans le tableau 6 doivent être remis à l'OFT. Si le GI estime que certains des documents énumérés ne sont pas pertinents pour le projet standard concerné, elle peut renoncer à les remettre en motivant brièvement sa décision (p. ex. "non concerné").

Si des documents tels que la table des matières, la demande d'approbation des plans, la fiche de pilotage du projet, une demande d'octroi d'une dérogation, les plans et le concept de mise à terre sont établis dans le cadre d'un projet global, il convient d'y intégrer les contenus selon le présent chapitre pour l'IS. Les documents susmentionnés ne doivent alors pas être rédigés séparément pour l'IS.

| Titre du document | Explications sur les exigences en matière de contenu |
|--|--|
| <i>Les documents qui sont mis à l'enquête publique sont colorés en rose. Pour les trois premiers documents, les chiffres de référence sont prédéfinis. Tous les autres documents doivent être numérotés avec le chiffre de référence <u>15.xx</u>. Les chiffres subordonnés xx sont à définir par le GI.</i> | |
| 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 (uniquement nécessaire pour le PAP ordinaire) | Chap. 1.6.2 |
| Rapport de sécurité | Chap. 2.2.4.2 |
| Demande de dérogation (dans la mesure où des dérogations par rapport aux prescriptions souveraines [1] – [10] sont nécessaires) | Chap. 1.10.1 |
| Tableaux pour : distances de glissement ; protection de flancs ; distances des signaux avancés (peuvent être indiquées séparément ou dans le rapport de sécurité) | [8] |
| Tableau des itinéraires (RADN) | [9] |
| Plan de signalisation/concept de signalisation/plan de situation/plan | Chap. 2.2.4.4 |
| Profils d'espace libre / profils transversaux | |
| Concept de mise à la terre (s'il n'est pas déjà couvert par les documents de niveau supérieur) | [35] |
| Plan détaillé du passage à niveau | Chap. 2.2.4.4 |
| Profil d'espace libre des éléments de passage à niveau | |
| Profils transversaux/profils d'espace libre route | |
| Diagramme distance-temps passage à niveau | [34] |
| Points clés de la cybersécurité | Chap. 1.14 |
| Documentation des compétences professionnelles de l'expert | Chap. 1.4.3 pt. (1) |
| Rapport d'examen de l'expert phase planification | Chap. 1.6.3 |

| Titre du document | Explications sur les exigences en matière de contenu |
|--|--|
| <i>Les documents qui sont mis à l'enquête publique sont colorés en rose. Pour les trois premiers documents, les chiffres de référence sont prédéfinis. Tous les autres documents doivent être numérotés avec le chiffre de référence <u>15.xx</u>. Les chiffres subordonnés xx sont à définir par le GI.</i> | |
| Prise de position sur la mise en œuvre des résultats de l'examen l'expert phase planification | Chap. 1.6.4 |

Tableau 5 : Documents PAP du projet standard

2.2.4.1 Table des matières

La table des matières contient des informations sur : le chiffre de référence, le titre du document, l'index ou la version, l'échelle, le numéro du plan et la date d'élaboration. Elle doit être remise à l'OFT sous forme de fichier Word modifiable.

2.2.4.2 Rapport de sécurité

Dans le rapport de sécurité, les informations suivantes sont requises :

- 1) Définition de l'objet de la demande :
 - état actuel de l'IS (brève description) ;
 - changements prévus pour les IS ;
 - conséquences de ces changements ;
 - interfaces ;
 - dépendance par rapport au projet global ;
 - utilisation de la voie ;
 - concept de manœuvre, en cas de manœuvres régulières, indiquer le nombre de trajets.
- 2) Interfaces avec d'autres produits et IS voisines ;
- 3) prescriptions déterminantes (chap. 1.3) ;
- 4) produits prévus, y compris leur release/version et type d'autorisation, pour autant que les produits soient connus (chap. 1.2) ;

Le type d'autorisation a les caractéristiques suivantes :

 - HdS no ;
 - démonstration de la sécurité par la mise à l'épreuve de la pratique ;
 - gestion du rapport de 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) Attribution de la catégorie d'application (chap. 2.2.1) ;
- 7) Sécurisation et signalisation des passages à niveau ainsi que leur commande avec les informations suivantes :
 - Utilisations, charge de trafic et, le cas échéant, vitesse maximale autorisée du côté route ;
 - Écoles, terrains de jeux, installations sportives et de loisirs et autres installations similaires à forte fréquentation à proximité ;
 - Preuve que les usagers de la route ont une visibilité suffisante pour voir les signaux au passage à niveau et, si nécessaire (p. ex. pour les passages à niveau signalés par une croix de Saint-André, signal "tramway"), les trains ;
 - Signalisations et tous les marquages routiers existants et nouveaux en rapport avec le projet ;

- Preuve de l'évacuation du passage à niveau ;
 - Il est très important d'impliquer suffisamment tôt les parties prenantes du côté de la route. C'est pourquoi le GI doit mentionner les déclarations relatives aux accords les plus importants.
- 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 du personnel impliqué. L'indépendance des rôles doit apparaître clairement dans l'organisation de la sécurité.

Si l'organisation de la sécurité est garantie par des processus appropriés, il n'est pas nécessaire de prouver l'organisation de la sécurité pour le projet spécifique.

- 9) Mandat pour l'examen de l'expert (chap. 1.9, 2.2.4.3) :
- 10) Analyse et évaluation du risque : Dans le projet standard, il existe des dangers standard qui sont maîtrisés par l'application des règles techniques reconnues (tableau 4). Cela signifie qu'en cas d'application des règles techniques reconnues, les risques liés à ces dangers ne doivent pas être analysés plus avant. La GI doit démontrer la mise en œuvre des règles techniques reconnues pertinentes.
- 11) les éventuelles dérogations et exceptions aux directives doivent être traitées conformément au chap. 1.10 ;
- 12) référence aux "Points clés de la cybersécurité" (chap. 1.14) ;
- 13) phases de construction (chap. 1.11) ;
- 14) intégration technique et d'exploitation (chapitre 1.12) :
- a) preuve de la mise en œuvre du SBAWB, si elle est pertinente pour la planification ;
 - b) documents d'étude de projet, de montage et les règles d'exploitation qui doivent être mis à jour et/ou créés en raison des modifications prévues ;
 - c) besoin de formation ou d'instruction du personnel d'exploitation, de conduite et de maintenance ;
- 15) conséquences en termes d'exploitation et de sécurité si le projet standard ne peut pas être réalisé.
- 16) conclusion que le projet standard prévu correspond aux prescriptions déterminantes ou que des dérogations correspondantes ont été demandées et que les IS construites selon ce projet peuvent être exploitées en toute sécurité.

Dans le cadre d'un projet global, les informations mentionnées au pt. 1), 7) et 15) sont déjà mentionnées dans le rapport technique de niveau supérieur. Dans ce cas, le rapport de sécurité doit faire référence au rapport technique.

2.2.4.3 Mandat d'examen d'expert

A. Phase de planification : en règle générale, l'expert doit effectuer les tâches suivantes :

- 1) Vérifier si le projet standard correspond à la définition "projet standard" (chap. 1.2) ;
- 2) Vérification de l'attribution correcte de la catégorie d'application²⁸ (chap. 2.2.1) ;
- 3) Vérification de l'exhaustivité des documents et informations requis (chap. 2.2.4) ;
- 4) Examen du respect des prescriptions déterminantes (chap. 1.3). Les éléments suivants, y compris leurs interactions, doivent être pris en compte :
 - Profils d'espace libre ;
 - Noms des éléments ;
 - Dispositifs d'annonce de voie libre, longueur des tronçons, contacts de rail ;
 - Aiguillages, protection de flanc ;

²⁸ Cette vérification peut également être effectuée par une autre personne compétente.

- Signaux principaux et avancés, distances de freinage, distances de glissement, visibilité ;
 - Signaux de manœuvre et complémentaires, panneaux de signalisation ;
 - Signaux et panneaux dans le domaine de la signalisation en cabine;
 - Protection des parcours (y compris bloc de ligne), accès aux quais par la voie ;
 - Contrôle de la marche des trains ;
 - Passages à niveau ;
 - Systèmes de télétransmission ;
 - Système de contrôle-commande ferroviaire.
- 5) Contrôle du type d'autorisation selon le chap. 2.2.4.2 pt. 4) pour les produits prévus ;
 - 6) Examen de l'organisation de la sécurité (chap. 2.2.4.2 pt. 8) ;
 - 7) Vérification si les dérogations par rapport aux prescriptions et les demandes de dérogations sont entièrement documentés (chap. 1.10.1). Vérifier et documenter si les dérogations sont acceptables.
 - 8) Examen de l'analyse et de l'évaluation du risque d'éventuels dérogations par rapport aux prescriptions souveraines [1] - [10] ;
 - 9) Vérification de la plausibilité des points clés sur la cybersécurité (chap. 1.14) ;
 - 10) Examen des phases de construction (chap. 1.11) ;
 - 11) Vérification si les tâches d'intégration technique et d'exploitation suivantes ont été effectuées (chap. 1.12) :
 - Mise en œuvre du SBAWB, si pertinentes pour la phase de planification ;
 - Présence des informations pour la mise à jour ou la création des documents de conception, de montage et des règles d'exploitation ;
 - Présence des informations sur les besoins en formation du personnel d'exploitation, de conduite et de maintenance ;
 - 12) Documentation de l'activité d'examen (chap. 1.6.3).
- B. Phase de réalisation : en règle générale, l'expert doit effectuer les tâches suivantes pour l'examen théorique et pratique (chap. 2.3.5)

Examen théorique (concerne les documents)

- 1) Vérifier si le projet correspond à la définition de "projet standard" (chap. 1.2) ;
- 2) Vérification que:
 - L'organisation de la sécurité est définie et que l'indépendance (c'est-à-dire aucune autre tâche en rapport avec l'objet de l'examen) entre différents rôles est garantie (chap. 2.2.4.2 pt. 8);
 - les modifications du projet sont documentées et conformes aux prescriptions (chap. 2.3.1) ;
 - les règles techniques reconnues définies lors de la phase de planification ont été respectées ;
 - les charges découlant de la DAP sur la PAP sont remplies, pour autant qu'elles concernent la sécurité ;
 - les charges du rapport d'examen d'expert phase planification sont mises en œuvre ;
 - les dossiers de construction ont été revus et approuvés (chap. 2.3.2.1) ;
 - les dossiers de construction sont conformes aux prescriptions déterminantes ; Il convient de sélectionner les prescriptions selon le chap. 1.3 qui sont pertinentes pour les dossiers de construction.

- mesures HTA [44] (enclenchement à relais, commande de passage à niveau) sont mis en œuvre ;
 - les documents de contrôle de tous les produits utilisés (y compris l'installation extérieure et intérieure) sont disponibles ;
 - la mise en œuvre des dossiers de construction est vérifiée et documentée
 - Release notes sont disponibles ;
 - L'IS est prête à être mise en service (chap. 2.3.2.3) ;
- 3) Vérification que les tâches d'intégration technique et d'exploitation suivantes ont été effectuées (chap. 1.12) :
- Mise en œuvre de la SBAWB ;
 - l'absence de rétroaction est démontrée ;
 - les documents d'étude de projet, de montage et les prescriptions d'exploitation sont disponibles et mis à jour ;
 - les formations ont eu lieu ;
- 4) Documentation de l'examen (chap. 1.6.3) ;

Examen pratique (concerne la réalisation technique de l'IS)

- 5) Vérification que les produits utilisés correspondent au type d'autorisation selon le chap. 2.2.4.2 pt. 4) ;
 - 6) Contrôle des fonctions des IS, y compris la réaction en cas de panne, ainsi que l'interaction des différents produits entre eux, y compris les IS voisines ;
 - 7) Examen des solutions provisoires, si pertinent (chap. 1.11) ;
 - 8) Évaluation de l'adéquation et de l'exhaustivité du contrôle d'usine en ce qui concerne la sécurité ;
 - 9) Documentation de l'examen (chap. 1.6.3).
- C. ETCS L2: le mandat confié à l'expert conformément aux exigences la tâche systémique ETCS CH doit être pris en compte dans les phases de planification et de réalisation.

2.2.4.4 Plans

Plans de l'installation extérieure IS

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

- Désignation de tous les éléments, y compris le kilométrage ;
- Tronçons de voie ;
- Aiguillages (avec géométrie) ;
- Signaux (avec images), panneaux de signalisation, contrôle de la marche des trains ;

Passages à niveau (signalisation complète, y compris tous les éléments ferroviaires tels que les éléments d'arrêt, les éléments de contrôle) ;

- Vitesses ;
- Pentes ;
- Quais, bâtiments techniques et d'exploitation.

Les informations susmentionnées peuvent par ex. être soumises avec un ou plusieurs des plans suivants, utilisés dans la pratique :

- Plan de signalisations, en règle générale à l'échelle 1:500 ou 1:1000 avec la représentation de la voie sous forme de trait simple ;
- Concept de signalisation : s'étend sur la zone pertinente (p. ex. plusieurs gares ou ligne entière) et est p. ex. à l'échelle 1:5000 ;
- Plan de situation : Plan de signalisation complété par des informations sur l'infrastructure adjacente (p. ex. passages à niveau, quais, routes, ponts, immeubles) ;
- Plan S : plus détaillé que le plan de signalisation et à l'échelle 1:500 ou 1:250 avec la représentation de la voie sous forme de double trait. Ce plan est déterminant pour la phase de réalisation.

Les gabarits, dans la mesure où ils concernent les signaux et les panneaux

- Type de gabarit
- Axe de la voie, surélévation de la voie, élargissement de la courbe
- Cotation (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 gabarit est généralement représenté dans les profils en travers.

Plans du passage à niveau

- Plan détaillé du passage à niveau à l'échelle 1:200 ou 1:100 avec la représentation de la voie sous forme de double trait. Les informations suivantes doivent être représentées ou indiquées :
 - Tous les éléments routiers (par ex. signaux, barrières, grillages suspendus) ;
 - Marquage des limites et des routes ;
 - Cotation (distances par rapport aux limites de la route et à l'axe de la voie) ;
 - Toutes les signalisations et tous les marquages existants côté route en rapport avec le projet.
- Profil d'espace libre des éléments du passage à niveau (y compris cotation)
- Profils en travers/profils d'espace libre de la route (y compris cotation)

Représentation dans les plans

- Le code couleur courant (D RTE 25100 [33]) doit être utilisé afin de montrer clairement quelles sont les parties IS existantes, nouvelles ou à supprimer. De même, les projets de tiers dans le même périmètre doivent être représentés afin de pouvoir évaluer les éventuelles influences sur le projet standard à soumettre ;
- Tous les nouveaux éléments doivent être dessinés dans leurs positions théoriques ;
- Toutes les dimensions et distances pertinentes doivent être représentées à l'échelle ;
- Les désignations, abréviations, signes, 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 PAP ;
- Tous les plans doivent être mis à jour afin de correspondre à la nouvelle situation. Les plans doivent être mis à jour au plus tard lors de la phase de réalisation.

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

L'OFT octroi la DAP (chap. 1.4.4) pour la nouvelle IS ou l'IS modifiée sans exiger une AE.

2.3 Phase de réalisation du projet standard

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

2.3.1 Modifications d'un projet standard

Si, après DAP des divergences apparaissent par rapport aux documents PAP approuvés, il convient de procéder conformément à la figure 8. Les étapes correspondantes sont expliquées ci-après.

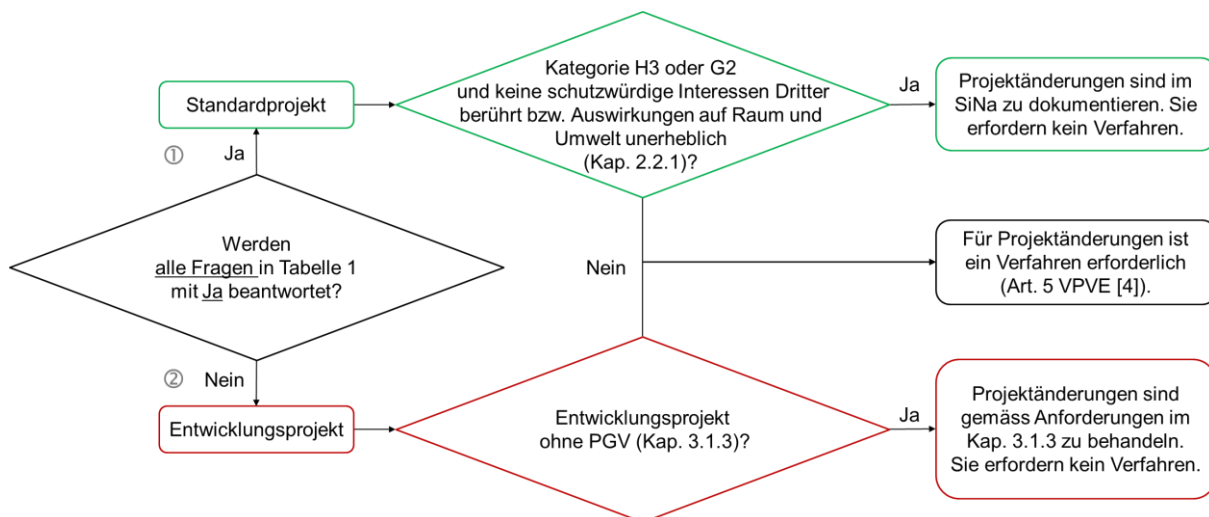


Figure 8: Modifications d'un projet standard

Clarification si les modifications du projet correspondent à la définition de "projet standard". Pour cela, il faut répondre aux questions figurant dans le tableau 1 (chap. 1.2).

- ① Si la réponse à toutes les questions est oui, les modifications apportées au projet sont considérées comme un projet standard.

Si les modifications du projet relèvent des catégories H3 ou G2 selon le chap. 2.2.1 et qu'elles ne touchent pas d'intérêts de tiers dignes de protection et n'ont qu'un impact négligeable sur le territoire et l'environnement, elles doivent être documentées dans le dossier de sécurité et examinées par l'expert (pour la catégorie H3).

Sinon, une procédure est nécessaire pour les modifications de projet (art. 5, al. 2, OPAPIF [5]). Pour les documents concernés par les modifications de projet, il faut mettre en œuvre les exigences selon le chap. 2.

- ② Si la réponse à toutes les questions n'est pas oui, les modifications apportées au projet sont considérées comme un projet de développement.

Si 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 nécessaire pour les modifications de projet (art. 5 al. 2 OPAPIF [5]). Les exigences mentionnées au chap. 3 doivent être mises en œuvre.

Si l'IS est déjà en construction, les travaux non concernés par les modifications du projet peuvent être poursuivis, sous réserve d'une intervention de l'OFT (art. 5, al. 3, OPAPIF[5]).

2.3.2 Documents et exigences relatives du contenu du projet standard

Le tableau 6 présente les documents de la phase de réalisation. En complément, il contient des renvois où l'on peut trouver des explications sur les exigences au contenu. Lors de l'élaboration de ces documents, les exigences formelles selon le chap. 1.1.3 doivent être prises en compte.

| Titre du document | Explications sur les exigences en matière de contenu |
|--|--|
| S-Plan (si pas disponible dans les documents PAP) | Chap. 2.2.4.4 |
| Dossiers de construction et documents de contrôle, y. c. review et libération des dossiers de construction | Chap. 2.3.2.1 |
| Dossier de sécurité | Chap. 2.3.2.2 |
| Programme de mise en service | Chap. 2.3.2.3 |
| Autorisation de mise en service | Chap. 2.3.2.3 |
| Rapports de contrôle d'usine | Chap. 2.3.4 |
| Rapport d'examen de l'expert phase réalisation | Chap. 1.6.3 |
| Prise de position du GI sur la mise en œuvre des résultats de l'examen l'expert phase réalisation | Chap. 1.6.4 |

Tableau 6 : Documents de la phase Réalisation du projet standard

2.3.2.1 Dossiers de construction et documents de contrôle

Dossiers de construction

Sont considérés comme dossiers de construction les documents détaillés relatifs au produit, qui indiquent l'application spécifique à l'installation du produit. Chaque document de construction établi et modifié doit être contrôlé comme suit :

- Révision de la part de l'auteur (généralement l'industrie ferroviaire) concernant
 - Respect des règles de conception;
 - Mise en œuvre des schémas de principe ou des principes de construction ;
 - Mise en œuvre de la SBAWB ;
 - Exhaustivité.
- Validation par le GI : Le GI contrôle en particulier que les exigences fonctionnelles et d'exploitation sont remplies. En outre, le GI doit s'assurer que les dossiers de construction sont conformes à la décision d'approbation des plans, y compris les documents PAP approuvés.

Documents de contrôle

En règle générale, les documents de contrôle doivent également être établis avec les dossiers de construction. Ils contiennent les cas contrôlés et décrivent la manière dont le contrôleur d'usine doit procéder lors du contrôle d'usine. Ils doivent être établis selon les modèles et les originaux des fournisseurs. Il convient de tenir compte de tous les produits utilisés pour l'installation extérieure et intérieure ainsi que de l'interaction des différents produits entre eux.

Implication de l'expert

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

2.3.2.2 Dossier de sécurité

Le dossier de sécurité doit être mené et signé par des spécialistes parallèlement aux travaux de projet standard (art. 5l al. 2 OCF [4]). Elle se base sur le rapport de sécurité et doit donner une image

complète de l'ensemble de l'IS, même si elle ne traite qu'une partie de l'IS. Il faut veiller à ce que tous les produits utilisés y soient traités.

Le dossier de sécurité est établi en deux étapes :

- Version initiale avant la mise en service (dossier de sécurité initial) : l'aptitude de l'IS à la mise en service y est démontrée. Les points 1) - 17) mentionnés ci-dessous doivent être traités, pour autant que les informations soient disponibles. Cette version de la preuve de sécurité doit être présentée à l'expert en temps utile avant la mise en service. La pertinence des points ouverts doit être évaluée pour la mise en service. En outre, les étapes pour leur résolution doivent être documentées.
- Version finale après la mise en service (dossier de sécurité final) : complète la version initiale afin d'apporter la preuve de la réalisation des points initialement déclarés comme ouverts.

Le dossier de sécurité doit contenir les informations suivantes. Si les informations sont entièrement contenues dans le rapport de sécurité, il est judicieux de faire référence au rapport de sécurité.

- 1) Définition de l'IS considérée : Si elle est identique à celle du rapport technique de niveau supérieur, il est possible d'y faire référence.
- 2) Documents de référence : par ex. spécifications, DAP, Plan S, dossiers de construction, documents de contrôle, documents d'étude de projet, de montage, consignes d'exploitation, Release notes, analyses de l'impact des modifications, révision et validation des dossiers de construction, protocoles de contrôle/check-lists, validation pour le début de l'exploitation, rapports d'examen ;
- 3) Produits utilisés, y compris leur version et leur type d'autorisation, conformément au chap.2.2.4.2 pt. 4) ;
- 4) Preuve que le projet correspond à la définition de "projet standard" selon le chap. 1.2 pt. ② ;
- 5) Organisation de la sécurité pour la phase de réalisation : documentation des rôles et des responsabilités du personnel. L'indépendance des rôles doit apparaître clairement dans l'organisation de la sécurité.
- 6) Mandat d'examen adressé à l'expert de la phase de réalisation (chap. 2.2.4.3 let. BB et CC) ;
- 7) Modifications du projet (chap. 2.3.1) ;
- 8) Documentation sur la manière dont il a été garanti que les règles techniques reconnues 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 dérogation par rapport aux prescriptions (chap. 2.2.4.2 pt. 11) ;
- 10) Obligations et la mise en œuvre des constats et des points en suspens :
 - Respect des charges de la DAP ;
 - Mise en œuvre des conclusions des rapports d'examen d'expert phases planification et réalisation ;
 - Réglage des points en suspens de la révision des dossiers de construction ;
 - Réglage des points en suspens de tous les rapports de contrôle d'usine.
- 11) Preuve du contrôle fonctionnel complet spécifique à l'installation : cette preuve peut par ex. être apportée par des rapports de contrôle d'usine et les documents de contrôle d'usine correspondants.
- 12) Preuve de la non-rétroactivité des mesures de protection en matière de cybersécurité et de leur mise en œuvre (chap. 1.14) ;
- 13) Installations provisoires (chap. 1.11) ;
- 14) Intégration technique et opérationnelle (chap. 1.12) :
 - a) Preuve de la mise en œuvre du SBAWB ;
 - b) Preuve de la non-rétroactivité, si elle n'est pas fournie à un niveau supérieur ;
 - c) Documents d'étude de projet, de montage et des prescriptions d'exploitation mis à jour et/ou nouvellement élaborés ;

- d) Fin de la formation ou des instructions du personnel d'exploitation, de conduite et de maintenance ;
- e) Preuve du respect des obligations découlant des HdS, y compris preuve de la mise en œuvre des exigences génériques ²⁷ des produits utilisés ayant une pertinence pour le GI.

15) Le cas échéant, liste des travaux restants :

- Évaluation de la pertinence pour la mise en service ;
- Responsabilités et délais.

16) Conclusion que :

- les IS sont construites conformément à la ou sont conformes aux plans approuvés, à l'exception des dérogations mentionnées au pt. 7) et
- sont conformes aux prescriptions déterminantes ou que des dérogations correspondantes ont été accordées, et peuvent être exploitées en toute sécurité.

La preuve de sécurité (y compris tous les documents de référence) doit être conservée et doit pouvoir être présentée à l'OFT dans le cadre de la surveillance de la sécurité pendant la phase d'exploitation (surveillance).

2.3.2.3 Programme et autorisation de mise en service

La sécurité doit être garantie à tout moment. Un programme doit être établi sous une forme appropriée pour la mise en service. Le niveau de détail requis dépend de l'ampleur du projet standard. Le programme doit énumérer

- Les travaux à effectuer
- Quand les travaux doivent être effectués.
- Comment et par qui ils sont contrôlés.

Avant qu'une IS puisse être mise en service, une autorisation de mise en service est nécessaire. Cette autorisation est une déclaration commune de l'expert et du GI confirmant que les conditions nécessaires à l'exploitation de l'IS sont remplies.

Avant d'accorder l'autorisation de mise en service, l'expert doit faire une évaluation de l'aptitude à la mise en service, qui se base sur les sources suivantes :

- Dossier de sécurité initial (chap. 2.3.2.2) ;
- Réglage des points en suspens de la preuve de sécurité initial ayant une pertinence pour la mise en service ;
- Résultats et évaluation de ses propres travaux de contrôle (chap. 2.3.5) ;
- Appréciation du contrôleur d'usine sur ses résultats de contrôle et confirmation par le contrôleur d'usine de l'achèvement complet de ses travaux (chap. 2.3.4) ;
- Confirmation qu'il n'y a pas de défauts importants pour la sécurité ou évaluation des défauts et des mesures d'exploitation nécessaires.

Le résultat de l'évaluation de l'expert est consigné lors de la mise en service dans le document "Autorisation de mise en service". En cas d'évaluation positive, ce document doit être signé, ce qui permet de mettre en service l'IS et de la remettre à l'exploitation.

2.3.3 Étude de projet

Par étude de projet, on entend la mise en œuvre spécifique à l'installation des fonctions techniques et opérationnelles requises en tenant compte des règles d'étude ou des schémas de principe ou des principes de construction spécifiques aux produits. La mise en œuvre des dossiers de construction dans l'étude de projet des différents produits doit être vérifiée et documentée.

2.3.4 Contrôle d'usine

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

La réalisation du contrôle d'usine s'effectue sur la base des documents de contrôle d'usine. Ils comprennent p. ex. les dossiers de construction et de contrôle, les schémas, les analyses des effets des modifications selon le chap. 1.12 pt. 5) qui sont nécessaires pour des 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 (à l'exception des tâches organisationnelles) en rapport avec l'objet de l'inspection.

Les constatations faites lors du contrôle d'usine doivent être documentées. Les défauts identifiés doivent être évalués avec le GI dans le cadre du contrôle d'usine. Le cas échéant, il faut décider si elles peuvent être compensées par des mesures d'exploitation et garantir ainsi 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 l'IS est soit exempt de défauts, soit qu'il reste des points en suspens suite au contrôle d'usine. Cette confirmation est nécessaire pour l'évaluation de l'aptitude de la IS à être mise en service (chap. 2.3.2.3).

Les faiblesses constatées lors du contrôle d'usine doivent être corrigées immédiatement et ensuite vérifiées par le contrôleur d'usine.

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

- Liste des documents de contrôle de l'usine ;

Identification univoque de l'objet du contrôle (p. ex. versions logicielles, release, sommes de contrôle) ;

- Environnement d'essai : laboratoire et/ou sur site (IS réelle) ;
- Les résultats de l'examen.

2.3.5 Examen d'expert phase de réalisation

L'examen d'expert phase réalisation doit être effectué conformément au mandat d'examen (chap. 1.9). L'élaboration et l'attribution de ce mandat d'examen sont effectuées par le GI.

Dans le cadre de la préparation de l'examen d'expert phase réalisation, l'expert doit définir le déroulement de l'examen et établir les documents nécessaires (p. ex. procès-verbal d'examen, procès-verbal, liste de contrôle). Cette préparation fait partie de son travail d'audit et devrait commencer suffisamment tôt.

L'examen d'expert phase réalisation comprend deux parties :

- Examen théorique des documents, notamment pour vérifier si les documents établis pendant la réalisation (p. ex. dossiers de construction et de contrôle, preuve de sécurité) correspondent aux documents PAP approuvés et si les charges découlant de la DAP, dans la mesure où elles concernent la sécurité, sont remplies.
- Vérification pratique de la réalisation technique de l'IS, notamment de son bon fonctionnement. Cette étape de contrôle nécessite la manipulation des produits utilisés sur l'IS.

Les détails concernant les tâches à accomplir dans le cadre de l'examen théorique et pratique figurent au chap. 2.2.4.3 let. B, CBC.

Si l'examen d'expert phase planification est effectué en même temps que l'examen d'expert phase réalisation en une seule étape, les documents PAP doivent également être examinés.

2.3.6 Travaux finaux

En règle générale, les travaux suivants sont prévus après la mise en service :

- Clôture des points en suspens du dossier de sécurité initial ;
- Régler les points en suspens de tous les rapports de contrôle d'usines et, le cas échéant, lever les mesures d'exploitation ;
- Mise en œuvre des charges issus du rapport d'examen d'expert phase réalisation ;
- Finalisation de la documentation comme les plans, les dossiers de construction, les Release notes ;
- Etablissement du dossier de sécurité final.

2.3.7 Documents à fournir et délais

Les documents suivants doivent être achevés dans les trois mois suivant la mise en service :

- Dossier de sécurité final ;
- Rapport d'examen de l'expert phase réalisation ;
- Prise de position du GI sur le rapport d'examen de l'expert phase réalisation.

La DAP définit quels documents doivent être remis à l'OFT jusqu'à quand après la MES par le GI.

3 Projet de développement

3.1 Principes du projet de développement

Contrairement au projet standard, les phases du cycle de vie selon la norme SN EN 50126-1 [15] doivent être parcourues dans le projet de développement (DE-OCF concernant l'art. 38, DE 38.1, ch. 1 [8]). Il est précisé ci-après quand et par qui les exigences des normes SN EN 50126-1 [15], SN EN 50129 [17] doivent être remplies (DE-OCF ad art. 38, DE 38.1, ch. 1.5 [8]). Une bonne compréhension de ces normes est nécessaire pour mettre en œuvre le contenu de ce chapitre.

3.1.1 Phases et déroulement du projet de développement

Le projet de développement comprend trois phases. Son déroulement est illustré sur la figure 9.

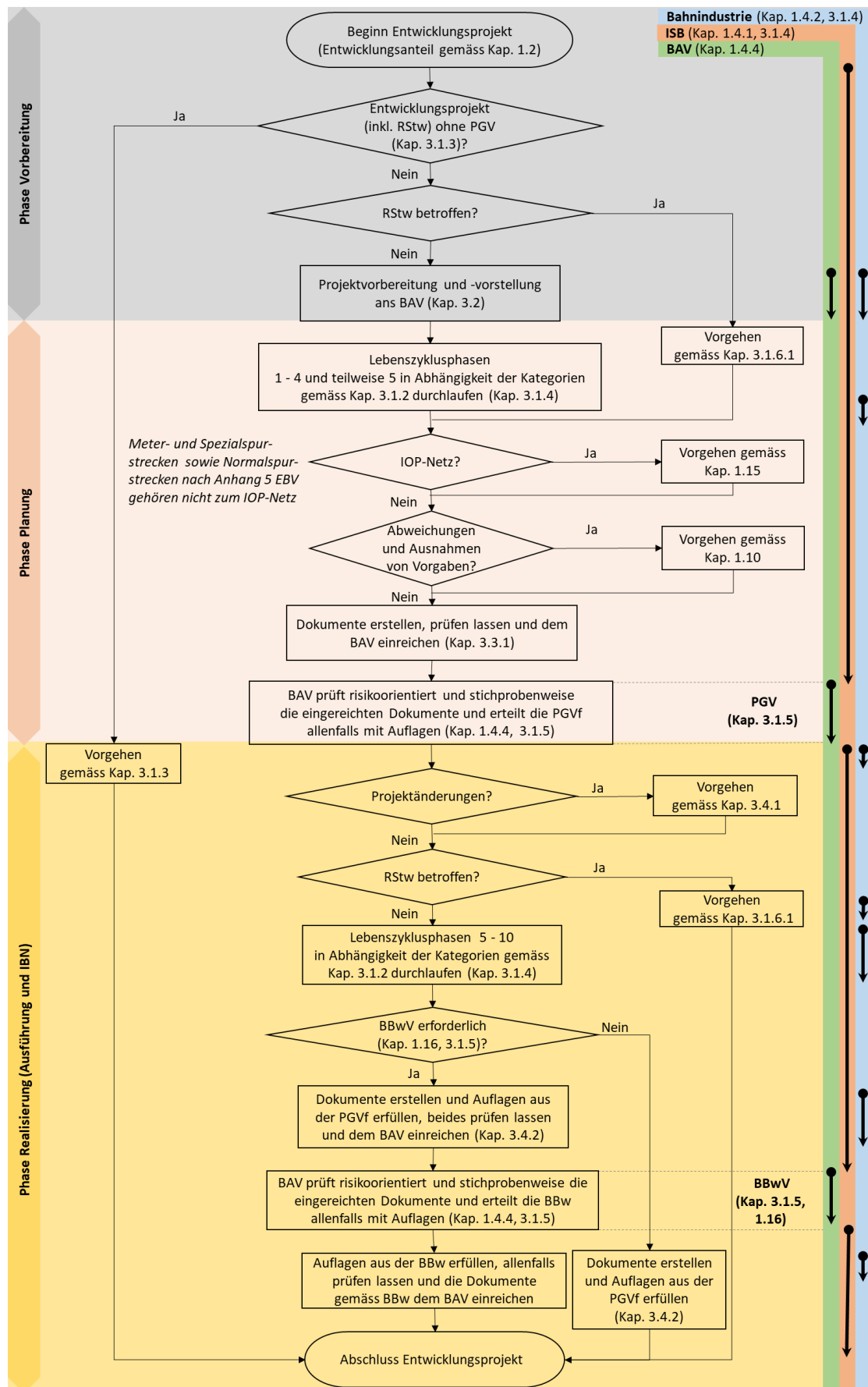


Figure 9 : Déroulement du projet de développement

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

Dans le projet de développement, on distingue trois catégories d'objets de développement :

- Première utilisation de produits nouvellement développés (le produit n'existe pas) :
 - Lors de la phase de planification, les exigences selon les chap. 3.1.4, 3.1.5, 3.1.7 et 3.3 doivent remplies.
 - Lors de la phase de réalisation, les exigences selon les chap. 3.1.4 et 3.4 doivent remplies.
- Première application de produits ultérieurement développés ou modifiés (un produit utilisé en Suisse est ultérieurement développés ou modifié) :
 - Il convient de déterminer, au moyen d'une analyse d'impact selon la norme SN EN 50126-1 [15], quelles phases du cycle de vie doivent être répétées en raison du développement ultérieure 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 dans les phases de planification et de réalisation.
 - Pour RStw les exigences du chap. 3.1.6 s'appliquent;
- Première utilisation de produits déjà développés (produit non utilisé jusqu'à présent en Suisse):
 - Dans la phase de planification, il faut démontrer que les produits déjà développés satisfont aux exigences du GI et que les tâches d'intégration technique et d'exploitation ont été accomplies au niveau de la planification. Pour cela, les phases 1 à 4 du cycle de vie selon les 3.1.4, 3.1.5, 3.1.7 et 3.3 doivent être parcourues.
 - Dans la phase de réalisation, il faut démontrer que les exigences des produits déjà développés sont remplies et que l'intégration technique et d'exploitation est achevée. Pour cela les exigences selon les chap. 3.1.4 et 3.4.3 doivent être remplies.
 - Dans le cas d'une procédure d'homologation de série en cours pour un produit générique, l'autorisation pour des tests en exploitation obtenue dans le cadre de cette procédure peut être prise en compte (chap. 1.7).
 - Les autorisations étrangères peuvent être prises en compte par l'OFT. Dans ce cas, au moins les documents ou informations suivants sont requis:
 - autorisations étrangères, y compris les documents qui y sont référencés;
 - Preuve de la conformité des objets du développement avec les objets des autorisations étrangères, y compris les SBAWB ;
 - Preuve de la mise en œuvre des prescriptions souveraines [1] - [10] pour les objets des autorisations étrangères selon le chap. 3.3.1.2.
 - Les certificats de conformité aux exigences des normes techniques (chap. 3.3.1.2) ne sont certes pas exigés dans les prescriptions souveraines [1] - [10], mais peuvent être pris en compte par l'OFT. Dans ce cas, au moins les documents ou informations suivants sont requis:
 - 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.
 - Preuve du respect des prescriptions souveraines [1] - [10] pour les objets du certificat selon le chap. 3.3.1.2.

3.1.3 Projets de développement sans PAP

La première application 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, pour autant qu'aucun intérêt de tiers digne de protection ne soit touché, que les effets sur le territoire et l'environnement soient insignifiants et que l'un des critères suivants soit rempli :

- (1) Il s'agit de modifications strictement techniques (par ex. correction d'erreurs, obsolescence de composants, modifications du processus de fabrication).
- (2) Le développement de fonctions, par ex. au moyen d'éléments librement configurables, est effectué par l'industrie ferroviaire conformément aux spécifications de processus correspondantes, qui satisfont aux exigences des normes SN EN 50126-1 [15], SN EN 50129 [17] et SN EN 50716 [39], pour autant que celles-ci soient 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) Confirmation du GI que la première application de produits ultérieurement développés ou modifiés n'altère pas sensiblement l'aspect extérieur du site, n'affecte pas les intérêts dignes de protection de tiers et n'ait que des effets minimes sur l'aménagement du territoire et sur l'environnement;
- b) Pour le critère(1) : respect des critères pour modifications strictement techniques selon l'annexe A4.3.1.2 de la Dir. HdS [14] par l'industrie ferroviaire et évaluation par l'expert des phases 5 à 10 du cycle de vie ou par le validateur de la phase 9 du cycle de vie (pour les fonctions BI) ;
- c) Pour le critère(2) : respect des spécifications de processus relatives à la fonction développée par l'industrie ferroviaire et évaluation par l'expert des phases 5 à 10 du cycle de vie ou par le validateur de la phase 9 du cycle de vie (pour les fonctions BI).
- d) Preuve de la mise en œuvre des prescriptions souveraines pertinentes pour le développement [1] - [10] par le GI avec l'industrie ferroviaire (chap. 3.3.1.2) ;

Dans la mesure où il s'agit d'une combinaison de projet standard et de projet de développement, la mise en œuvre des points a) - c) peut être démontrée dans le dossier de sécurité du projet standard dans un chapitre distinct. Sinon, la mise en œuvre des points a) -c) doit être démontrée dans le dossier de sécurité pour la première application.

Si des RStw sont concernés, il est défini au chap.3.1.6 quand aucune PAP n'est nécessaire et quelles exigences s'applique à la démonstration de sécurité.

Les documents de la démonstration de la sécurité ne doivent pas être remis 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 lors de la phase d'exploitation (surveillance).

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

Pour l'objet de développement²⁹, les phases 1 à 10 du cycle de vie selon SN EN 50126-1 [15] doivent en général être parcourues dans les phases de planification et de réalisation du projet de développement.

Le passage par les phases 11 à 12 du cycle de vie ne fait pas partie du projet de développement. Ces phases du cycle de vie sont néanmoins mentionnées car le projet de développement fournit pour elles des informations concernant l'exploitation, la maintenance, la surveillance des performances et la mise hors service.

La figure 10 présente le cycle de vie de l'objet en développement selon SN EN 50126-1 [15]. La phase de planification comprend les phases 1 - 4 et en partie 5 du cycle de vie. La phase de réalisation comprend les phases 5 - 10 du cycle de vie. Les trois flèches indiquent la coordination de contenu entre le GI et l'industrie ferroviaire.

²⁹ Système au sens de la norme SN EN 50126-1 [15]

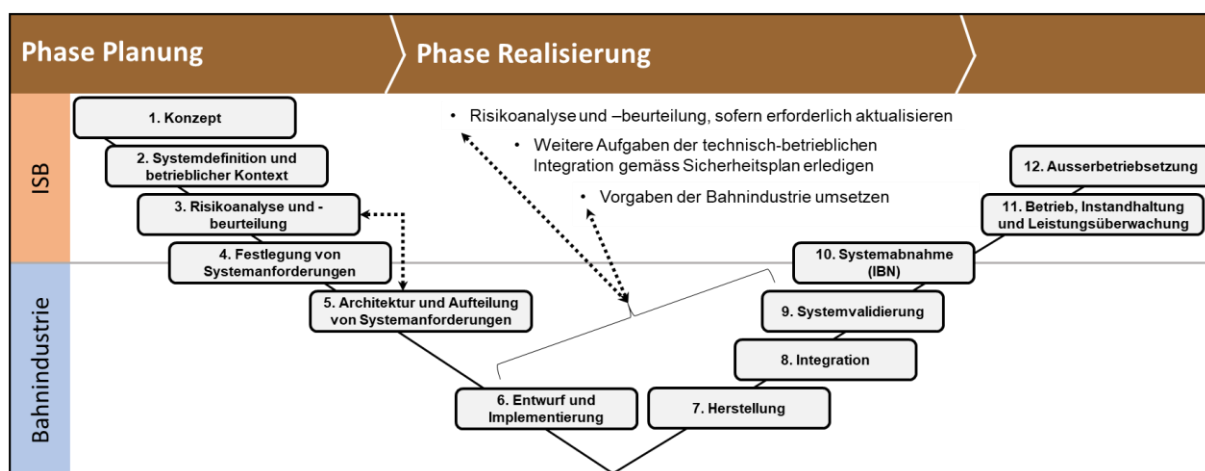


Figure 10 : Cycle de vie de l'objet de développement

Les phases 1 à 10 du cycle de vie doivent être documentées conformément à SN EN 50126-1 [15]. Il faut montrer que les activités de sécurité requises ont été réalisées, que les livrables nécessaires sont disponibles et que les objectifs des phases de cycle de vie correspondantes ont été atteints. Les exigences de la SN EN 50126-1 [15] s'appliquent à cet effet, avec les concrétisations et compléments suivants :

- 1) Le GI doit réaliser les activités de sécurité conformément à SN EN 50126-1 [15] pour les phases 1 à 4 du cycle de vie. Idéalement, l'industrie ferroviaire est déjà impliquée dans ces phases du cycle de vie.
- 2) Les prescriptions déterminantes doivent être prises en compte (chap.1.3).
- 3) Les exigences relatives à l'indépendance et à la compétence spécialisé des rôles selon SN EN 50126-2 [16] s'appliquent. Dans ce contexte, les experts doivent remplir les exigences selon le chap. 1.4.3.
- 4) Le plan de sécurité doit être établi dans la phase 2 du cycle de vie. Celui-ci doit indiquer les activités de sécurité à réaliser afin de satisfaire aux exigences déterminantes. Des informations doivent être fournies pour chaque exigence du plan de sécurité de la SN EN 50126-1 [15]. Pour certaines exigences, des concrétisations et des compléments sont apportés ci-après.

— Planification des activités de sécurité : La forme tabulaire selon SN EN 50126-1 [15] 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 une analyse et une l'évaluation du risque conformément à la Dir. IS. | Prénom Nom | - Concept - Définition du système et contexte opérationnel | - Analyse et évaluation du risque - Registre des dangers |
| x+1 | 3 | Etablir un plan d'examen d'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 d'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 art. et ch. pertinents des prescriptions souveraines et 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 d'essai de qualification de sécurité conformément à la Dir. IS. | Prénom Nom | - Concept - Définition du système et contexte opérationnel - Analyse et évaluation du risque - Registre des dangers | Concept d'essai de qualification de sécurité |

Tableau 7 : Exemple de planification des activités de sécurité

- Le cycle de vie de l'objet de développement est représenté sur la figure 10. En fonction des catégories d'objets en développement mentionnées au chap.3.1.2 , il convient de définir les phases du cycle de vie à parcourir.
 - Vérification : procédure selon le point ;12)
 - Validation : procédure selon le point 13) ;
 - Processus pour l'autorisation de sécurité : procédure selon le chap. 3.1.5
- Outre les concrétisations ci-dessus des exigences de la SN EN 50126-1 [15] , la planification des points suivants doit être définie dans le plan de sécurité :
- Preuve de la mise en œuvre des prescriptions souveraines [1] - [10] (chap. 3.3.1.2) ;
 - d'autres tâches d'intégration technique et d'exploitation (chap. 1.12) ;
 - Points clés concernant la cybersécurité (chap. 1.14) ;
 - Établir le dossier de sécurité pour la première application (chap.3.4.2.2) ;
- 5) Dans la phase 2 du cycle de vie, le plan FDM doit être établi. Au moment de son élaboration, l'accent est mis sur la déduction des exigences FDM selon SN EN 50126-1 [15]. Le plan FDM peut être établi séparément ou être regroupé avec le plan de sécurité dans un plan FDMS.
- D'autres contenus du plan FDM conformément aux 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, conformément au point 8).
- 6) Dans la phase 3 du cycle de vie, l'analyse et l'évaluation du risque doivent être effectuées conformément au chap. 1.8. Elle se réfère à l'objet du développement défini dans les phases 1 - 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 nouveaux dangers sont identifiés dans le processus de maîtrise des situations dangereuses (SN EN 50126-2 [16]). Les mesures de maîtrise des situations dangereuses ou les contraintes définies pour l'utilisation des fonctions de l'objet de développement peuvent donner lieu à des SBAWB adressés au GI.
 - à partir de la phase 5 du cycle de vie, mettre à jour le plan de sécurité et le plan FDM ou le plan FDMS pour les phases 6 à 9 du cycle de vie ou de les compléter par des documents propres. Il convient également de définir comment garantir que les prescriptions déterminantes issues du développement selon la norme SN EN 50126-1 [15] soient transmises aux phases 11 - 12 du cycle de vie (concernant l'exploitation, la maintenance, la surveillance des performances et la mise hors service).
 - établir la documentation relative à la planification du SW conformément au tableau A.1 de la norme 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 [17];
- prouver le développement du logiciel conformément à la SN EN 50716 [39]. Les prescriptions relatives aux outils de développement de SW se trouvent dans la norme SN EN 50716 [39]. Pour tous les autres outils, il convient de tenir compte des prescriptions selon la norme SN EN 50129 [17].
- établir et de mettre à jour le dossier de sécurité pour l'application spécifique. Ce dossier de sécurité peut s'appuyer sur des dossiers de sécurité pour un produit générique et/ou une application générique. Ces dossiers de sécurité doivent être conformes aux exigences de la SN EN 50129 [17] en termes de structure et de contenu.
- transmettre au GI toutes les prescriptions nécessaires au déroulement des phases 11 - 12 du cycle de vie (concernant l'exploitation, la maintenance, la performance et la mise hors service selon la SN EN 50126-1 [15]).

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 [16]) au cas où :
 - des dangers supplémentaires sont identifiés pour l'objet du développement ;
 - il est nécessaire d'établir des nouvelles prescriptions d'exploitation ;
 - 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 technique et d'exploitation conformément au plan de sécurité pt. 4) ;
- établir et de mettre à jour le dossier de sécurité pour la première application conformément au chap. 3.4.2.2 .

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.

12) Vérification :

- A la fin de chaque phase du cycle de vie, la vérification doit être effectuée et documentée conformément à la SN EN 50126-1 [15]. Idéalement, les activités de vérification à effectuer sont définies dans le plan de vérification et les résultats de la vérification sont documentés dans le rapport de vérification. La rédaction et l'attribution du mandat de vérification sont effectuées soit par le GI, soit par l'industrie ferroviaire. Les informations contenues dans les points 1) - 11) permettent de voir qui doit respectivement établir et délivrer ce mandat. Dans le mandat de vérification, il faut tenir compte des exigences selon le tableau 8, qui proviennent des SN EN 50126-1 [15] et SN EN 50126-2 [17].

| Exigences pour le chargé de vérification | |
|--|--|
| 1. | Confirmer l'indépendance selon SN EN 50126-2 [16]. |
| 2. | Confirmer les compétences spécialisées selon SN EN 50126-2 [16]. |
| 3. | Établir un plan de vérification en précisant ce qui doit être vérifié, ainsi que le type de processus (par ex. revue, analyse) et d'essais à mettre en œuvre pour la démonstration. |
| 4. | Effectuer la vérification conformément au plan de vérification. Dans les phases du cycle de vie, les éléments suivants doivent être vérifiés : <ul style="list-style-type: none"> - respect des exigences définies dans la SN EN 50126-1 [15] par phase du cycle de vie pour les activités et les livrables requis ; - exactitude et adéquation de l'analyse de la FDMS, si cela est spécifié; - la conformité des livrables requis pour la phase du cycle de vie avec ceux des phases antérieures du cycle de vie; - l'adéquation des procédures, outils et techniques utilisés pendant la phase du cycle de vie, si cela est spécifié ; - l'exactitude, la cohérence et l'adéquation des spécifications d'essai et des essais exécutés, le cas échéant. - tâches de vérification spécifiques des phases 6 et 8 du cycle de vie selon SN EN 50126-1 [15]. |
| 5. | Enregistrer les écarts constatés pendant 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. | Rédiger le rapport de vérification. Idéalement, la vérification est documentée dans un rapport de vérification qui contient un chapitre 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 soit par le chargé de vérification, soit, 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. Le plan de validation de la sécurité peut être établi séparément ou être regroupé 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, qui proviennent des SN EN 50126-1 [15] et SN EN 50126-2 [16]. Elles sont harmonisées avec les exigences relatives à l'expert (chap. 3.3.1.3 let. A) afin d'éviter les doubles vérifications.

| Exigences pour le chargé de validation |
|--|
| 1. Confirmer l'indépendance selon SN EN 50126-2 [16] . |
| 2. Confirmer les compétences spécialisées selon SN EN 50126-2 [16] . |
| 3. Etablir un plan de validation selon SN EN 50126-1 [15] et le coordonner avec l'expert. |
| 4. Effectuer la validation conformément au plan de validation et justifier les éventuels écarts par rapport au plan de validation. |
| 5. Vérifier la conformité du processus et des résultats du développement par rapport aux exigences de la SN EN 50126-1 [15]. |
| 6. Prendre en compte les concrétisations et les compléments aux ch. 4), 5) et 12) 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. Consigner les écarts constatés lors de la validation, les classer en fonction du risque et les transmettre aux responsables de la gestion des modifications et de la prise de décision. |
| 10. Etablir un rapport de validation conformément à la SN EN 50126-1 [15] . |

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 conformément au plan de validation et documentée dans le rapport de validation. L'établissement et l'attribution du mandat de validation sont effectués par l'industrie ferroviaire.
 - Les constats issus des rapports de validation doivent être traités et réexaminés soit par le chargé de validation, soit, le cas échéant, par l'expert concerné.
 - La validation peut être effectuée par plus d'un chargé de validation.
- 14) Examen d'expert :
- Les explications concernant l'examen d'expert se trouvent au chap. 1.9.
 - L'examen d'expert des phases 1 à 4 du cycle de vie doit toujours être effectué. L'établissement et l'attribution du mandat d'examen sont effectués par le GI conformément aux spécifications du chap. 3.3.1.3 let. A. L'expert doit établir un plan d'examen³⁰ pour la mise en œuvre du mandat d'examen. L'examen d'expert doit être effectué conformément au plan d'examen et documenté dans le rapport d'examen d'expert phases 1 - 4 du cycle de vie selon le chap. 1.6.3.
 - Si aucune exigence de sécurité n'a été posée aux fonctions ou le taux d'occurrence maximal acceptable de danger (THR) $\geq 10^{-5}h^{-1}$ a été défini, l'expert confirme l'allocation de la BI (SN EN 50126-2 [16]) dans le rapport d'examen d'expert phases 1 à 4 du cycle de vie. Si nécessaire, l'expert peut à cet effet prendre connaissance de l'architecture prévue de la phase 5 de cycle de vie ou il peut fixer des conditions cadre concernant l'architecture ou la mise en œuvre technique en tant que charges.
- Si l'expert confirme uniquement la BI pour toutes les fonctions du projet de développement, aucun autre examen d'expert n'est exigé (SN EN 50126-2 [16]).
- Chaque fois qu'un examen d'expert des phases 5 à 10 du cycle de vie est nécessaire, il est effectué avant la MES³¹. L'établissement et l'attribution du mandat d'examen d'expert sont effectués par l'industrie ferroviaire conformément aux exigences du 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 d'expert doit être réalisé conformément au plan d'examen et documenté dans le rapport d'examen d'expert phases 5 - 10 du cycle de vie selon le chap. 1.6.3.
 - L'examen d'expert de la première application fait suite à l'examen d'expert des phases 1 à 4 du cycle de vie. Il doit prendre en compte les résultats pertinents de l'examen d'expert des phases 5 à 10 du cycle de vie pour la première application. L'élaboration et l'attribution du mandat d'examen sont effectuées par le GI conformément aux exigences du chap.3.3.1.3

³⁰ plan l'évaluation indépendante de la sécurité selon SN EN 50126-1 [15]

³¹ acceptation du système selon SN EN 50126-1 [15]

let. C. L'expert doit établir un plan d'examen pour la mise en œuvre du mandat d'examen. L'examen d'expert doit être réalisé conformément au plan d'examen et documenté dans le rapport d'examen d'expert première application selon le chap. 1.6.3.

- Dans la mesure où l'OFT ordonne une AE pour la MES, les experts des phases 5 à 10 du cycle de vie et de la première application doivent documenter le résultat de leur examen dans leurs rapports d'examen d'expert avant la MES dans de la phase 9 du cycle de vie.
- 15) Pour l'objet de développement avec exclusivement des fonctions de BI, au moins les informations suivantes sont nécessaires selon les exigences des SN EN 50126-2 ü16], SN EN 50129 [17] et SN EN 50716 [39] dans les phases 5 à 10 du cycle de vie:
- Exigences organisationnelles : Il faut démontrer que l'organisation définie selon le plan de sécurité répond aux exigences de la SN EN 50129 [17] en ce qui concerne l'indépendance des rôles pour la 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
 - formations nécessaires ou les instructions du personnel d'exploitation, roulant et d'entretien ont eu lieu ;
 - 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 pt. 4).
 - Preuve de la sécurité : l'industrie ferroviaire doit :
 - démontrer le respect des exigences système et de sécurité de ces fonctions (par ex. en faisant référence à un rapport de validation) ;
 - justifier le respect du taux de défaillance fonctionnelle tolérable (TFFR) ;
 - définir les conditions d'environnement et les SBAWB; les hypothèses formulées lors du processus d'allocation des exigences de sécurité doivent être consignées en tant que SBAWB.
 - définir des mesures adéquates de management des pannes (diagnostics, maintenance, formation du GI ;
 - démontrer la non-intrusion (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 essais de qualification de sécurité (chap. 3.4.3).
 - Si nécessaire, l'industrie ferroviaire doit soutenir le GI lors des tests en exploitation (chap. 3.4.2.4).

3.1.5 Types de procédures

Les types de procédure possibles sont représentés sur la figure 11. Le type de procédure est déterminé en fonction des trois étapes suivantes :

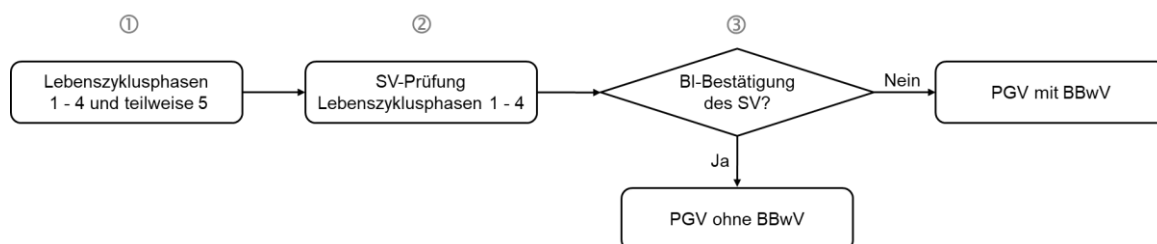


Figure 11: Types de procédé

- ① Le passage par des phases 1 à 4 du cycle de vie et en partie 5 doit être documenté conformément au chap. 3.1.4 et 3.3.1 doit être documenté.

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

- ② Les documents selon ① doivent être contrôlés par l'expert des phases 1 à 4 du cycle de vie selon le 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 sur RStw et exigences pour la démonstration de la sécurité

Pour les développements sur RStw, la procédure selon la figure 12 s'applique. Les étapes correspondantes sont expliquées ci-dessous.

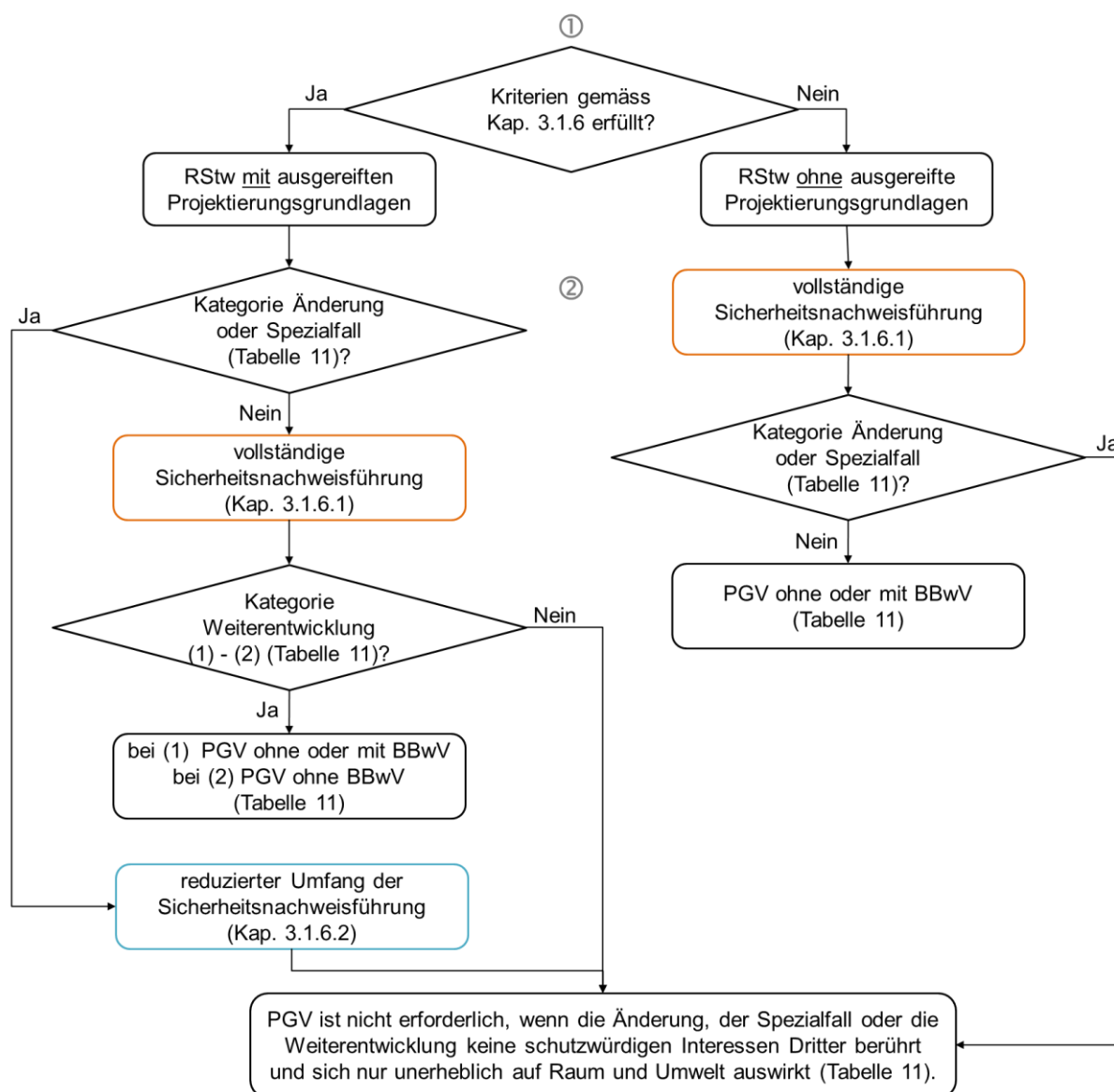


Figure 12 : Procédure pour les développements sur RStw

- ① Déterminer s'il s'agit d'un RStw avec des bases de conception éprouvées ou non. Pour cela, le GI doit vérifier que les critères suivants sont remplis :

- a) RStw s'appuie sur des bases de conception éprouvées, c'est-à-dire sur des schémas de principe ou des principes de construction avec des cas définis et des fonctions de base.
- b) RStw est par ex. entretenu et développé par l'industrie ferroviaire ou le centre de compétence du GI. Les bases actuelles de conception sont par ex. consignées dans un répertoire.

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

- ② Les développements sur 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 révélé ;
- aucun développement sur les interfaces (par ex. systèmes de contrôle-commande) n'est autorisé ;
- aucun écart par rapport aux fonctions de base n'est autorisé ;
- les contrôles de travail et de position de base sont installés aux endroits prévus à cet effet ;
- poste d'enclenchement à plan de circuits: les fonctions ne peuvent être intégrées que dans des circuits déjà prévus à cet effet ;
- poste d'enclenchement à plan de verrouillage : les nouveaux verrouillages ne peuvent être intégrés que dans la logique de verrouillage déjà existante.
- Les principes de commande et d'exclusion mutuelle concernant les différentes possibilités de commande doivent être maintenus.

Un circuit qui est déjà utilisé dans une installation spécifique chez un GP et qui dispose d'un dossier de sécurité y compris un rapport d'examen d'expert peut être utilisé comme base de conception.

Autrement, il s'agit de la catégorie développement ultérieur.

En fonction de la distinction selon ① et des catégories mentionnées ici, les exigences pour la démonstration de la sécurité sont prescrites. Des Informations complémentaires se trouvent dans le tableau 10.

| Catégorie | RStw <u>avec</u> des bases de conception éprouvées | RStw <u>sans</u> bases de conceptions éprouvées |
|---------------------|--|---|
| Modification | Souvent, des modifications non fonctionnelles doivent être apportées aux IS existantes. La raison en est, par ex., qu'il n'y a plus de contact de relais libre. Sur la base du circuit existant, on décide où la prise peut être réalisée sans modifier la fonction. Si le circuit de principe ne couvre pas exactement la topologie des voies, il doit être adapté en fonction de l'installation. | |
| | Démonstration de la sécurité | |
| | étendue réduite selon chap. 3.1.6.2 | entièrement selon le chap. 3.1.6.1 |
| | PAP | |
| | La PAP n'est pas requise si la modification n'altère 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. | |
| Cas spécial | Les fonctions d'un RStw qui sont déjà utilisées par d'autres RStw du même type sont considérées comme des cas spéciaux. | |
| | Démonstration de la sécurité | |
| | étendue réduite selon chap. 3.1.6.2 | entièrement selon le chap. 3.1.6.1 |

| Catégorie | RStw <u>avec</u> des bases de conception éprouvées | RStw <u>sans</u> bases de conceptions éprouvées |
|--------------------------------|--|---|
| Développement ultérieur | PAP | |
| | La PAP n'est pas requise si le cas spécial n'altère 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. | |
| | Le développement ultérieur comprend par. ex. : | |
| | (1) développement de nouvelles fonctions et/ou de nouvelles interfaces ; | |
| | (2) Reproduction d'une fonction connue (par exemple, 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 de RStw et qui doit être utilisée pour la première fois, par ex. dans un RStw. | |
| | (3) Transformation d'une fonction en circuits de principe qui ont déjà été utilisés plusieurs fois. | |
| | Démonstration de la sécurité | |
| | entièrement selon le chap. 3.1.6.1 | |
| | PAP, PAE | |
| | <ul style="list-style-type: none"> Pour (1) , une PAP est requise (chap. 1.5). Une PAE peut être requise (chap. 1.16) ; Pour (2) , une PAP sans PAE est requise; Pour (3) ou les cas non couverts ici, une PAP n'est pas requise si le développement ultérieur n'altère 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. | une PAP est requise ; une PAE peut être requise (chap. 1.16). |

Tableau 10 : Détails concernant les développements sur RStw

Le respect des exigences pour la démonstration de la sécurité des RStw pour les phases de planification et de réalisation peut être démontré dans les documents du projet standard (rapport de sécurité, dossier de sécurité, rapport de contrôle d'usine, rapport d'examen d'expert) dans un chapitre distinct ou dans des documents séparés. Les exigences formelles selon le chap. 1.1.3 doivent être prises en compte.

3.1.6.1 Démonstration complète de la sécurité

Selon le tableau 11 , la démonstration complète de la sécurité est requise dans les phases de planification et de réalisation pour

- RStw avec des bases de conception éprouvées en cas de développement ultérieur ;
- RStw sans bases de conception éprouvées en cas de développement ultérieur ou de modification.

Phase de planification

1) Le GI doit :

- décrire développement ultérieur ou de modification susmentionnée
- prouver 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 du personnel impliqué ;

- coordonner le mandat de développement ultérieur ou de modification avec l'industrie ferroviaire ou le centre de compétence du GI ;
- établir et attribuer le mandat d'examen à l'expert pour les phases de planification et de réalisation. En règle générale, l'expert doit effectuer les tâches selon le tableau 11.

| Phase de planification |
|---|
| A1. Examen de la description du développement ultérieur ou de la modification ; |
| A2. Examen de l'analyse et de l'évaluation du risque ainsi que de toutes les exigences définies ; |
| A3. Examiner si les bases de conception référencées sont adaptées au développement ultérieur ou à la modification ; |
| A4. Examiner la preuve de la mise en œuvre des prescriptions souveraines [1] - [10] (chap. 3.3.1.2) ; |
| A5. Examiner si les écarts par rapport aux spécifications et la demande d'autorisation exceptionnelle sont entièrement documentés (chap. 1.10). Examen et documentation de l'adéquation des écarts ; |
| A6. Examiner l'analyse et évaluation du risque d'éventuels écarts par rapport aux prescriptions souveraines [1] - [10] ; |
| A7. Examen des rôles, des responsabilités et des compétences professionnelles du personnel impliqué ; |
| A8. Documenter l'activité d'examen (chap. 1.6.3) ; |
| Phase de réalisation |
| B1. Examiner si les tâches d'intégration technique et d'exploitation ont été effectuées (chap. 1.12) ; |
| B2. Examiner si les charges de la DAP sont réglées, dans la mesure où elles concernent la sécurité ; |
| B3. Examiner si les résultats de l'examen d'expert de la phase planification ont été pris en compte. |
| B4. Examiner que les modifications apportées au projet sont documentées et conformes aux spécifications (chap. 3.4) ; |
| B5. Contrôle des fonctions des IS, y compris la réaction en cas de panne, ainsi que l'interaction des différents produits entre eux, y compris les IS voisines ; |
| B6. Examen des feuilles de circuit ; |
| B7. Examiner que : <ul style="list-style-type: none"> - les exigences de la phase de planification sont mises en œuvre ; - la sécurité en cas de panne de chaque circuit concerné est démontrée en cas de défaillance, de dérangement et dysfonctionnement ; - les impacts sur les prescriptions d'exploitation sont indiqués - les impacts sur les interfaces sont indiqués ; - les éventuels SBAWB sont conformes aux exigences de la SN EN 50129 [17] ; - les documents de contrôle pour le contrôle d'usine sont disponibles ; - les constats du rapport de contrôle d'usine sont mis en œuvre ; |
| B8. Évaluation de l'adéquation et de l'exhaustivité du contrôle d'usine en ce qui concerne la sécurité. |
| B9. Documenter l'activité d'examen (chap. 1.6.3). Dans la mesure où l'OFT ordonne une AE pour la MES, l'expert doit documenter le résultat de son examen avant la MES dans le rapport d'examen d'expert. |

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, le cas échéant dossier de sécurité, y compris le rapport d'examen d'expert des circuits ;
 - 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 le résultat de son examen conformément au chap. 1.6.3.

Phase de réalisation

- 1) Le GI doit :
 - montrer que l'intégration technique et opérationnelle est achevée (chap. 1.12) ;
 - prouver que les charge de la DAP ont été remplies ;
 - prouver que les points en suspens du rapport de contrôle d'usine ont été réglés ;
 - prouver que les points en suspens du rapport d'examen d'expert de la phase de planification ont été réglés ;
 - documenter les modifications du projet (chap.3.4) ;
 - évaluer les points en suspens en fonction de leur pertinence pour la MES, définir les responsabilités et les délais pour leur résolution ;
- 2) L'industrie ferroviaire ou le centre de compétence du GI doit :
 - mettre en œuvre les exigences de la phase de planification ;
 - montrer à quels endroits l'adaptation du circuit a été effectuée par rapport aux bases de conception ;
 - démontrer la sécurité en cas de panne de chaque circuit concerné est démontrée en cas de défaillance, de dérangement et dysfonctionnement³² ;
 - indiquer les impacts sur les prescriptions d'exploitation. Les clarifications avec l'exploitation et l'entretien doivent être indiquées ;
 - indiquer l'impact sur les interfaces ;
 - définir d'éventuels SBAWB (si nécessaire) ; les exigences de la SN EN 50129 [17] doivent être prises en compte ;
 - démontrer la non-intrusion 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 le résultat de son contrôle dans le rapport de contrôle d'usine conformément au chap. 2.4.3 .
- 4) Les constats issus du rapport de contrôle d'usine doivent être réexaminées 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 le résultat de son examen conformément au chap. 1.6.3.
- 6) essais de qualification de sécurité : la procédure au sens du chap.3.4.3 s'applique.
- 7) MES : La procédure au sens du chap.2.3.2.3 s'applique.

3.1.6.2 Etendue réduite de la démonstration de la sécurité

Selon le Tableau 10 : , l'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 conceptions sont éprouvées en cas de modification ou de cas spécial.

Pour la modification ou le cas spécial susmentionné, il n'est pas nécessaire, du point de vue de la démonstration de la sécurité, de faire une distinction entre les phases de planification et de réalisation. Pour la démonstration de la sécurité, les points suivants doivent être pris en compte :

- 1) Le GI doit décrire la modification susmentionnée ou le cas spécial. Il doit être clairement indiqué à quels endroits l'adaptation du circuit a été effectuée par rapport aux bases de conception.

³² par ex., l'activation ou la désactivation intempestive d'un contact de relais.

- 2) Si nécessaire, l'industrie ferroviaire ou le centre de compétence du GI assiste le GI pour la modification ou le cas spécial.
- 3) l'expert doit examiner l'adaptation du circuit par rapport aux bases de conception et documenter le résultat de son examen conformément au chap. 1.6.3.
- 4) MES : La procédure au sens du chap.2.3.2.3 s'applique.

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

Les dépendances entre les phases du cycle de vie, les types de procédures, la documentation et les délais de l'objet de développement sont représentées dans la figure 13. Pour plus de détails sur les phases du cycle de vie, les types de procédures et la documentation, voir les chap. 3.1.4, 3.1.5, 3.3 et 0. Des informations complémentaires sont fournies ci-après pour les types de procédures et les délais.

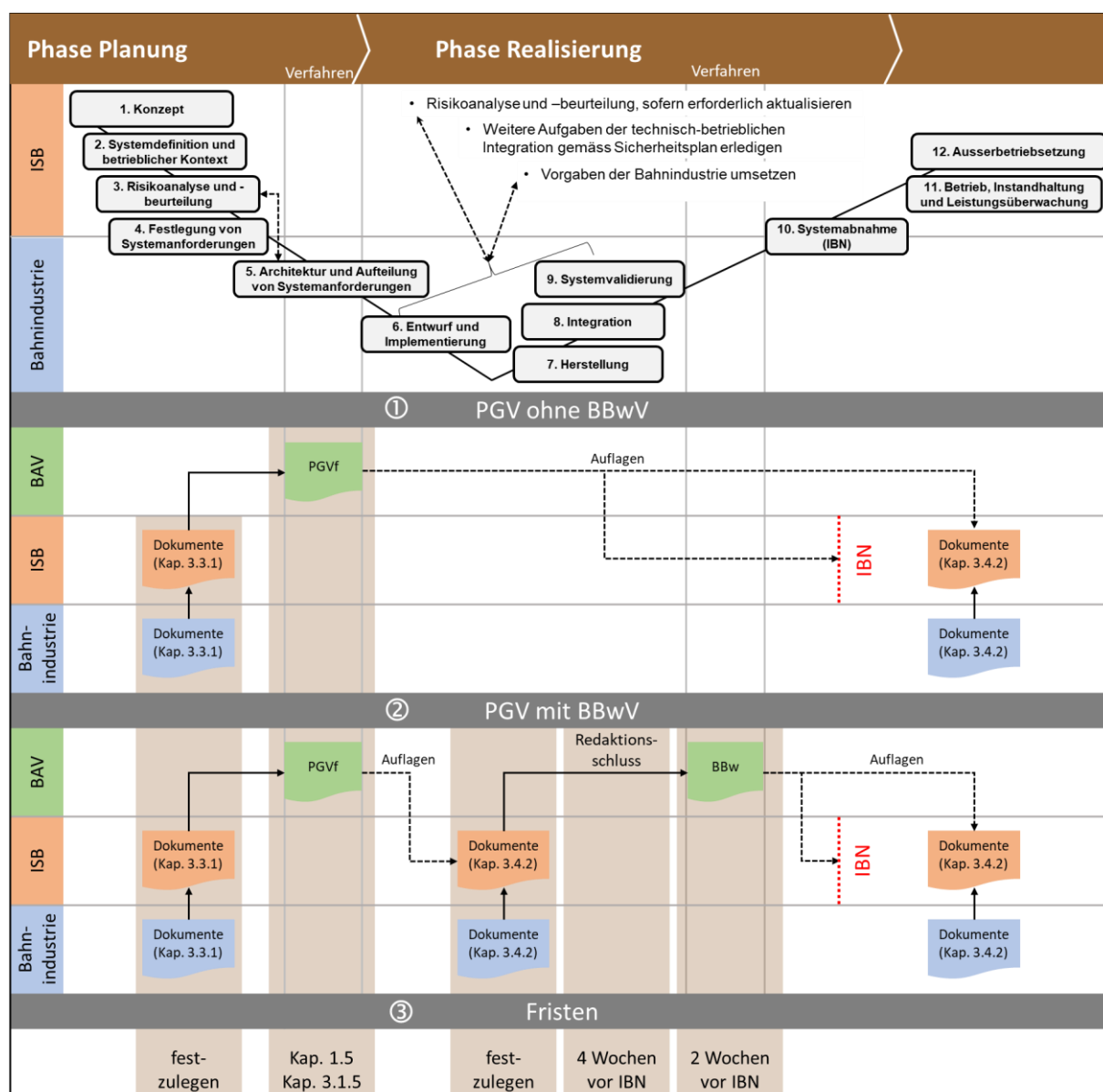


Figure 13 : Aperçu des phases du cycle de vie, des types de procédures, de la documentation et des délais

- ① La PAP sans PAE s'applique, conformément au chap. 3.1.5, aux projets de développement comportant exclusivement des fonctionnalités BI. L'OFT octroie la DAP dans la phase 5 du cycle de vie.
- ② La PAP avec PAE s'applique, conformément au chap. 3.1.5, aux projets de développement dotés de fonctionnalités SIL. L'OFT octroie la DAP avec l'AE ordonnée dans la phase 5 du cycle de vie.
- ③ La date de remise des documents PAP doit être fixée par le GI. La date de remise des documents pour la PAE doit être fixée par le GI et coordonnée avec l'OFT. Il en va de même pour les éventuels soumissions ultérieures. En règle générale, l'OFT accepte la dernière remise complémentaire quatre semaines avant la MES (délai de rédaction pour le GI). Deux semaines avant la MES, l'OFT octroi l'AE. Le GI peut ainsi utiliser les deux semaines restantes jusqu'à la MES pour remplir les éventuelles charges.

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

3.2 Phase de préparation du projet de développement

On passe par la phase de préparation 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 le KIP³³ avant de soumettre les documents du projet de développement. La KIP organise ensuite une concertation commune et garantit la consultation des sections spécialisées concernées de l'OFT. Dans l'idéal, les parties prenantes de l'industrie ferroviaire y participent également.

Les exigences supérieures de l'OFT s'appliquent à cette concertation : les projets de développement ne doivent pas être évalués uniquement en fonction de la technique, mais en tenant compte de critères globaux tels que le rapport coût/utilité et/ou la conformité à la stratégie.

La concertation a pour but de lancer le projet de développement dans les règles de l'art. Elle porte notamment sur les points suivants, qui font partie du plan de sécurité :

- prescriptions déterminantes (chap.1.3) et les éventuels dérogations (chap. 1.10),
- analyse et évaluation du risque (chap. 1.8) ;
- points clés concernant la cybersécurité (chap. 1.14) ;
- adéquation des experts et mandats d'examen confiés aux experts (chap.3.3.1.3) ;
- Définition du type de procédure (chap.3.1.5) ;
- Procédure d'élaboration de la première application preuve de sécurité (chap.3.4.2.2) ;
- Essais de qualification de sécurité et tests en exploitation (chap. 3.4.3) ;
- Si *d'autres procédures* sont appliquées conformément au chapitre 1.1.2, la PAP prévoit que le développement de l'objet doit être suffisamment avancé pour que les informations spécifiques à l'installation soient prises en compte dans les documents de la phase de planification du projet de développement (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 du projet de développement sont énumérés et attribués aux phases du cycle de vie. En complément, des renvois indiquent où trouver des explications sur les exigences relatives au contenu des documents (art. 3 al. 1 - 2 OPAPIF [5]). Lors de l'élaboration de ces documents,

³³ KIP@bav.admin.ch

les exigences formelles selon le chap. 1.1.3 et les exigences relatives à la documentation de FDMS de la SN EN 50126-1 [15] doivent être mises en œuvre.

Les documents mentionnés dans le tableau 12 doivent être soumis à l'OFT. Si le GI estime que certains des documents mentionnés ne sont pas pertinents pour le projet de développement concret, elle peut renoncer à les soumettre en justifiant brièvement sa décision (p. ex. "non concerné").

Si des documents tels que la demande d'approbation des plans, le condensé du projet et la demande d'octroi d'une dérogation sont établis dans le cadre d'un projet standard ou d'un projet global, il n'est alors pas nécessaire d'établir à nouveau ces documents séparément pour le projet de développement.

Les exigences relatives au contenu du rapport de sécurité selon l'art. 5m 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, le rapport de sécurité et le rapport technique ne sont pas nécessaires en tant que documents distincts.

| Titre du document | Auteur (mandant) | Explications sur les exigences relatives au contenu |
|---|---------------------------------|--|
| <i>Les documents qui sont mis à l'enquête publique sont colorés en rose.</i> <i>Pour les deux premiers documents, les chiffres de référence sont prédéfinis. Tous les autres documents doivent être numérotés avec le chiffre de référence 15.xx. Les chiffres surlignés xx sont à définir par le GI ou l'industrie ferroviaire.</i> | | |
| Documents généraux | | |
| 01.01 Demande d'approbation des plans (si elle n'est pas déjà couverte par le projet standard) | GI | chap. 1.6.1 |
| 01.02 Condensé du projet (uniquement nécessaire pour la PAP ordinaire) | GI | chap. 1.6.1 |
| 00 Table des matières ³⁴ | GI | chap. 3.3.1.1 |
| Demande d'octroi d'une dérogation (dans la mesure où des dérogations par rapport aux prescriptions souveraines [1] – [10] sont nécessaires) | GI industrie ferroviaire | chap. 1.10.1 |
| Analyse d'impact (si nécessaire) | GI industrie ferroviaire | chap. 3.1.2, [15] |
| Documents pour RStw (s'ils ne sont pas déjà couverts par les documents du projet standard) | GI | chap. 3.1.6 |
| Documentation permettant de suivre les compétences spécialisées de l'expert des phases 1 - 4 du cycle de vie | expert (GI) | chap. 1.4.3 pt. (1) |
| Documentation permettant de suivre les compétences spécialisées de l'expert de la première application (non requis pour BI) | expert (GI) | chap. 1.4.3 pt. (1) |
| Documents de la phase 1 du cycle de vie | | |
| Concept | GI | [15] |
| Plan de vérification | VER (GI, industrie ferroviaire) | chap.3.1.4 pt. 12), [15] |
| Mandat d'examen d'expert phases 1 - 4 du cycle de vie | GI | chap. 3.3.1.3 Bst. A |
| Documents de la phase 2 du cycle de vie | | |
| Définition du système | GI | [15] |
| Plan de sécurité | GI | chap. 3.1.4 pt 4), [15] |
| Plan de FDM | GI | chap. 3.1.4 pt 5), [15] |

³⁴ Dans la mesure où il s'agit d'une combinaison de projet standard et de projet de développement, la table des matières du projet standard doit être complétée par les informations selon le chap.3.3.1.1.

| Titre du document | Auteur (mandant) | Explications sur les exigences relatives au contenu |
|---|-----------------------------------|--|
| <i>Les documents qui sont mis à l'enquête publique sont colorés en rose.</i> <i>Pour les deux premiers documents, les chiffres de référence sont prédéfinis. Tous les autres documents doivent être numérotés avec le chiffre de référence 15.xx. Les chiffres subordonnés xx sont à définir par le GI ou l'industrie ferroviaire.</i> | | |
| Documents de la phase 3 du cycle de vie | | |
| Analyse et évaluation du risque | GI | chap. 3.1.4 ch. 6) |
| Registre des dangers | GI | chap. 1.8, [15] |
| Plan d'examen d'expert phases 1 - 4 du cycle de vie | expert (GI) | chap. 3.1.4 pt. 14) |
| Plan d'examen d'expert première application | expert (GI) | chap. 3.1.4 pt. 14) |
| Documents de la phase 4 du cycle de vie | | |
| Spécification des exigences | GI | 15] |
| SBAWB | GI | [15] |
| Plan de validation | VAL (GI) | chap. 3.1.4 pt.13), [15] |
| Rapport de vérification phases 1 à 4 du cycle de vie | VER (GI) | chap. 3.1.4 pt. 12), [15] |
| Rapport de validation phases 1 à 4 du cycle de vie | VAL (GI) | chap. 3.1.4 pt.13), [15] |
| Points clés de la 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 d'expert phases 1 - 4 du cycle de vie y compris confirmation BI de l'expert (requis en cas de BI) | expert (GI) | chap. 3.1.4 pt.14), [15] |
| Prise de position du GI sur la mise en œuvre des résultats de l'examen d'expert phases 1 - 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), [15] |
| Plan de FDM mis à jour | industrie ferroviaire | chap. 3.1.4 pt. 8), [15] |
| Concept d'essais de qualification de sécurité et des tests d'exploitation (si nécessaire) | GI | chap. 3.4.3 |
| Documentation sur la planification du logiciel | industrie ferroviaire | tableau A.1 A.1 [39] |
| Mandat d'examen d'expert phases 5 - 10 du cycle de vie (non requis pour BI) | industrie ferroviaire | chap. 3.3.1.3 let. B |
| Documentation pour le suivi de la compétence spécialisé de l'expert phases 5 - 10 du cycle de vie (non requis pour BI) | expert (industrie ferroviaire) | chap. 1.4.3 pt. (1) |
| Plan d'examen d'expert phases 5 - 10 du cycle de vie (non requis pour BI) | expert (industrie ferroviaire) | chap. 3.1.4 pt. 14) |
| Mandat d'examen d'expert première application (non requis pour BI) | GI | chap. 3.3.1.3 let. C |

Tableau 12 : Documents de la phase de planification du projet de développement

3.3.1.1 Table des matières

Les informations suivantes doivent figurer dans la table des matières :

- Référencement de chaque document avec des informations sur : le chiffre de référence, le titre du document, l'index ou la version, la date de création ;
- Attribution aux phases du cycle de vie selon SN EN 50716 [39].

La table des matières doit être soumise sous forme de fichier Word modifiable.

3.3.1.2 Preuve de la mise en œuvre des prescriptions souveraines

Les art. ou ch. pertinents issus des prescriptions souveraines [1] - [10] doivent être énumérés et leur mise en œuvre doit être prouvée, comme le montre à titre d'exemple 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 - 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.] et mise en œuvre 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 d'expert aux experts

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

- 1) Etablir le plan d'examen ³⁰ selon SN EN 50126-1 [15] pour la mise en œuvre du mandat d'examen, le mettre à la disposition du mandant et de l'OFT ;
- 2) Effectuer l'examen conformément au plan d'examen et justifier les éventuels écarts par rapport au plan d'examen ;
- 3) Examiner l'analyse et l'évaluation du risque ;
- 4) Confirmer l'allocation de la BI selon SN EN 50126-2 [17], dans la mesure où il n'y a que des fonctions BI (chap. 3.1.4 pt. 14) ;
- 5) Examiner la preuve de la mise en œuvre des prescriptions souveraines [1] - [10] (chap. 3.3.1.2) ;
- 6) Examiner si les dérogations par rapport aux prescriptions et la demande d'octroi d'une dérogation sont entièrement documentés (chap. 1.10). Examen et documentation de l'adéquation des dérogations ;
- 7) Examiner l'analyse et l'évaluation du risque d'éventuels dérogations par rapport aux prescriptions souveraines [1] - [10] ;
- 8) Évaluer l'adéquation et l'exhaustivité du plan de validation FDMS en termes de sécurité
- 9) Évaluer les compétences spécialisées au sein de l'organisation du projet de développement ;
- 10) Évaluer le système de gestion de la qualité ;
- 11) Évaluer le système de gestion de la configuration et des modifications ;
- 12) Si nécessaire, réaliser un audit pour les phases 1 à 4 du cycle de vie ;
- 13) Plausibilité des points clés concernant la cybersécurité du GI (chap. 1.14) ;
- 14) Consigner les écarts constatés lors de l'examen d'expert, les classer en fonction du risque et les transmettre aux responsables de la gestion des modifications et de la prise de décision.
- 15) Etablir un rapport d'examen d'expert selon le chap. 1.6.3.

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

- 1) Examiner la preuve de la mise en œuvre des prescriptions souveraines [1] - [10] (chap. 3.3.1.2) ;

- 2) Examiner si les exigences des phases 5 à 10 du cycle de vie selon la SN EN 50126-1 [15] sont remplies, en tenant compte des vérifications et de la validation effectuées. Il convient de vérifier si les objectifs des phases du cycle de vie sont remplis, si les activités de sécurité requises ont été réalisées et si les livrables requis sont disponibles.
- 3) Les concrétisations et compléments selon le chap. 3.1.4 doivent être pris en compte.
- 4) Examen de la conformité aux exigences de la SN EN 50129 [17].
- 5) Examen de la conformité aux exigences de la SN EN 50716 [39].
- 6) Les écarts éventuellement constatés pendant l'examen par rapport aux exigences des SN EN 50126-1 [15], SN EN 50129 [17] et SN EN 50716 [39] doivent être indiqués et leur admissibilité doit être justifiée.
- 7) Evaluer la mise en œuvre des techniques/mesures selon SN EN 50129 [17] et SN EN 50716 [39].
- 8) Examen si les constats des rapports de vérification et de validation ont été mises en œuvre ;
- 9) Évaluer si des audits de sécurité ont été réalisés et documentés de manière appropriée ;
- 10) Examiner si les constats du rapport d'examen phases 1 à 4 du cycle de vie pertinents pour les phases 5 à 10 du cycle de vie ont été traités ;
- 11) Plausibilité des points clés et examen de la mise en œuvre des mesures de protection pour la cybersécurité de l'industrie ferroviaire (chap.1.14) ;
- 12) Documenter l'activité d'examen (chap. 1.6.3).

C. Phase de réalisation (première application) : En règle générale, l'expert doit effectuer les tâches suivantes :

- 1) Examiner que les :
 - a) activités de sécurité ont été réalisées conformément au plan de sécurité. Les concrétisations et compléments selon le chap.3.1.4 doivent être pris en compte.
 - b) tâches d'intégration technique et d'exploitation sont accomplies (chap. 1.12) ;
 - c) constats du rapport d'examen d'expert phases 1 - 4 du cycle de vie sont traités ;
 - d) constats du rapport d'examen d'expert phases 5 - 10 de cycle de vie pertinents pour la première application sont traités ;
 - e) conditions pour la MES selon SN EN 50126-2 [16] sont remplies ;
 - f) charges issues de la DAP sont remplies, pour autant qu'elles concernent la sécurité ;
 - g) modifications du projet sont documentées et conformes aux directives (chap. 3.4.1) ;
 - h) Release notes sont disponibles ;
- 2) Examen des fonctions des SA, y compris la réaction en cas de dérangement, ainsi que l'interaction des différents produits entre eux, y compris les IS voisines ;
- 3) Examen de la mise en œuvre des mesures de protection en matière de cybersécurité du GI (chap. 1.14) ;
- 4) Documenter l'activité d'examen (chap. 1.6.3).

3.4 Phase de réalisation du projet de développement

3.4.1 Modifications du projet de développement

Si, après l'octroi de la DAP, des divergences apparaissent par rapport aux documents approuvés, il convient de procéder comme suit :

- Si les modifications du projet répondent aux critères du chap. 3.1.3, elles doivent être documentées dans le dossier de sécurité de la première application et examiner par l'expert de la première application ou par le chargé de validation de la phase 9 du cycle de vie (pour les fonctions BI).
- Si les modifications de projet apportées aux RStw selon le tableau 11 ne nécessitent pas de PAP, elles doivent être documentées dans le dossier de sécurité et examiner par l'expert.
- Dans le cas contraire, une procédure est nécessaire pour les modifications de projet (art. 5 al. 2 OPAPIF [5]). Pour les documents concernés par les modifications de projet, les exigences selon le chap. 3 doivent être mises en œuvre. Pour les RStw, les exigences selon le chap. 3.1.6 doivent être mises en œuvre.

Si l'IS est déjà en construction, les travaux non concernés par les modifications du projet peuvent se poursuivre, sous réserve d'une autre disposition de l'OFT (art. 5 al. 3 OPAPIF [5]).

3.4.2 Documents et exigences relatives au contenu du projet de développement

Le tableau 14 présente les documents requis pour la phase de réalisation. En complément, des renvois indiquent où trouver des explications sur les exigences relatives au contenu. Lors de l'élaboration de ces documents, il convient de tenir compte des exigences formelles selon le chap. 1.1.3 et des exigences relatives à la documentation FDMS de la SN EN 50126-1 [15].

| Titre du document | Auteur (mandant) | Explications sur les exigences relatives au contenu |
|---|-----------------------------|---|
| Documents généraux | | |
| 00 Table des matières | GI industrie ferroviaire | chap. 3.3.1.1 |
| Demande d'AE (si PAE requise) | GI | |
| Échéancier PAE (si PAE requise) | 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 nécessaire) | GI industrie ferroviaire | [35] |
| Documentation des informations sur la BI, si elles ne sont pas déjà incluses dans d'autres documents de ce tableau. | GI industrie ferroviaire | chap. 3.1.4 pt. 15) |
| Points clés de la cybersécurité | industrie ferroviaire | chap. 1.14 |
| Attestations requises d'interopérabilité (si nécessaire) | GI | chap. 1.15, 1.16 |
| Déclarations de conformité des constituants d'interopérabilité (s'ils sont été co-développés) | industrie ferroviaire | art. 15 ^{ier} OCF [4] |
| Documents de la phase 5 du cycle de vie | | |
| Architecture du système | industrie ferroviaire | [15] |
| Analyse des dangers, y compris le registre des dangers | industrie ferroviaire | [15] |
| Allocations des exigences de sécurité | industrie ferroviaire | [15] |
| Critères d'acceptation, ainsi que les processus et procédures de démonstration et d'acceptation | GI | [15] |
| Documents de la phase 6 du cycle de vie | | |
| Analyse de la FDM | industrie ferroviaire | [15] |
| Analyse des dangers | industrie ferroviaire | [15] |
| Procédures d'installation et de mise en service | industrie ferroviaire | [15] |
| Procédures d'exploitation et de maintenance | industrie ferroviaire | [15] |

| Titre du document | Auteur (mandant) | Explications sur les exigences relatives au contenu |
|---|--------------------------------|---|
| Procédé de fabrication | industrie ferroviaire | [15] |
| Mesures de formation | industrie ferroviaire | [15] |
| Dossier de sécurité pour l'application spécifique (pas nécessaire pour BI) | industrie ferroviaire | chap. 3.1.4 pt. 9), [17] |
| Dossier de sécurité pour la première application (pas nécessaire pour BI) | GI | chap. 3.4.2.2 |
| Documents de la phase 7 du cycle de vie | | |
| Rapports d'assurance qualité (concernant le procédé de fabrication et les mesures de FDMS applicables) | industrie ferroviaire | [15] |
| Rapports d'inspection et d'essai | industrie ferroviaire | [15] |
| Dispositions pour la manipulation du matériel et la logistique | industrie ferroviaire | [15] |
| | | |
| Documentation d'installation | industrie ferroviaire | [15] |
| Rapport d'intégration (si nécessaire) | industrie ferroviaire | [15] |
| Mesures prises pour résoudre les problèmes de défaillances et d'incompatibilités | industrie ferroviaire | [15] |
| Analyse d'impact (si nécessaire) | industrie ferroviaire | [15] |
| Dispositions logistiques du système | industrie ferroviaire | [15] |
| Documents de la phase 9 du cycle de vie | | |
| Rapport de validation | VAL (industrie ferroviaire) | chap. 3.1.4 pt. 13), [15] |
| Documents de la phase 10 du cycle de vie | | |
| Rapport d'examen d'expert phases 5 - 10 du cycle de vie (pas nécessaire pour BI) | expert (industrie ferroviaire) | chap. 3.1.4 pt. 14), [15] |
| Acceptation des SBAWB (si nécessaire) | GI | [15] |
| Rapport d'acceptation | GI | [15] |
| Rapport de vérification des phases 5 à 10 du cycle de vie | VER (industrie ferroviaire) | chap. 3.1.4 pt. 12), [15] |
| Rapport d'examen d'expert première application (non requis pour BI) | expert (GI) | chap 3.1.4 pt. 14), [15] |
| Documentation SW | 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 SN EN 50129 [17] et SN EN 50716 [39] | industrie ferroviaire | chap. 3.4.2.4 |
| Prise de position du GI sur la mise en œuvre des résultats de l'examen d'expert première application (non requis pour BI) | GI | chap. 1.6.4 |
| Prise de position de l'industrie ferroviaire sur la mise en œuvre des résultats de l'examen d'expert phases 5 - 10 du cycle de vie (non requis pour BI) | industrie ferroviaire | chap. 1.6.4 |

Tableau 14: Documents de la phase de réalisation du projet de développement

3.4.2.1 Échéancier PAE

Le l'échéancier pour l'obtention de AE doit montrer comment les activités de sécurité sont planifiées dans le temps. Il convient de tenir compte des interdépendances avec la planification des activités de sécurité des phases 5 à 10 du cycle de vie. Les délais prévus au chap. 3.1.7 ch. ③ doivent également être pris en compte.

3.4.2.2 Dossier de sécurité première application

Le dossier de sécurité pour la première application correspond au dossier de sécurité selon l'art. 5l al. 1 OCF [4] et est nécessaire pour la première application de l'objet de développement (chap. 3.1.2) en Suisse auprès d'un GI. Il doit être établi et signé par des spécialistes parallèlement aux travaux du projet de développement (art. 5l al. 2 OCF [4]). Lors de son établissement, les exigences selon le chap. 1.1.3 et la SN EN 50126-1 [15] doivent être prises en compte. La figure 14 présente le contenu du dossier de sécurité pour la première application. La structure peut être adaptée aux conditions du GI et aux exigences du projet de développement.



Figure 14: Contenu du dossier de sécurité pour la première application

3.4.2.3 Release note

L'objet du développement doit être identifiable au moyen d'une Release note. Pour cela, les informations suivantes sont nécessaires :

- identification univoque des HW : désignation, numéro d'article, état d'émission ;
- Identification claire du SW resp. des fonctions du SW : versions du SW, release, sommes de contrôle ;
- une identification claire des interfaces ;
- Documents d'utilisation : comprennent essentiellement les SBAWB et les documents relatifs à la conception, au montage, à la MES, à l'exploitation et à la maintenance ;
- Erreurs et limitations connues ;
- Modifications par rapport aux versions/releases précédentes ;
- 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 selon SN EN 50129 [17] et SN EN 50716 [39] doivent être énumérées et leur mise en œuvre doit être décrite et démontrée. La liste et la description de la mise en œuvre des techniques/mesures sont présentées à titre d'exemple dans le

tableau 15. La preuve de la mise en œuvre de ces techniques/mesures est généralement apportée dans le rapport de vérification ou de validation. Tout cela fait partie du dossier de sécurité pour l'application spécifique ou produits génériques et/ou applications génériques.

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

Tabelle 15: Techniques/Mesures

3.4.3 Essais de qualification de sécurité et tests en exploitation

3.4.3.1 Essais de qualification de sécurité

La nécessité de procéder à des essais de qualification de sécurité doit faire l'objet d'une concertation entre les parties concernées (GI, industrie ferroviaire) et être justifiée (SN EN 50129 [17]). Les essais de qualification de sécurité doivent être effectués auprès du GI.

Si les essais de qualification de sécurité sont prévus pour un objet en développement avec une certaine responsabilité en matière de sécurité lors de l'exploitation opérationnelle, une autorisation de l'OFT est nécessaire. Le GI doit consigner les mesures appropriées pour assurer la sécurité de l'exploitation pendant les essais de qualification de sécurité.

Pour obtenir l'autorisation de procéder à des essais de qualification de sécurité, le GI doit remettre à l'OFT un concept d'essais de qualification de sécurité au plus tard deux mois avant le début des essais de qualification de sécurité. Le contenu typique de ce concept est le suivant :

- 1) objet du développement, y compris les release notes ;
- 2) lieu, l'étendue et la durée ;
- 3) responsabilités ;
- 4) dépendances ;
- 5) tests à effectuer, les résultats attendus et les critères de réussite du test ;
- 6) Traitement des défaillances, des dérangements et des dysfonctionnements ;
- 7) Mesures permettant de garantir une sécurité suffisante pendant les essais de sécurité. Pour ce faire, il convient d'identifier les dangers ainsi que d'analyser et d'évaluer les risques qui y sont liés. Lors de l'identification des dangers, il convient de prendre en compte aussi bien l'environnement de test que 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, opérationnelles ou organisationnelles.
- 8) Prescriptions d'exploitation pour le personnel d'exploitation, de conduite et éventuellement de maintenance ;
- 9) Traitement des modifications de l'objet du développement : si des modifications de l'objet du développement sont nécessaires pendant l'essai de qualification de sécurité, il convient d'examiner dans quelle mesure l'essai de qualification de sécurité doit être effectué à nouveau ou dans quelle mesure il doit être répété ;
- 10) Traitement des résultats (notamment en cas d'échec aux tests) ;
- 11) Preuve du respect des charges de la DAP.

Si, pour un objet en développement, les essais de qualification de sécurité sont prévus de manière générale sans responsabilité en matière de sécurité ou avec une certaine responsabilité en matière de sécurité dans des zones sécurisées (PCT [9]) en dehors de l'exploitation opérationnelle, aucune autorisation de l'OFT n'est nécessaire. Le GI est chargé d'établir un concept d'essais de qualification de sécurité selon les points 1) - 10), puis de le mettre en œuvre.

Dans la mesure où les contenus susmentionnés sont déjà mentionnés dans le dossier de sécurité pour produit générique et/ou de l'application générique, il est possible d'y faire référence.

Après les essais de qualification de sécurité, les tests effectués et leurs résultats doivent être documentés dans le rapport technique de sécurité du dossier de sécurité pour l'application spécifique ou produit générique et/ou l'application générique (SN EN 50129 [17]).

3.4.3.2 Tests en exploitation

Si l'essai de qualification de sécurité de l'objet du développement (chap. 3.4.3) a été effectué, il couvre 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 d'augmenter la confiance dans le fait que l'objet du développement, par ex.:

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

Pour obtenir l'autorisation pour des tests en exploitation, le GI doit soumettre à l'OFT un concept de tests en exploitation. Le contenu de ce concept est typiquement celui décrit au chap. 3.4.3, ch.1) - 6), 9) et 10).

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

- dans la PAP, si l'objet du développement a exclusivement des fonctions liées à la sécurité avec BI.
- dans la PAE, si le développement de l'objet du développement n'est pas encore achevé au moment de la planification.
- dans la procédure d'homologation de série, lorsque le développement de l'objet du développement est achevé au moment de la planification et que l'exigence prévue à l'art. 7 al. 1 OCF [4] est remplie. Le déroulement de cette procédure est décrit dans la Dir. HdS [14].

Une fois les tests en exploitation terminés, le GI doit remettre à l'OFT le rapport de tests en exploitation, qui contient les éléments suivants :

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

Termes et abréviations

| Terme | Abréviation | Explication | Source |
|--|-------------|--|------------|
| Déroptions aux spécifications | | selon chap. 1.10 | |
| Règles reconnues de la technique | | Ont fait leurs preuves et se sont imposés dans la pratique. Les DE-OCF relatives à l'art. 2, DE 2.3 contiennent des informations sur la manière dont elles sont identifiées. | |
| autorisé à un autre titre | | selon chap. 1.2 pt. ② | |
| Documents d'utilisateur | | selon chap. 3.4.2.3 | |
| Audit | | selon la source | [15] |
| Panne | | selon la source | [15] |
| Exceptions aux spécifications | | selon chap. 1.10 | |
| Analyse d'impact | | selon la source | [15] |
| Analyse de l'impact des modifications | | conformément au chap. 1.12 pt. 5) | |
| Intégrité de base | BI | selon les sources | [15], [17] |
| Procédure d'autorisation d'exploitation | PAE | | |
| Autorisation d'exploiter | AE | | |
| Essais de qualification de sécurité | | selon chap. 3.4.3.1 | |
| Prescriptions d'exploitation | | Sont définies dans les DE-OCF relatives à l'art. 12, DE 12.1, ch. 1. Il s'agit par ex. du tableau des itinéraires, des instructions de service, des listes de contrôle, de la gestion des interventions et des pannes, des manuels de maintenance. | [8] |
| Expropriation | | selon la note de bas de page ¹⁶ | |
| Part de développement | | Il s'agit par ex. de nouvelles fonctions, d'un nouveau type de poste d'enclenchement, de nouvelles interfaces, d'une modification de l'objectif d'utilisation de fonctions existantes, de schémas différents des schémas de principe ou des principes de construction. | |
| Première application | | Première utilisation en Suisse de produits nouvellement développés, modifiés ou entièrement développés. | |
| Système européen de contrôle de la marche des trains | ETCS | | [42] |
| Compétence spécialisée | | selon chap. 1.4.3 pt. (1) | |
| Mise en danger | | selon la source | [15] |
| Registre des dangers | | selon la source | [15] |
| Projet global | | Projet supérieur avec divers domaines spécialisés tels que les installations techniques de construction, les installations électriques. | |
| Total SA | | L'IS de niveau supérieur d'un point de vue technique et opérationnel, lorsque le projet traité ne concerne qu'une partie de l'IS. | |
| importance de la sécurité élevé | | selon chap. 2.2.1 | |
| importance de la sécurité faible | | selon chap. 2.2.1 | |
| prescriptions souveraines | | On entend par là les prescriptions [1] - [10]. | |

| Terme | Abréviation | Explication | Source |
|--|-------------|---|--------|
| Technologies de l'information et de la communication | TIC | selon la source | [13] |
| Gestionnaire d'infrastructure | GI | Entreprise qui construit et exploite l'infrastructure. | [1] |
| Interopérabilité | IOP | | |
| Niveau 1 Supervision limitée | L1 LS | | [42] |
| Système de management de la sécurité de l'information | SMSI | selon la source | [13] |
| mis à l'enquête publique | | Il s'agit notamment des documents qui peuvent avoir des répercussions sur des tiers (particuliers, organisations, autorités). | |
| Modifications du projet | | Les modifications apportées pendant le PAP ainsi qu'après l'octroi du DAP. | |
| Procédure d'approbation des plans | PAP | | |
| décision d'approbation des plans | DAP | | |
| Ouvrage de référence en matière de technique ferroviaire | RTE | | |
| Note de publication | | selon chap. 3.4.2.3 | |
| modification strictement technique | | Modifications répondant à <u>tous les</u> critères de l'annexe A4.3.1.2 de la directive HdS. Le terme "modification purement technique" est utilisé comme synonyme de "modification de l'état technique de l'appareil" selon la directive HdS. | [14] |
| analyse et évaluation du risque | | selon la source L'évaluation du risque comprend l'analyse et l'évaluation du risque. | [15] |
| Risque | | selon la source | [15] |
| Centre d'évaluation des risques | | selon la source (2ème section) | [4] |
| Gestion des risques | | selon chap.1.8 et source | [15] |
| Procédures de gestion des risques | | Annexe I du règlement d'exécution (UE) no 402/2013 (art. 8c, al. 2, OCF) | [4] |
| Poste d'enclenchement à relais | RStw | | |
| Non-rétroactivité | | conformément au chap. 1.12 pt. 5). | |
| Expert | SV | Personne qui effectue des contrôles indépendants et qui remplit les exigences du chap. 1.4.3. | |
| Besoin de protection | | selon la source | [13] |
| Niveau d'intégrité de la sécurité | SIL | selon la source | [15] |
| conditions d'application relatives à la sécurité | SBAWB | selon la source | [15] |
| fonction liée à la sécurité | | selon la source | [15] |
| Démonstration de la sécurité | | Ensemble des activités ayant pour but de confirmer la sécurité, y compris la documentation. Comprend donc par ex. les tests, la validation, l'établissement des preuves et l'éventuel contrôle . | |
| Démonstration de la sécurité par la pratique | | Sont également considérées comme des bases suffisantes les preuves de sécurité selon les mét | |

| Terme | Abréviation | Explication | Source |
|--|-------------|---|-------------------------------------|
| | | hodes antérieures ou l'épreuve de la pratique, pout autant que la traçabilité soit garantie. | |
| Dossier de sécurité | DoSe | selon la source | [15] |
| Relatif à la sécurité | | selon la source | [15] |
| Installations de sécurité | SA | selon Kap. 1.1.2 | |
| mise en service | MES | | |
| - 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. | |
| Catégories de réseaux : - Réseau non-IOP - Réseau principal IOP et - Réseau complémentaire IOP | | selon chap. 1.15 | |
| Logiciel | SW | selon la source | [15] |
| Examen SV (évaluation indépendante de la sécurité) | | selon la source | [15] |
| spécification technique d'interopérabilité concernant les sous-systèmes «contrôle-commande et signalisation» | STI CCS | | [8] |
| Intégration technique et d'exploitation | | Intégration des produits utilisés dans l'ensemble de l'IS en tenant compte de toutes les directives techniques et opérationnelles pertinentes. | |
| taux de défaillance fonctionnelle tolérable | TFFR | selon la source | [15] |
| taux de risque tolérable | THR | selon la source | [15] |
| Homologation de série | TZL | | |
| Sous-traitant | | selon la source | [40] |
| Proportionnel (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 CHF 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. | Politique de sécurité ³⁵ |
| Prescriptions | | Tableau 2 | |
| Contrôle de la marche des trains voie métrique et voie spéciale | ZBMS | selon la source | [10] |
| Autorisation | | Terme générique généralement utilisé pour désigner le processus de contrôle ou la décision qui en résulte. | |
| chargé de vérification | VER | selon la source | [16] |
| chargé de validation | VAL | selon la source | [16] |

³⁵ www.bav.admin.ch (Thèmes généraux → Sécurité)