



V 3.0_f, 23.10.2015, version française publiée le 01.02.2016

Référence du dossier : BAV-511.5-00015/00003/00004

Directive

Démonstration de la sécurité Installations de sécurité¹

Installations selon l'OCF, chap. 2,
sections 6, 7 et 8,
Procédures d'approbation des plans et
d'autorisation d'exploiter

OFT Divisions Infrastructure et Sécurité

¹ Par souci de concision, la notion « installations de sécurité » est utilisée au sens large, conformément à la précision dans la deuxième partie du titre.

Impressum

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

Auteurs : Christian Moy et GT Révision LF SA 2014

Distribution : Publication sur le site Internet de l'OFT

Langues : Allemand (original)
Français

La présente directive est entrée en vigueur le 1^{er} mai 2007 à titre de guide, version 1.0 ; la présente version 3.0 est la première à titre de directive et entre en vigueur le 23 octobre 2015.

Office fédéral des transports
Division Sécurité

Division Infrastructure

Pieter Zeilstra, sous-directeur

Toni Eder, sous-directeur

Modifications

V	Date	Auteur	Modifications	Statut ²
V 1.0	1 ^{er} mai 2007	Christian Moy	1 ^{re} édition (guide)	Obsolète
V 2.0	1 ^{er} juillet 2010	Christian Moy	Révision et complément après 3 ans d'expérience et adaptation à l'état de la LCdF, de l'OCF et des DE-OCF	Obsolète
V 2.1_d	1 ^{er} juillet 2011	Christian Moy	Améliorations aux ch. 4.3.4 / fig. 2 et ch. 6.3.2, 7.1.1, 7.1.3	Obsolète
V 3.0_f	23 oct. 2015 publiée 1. fev. 2016	Christian Moy	Révision et complément après la réforme des chemins de fer 2.2 : refonte en directive	En vigueur (ZEP, EDT)

² Etat du document ; sont prévus : en élaboration / en revue / en vigueur (avec visa) / obsolète

Table des matières

1	Généralités	5
1.1	But et champ d'application	5
1.2	Structure	5
2	Rôles et responsabilités.....	6
2.1	Entreprises ferroviaires	6
2.2	Bureaux d'ingénieurs / industrie.....	6
2.3	Organismes de contrôle indépendants	6
2.4	OFT	6
3	Bases	7
3.1	Principes, règles de l'art.....	7
3.2	Normes SN EN 50126 et SN EN 50129	7
3.3	Terminologie	8
3.4	Dossier de sécurité selon l'art. 8a, OCF et la norme SN EN 50129.....	8
3.5	Procédure d'approbation des plans : types et pertinence.....	8
3.6	Documents à soumettre	9
4	Déroulement principaux des projets	9
4.1	Déroulement standard : projet de construction – approbation des plans – réalisation (Fig. 1)	9
4.2	Déroulement simplifié : sans remise de documentation pour la « réalisation ».....	10
4.3	Déroulement avec une autorisation d'exploiter (fig. 2)	11
5	Spécificités de procédure selon le type de projet	11
5.1	Maturité du projet	12
5.1.1	Plan A : « tout inclus »	12
5.1.2	Plan B : documents des installations de sécurité livrés ultérieurement.....	12
5.1.3	Plan C : projet de détail différé des installations de sécurité	12
5.2	Type de tronçon	12
5.2.1	Tronçons non interopérables (en rouge)	12
5.2.2	Réseau principal interopérable (en vert foncé).....	13
5.2.3	Réseau complémentaire interopérable (en vert clair).....	13
5.3	Spécifications	14
5.3.1	Elaboration des nouvelles exigences	14
5.3.2	Mise en œuvre des nouvelles fonctionnalités et des possibilités de planification	14
5.3.3	Besoin de nouveaux processus d'exploitation.....	14
5.3.4	Modification du but d'utilisation	14
5.4	Catégories d'application.....	15
5.5	Dérogations	15
5.5.1	Dérogation aux prescriptions (art. 5, al. 2, OCF).....	15
5.5.2	Dérogation aux prescriptions d'interopérabilité (art. 15e OCF)	15
5.6	Maturité du produit	15
5.6.1	Projet standard.....	15
5.6.2	Projets liés à la première utilisation de nouvelles fonctions	15
5.6.3	Projets liés à l'utilisation de nouveaux produits	16
5.6.4	Evaluation du degré de maturité en vue de l'application du produit.....	16
5.6.5	Harmonisation du développement de l'application et du projet d'installation	16
5.7	Changements essentiels.....	16
6	Procédure d'approbation des plans (PAP)	16
6.1	Documents à présenter.....	17
6.2	Exigences quant au contenu des documents	17
6.2.1	Rapport de sécurité des installations de sécurité, phase « Planification ».....	17
6.2.2	Rapport d'examen d'expert relatif à la phase « Planification »	19
6.3	Moment de la présentation des documents / délais de traitement	20

6.4	Autorisation d'exploiter.....	20
7	Réalisation de l'installation (construction et mise en service).....	21
7.1	Documents à élaborer.....	21
7.2	Exigences quant au contenu des documents	21
7.2.1	Dossier de sécurité pour la réalisation.....	21
7.2.2	Rapport d'examen d'expert pour la phase « Réalisation » (« rapport d'évaluation de la sécurité »)	23
7.3	Moment de la présentation des documents	24
7.3.1	Sans autorisation d'exploiter.....	24
7.3.2	Avec autorisation d'exploiter	24
7.4	Modifications du projet	24
8	Catégories d'application	25
8.1	Critères.....	25
8.1.1	Importance pour la sécurité	25
8.1.2	Type de projet	25
8.1.3	Classement	26
8.2	Vue d'ensemble des exigences	27
8.3	Exigences.....	27
8.3.1	Catégorie d'application H1 (carré rouge).....	28
8.3.2	Catégorie d'application H2, ainsi que G1 (carré orange)	28
8.3.3	Catégorie d'application H3, ainsi que G2 et K1 (carré jaune)	28
8.3.4	Exigences pour les autres catégories d'application.....	28
8.4	Diffusion des systèmes et de leurs versions (problématique du déploiement [rollout]).....	29
8.5	Applications télématiques, automatisation des postes d'enclenchement.....	29
8.6	Construction ou modification dans les postes d'enclenchement à relais	30
8.7	Modifications temporaires sur des installations de sécurité dans le cadre d'un projet.....	30
Annexe 1	Définitions et abréviations (par ordre alphabétique)	31
Annexe 2	Documents de référence.....	34
Annexe 3	Illustration du chap. 5	35
Annexe 4	Illustration du ch. 5.6.4	36

1 Généralités

1.1 But et champ d'application

La présente directive décrit la démonstration de la sécurité et de la conformité en matière d'interopérabilité des installations de sécurité (dans la présente directive, le terme « installations de sécurité » vise les installations conformément au chap. 2, sections 6 à 8, OCF) en vue de l'approbation des plans et de l'autorisation d'exploiter. Elle définit aussi les exigences auxquelles doit satisfaire le contenu des documents de démonstration de la sécurité et elle indique quand ceux-ci doivent être présentés. Elle énonce quels règlements, directives et normes techniques s'appliquent pour la démonstration de la sécurité. Les buts recherchés sont une égalité de droit et une sécurité juridique aussi grandes que possible de même qu'une bonne adaptation à la pratique, eu égard à la multitude des types de projets de construction et de modifications de projets.

La présente directive est en principe applicable à toute construction ou modification d'installations de sécurité, indépendamment de la technologie utilisée.

Elle présente les exigences des documents de démonstration de la sécurité nécessaires à l'approbation des plans et à l'autorisation d'exploiter selon le droit en vigueur (LCdF, OCF, OPAPIF) en tenant compte des normes SN EN 50126 et SN EN 50129 dont l'application est exigée par la DE-OCF 38.1, ch. 1.3, et la DE-OCF 44.1, ch. 2.3.

La présente directive n'a valeur ni de loi ni d'ordonnance. Si le requérant l'observe, il a la garantie que l'autorité acceptera la méthode d'élaboration des résultats ou des documents.

Les exigences énumérées ici et auxquelles doivent satisfaire les documents de démonstration de la sécurité permettent d'obtenir une démonstration de la sécurité adaptée aux risques. Les activités sécuritaires doivent toujours être régies par le sens des responsabilités dans l'exécution du travail, que la documentation doit soutenir et rendre compréhensible.

1.2 Structure

La présente directive est structurée en une partie préliminaire (chap. 1 à 3) et une partie substantielle (chap. 4 à 8) ainsi qu'une annexe.

Le chap. 2 décrit brièvement les rôles et les responsabilités des parties impliquées.

Le chap. 3 précise les bases juridiques essentielles et traite l'application des normes SN EN 50126 et SN EN 50129 en rapport avec les exigences de l'OCF et de l'OPAPIF.

Le chap. 4 fournit une vue d'ensemble du déroulement des projets. Les différents rôles, les processus, l'envoi des documents et les rapports entre ces éléments sont représentés sur un axe temporel pour le « cas normal », compte tenu de la présentation en « V » du cycle de vie d'un produit selon la norme SN EN 50126.

Le chap. 5 traite des détails des procédures relatives aux différents projets.

Le chap. 6 énumère les documents à présenter dans le cadre de la procédure d'approbation des plans (PAP), commente les exigences quant à leur contenu requis par les bases légales en vigueur, la directive de l'OFT du 1^{er} juillet 2013 relative à l'OPAPIF et les normes SN EN 50126 et 50129, et elle fixe les échéances pour présenter ces documents. De plus, elle décrit les critères permettant de déroger à l'obligation d'une autorisation d'exploiter.

Le chap. 7 énumère les documents de preuve à fournir après l'approbation des plans. Les documents à soumettre en cours de réalisation d'une installation et/ou d'un système sont spécifiés par analogie au chapitre 6 et la marche à suivre lors d'une modification de projet est décrite.

Le chap. 8 traite des différentes catégories d'applications. Il définit les catégories qui nécessitent une PAP et le type de démonstration de la sécurité nécessaire.

L'annexe contient des définitions, explique les abréviations et énumère les documents de référence.

2 Rôles et responsabilités

2.1 Entreprises ferroviaires

L'entreprise ferroviaire (en l'occurrence le gestionnaire d'infrastructure [GI]) est responsable de la conformité aux prescriptions, de la sécurité de l'exploitation et de l'entretien des installations ferroviaires (art.10 OCF). Elle soumet des demandes d'approbation des plans selon l'art. 18 ss LCdF et doit fournir à cette occasion toutes les indications nécessaires à l'évaluation (art. 3, al. 1, OPAPIF). Elle peut déléguer une partie de ces tâches à des tiers (bureaux d'ingénieurs) ou à des fournisseurs (industrie), mais reste toutefois l'interlocuteur de l'OFT au cours de la PAP.

2.2 Bureaux d'ingénieurs / industrie

L'industrie et les bureaux d'ingénieurs sont responsables de la sécurité de leurs produits et de leurs services. Dans le cadre des contrats, ils élaborent les documents de preuve, donnent aux organismes de contrôle indépendants (OCI) accès aux documents importants pour l'analyse de la sécurité et leur permettent de pratiquer les contrôles nécessaires sur les installations.

2.3 Organismes de contrôle indépendants

Le recours aux organismes de contrôle indépendants est réglé dans la directive ad hoc du 1^{er} juillet 2013 sur les organismes de contrôle indépendants dans le domaine des chemins de fer (Dir. OCI-CF). Celle-ci décrit les rôles et les tâches des différents organismes de contrôle, les exigences auxquelles ils doivent satisfaire en matière de compétence professionnelle, d'indépendance et de reconnaissance. Elle règle aussi les méthodes de travail des experts et les exigences auxquelles doivent satisfaire leurs rapports d'examen (« expertises »). Elle décrit en outre comment les requérants et l'OFT doivent tenir compte des rapports des organismes de contrôle indépendants. La partie « dispositions spécifiques » de la directive définit quels organismes contrôlent quels objets. Ces définitions sont également valables lors des procédures d'approbation des plans et d'autorisation d'exploiter.

2.4 OFT

Après un examen approprié, l'OFT donne l'autorisation pour l'élaboration/la modification des installations ferroviaires (approbation des plans) ainsi que pour la mise en service (autorisation d'exploiter), s'il n'a pas renoncé à l'octroi d'une autorisation d'exploiter dans le cadre de l'approbation des plans ou de l'homologation de série.

Conformément à la SN EN 50129, ch. 5.5.2, l'OFT s'appuie sur les documents de démonstration de la sécurité, en particulier sur le rapport d'examen de l'expert (« rapport d'examen »). Il n'examine donc pas directement le projet ou l'installation, mais s'assure que le déroulement de la démonstration de la sécurité correspond aux attentes.

Pour pouvoir estimer la qualité de la démonstration de la sécurité, l'OFT doit disposer, en plus des preuves de la sécurité et des rapports d'examen, des documents auxquels il y est fait référence.

L'OFT se réserve le droit de contrôler par sondages les preuves de la sécurité et les installations.

Si, lors de l'approbation, l'OFT demande des plans et des documents « pour examen » ou « pour approbation », il faut prévoir le temps nécessaire pour leur traitement et la prise de position (réponse) de l'OFT.

Si, lors de l'approbation, l'OFT demande des plans et des documents « pour connaissance », « pour information » ou « sans indication », il n'est pas nécessaire d'attendre de prise de position (réponse) de l'OFT.

3 Bases

3.1 Principes, règles techniques reconnues

Selon l'art. 17, al. 1, LCdF, les installations ferroviaires et les véhicules doivent être construits, exploités, entretenus et renouvelés conformément aux exigences du trafic, de la protection de l'environnement et aux progrès de la technique.

Les normes SN EN 50126, SN EN 50128, SN EN 50129 et SN EN 50159 sont reconnues comme règles de l'art. De plus, les dispositions d'exécution de l'ordonnance sur les chemins de fer (DE-OCF), DE 38.1 et 41.1, indiquent dans quels cas les normes SN EN 50126, SN EN 50129 et SN EN 50159 sont impérativement applicables.

La norme SN EN 50126 est la « norme de base ». Elle décrit un processus permettant de mettre en œuvre une démarche cohérente de gestion de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS/ RAMS) pour des applications ferroviaires.

La norme SN EN 50129 définit les exigences pour l'acceptation et l'approbation des systèmes électroniques relatifs à la sécurité dans le domaine ferroviaire. Elle décrit en détail les mesures et la documentation nécessaires à l'élaboration de la preuve de la sécurité. Elle est par conséquent un élément central de la présente directive.

La norme SN EN 50128 se concentre sur les processus de développement de logiciels sécuritaires. Elle décrit quels processus doivent être appliqués pour que le logiciel réponde aux exigences de sécurité fixées à un niveau supérieur.

La norme SN EN 50159 est appliquée aux systèmes de communication déterminants pour la sécurité.

Ces normes sont valables pour la spécification, la conception, la construction, l'installation, la réception technique, l'exploitation, la maintenance et la modification / l'extension des installations de sécurité.

3.2 Normes SN EN 50126 et SN EN 50129

La norme SN EN 50126 couvre l'ensemble du cycle de développement, de la conception à l'exploitation et à la maintenance, en passant par l'analyse de risque, le projet et la construction.

La norme SN EN 50129 décrit en détail quelles mesures et informations sont nécessaires pour l'élaboration d'un dossier de sécurité. Ses annexes contiennent d'autres détails sur certaines étapes de la démonstration de la sécurité.

Elle prescrit l'établissement de systèmes de gestion de la qualité et de la sécurité. Elle exige une affectation claire des rôles spécifiques et un degré d'indépendance approprié entre le concepteur, le chargé de la vérification, le chargé de la validation et l'expert.

La SN EN 50129 exige une approche systématique et documentée pour :

- la preuve de la gestion de la qualité
- la preuve de la gestion de la sécurité
- la preuve de la sécurité fonctionnelle et technique
- l'acceptation et l'approbation de la sécurité

Elle favorise la définition complète et correcte des conditions d'utilisation relatives à la sécurité des produits et des systèmes. Elle contribue à ce que les produits soient utilisés conformément à leurs définitions et que toutes les conditions d'application prescrites soient observées lors de leur emploi.

Les procédures et exigences en matière de documentation commentées ici et requises conformément aux prescriptions favorisent une démonstration de la sécurité responsable, appropriée à l'objet sur lequel elle porte. Ni les normes SN EN 50126 et 50129 ni les autres bases énumérées au présent chapitre ne sont des « recettes à suivre à la lettre » ; en fin de compte, la sécurité dépend de la qualification des organisations impliquées.

3.3 Terminologie

Les définitions de la législation suisse, les termes couramment utilisés par les chemins de fer et les définitions des normes SN EN 50129 et 50126 ne correspondent pas toujours. Pour éviter les malentendus, les définitions utilisées dans la présente directive et leur provenance sont indiquées dans l'annexe 1 du présent document. En outre, les dispositions et les illustrations suivantes doivent également aider à clarifier les définitions.

3.4 Dossier de sécurité selon l'art. 8a, OCF et la norme SN EN 50129

Dans la LCdF et dans l'OCF, le terme de dossier de sécurité est utilisé sans être défini de manière uniforme. Comme dans le langage quotidien, la signification de ce terme varie selon le contexte ; il est parfois utilisé à titre générique ou bien il vise la démonstration de la sécurité (annexe 1) ou encore les documents de cette démonstration conformément à la norme SN EN 50129.

La norme SN EN 50129 fait la distinction entre le dossier de sécurité pour la conception de l'application et celui de l'implémentation physique. Elle définit à cet effet la structure et les exigences en matière de contenu.

Dans la présente directive, les définitions de la norme sont appliquées au dossier de sécurité conformément à l'art. 8a OCF.

3.5 Procédure d'approbation des plans : types et pertinence

Selon l'art. 18, al. 1, LCdF, les installations ferroviaires ne peuvent être élaborées ou modifiées qu'avec une approbation des plans. L'approbation des plans a lieu dans le cadre d'une procédure *ordinaire* (art. 18a à 18h LCdF) ou *simplifiée* (art. 18i LCdF).

La *procédure ordinaire* exige impérativement la publication officielle du projet et sa mise à l'enquête publique, la consultation des autorités fédérales concernées ainsi que l'avis des cantons concernés.

Conformément à l'art. 18i LCdF, la procédure simplifiée peut être demandée dans les cas suivants :

- Un projet affecte un espace limité et ne concerne qu'un ensemble restreint et bien défini de personnes ;
- La modification ou la réaffectation d'une installation ferroviaire 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 installation ferroviaire sera démontée après trois ans au plus.

L'OFT décide si les conditions sont réunies. En cas de doute, il y a lieu d'appliquer la procédure ordinaire.

La *procédure simplifiée* ne requiert ni publication ni mise à l'enquête publique, et la demande de prise de position du canton ou de la commune est facultative (formulation potestative). Les autorités fédérales concernées seront consultées et le projet sera soumis à d'éventuels tiers (privés), sauf s'ils ont donné préalablement leur accord écrit.

Les plans détaillés qui se fondent sur un projet déjà approuvé (ce qui est en général le cas pour les projets de détail d'installations de sécurité) sont, en règle générale, approuvés dans le cadre d'une *procédure simplifiée* (cf. ch. 5.1.3).

Pour les demandes d'approbation des plans qui ne comprennent que les aspects techniques d'une installation de sécurité et qui ne produisent pas d'effets sur des tiers (mesures architecturales perceptibles, restrictions sur le trafic routier et piétonnier existants, par ex. temps de fermeture d'un passage à niveau), l'OFT peut renoncer à demander une prise de position des autorités fédérales, du canton et de la commune ; il peut également renoncer à consulter des tiers.

Les indications concernant la nécessité d'une PAP pour les installations de sécurité se trouvent aux chapitres 5.4 et 8.

3.6 Documents à soumettre

Selon l'art. 18b LCdF, la demande d'approbation des plans doit être adressée avec les documents requis à l'OFT.

L'art. 6, al. 1, OCF fixe que les plans doivent être soumis conformément à l'OPAPIF. Selon l'art. 3, al. 1, OPAPIF, la demande d'approbation des plans doit contenir toutes les indications nécessaires à l'évaluation du projet. En l'occurrence, il s'agit notamment du rapport de sécurité (art. 3, al. 2, let. k, OPAPIF), du rapport d'examen de l'expert accompagné de la prise de position du requérant sur la mise en œuvre des mesures découlant des résultats de l'examen (let. m) et, le cas échéant, du rapport d'examen (let. l).

La Dir. OPAPIF contient des indications complémentaires et renvoie aussi à la présente directive.

La Dir. OCI-CF définit pour quels projets il faut présenter des rapports d'examen établis par des organismes de contrôle indépendants.

L'OFT peut déterminer selon l'art. 6, al. 4, OCF, en se fondant sur le rapport de sécurité de l'approbation des plans, quelles preuves de la sécurité supplémentaires selon l'art. 8a OCF devront être présentées pour les ouvrages, installations ou parties de ceux-ci.

4 Déroulement principaux des projets

Ce chapitre donne un aperçu des définitions, des rôles, des déroulements et des documents pour les « cas normaux », c.-à-d. sans tenir compte des spécificités mentionnées au chap. 5.

Les figures 1 et 2 présentent les rapports entre les exigences de l'OCF, de l'OPAPIF, des normes SN EN 50126 et SN EN 50129 ainsi qu'entre les processus venant de la pratique. Les différents rôles, les processus, l'envoi des documents et les rapports entre ces éléments sont présentés sur un axe temporel basé sur la représentation en « V » du cycle de vie d'un produit selon la norme SN EN 50126.

4.1 Déroulement standard : projet de construction – approbation des plans – réalisation (Fig. 1)

A la date T1, le GI envoie la demande d'approbation des plans avec les documents complets pour les installations de sécurité conformément au chap. 6. Il en va de même si la demande s'effectue en tant que présentation d'un projet global, qu'approbation de détail selon le ch. 5.1.3 ou que projet touchant uniquement les installations de sécurité.

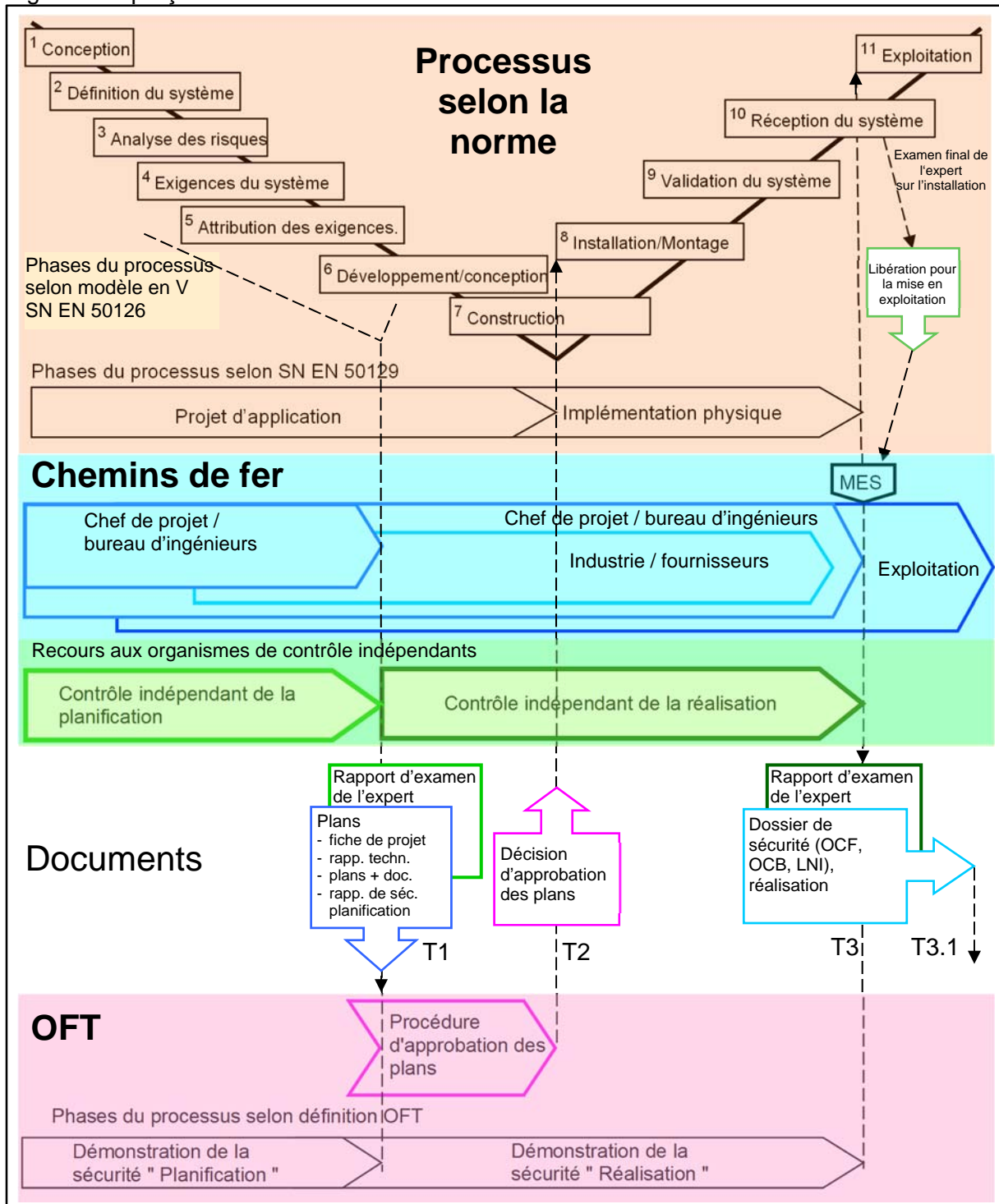
L'OFT doit rendre sa décision d'approbation des plans pour la date T2, c.-à-d. au plus tard avant le début des travaux de construction ; dans un « cas normal », l'OFT renonce à l'autorisation d'exploiter (voir ch. 6.4).

A la date T3, c.-à-d. avant la mise en service, le GI a terminé l'élaboration de la preuve de la sécurité et le rapport d'examen de la sécurité en vue de la réalisation selon le chap. 7, et plus spécialement selon le ch. 7.3.1, du moins en ce qui concerne le contenu, c.-à-d. que les documents peuvent contenir des compléments manuscrits aux points encore ouverts dans la version précédente, des protocoles d'essai ou des notes afférentes ; ces compléments serviront ensuite à finaliser formellement les documents de démonstration de la sécurité.

Un acte formel est prévu avant la mise en service : la libération pour la mise en exploitation signée par le chef de projet et l'expert.

A la date T3.1, en règle générale au plus tard un mois après la mise en service de l'installation, le requérant remet à l'OFT tous les documents de preuve en version définitive, pour information.

Figure 1 : Aperçu d'un déroulement standard



4.2 Déroulement simplifié : sans remise de documentation pour la « réalisation »

Dans quelques cas définis au chap. 8, l'OFT renonce à exiger les documents de preuve de la phase « Réalisation ». Les documents qui doivent être terminés à la date T3 restent en possession du GI (en règle générale dans l'installation). Ils doivent pouvoir être présentés sur demande à l'OFT dans le cadre d'un audit de sécurité lors de la phase d'exploitation (surveillance).

4.3 Déroulement avec une autorisation d'exploiter (fig. 2)

Le déroulement « avec une autorisation d'exploiter » ne diffère qu'à partir de la date T2 à laquelle l'OFT ordonne une autorisation d'exploiter dans l'approbation des plans (cf. ch. 6.4).

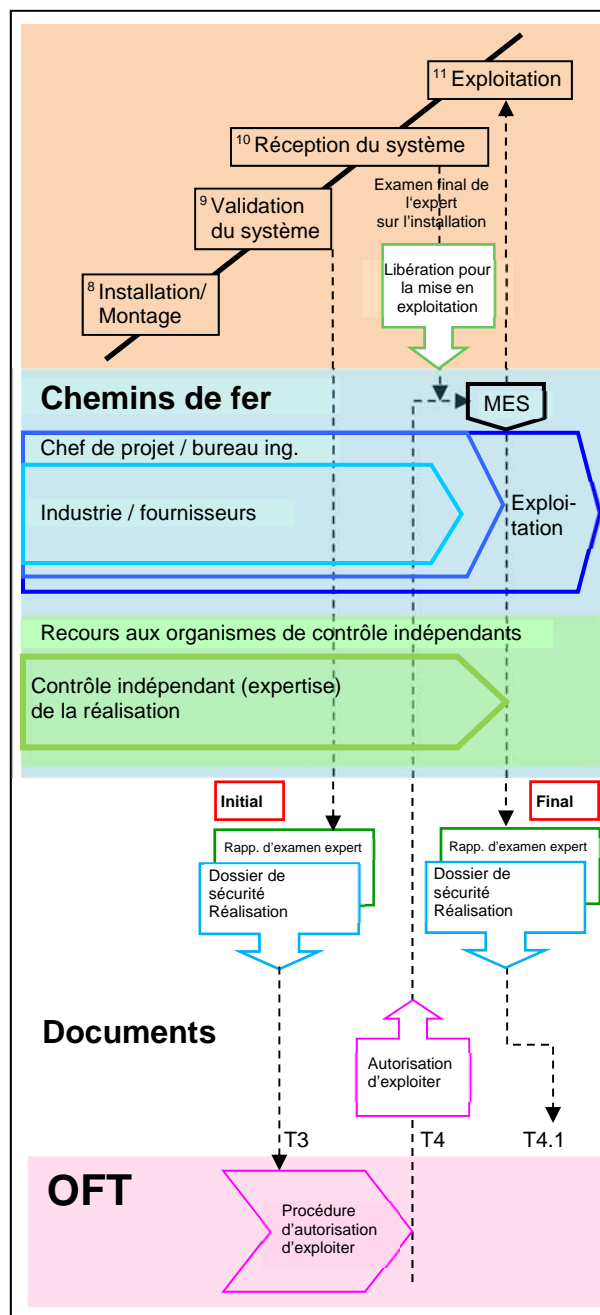
A la date T3, c.-à-d. après l'achèvement de la phase 9 (Validation), mais suffisamment tôt avant la mise en service, le GI transmet à l'OFT la preuve de la sécurité et le rapport d'examen de l'expert en vue de la réalisation selon le ch. 7.3.2. Ces documents contiennent éventuellement encore des points en suspens / à terminer (« Initial »).

A la date T4, l'OFT accorde l'autorisation d'exploiter.

A partir de cette date, l'installation peut être mise en service.

L'OFT définit dans l'autorisation d'exploiter les documents de preuve définitifs pour la démonstration de la sécurité qui devront encore être transmis (date T4.1, « Final »).

Fig. 2 : déroulement partiel de l'octroi d'une autorisation d'exploiter



MES = mise en service

5 Spécificités de procédure selon le type de projet

Selon le type de projet, différentes prescriptions doivent être respectées. Les descriptions ci-après indiquent ce dont il faut tenir compte lors de la phase de planification.

En complément au texte, la figure 3 à l'annexe 3 présente schématiquement les décisions à prendre et les points dont il faut tenir compte dans la suite du déroulement. A titre de proposition, les décisions sont intégrées aux phases visées par la norme SN EN 50126, dans lesquelles des bases de décision suffisantes devraient être disponibles.

Il va de soi que l'axe temporel n'est pas rigide ; il s'agit plutôt de la progression du contenu du projet et aussi, en règle générale, du processus itératif de l'ensemble. Le parcours des documents n'est présenté que très succinctement.

5.1 Maturité du projet

Afin de pouvoir avancer plus rapidement lors d'une procédure ordinaire, surtout pour les projets importants, les documents doivent souvent être soumis à l'OFT sans qu'ils contiennent des déclarations suffisantes dans le domaine des installations de sécurité. Il faut prendre en compte cet aspect dès que possible, c.-à-d. dès la phase 1 « Conception », et organiser l'intégration du projet d'installations de sécurité au projet global.

Cela étant, il faut distinguer les cas de figure suivants :

5.1.1 Plan A : « tout inclus »

Tous les documents relatifs au domaine des installations de sécurité sont présentés en même temps que le projet global : « cas normal » conformément aux explications du chap. 4.

5.1.2 Plan B : documents des installations de sécurité livrés ultérieurement

Les documents relatifs au domaine des installations de sécurité ne sont que partiellement prêts au moment de la présentation du projet global. Les documents manquants peuvent être livrés ultérieurement en cours de procédure, de sorte qu'ils puissent être intégrés à l'examen et à la décision d'approbation des plans du projet global.

La condition pour cela est que la partie « Installations de sécurité » concernant des tiers (par ex. nouveaux emplacements des signaux) soit déjà fixée et documentée dans le dossier du projet global. L'échéancier de présentation ultérieure des documents relatifs aux installations de sécurité doit être fourni au moment de la présentation du projet global.

La responsabilité en matière de délais incombe au requérant.

5.1.3 Plan C : projet de détail différé des installations de sécurité

Les documents relatifs au domaine des installations de sécurité ne sont pas prêts au moment de la présentation du projet global et la décision d'approbation des plans du projet global est requise avant celle des installations de sécurité : l'approbation des plans des installations de sécurité fait l'objet d'une procédure ultérieure de planification détaillée (art. 18j, al. 2, LCdF).

S'il n'y a pas d'éléments de l'installation de sécurité qui concernent des tiers (par ex. emplacement des signaux) ou si ces éléments ont déjà été fixés et documentés dans la procédure principale et restent inchangés, le projet de détail fait l'objet d'une procédure simplifiée (avec ou sans consultation du canton / de la commune). Sinon, l'approbation des plans détaillés doit également suivre la procédure ordinaire.

La demande d'effectuer ultérieurement une procédure de planification détaillée peut provenir du requérant. Cette demande doit être documentée et les échéances planifiées dans le dossier destiné à la procédure principale.

L'OFT peut également ordonner une procédure ultérieure si le dossier de demande n'est pas complet.

5.2 Type de tronçon

Selon le type de tronçon au sens de l'art. 15a OCF / de la Dir. IOP, le domaine de l'interopérabilité est régi par des exigences différentes. Cet aspect doit être pris en considération aussi tôt que possible et les travaux entamés en conséquence.

Cela étant, on distingue les cas suivants :

5.2.1 Tronçons non interopérables (en rouge)

Aucune exigence en matière d'interopérabilité : « cas normal » conformément au chap. 4

5.2.2 Réseau principal interopérable (en vert foncé)

Les exigences techniques en matière d'interopérabilité sont applicables dans leur intégralité, cf. Dir. IOP, ch. 4.1.

Les déclarations de conformité énumérées ci-après au niveau des constituants et du sous-système au sol CCS, et donc les activités d'examen des organismes notifiés sont limitées aux champs d'application de la STI CCS (GSM-R, ETCS, exigences en matière d'interface localisation de trains/annonce de voie libre) et aux constituants d'interopérabilité du CCS au sol (RBC, Radio-Infill-Unit, Eurobalise, Euroloop, LEU Eurobalise, LEU Euroloop).

Afin d'obtenir la preuve que ces exigences sont respectées, l'OFT demande au requérant durant la procédure d'approbation des plans, en précision de l'art. 3, al. 4, OPAPIF / ch. 6.1 et 6.2 de la directive sur l'OPAPIF, une déclaration de conformité IOP³ et toutes les annexes requises (« dossier technique »).

5.2.2.1 Modifications mineures et renouvellements sur des tronçons existants

Lorsqu'il s'agit de modifications simples ou du renouvellement (modification importante sans augmentation des performances) d'un tronçon existant et que l'intégration des constituants d'interopérabilité au sous-système CCS au sol suit intégralement les règles, la déclaration de conformité IOP peut être fondée sur

- (1) les déclarations de conformité des constructeurs des constituants d'interopérabilité utilisés ou les homologations de série (év. aussi pour les processus) qui incluent cette déclaration de conformité,
- (2) la mise en œuvre des dispositions déterminantes des DE-OCF, des RTE et des documents du gestionnaire du système ETCS, et
- (3) la vérification du respect de ces prescriptions par l'expert.

5.2.2.2 Nouveaux tronçons, rééquipements de tronçons existants ou changements significatifs

Lorsqu'il s'agit d'un nouveau tronçon, du rééquipement (modification importante avec augmentation des performances)⁴ d'un tronçon existant, ou lors d'un changement significatif, la déclaration de conformité IOP doit être fondée sur un certificat « CE » d'essai spécifique au projet et établi par un organisme notifié lors du suivi du projet (art. 18 de la directive [CE] sur l'interopérabilité).

Dans les deux cas, les documents basés sur la déclaration de conformité IOP du requérant (dossier de sécurité) doivent être joints à ladite déclaration (cf. art. 3, al. 3, OPAPIF / ch. 6.1 et 6.2 de la Dir. OPAPIF). Le cas échéant, il peut suffire de renvoyer à la procédure lors de laquelle les documents ont déjà été remis à l'OFT précédemment.

5.2.3 Réseau complémentaire interopérable (en vert clair)

Conformément à l'art. 15a, al. 2, OCF, il y a moins d'exigences à respecter sur le réseau complémentaire interopérable que sur le réseau principal interopérable (ch. 5.2.2), cf. Dir. IOP, ch. 4.2 et 10.

De plus, conformément à l'art. 15k, al. 3, OCF, il est possible de fournir une attestation simplifiée de conformité, établie par un organisme désigné ou par un expert ; cf. Dir. OCI-CF, partie B.

Dans ce cas également, le requérant doit présenter, en précision de l'art. 3, al. 4, OPAPIF / ch. 6.1 et 6.2 de la Dir. OPAPIF, une déclaration de conformité IOP assortie de tous les documents nécessaires (« dossier technique »).

³ Un modèle est présenté dans la RTE 25100.

⁴ Une définition plus précise et plus spécifique sera intégrée à la Dir. OCI-CF

5.3 Maturité des spécifications

Dans le cadre de la phase 2 « Définition du système », il faut évaluer les projets afin de déterminer s'ils contiennent de nouvelles exigences qui ne peuvent être respectées que par de nouvelles fonctionnalités techniques, de nouvelles possibilités de planification ou de nouveaux processus d'exploitation. Selon les cas de figure, tous ces aspects peuvent entrer en ligne de compte ou seulement une partie.

Le cas échéant, il faut lancer les travaux suivants :

5.3.1 Elaboration des nouvelles exigences

Pour les nouvelles exigences, les exploitants doivent traiter les phases 1 à 4, év. 5, afin de disposer de bases suffisantes pour le développement des sous-systèmes et des processus d'exploitation (cf. aussi fig. 4).

5.3.2 Mise en œuvre des nouvelles fonctionnalités et des possibilités de planification

5.3.2.1 Fonctionnalités techniques

Le résultat des phases susmentionnées 4 et 5 sont des spécifications d'exigences pour ces fonctionnalités, le THR afférent et le PSIA requis qui sont transmis aux sous-systèmes prévus à cet effet.

Lors de la procédure, il faut toujours prévoir une phase de test d'exploitation des nouvelles fonctionnalités.

5.3.2.2 Possibilités de planification

Les nouvelles possibilités de planification peuvent étendre des fonctionnalités existantes dans le cadre de certaines conditions d'application. Elles doivent être spécifiées de manière exhaustive à titre de référence dans la phase 4, afin d'évaluer les possibilités de planification du sous-système développé dans la phase 6.

Si la phase 6 révèle des possibilités de planification plus différenciées, celles-ci doivent être évaluées dans un nouveau processus démarrant à la phase 3.

Les paramètres de planification qui ne servent qu'à refléter l'installation et non, en premier lieu, à commander une fonctionnalité, doivent être évalués quant à leur importance pour la sécurité. De cette évaluation découlent les exigences de sécurité auxquelles doivent satisfaire les sources de données à utiliser pour la planification.

5.3.3 Besoin de nouveaux processus d'exploitation

Il s'agit de déceler dès que possible dans le projet si le choix des systèmes et constituants nécessite de nouveaux processus d'exploitation (y c. d'entretien), que ce soit pour les raisons susmentionnées ou pour d'autres motifs.

Ces processus doivent être conçus, développés et validés aussi tôt que possible, afin qu'ils puissent être intégrés en temps voulu dans la démonstration de la sécurité Planification et Réalisation.

Outre la description des processus d'exploitation, il faut déterminer dans quelles prescriptions d'exploitation les insérer et, pour chacune de celles-ci, prévoir la procédure de modification ad hoc.

5.3.4 Modification du but d'utilisation

Si seul le but d'utilisation de fonctionnalités, de possibilités de planification et de processus d'exploitation change, on appliquera en principe les règles décrites ci-dessus ; des conclusions par analogie au but d'utilisation actuel sont permises.

5.4 Catégories d'application

Lors de la phase 3 « Analyse des risques », les projets doivent être répartis en catégories d'utilisation conformément au chap. 8. La suite des travaux du projet dépend alors de cette répartition.

5.5 Dérogations

Lors de la phase 4 « Exigences du système », les projets doivent être évalués de manière à déterminer s'ils contiennent des écarts par rapport aux prescriptions d'ordre supérieur. Ces écarts doivent faire l'objet d'une demande de dérogation.

Les scénarios suivants sont envisageables :

5.5.1 Dérogation aux prescriptions (art. 5, al. 2, OCF)

Le ch. 36 de la Dir. OPAPIF indique les motifs et les documents à présenter lors de la PAP en vue de demandes de dérogation aux prescriptions conformément à l'art. 5, al. 2, OCF.

5.5.2 Dérogation aux prescriptions d'interopérabilité (art. 15e OCF)

L'art. 15e OCF définit dans quels cas il est possible de déroger aux STI (al. 2) et à quelles exigences une demande de dérogation doit satisfaire (al. 3) en renvoyant à la Directive (CE) sur l'interopérabilité (conformément à la Dir. OPAPIF, partie D complétée).

5.6 Maturité d'application du produit

Lors de la phase 5 « Attribution des exigences du système », il faut déterminer le degré de maturité technico-sécuritaire des composants prévus pour le système.

On peut distinguer les cas suivants :

5.6.1 Projet standard

Par « projets standards », on entend les projets dans lesquels sont utilisés exclusivement des produits et des fonctions homologués ou déjà vérifiés et éprouvés ailleurs, qui sont fondés intégralement sur la RTE Compendium Installations de sécurité et qui mettent en œuvre les prescriptions d'ordre supérieur (DE-OCF, PCT).

La phase « Planification » de la démonstration de la sécurité spécifique à une installation peut, en règle générale, être achevée dès que les résultats de la phase 5 (conformément à la norme SN EN 50126, fig. 9, principalement la « spécification des exigences relatives aux sous-systèmes et aux composants » [dossier de construction]) sont disponibles. Lors de projets standards, il est possible de présenter le dossier de construction plus tôt, puisqu'il est connu et qu'il peut renvoyer aux homologations de série, confirmer le respect des conditions d'utilisation importantes pour la sécurité et se fonder sur la sécurité fournie grâce à l'approche basée sur les règles.

Par conséquent, on applique la procédure « cas normal » conformément au chap. 4.

5.6.2 Projets de produits liés à une première utilisation de nouvelles fonctions

Utilisation de nouvelles fonctions qui ne sont pas encore homologuées ni éprouvées sur le plan technico-sécuritaire 5.6.3.

Exemples : la PAP se fonde sur une démonstration de la sécurité encore inachevée dans le cadre d'une procédure d'homologation en cours, ou bien il est prévu de perfectionner un produit déjà homologué pour son utilisation (modifications prototypiques).

Le rapport de sécurité pour la phase « Planification » doit démontrer qu'un dossier de sécurité existe, qu'il permet l'application générique de ces fonctions et que ladite application générique présente un degré de maturité suffisant pour projeter des applications spécifiques de façon sûre.

5.6.3 Projets liés à l'utilisation de nouveaux produits

Lors de projets qui prévoient l'utilisation de nouveaux produits (c.-à-d. non homologués), le requérant doit attendre, avant de présenter la demande d'approbation des plans, que les conditions essentielles d'application spécifique soient connues, de même que le moment à partir duquel le produit générique sera disponible pour les tests appropriés pour l'application spécifique.

Le rapport de sécurité pour la phase « Planification » doit démontrer qu'un dossier de sécurité existe, qu'il permet l'application générique de ces fonctions et que ladite application générique présente un degré de maturité suffisant pour projeter des applications spécifiques de façon sûre.

Lorsque cela n'est pas possible, une procédure ultérieure de planification détaillée est envisageable pour cet élément ; il est aussi possible d'indiquer la solution de remplacement au cas où le produit n'atteint pas à temps le degré de maturité requis.

Dans le cas contraire, l'OFT n'octroie pas d'approbation des plans pour l'élément concerné.

5.6.4 Evaluation du degré de maturité en vue de l'application du produit

La figure 4 à l'annexe 4 présente l'évaluation en question à l'aide du modèle en « V » et de la relation PAP du projet – développement du sous-système (produit).

5.6.5 Harmonisation du développement de l'application et du projet d'installation

Lors de projets conformément aux ch. 5.6.2 et 5.6.3, il faut tenir compte des points suivants :

- Il faut indiquer la collaboration entre le développement de l'application et le projet d'installation ; les domaines de responsabilité doivent être définis.
- Les plans de sécurité doivent être établis dès les premières phases du projet et ce, de manière exhaustive et dans une qualité élevée ; ils doivent être coordonnés entre eux.
- La planification doit tenir compte des risques liés aux développements non achevés de produits et d'applications.

5.7 Changements significatifs

Dans le contexte des évaluations visées aux ch. 5.3 à 5.6, il faut vérifier si les nouveaux développements constituent des changements significatifs au sens de l'art. 8c OCF / du chap. 18 Dir. OCI-CF.

Si tel est le cas, il faut prévoir la suite de la procédure conformément au chap. 18 Dir. OCI-CF (exécution d'une procédure de gestion des risques conformément au règlement MSC et recours à un organisme d'évaluation des risques en vue d'un contrôle indépendant et de l'établissement du rapport d'évaluation de la sécurité).

Ladite procédure de gestion des risques prescrit des démarches spécifiques dont la plupart ont lieu lors des phases 1 à 4 visées par la norme SN EN 50126, mais elle prescrit aussi l'évaluation, par l'organisme d'évaluation des risques, de la démonstration de la sécurité.

Ainsi, le rapport d'évaluation de la sécurité dressé par l'organisme d'évaluation des risques doit être joint au dossier de PAP.

6 Procédure d'approbation des plans (PAP)

Ce chapitre précise les documents à soumettre dans le cadre d'une PAP pour le domaine des installations de sécurité et les exigences de fond prévues, compte tenu des bases juridiques existantes, de la Dir. OPAPIF, de la Dir. OCI-CF et de la norme SN EN 50129. Les délais à

prendre en compte pour la soumission et les critères pour renoncer à l'autorisation d'exploiter par l'OFT sont décrits.

Les exigences spécifiées dans ce chapitre partent du principe de la construction ou du renouvellement complet d'installations de sécurité avec un haut niveau de sécurité (par ex. poste d'enclenchement) (catégorie H1 au ch. 8.2).

6.1 Documents à présenter

Les exigences à remplir pour les demandes d'approbation des plans pour les projets d'installations de sécurité sont fixées dans la Dir. OPAPIF, parties C et E, et au ch. 6.2.

Pour une installation de sécurité, il faut par conséquent présenter notamment les documents suivants :

- Fiche de projet (ch. 28 de la Dir. OPAPIF)
- Rapport technique (ch. 29 de la Dir. OPAPIF)
- Rapport de sécurité (ch. 37 de la Dir. OPAPIF) [Rapport de sécurité pour la phase « Planification » conformément au ch. 6.2.1]
- Le cas échéant, rapport d'évaluation de la sécurité (ch. 38 de la Dir. OPAPIF)
- Rapport d'examen de l'expert y c. une prise de position sur la mise en œuvre des mesures issues des résultats des examens (ch. 39 de la Dir. OPAPIF)
- Le cas échéant, déclarations de conformité IOP, assorties des dossiers techniques afférents (cf. ch. 5.2.2 et 5.2.3)
- Plans détaillés et indications détaillées conformément à la Dir. OPAPIF, ch. 47.1.2.1 à 47.1.2.6, ch. 47.1.3 et ch. 47.1.4, ch. 47.2.1 à 47.2.5 et ch. 47.3

6.2 Exigences quant au contenu des documents

La norme SN EN 50126 décrit le cycle de vie d'un système au moyen d'un modèle de phases (cf. fig. 1 au chap. 4). La PAP commence, selon le degré de maturité de l'application du produit conformément au ch. 5.6, lorsque les résultats de la phase 5 (conformément à la norme SN EN 50126, figure 9, principalement la « spécification des exigences relatives aux sous-systèmes et aux constituants » [dossier de construction]) sont disponibles⁵ et que la démonstration de la sécurité et l'expertise sont achevées pour la phase « Planification ». Les informations afférentes doivent donc figurer dans les documents susmentionnés du projet, de la démonstration de la sécurité ou de l'expertise.

Lors de l'examen technique dans le cadre d'une PAP, l'OFT contrôle principalement les aspects de la sécurité de la construction et de l'exploitation ainsi que l'interopérabilité. Les aspects de fiabilité, de disponibilité et de maintenabilité sont pris en compte notamment dans la mesure où ils ont une influence sur la sécurité et sur l'interopérabilité.

6.2.1 Rapport de sécurité des installations de sécurité, phase « Planification »

Afin que le rapport de sécurité conformément à la Dir. OPAPIF satisfasse aux exigences en ce qui concerne les installations de sécurité, il doit être établi sous forme de preuve de la sécurité pour une application spécifique pour la « conception de l'application » selon la norme SN EN 50129, ch. 5.5.1.

Le rapport de sécurité de la phase « Planification » doit contenir les résultats des activités de sécurité en fonction des phases 1 à 4 ou 1 à 6⁶ conformément à la norme SN EN 50126.

⁵ Pour les projets standards, on considère qu'il est suffisant d'en connaître l'existence, dans la mesure où il est indiqué comment la concrétisation du dossier de construction est vérifiée avant le début de l'implémentation physique.

⁶ Selon le degré de maturité de l'application du produit, cf. ch. 5.6

Voici les exigences quant au contenu⁷:

Remarque :

Les passages en *italique* renvoient aux chapitres et termes correspondants de la norme SN EN 50129.

6.2.1.1 Définition du système

Ici, l'objet de l'approbation auquel se réfère le rapport de sécurité doit être défini ou référencé avec précision. Les aspects suivants doivent obligatoirement être couverts :

- Fonctionnalité, états d'utilisation
- Champ d'action, délimitation
- Architecture du système

Selon la Dir. OPAPIF, cette définition fait partie intégrante du rapport technique. Dans le rapport de sécurité, il peut par conséquent être judicieux de faire référence au rapport technique (et inversement).

6.2.1.2 Rapport de la gestion de la qualité

Cette partie doit contenir la preuve que, pour tous les participants, la qualité de la planification a été garantie par un système de gestion de la qualité.

A titre de base, on peut renvoyer à un système de gestion de la qualité (QMS) certifié et établi au sein de l'entreprise requérante, ainsi qu'à la réglementation contractuelle des exigences QMS avec les fournisseurs concernés.

Le respect des étapes prévues de garantie de la qualité doit être indiqué dans la partie « Gestion de la sécurité ».

6.2.1.3 Rapport de la gestion de la sécurité

Cette partie doit contenir la preuve que la sécurité de l'installation est garantie par l'utilisation d'un système de gestion de la sécurité lors de la planification.

A titre de base, on peut renvoyer au QMS reconnu dans le cadre de la procédure d'agrément de sécurité conformément à l'art. 8a LCdF, si ce système tient suffisamment compte des exigences de la norme SN EN 50129.

Il faut en particulier indiquer les informations spécifiques au projet (cf. également remarque au ch. 6.2.1.4) concernant les domaines et mots-clés suivants :

- *Organisation sécurité de la phase Planification et, si elle existe, de la phase Réalisation*
 - responsabilités, compétences, indépendances
- *Plan d'assurance sécurité de la phase Planification et, s'il existe, de la phase Réalisation*
 - délais, responsabilités pour la démonstration de la sécurité et l'expertise
 - éven. les jalons des procédures d'homologation de série concernées
- *Analyse de risques (registre des situations dangereuses, spécification des exigences de sécurité)*
 - méthodes (règles de base, prise en compte des risques), principes
 - exigences de la sécurité
- *Reviews et vérification de sécurité*

En général, les autres sous-sections des ch. 5.3 et 5.4 de la norme SN EN 50129 ne requièrent pas d'informations explicites dans le rapport de sécurité, en particulier pas lors de l'utilisation de systèmes homologués ou de systèmes éprouvés, sujets à la garantie des droits acquis.

⁷ Il est prévu d'intégrer les parties suivantes du ch. 6.2.1 à la D RTE 25100 (en cours d'élaboration) et de les supprimer de la présente directive lors de la prochaine révision.

6.2.1.4 Rapport de sécurité technique

Dans ce chapitre (ou dans un document séparé référencé), il y a lieu d'apporter la preuve d'une sécurité technique et fonctionnelle suffisante de l'installation, au niveau de la conception de l'application.

Le rapport de sécurité technique doit contenir au moins les informations suivantes concernant les domaines et les mots-clés suivants :

- *Introduction*
- Preuve d'une conception correcte (*assurance d'une exploitation fonctionnelle correcte*)
 - description de l'architecture du système, identification des sous-systèmes/composants
 - définition des interfaces (conception, exploitation, maintenance, interfaces internes et externes du système)
 - respect des spécifications des exigences du système et de sécurité
 - respect des bases juridiques
- *Effets des pannes*
- *Exploitation en présence d'influences externes*
- *Conditions d'utilisation relatives à la sécurité*
 - Conditions d'utilisation prévues pour la réalisation et l'exploitation de l'installation
 - Processus d'exploitation et de maintenance
- *Tests de qualification de la sécurité*

Si des sous-systèmes ou composants homologués sont utilisés, on peut faire référence à leur homologation de série. Dans le rapport de sécurité technique, il faut prouver qu'en l'occurrence, les exigences de sécurité et les conditions d'utilisation peuvent être remplies.

Remarque :

Une simplification est possible en distinguant les contenus qui restent identiques pour toutes les installations d'une classe (application générique) et ceux qui doivent être déterminés particulièrement pour chaque installation (application spécifique). Des contenus identiques pour une classe d'installation peuvent être résumés dans une preuve de la sécurité pour cette classe. Ce document peut être référencé dans le rapport de sécurité de chaque installation. S'il existe des processus d'entretien et d'exploitation ou des prescriptions qui sont appliqués de la même manière à différentes reprises, on peut référencer la documentation correspondante. L'OFT fixera de cas en cas l'ampleur de la documentation à présenter. Cette référence est habituellement suffisante, quand les réglementations citées des processus ont été déposées préalablement à l'OFT pour un examen unique et lorsque le service des modifications est garanti. L'OFT se réserve le droit de demander, le cas échéant, les documents de la gestion de la qualité et la preuve de leur observation.

6.2.1.5 Dossiers de sécurité connexes

Dans cette partie, il faut démontrer les relations entre les preuves de la sécurité, les rapports d'examen de la sécurité et les homologations de série des composants et des sous-systèmes ainsi que les systèmes voisins. Il faut notamment démontrer comment les conditions d'utilisation relatives à la sécurité des différents systèmes sont remplies.

6.2.1.6 Conclusion

Dans cette partie, il faut confirmer que le projet correspond aux bases juridiques déterminantes (par ex. du fait de l'application de la RTE et de règlements internes au chemin de fer) ou que les dérogations ont été demandées et que l'installation construite selon ces prescriptions peut être exploitée de manière sûre.

6.2.2 Rapport d'examen de l'expert relatif à la phase « Planification »

Le rapport doit couvrir les phases 1 à 4 et 1 à 6 selon la norme SN EN 50126.

Les chap. 8 et 9 de la Dir. OCI-CF fournissent des indications quant aux exigences concernant le mandat d'expertise, l'étendue de l'expertise et le rapport d'examen de l'expert. La description de l'activité d'expertise au ch. 5.5.2, de la SN EN 50129, s'applique également.

Il est recommandé de clarifier et d'octroyer le mandat d'expertise (bases, étendue, profondeur, documentation) dès que possible. Les indications relatives au mandat et au mandataire font partie de la gestion de la sécurité (ch. 6.2.1.3). Elles doivent être intégrées au rapport de sécurité ou au moins y être référencées, afin que l'OFT puisse les consulter.

Conformément à l'art. 3, al. 2, let. m, OPAPIF, le rapport d'examen de l'expert doit être assorti d'une prise de position du requérant sur la mise en œuvre des mesures qui découlent des résultats de l'examen. Pour plus de détails à ce sujet, cf. ch. 10.1 de la Dir. OCI-CF.

6.3 Moment de la présentation des documents / délais de traitement

Conformément aux principes juridiques généraux, la construction d'une installation ne peut commencer qu'une fois la décision d'approbation entrée en force ; cela étant, l'OFT peut autoriser des exceptions dans certaines conditions, conformément à l'art. 6, al. 3, OPAPIF.

Aux termes de l'art. 8, al. 1, OPAPIF, les demandes sont traitées en général dans les délais suivants : 12 mois pour la procédure ordinaire (sans expropriation) et 4 mois pour la procédure simplifiée. Il s'agit de délais d'ordre dont le but est d'assurer le bon déroulement de la procédure mais sans avoir de conséquences juridiques ni ne conférer des droits au requérant en cas de non-respect.

Le délai de traitement commence à courir dès que l'OFT a reçu tous les documents à présenter à l'appui de la demande (art. 8, al. 2, OPAPIF) ; exceptions cf. ch. 5.1 (envoi échelonné et planifié des documents). L'OFT vérifie si le dossier est complet (art. 18b LCdF). Pendant la PAP, il peut exiger des preuves approfondies spécifiques et des examens d'experts (cf. également ch. 5.5).

Si des changements significatifs surviennent par rapport au projet original pendant la procédure d'approbation des plans, les modifications doivent être soumises immédiatement à l'OFT. Selon l'état de la procédure et le type de modification, celles-ci seront traitées comme au ch. 7.4.

6.4 Autorisation d'exploiter

L'OFT définit au cas par cas, autrement dit dans la décision d'approbation des plans, s'il peut renoncer à délivrer une autorisation d'exploiter.

Une autorisation d'exploiter de l'OFT est indispensable lorsqu'elle est requise en vertu de l'art. 8, al. 1, let. a, ou de l'art. 15d OCF (« changement significatif » ou « rééquipement »). Pour vérifier l'évaluation du requérant (cf. ch. 5.7) quant à un changement significatif conformément à l'art. 8c OCF, l'OFT se fonde sur les définitions du chap. 18 de la Dir. OCI-CF.

Par ailleurs, en vertu de l'art. 8, al. 2, OCF (marge d'appréciation), l'OFT exige une autorisation d'exploiter s'il a d'autres motifs d'accompagner étroitement un projet jusqu'à sa mise en service.

Ces motifs peuvent notamment exister :

- lorsqu'un GI utilise pour la première fois un système important pour la sécurité sur son réseau
- lorsqu'un GI introduit un nouveau processus dans le déroulement d'un projet (par ex. nouveaux outils pour l'étude d'un projet, sous-traitance des processus internes)
- lorsque le développement d'un produit n'est pas encore achevé au moment de l'approbation des plans (cf. ch. 5.6.2).

7 Réalisation de l'installation (construction et mise en service)

Ce chapitre définit quels documents doivent être soumis en rapport avec la construction ou la réalisation d'une installation de sécurité. Les exigences de fond de ces documents sont fixées en tenant compte des bases juridiques existantes, de la Dir. OPAPIF et de la norme SN EN 50129. Les délais de soumission à prendre en considération et les démarches nécessaires lors des modifications de projet y sont expliqués.

Les exigences spécifiées dans ce chapitre partent du principe de la construction ou du renouvellement complet d'installations de sécurité avec un haut niveau de sécurité (par ex. poste d'enclenchement) (catégorie H1, cf. ch. 8.2).

7.1 Documents à élaborer

La preuve doit être apportée que les installations de sécurité ont été construites conformément aux approbations des plans correspondantes et qu'elles permettent une exploitation sûre.

L'OFT requiert généralement, avec l'approbation des plans, l'élaboration d'une preuve de la sécurité selon l'art. 8a, OCF. Celle-ci doit être fournie, que l'OFT ait renoncé ou non à une autorisation d'exploiter (cf. ch. 6.4).

Selon l'art. 8a, al. 4, OCF, l'OFT requiert généralement le recours à un expert – nommé « chargé d'évaluation » dans la norme SN EN 50129 – pour l'examen de cette preuve de la sécurité. Cet expert doit satisfaire aux exigences du ch. 6.3 de la Dir. OCI-CF.

Le rapport d'examen à établir conformément au chap. 9 de la Dir. OCI-CF est appelé ci-après rapport d'examen de l'expert pour la phase « Réalisation » ; dans la norme SN EN 50129, ce document est appelé rapport d'évaluation de la sécurité.

Ainsi, pour une installation de sécurité, il faut élaborer et soumettre :

- la preuve de la sécurité pour la réalisation (*réalisation physique*),
- le rapport d'examen de l'expert pour la phase « Réalisation ».

7.2 Exigences quant au contenu des documents

Afin que la preuve de la sécurité selon l'art. 8a OCF satisfasse aux exigences, elle doit être fournie sous la forme du dossier de sécurité pour la réalisation physique d'une application spécifique selon la SN EN 50129, ch. 5.5.1.

Le rapport d'examen de l'expert pour la phase « Réalisation » doit contenir les indications visées au chap. 9 de la Dir. OCI-CF et satisfaire aussi aux exigences de la norme SN EN 50129.

Il va de soi que ces documents peuvent se baser sur les documents correspondants de la phase PAP/Planification selon le ch. 6.2. Les contenus exigés sont indiqués explicitement ici pour plus de clarté. Il faut décider, selon les cas, ce qui peut être repris des anciens documents ou adapté.

7.2.1 Dossier de sécurité pour la réalisation

Le dossier de sécurité pour la réalisation doit couvrir les activités sécuritaires des phases qui n'ont pas encore été traitées lors de la phase de planification ; il s'agit, en règle générale, des phases 6 (développement/construction et implémentation) à 9 (validation du système) conformément à la norme SN EN 50126.

Les exigences quant au contenu sont spécifiées ci-après⁸ :

⁸ Il est prévu d'intégrer les parties suivantes du ch. 7.2.1 à la D RTE 25100 (en cours d'élaboration) et de les supprimer de la présente directive lors de la prochaine révision.

Remarque :

Les passages en *italique* renvoient aux chapitres et termes correspondants de la norme SN EN 50129.

7.2.1.1 Définition du système

Cf. ch. 6.2.1.1

7.2.1.2 Rapport de gestion de la qualité

Cette partie doit apporter la preuve que la qualité de la réalisation a été assurée par toutes les parties impliquées moyennant un système de gestion de la qualité.

Cf. aussi ch. 6.2.1.2.

7.2.1.3 Rapport de gestion de la sécurité

Cette partie doit apporter la preuve que la sécurité de l'installation a été garantie, lors de la réalisation, moyennant un système approprié de gestion de la sécurité. En règle générale, cette partie se fonde sur le rapport de gestion de la sécurité pour la phase « Planification ».

Remarques sur les bases générales cf. ch. 6.2.1.3.

Il y a lieu, en particulier, de fournir les informations spécifiques au projet (cf. remarques afférentes au ch. 6.2.1.4) concernant les domaines et mots-clés suivants :

- *Organisation de la sécurité*
 - Responsabilités, compétences, indépendances
- *Analyse de risques (registre des situations dangereuses)*
 - Processus visant la mise à jour de l'analyse des risques (si nécessaire)
- *Conception de l'installation (conception du système/sous-système/remise de l'équipement)*
 - Processus, méthode pour la conception de l'installation
 - Démarche avec les produits génériques
- *Reviews, vérification et validation de la sécurité*
- *Exploitation et maintenance*
 - Prise en considération des conditions d'utilisation relatives à la sécurité lors de la phase d'exploitation

En général, les autres sous-sections des ch. 5.3 et 5.4 de la norme SN EN 50129 ne requièrent pas d'informations explicites dans le dossier de sécurité pour la réalisation, en particulier pas lors de l'utilisation de systèmes homologués ou de systèmes éprouvés, sujets à la garantie des droits acquis.

7.2.1.4 Rapport de sécurité technique

Dans ce chapitre (ou dans un document séparé référencé), il y a lieu d'apporter la preuve d'une sécurité technique et fonctionnelle suffisante de l'installation réalisée.

Le rapport de sécurité technique doit contenir au moins les informations sur les domaines et mots-clés suivants:

- *Introduction*
- *Preuve d'un fonctionnement correct (assurance d'une exploitation fonctionnelle correcte)*
 - Réalisation des exigences du système
 - Réalisation des exigences de sécurité
 - Fonctionnement correct des interfaces
- *Effets des pannes*
 - Indépendance des unités prises en considération
 - Détection et effets de pannes
 - Action après détection d'une panne
- *Exploitation en présence d'influences externes*

- *Conditions d'utilisation relatives à la sécurité*
 - Conditions d'utilisation spécifiques pour l'exploitation de l'installation
 - Prescriptions d'exploitation et de maintenance
- *Tests de qualification de la sécurité*

Cf. aussi remarque au ch. 6.2.1.4.

7.2.1.5 Dossiers de sécurité connexes

Cette partie doit démontrer les relations entre les preuves de la sécurité, les rapports d'examen de la phase planification et les homologations de série des composants et des sous-systèmes ainsi que les systèmes voisins. En particulier, on doit démontrer ici comment les conditions d'utilisation relatives à la sécurité des différents systèmes sont remplies.

Cette partie doit également démontrer que les conditions d'utilisation relatives à la sécurité qui sont spécifiées dans les preuves de sécurité des sous-systèmes connexes sont respectées, ou qu'elles ont été incorporées dans les prescriptions techniques et d'exploitation.

Remarque :

Si des équipements ou des sous-systèmes avec une homologation de série sont utilisés, le GI doit prouver que les équipements et sous-systèmes homologués sont employés conformément à l'homologation de série et que les exigences de sécurité ainsi que les conditions d'utilisation de l'homologation de série sont réalisées dans ce cas concret.

7.2.1.6 Conclusion

Cette partie doit confirmer que l'installation est construite conformément à l'approbation des plans, qu'elle correspond aux bases juridiques et qu'elle permet une exploitation sûre.

7.2.2 Rapport d'examen de l'expert pour la phase « Réalisation » (« rapport d'évaluation de la sécurité »)

Le rapport d'examen de l'expert pour la réalisation doit contenir les indications visées au chap. 9 de la Dir. OCI-CF et satisfaire aussi aux exigences de la norme SN EN 50129.

L'examen couvre en principe toutes les phases du projet. Du point de vue du contenu, il se limite aux phases qui n'ont pas encore été traitées lors de la planification ; en général, il s'agit des phases 6 (développement/construction et implémentation) à 9 (validation du système, y c. acceptation de la sécurité) conformément à la norme SN EN 50126. Les résultats du rapport d'examen de l'expert pour la phase « Planification » conformément au ch. 6.2.2 doivent être pris en compte et examinés quant à leur validité et à leur mise en œuvre.

Le mandat d'examen des experts (bases, ampleur et degré d'approfondissement de l'examen, év. essais sur l'installation, documentation) fait partie de la gestion de la sécurité (ch. 7.2.1.3). Il doit être incorporé ou référencé dans le rapport d'examen de l'expert afin qu'il puisse être consulté par l'OFT.

Il faut confirmer au plus tard avec le rapport d'examen de l'expert pour la phase « Réalisation » que les charges importantes pour la sécurité formulées dans la décision d'approbation des plans ont été exécutées ; la conclusion doit indiquer si l'expert estime que l'installation peut être mise en service ou non (cf. ch. 9.2.2, chap. 7, Dir. OCI-CF).

Par analogie à l'art. 3, al. 2, let. m, OPAPIF, le rapport d'examen de l'expert pour la phase « Réalisation » doit également être assorti d'une prise de position sur les mesures découlant des résultats de l'examen. Pour plus de détails, cf. ch. 10.1 de la Dir. OCI-CF.

7.3 Moment de la présentation des documents

Comme le prévoit le ch. 7.1, les documents de preuve doivent être établis de toute manière, que l'OFT renonce ou non à une autorisation d'exploiter (cf. ch. 6.4).

L'octroi d'une autorisation d'exploiter entraîne des étapes de procédure supplémentaires et influe sur le moment auquel les documents de preuve doivent être présentés.

7.3.1 Sans autorisation d'exploiter

Le dossier de sécurité et le rapport d'examen de l'expert pour la phase « Réalisation » (c.-à-d. la démonstration de la sécurité toute entière) doivent être achevés avant la mise en service. En règle générale, ils doivent être portés à la connaissance de l'OFT en même temps que la prise de position visée au ch. 7.2.2, dernier paragraphe, au plus tard un mois après la mise en service.

Dans la pratique, les derniers travaux sont souvent effectués directement avant la mise en service. Dans ces cas, il est tout de même possible de terminer et de valider une version définitive de la preuve de la sécurité avant la conclusion des travaux. Les points non résolus à ce moment doivent être clairement identifiés dans la preuve de la sécurité ; les risques pouvant en découler doivent être connus et les processus pour régler ces points doivent être fixés et documentés.

Si le dossier de sécurité n'est achevé que peu avant la mise en service d'une installation, il n'est souvent pas possible d'achever le rapport d'examen de l'expert pour la phase « Réalisation » avant la mise en service. Les contrôles proprement dits de l'expert doivent toutefois être achevés impérativement avant la mise en service de l'installation. L'expert doit avoir confirmé par écrit que l'installation est prête à l'exploitation. Le rapport d'examen de l'expert (c.-à-d. la documentation complète de l'examen et du contrôle) doit ensuite être achevé.

7.3.2 Avec autorisation d'exploiter

L'OFT octroie l'autorisation d'exploiter selon l'art. 8, al. 4, OCF lorsque la preuve de la sécurité a été examinée et que les autres charges prévues par l'approbation des plans ou l'homologation de série sont remplies.

Afin que l'autorisation d'exploiter puisse être donnée à la date de la mise en service souhaitée par le requérant, le dossier de sécurité et le rapport d'examen de l'expert pour la phase « Réalisation », y c. la prise de position visée au ch. 7.2.2, dernier paragraphe, doivent être présentés à temps à l'OFT pour examen. Les points non résolus au moment de l'édition définitive de ces documents doivent y être clairement identifiés; les risques pouvant en découler doivent être connus et les processus pour régler ces points doivent être fixés et documentés.

Le temps nécessaire à l'examen des documents et à l'établissement d'une autorisation d'exploiter est généralement court, mais peut toutefois fortement varier selon les projets. Une coordination anticipée entre le requérant et l'OFT est recommandée.

7.4 Modifications du projet

Si les plans approuvés subissent des modifications, il faut lancer une nouvelle procédure pour les éléments modifiés (art. 5, al. 2, OPAPIF). Le type de procédure (voir ch. 3.5) dépend du genre de modification, mais comme cela n'affecte généralement pas les droits des tiers (intérêts dignes de protection), une procédure technique simplifiée sera suffisante.

De légères différences par rapport aux plans approuvés doivent être documentées et remises à l'OFT pour information en même temps que le dossier de sécurité pour la phase « Réalisation ».

Des différences peuvent être considérées comme légères si elles n'affectent pas les droits de tiers, si elles n'entrent pas dans les catégories H1, H2 ou G1 ou si elles sont évaluées selon le chapitre 8.2.

8 Catégories d'application

Selon le ch. 22 de la Dir. OPAPIF, le degré d'approfondissement du contrôle des documents du projet dépend des conditions spécifiques à la matière et à la situation. Pour les installations de sécurité, cette exigence est spécifiée ci-dessous.

Les chap. 6 et 7 de la présente directive se réfèrent aux bases juridiques existantes, à la Dir. OPAPIF et à la norme SN EN 50129. Ils spécifient entre autres quels documents de preuve doivent être élaborés pour les installations de sécurité, à quelles exigences de fond ces documents doivent satisfaire et lesquels de ces documents doivent être soumis à l'OFT dans quels délais. On se fonde sur le principe de la construction ou du renouvellement complet d'installations de sécurité présentant un haut niveau de sécurité (par ex. poste d'enclenchement).

En principe, ces deux chapitres s'appliquent aussi à tous les autres projets de modification et de construction qui concernent des installations de sécurité. En ce qui concerne la méthodologie à appliquer, les exigences de ces chapitres sont pratiquement inchangées pour les projets les plus simples. Pour certains projets, les exigences peuvent toutefois être réduites quant à l'ampleur des documents de preuve à fournir ou à soumettre.

Dans ce chapitre, on définit des catégories d'application dans le but de pouvoir en assigner une à chaque projet de modification ou de construction sur la base de caractéristiques typiques.

8.1 Critères

Pour la fixation des catégories d'application, les niveaux d'intégrité de la sécurité des objets d'approbation (effets/conséquences) et le genre des projets de construction ou de modification (probabilité d'erreurs) sont pris en considération :

8.1.1 Importance pour la sécurité

- H Haute : systèmes/fonctions avec une grande importance pour la sécurité (THR < 10^{-5} /h, SIL 1 – 4)
- G Faible : systèmes/fonctions avec une faible importance pour la sécurité mais avec de hautes exigences FDM
- K Aucune : systèmes/fonctions avec une faible importance pour la sécurité et de faibles exigences FDM ainsi que systèmes/fonctions sans importance pour la sécurité (aucune exigence de sécurité)

Pour déterminer l'importance pour la sécurité d'un projet, il faut considérer non seulement les systèmes/fonctions directement concernés, mais aussi leurs effets/conséquences sur l'ensemble du système et sur les systèmes voisins.

8.1.2 Type de projet

Les quatre catégories suivantes sont déterminées sur la base de la probabilité d'erreurs (en particulier les défaillances systématiques) :

- 1) Construction ou renouvellement d'installations de sécurité, modifications majeures et/ou complexes d'installations de sécurité.
Exemples :
 - renouvellement d'un poste d'enclenchement

- nouvelle commande d'un passage à niveau
- transformation complexe d'une installation de sécurité
- première utilisation de composants ou de systèmes partiels

2) Modifications **influant** sur les aspects fonctionnels ou conceptuels et/ou les prescriptions de service du système ou de l'installation, avec toutefois une ampleur et/ou une complexité limitée, avec une faible probabilité de défaillances systématiques.

Exemples:

- complément/transformation d'une installation de sécurité
- augmentation de la vitesse admise

3) Modifications de l'installation de sécurité **n'influant pas** sur les aspects fonctionnels ou conceptuels ni sur les prescriptions de service du système ou de l'installation; la probabilité de défaillances systématiques est très faible ou est couverte par l'homologation de série des composants.

Exemples:

- correction d'erreurs de l'installation (implémentation d'une application spécifique)
- correction des erreurs du système/produit (produit générique/application)
- remplacement des sous-systèmes par une génération plus récente (fonction et technologie identiques)

4) Démontage/remontage au même endroit. Aucun danger de défaillance systématique.

Exemple:

- démontage/montage de composants ou de sous-systèmes d'une installation de sécurité sans changement, par ex. en cas de renouvellement de la voie

Les projets de la catégorie (4) sont placés sous la responsabilité du GI et ne font pas l'objet de la présente directive.

8.1.3 Classement

Sur la base de l'estimation des risques, les GI assignent une catégorie d'application à chaque projet et documentent leur décision et leurs réflexions.

En plus des descriptions des critères ci-dessus, les questions suivantes peuvent aider à l'attribution d'une catégorie déterminée (position dans la matrice, voir ch. 8.2) à un projet:

- Où se trouve le projet sur les axes du tableau « probabilité d'erreurs » et « effets/conséquences » ci-dessous?
- Quelles phases visées par la représentation en « V » de la SN EN 50126 sont concernées?
- Des processus d'exploitation sont-ils concernés ? Lesquels ? Comment ?
- Quel tests ou contrôles doivent être répétés?

L'OFT examine par sondages dans les procédures d'approbation des plans ainsi que dans le cadre de la surveillance durant la phase d'exploitation, si les catégories d'application appropriées ont été appliquées, notamment dans le but de s'assurer que les processus et les responsabilités pour ces classements sont définis et implémentés dans l'entreprise.

8.2 Vue d'ensemble des exigences

Type de projet		Importance pour la sécurité		
		Aucune	Faible	Haute
1 Construction, renouvellement, modification majeure		K1	G1	H1
2 Modifications ayant une influence sur le concept, le fonctionnement, les prescriptions d'exploitation		K2	G2	H2
3 Modifications sans influence sur le concept, le fonctionnement, les prescriptions d'exploitation		K3	G3	H3

Couleur Signification en bref



PAP nécessaire
 Démonstration de la sécurité complète selon les chapitres 6 et 7.
 Les documents de démonstration de la sécurité « Réalisation » doivent être remis.



PAP nécessaire
 Démonstration de la sécurité selon les chapitres 6 et 7 avec des exigences réduites (se focaliser sur les effets ; validation et expertise peuvent être groupées, voir ch. 8.3.2).

Les documents de démonstration de la sécurité « Réalisation » ne doivent pas être remis, à moins qu'il en soit décidé autrement (par des charges) ou qu'ils soient nécessaires pour l'octroi d'une autorisation d'exploiter.



Du point de vue des installations de sécurité, une PAP n'est pas nécessaire. Démonstration de la sécurité interne au GI.
 Il est recommandé de suivre la méthodologie de la directive.



Du point de vue des installations de sécurité, une PAP n'est pas nécessaire. Situé en dehors de l'objectif de la présente directive.

8.3 Exigences

En complément des légendes ci-dessus, les chapitres ci-après indiquent dans quels cas l'ampleur de la démonstration de la sécurité à élaborer ou des documents de preuve à soumettre peut être réduite.

8.3.1 Catégorie d'application H1 (carré rouge)

Les exigences conformément aux chap. 6 et 7 s'appliquent pleinement aux objets d'approbation de la catégorie d'application H1.

8.3.2 Catégorie d'application H2, ainsi que G1 (carré orange)

D'une façon générale, les exigences conformément aux chap. 6 et 7 s'appliquent aux objets d'approbation de la catégorie d'application H2. Substantiellement, il suffit de traiter les aspects essentiels.

L'objet de l'approbation est la modification. Les documents de démonstration de la sécurité doivent se focaliser par conséquent sur la modification et ses répercussions sur l'ensemble du système. Une considération du delta (des changements / des différences) est opportune, pour autant que des bases (documentation) suffisantes de l'installation originale soient disponibles pour l'analyse des conséquences dues aux modifications. Les questions de délimitation doivent également être incluses.

Des preuves de la sécurité effectuées selon d'anciennes méthodes ou éprouvées en pratique (garantie des droits acquis) peuvent aussi être considérées comme des bases (documentation) suffisantes, pour autant qu'elles soient assez explicites et que la compréhension soit garantie.

Compte tenu du plus faible risque d'erreur par rapport à la catégorie H1, les exigences en matière d'indépendance entre la validation et le rapport d'examen de l'expert sont également réduites.

Un mandat d'expertise (ch. 6.2.2 et 7.2.2) peut attribuer la validation et l'examen de l'expert à la même personne. Cela étant, l'indépendance de cette personne doit être garantie (principe des quatre yeux).

Pour des projets comportant un faible risque d'erreur lors de la planification, il est aussi admis d'inclure l'examen du rapport de sécurité pour la planification dans le rapport d'examen de l'expert pour la réalisation.

Le requérant assume le risque que des erreurs éventuelles de la phase planification ne soient découvertes que tardivement. L'OFT décide, dans la procédure d'approbation des plans, sur la base des documents en sa possession si ce risque est suffisamment faible et se réserve le droit d'exiger un rapport d'examen de l'expert pour la phase « Planification » selon le chapitre 6.2.2.

8.3.3 Catégorie d'application H3, ainsi que G2 et K1 (carré jaune)

Pour les projets de la catégorie d'application H3, aucune PAP n'est nécessaire⁹. Il incombe au GI de démontrer que la sécurité est adaptée au projet. Une application dans le sens de la méthodologie de la présente directive est recommandée. Les documents de preuve ne doivent être soumis à l'OFT ni pour examen ni pour information. La documentation reste en possession du GI / dans l'installation. Elle doit pouvoir être présentée sur demande à l'OFT dans le cadre de la surveillance de la sécurité lors de la phase d'exploitation (surveillance).

8.3.4 Exigences pour les autres catégories d'application

Les exigences en vigueur dans les autres catégories d'application peuvent être déduites des dispositions et de la matrice ci-dessus selon le ch. 8.2.

⁹ Pour mémoire : la présente directive porte sur la démonstration de la sécurité des installations de sécurité. Son contenu n'est donc valable que pour ce domaine. D'autres aspects peuvent nécessiter une PAP.

8.4 Diffusion des systèmes et de leurs versions (problématique du déploiement; [rollout])

Voici des exemples de diffusion des systèmes et de leurs versions : l'introduction sur tout le réseau d'un nouveau système, la mise à jour d'un logiciel, la réalisation de modifications sur un grand nombre d'installations.

Généralement, les systèmes en question et leurs développements ultérieurs sont examinés dans les procédures d'homologation de série. L'OFT peut décider si la modification nécessite une PAP.

Les principes de la présente directive sont applicables par analogie à la diffusion des systèmes informatiques et de leurs versions.

Avec des modifications nécessitant une PAP, comme lors d'autres modifications des systèmes/composants indépendants des installations – une **demande collective** d'approbation des plans peut être appropriée (voir l'indication sous 6.2.1.4) :

- Chaque demande doit contenir les documents de preuve et une liste des installations concernées.
- Pour l'évaluation technique par l'OFT, ces documents de preuve doivent contenir en particulier les informations suivantes:
 - Documents de preuve pour le système générique (ex. référence à des homologations existantes)
 - Preuve attestant que le dossier de sécurité des applications spécifiques reste *matériellement* valable sans changements ou
 - Preuve attestant que les nouvelles conditions d'utilisation sont observées
 - Informations concernant les conséquences sur les prescriptions d'exploitation (entretien et exploitation)
 - Tests et essais à mettre en œuvre lors de l'implémentation de chaque installation
 - Description du processus pour l'implémentation dans les installations (tâches, responsabilités,...)
 - Description de la démonstration prévue avec les examens d'experts des aspects spécifiques à chaque installation

L'OFT décide, dans les cas concrets et sur la base des documents présentés, de la forme sous laquelle le projet sera approuvé (en entier ou par installation, avec ou sans autorisation d'exploiter).

8.5 Applications télématiques, automatisation des postes d'enclenchement

Toutes les applications télématiques qui sont en lien direct avec la sécurité et la fiabilité de l'exploitation ferroviaire sont en principe soumises au régime de la PAP. Cela inclut les automatisations de postes d'enclenchement avec système de commande.

- La PAP est en principe obligatoire pour tous les projets d'automatisation (construction, adaptation) pour lesquels il est prévu d'utiliser des circuits, des composants et des sous-systèmes destinés à des fonctions à haute importance pour la sécurité (THR < 10⁻⁵/h, SIL 1-4) (H1 ou H2).

- La PAP est également obligatoire pour le projet entier, même si seules quelques fonctions ont une haute importance pour la sécurité (commande, affichage ou automatisation).
- Lors de projets d'automatisation en principe soumis au régime de la PAP, on peut renoncer à cette dernière dans les cas suivants, du point de vue de la technique d'exploitation :
 - Le GI estime, sur la base des critères d'importance pour la sécurité (effets) et de type de projet (probabilité d'erreur) conformément à la directive, qu'une PAP n'est pas obligatoire pour un projet (H3, G2, G3). Le GI documente cette évaluation dans son dossier de projet.
 - Les systèmes, fonctions et circuits prévus sont utilisés uniquement dans le cadre d'homologations de série dans lesquelles il est explicitement renoncé à une PAP.

8.6 Construction ou modification dans les postes d'enclenchement à relais

Selon le ch. 1.1, la présente directive doit aussi être appliquée à ces projets.

Comme mentionné au ch. 8.3.2, des preuves de sécurité effectuées selon d'anciennes méthodes ou éprouvées en pratique (garantie des droits acquis) sont aussi considérées comme des bases (documentation) suffisantes pour la démonstration de la sécurité, pour autant qu'elles soient assez explicites et que la compréhension soit garantie. Il est possible de se baser sur ces documents lorsque les éléments (schémas de principe, schémas de câblage libre, composants) peuvent être repris tels quels ou que les interventions et les modifications peuvent être localisées et délimitées exactement.

8.7 Modifications temporaires sur des installations de sécurité dans le cadre d'un projet

(Eléments provisoires dans une phase de construction)

Les phases de construction doivent être documentées dans le dossier d'après leur classification selon le ch. 7.2. La démonstration de la sécurité doit être conforme à la catégorie.

Si les effets des phases de construction sur les installations de sécurité, au moment de la PAP, ne sont pas encore définitivement élucidés, ils peuvent être expliqués dans les plans (documentation) du projet, quand les informations seront fournies.

L'OFT peut demander la preuve de la réalisation de l'état intermédiaire (de l'installation) pour des différentes phases lors de l'approbation des plans, ou requérir une autorisation d'exploitation.

Annexe 1 Définitions et abréviations (par ordre alphabétique)

Les définitions et abréviations issues des normes SN EN 5012x et de la Dir. OCI-CF sont considérées comme connues.

Cf. également les fig. 1 et 2, qui contribuent à l'éclaircissement des appellations.

Définition/ (source)	Définition / « autres désignations ou désignations équivalentes »
Analyse de sécurité	Par analyse de sécurité d'un système complexe et responsable de la sécurité, on entend l'examen systématique et compréhensible pour savoir si ce système remplit toutes les exigences de sécurité.
Analyse des risques	Procédure systématique afin de caractériser un événement (indésirable) d'après sa fréquence d'occurrence et l'ampleur des conséquences.
CCS	Dans le domaine interopérable : sous-système <i>Control, Command and Signalling</i> (contrôle, commande, signalisation)
Chargé d'évaluation (SN EN 50129)	Défini indirectement dans la norme : synonyme d'expert dans la Dir. OCI-CF et dans la présente directive.
Conditions d'utilisation relatives à la sécurité (SN EN 50129)	Règles, conditions et contraintes qui doivent être respectées lors de l'utilisation du système afin d'assurer la sécurité. « Conditions d'application relatives à la sécurité », « Conditions liées à la sécurité », « Règles d'application de la sécurité »
Contrôle orienté sur la sécurité	Terme courant désignant un examen du projet, effectué par une personne indépendante, orienté sur la sécurité du système et décrit plus en détail dans la Dir. OCI-CF.
DAP	Décision d'approbation des plans
Déclaration de conformité IOP	Terme générique pour toutes les déclarations, établies par un constructeur / requérant sur la base de certificats d'essai (intermédiaires) d'un organisme notifié ou d'un organisme désigné ou sur une base équivalente conformément au ch. 5.2.2 et selon lesquelles les exigences CE sont respectées en matière d'interopérabilité / RTNN et d'aptitude à l'emploi. Définition au sens strict : cf. Directive (CE) sur l'interopérabilité, art. 13 et 18, et annexes IV et VI.
Démonstration de la sécurité	Ensemble de toutes les activités nécessaires pour démontrer et prouver la sécurité d'un système et de son application, y compris leur documentation.
Pour les installations de sécurité, cette définition est appliquée au dossier de sécurité visé aux art. 18w, 18x et 23c LCdF.	Comprend par conséquent les essais, la validation, l'établissement des preuves de la sécurité ainsi que leur expertise.
Documents de démonstration de la sécurité	Définition générique englobant les preuves de sécurité, plans, rapports d'examen, rapports de sécurité, rapports d'essais et rapports d'examen de l'expert.

Définition/ (source)	Définition / « autres désignations ou désignations équivalentes »
<p>Dossier de sécurité, (SN EN 50129).</p> <p>Pour les installations de sécurité, cette définition est appliquée au dossier de sécurité visé à l'art. 8a OCF.</p>	<p>Démonstration documentée que le produit répond aux exigences de sécurité spécifiées.</p> <p>La norme différencie les types de dossiers de sécurité suivants :</p> <ul style="list-style-type: none"> - pour un produit générique, indépendant de l'application, - pour une application générique, pour une classe d'application, - pour une application spécifique ; celle-ci se divise en deux phases : <ul style="list-style-type: none"> a) dossier de sécurité pour la conception de l'application (phase « Planification »), b) dossier de sécurité pour la réalisation physique (phase « Réalisation »). <p>Si un dossier de sécurité ne correspond pas en tous points à la norme, il pourra être accepté pour autant qu'il ait été établi au sens de la norme et que son contenu soit suffisant.</p>
<p>Dossier technique</p>	<p>Annexe à la déclaration de conformité IOP, contient tous les documents sur laquelle ladite déclaration est fondée. Définition au sens strict : cf. Directive (CE) sur l'interopérabilité, art. 13 et 18, et annexes IV et VI.</p>
<p>Evaluation (SN EN 50129) Synonyme : expertise.</p>	<p>Processus d'analyse d'un produit visant à déterminer d'une part si l'autorité de conception et le chargé de validation ont réussi à aboutir à un produit qui satisfait aux exigences spécifiées, et d'autre part à formuler un jugement sur le fait que le produit répond à l'objectif attendu.</p>
<p>Expert (Dir. OCI-CF)</p>	<p>Personne compétente et expérimentée dans le domaine des IS mais indépendante des auteurs du projet. L'expert effectue un examen d'après le principe des 4 yeux.</p>
<p>FDMS / RAMS (SN EN 50126)</p>	<p>Fiabilité, disponibilité, maintenance et sécurité <i>Reliability, Availability, Maintainability, Safety</i></p>
<p>Installation de sécurité (IS) (PCT R 300.1, chap. 2 ; sections 6, 7 & 8, OCF)</p>	<p>Au sens strict : installation servant à protéger techniquement les trains et les mouvements de manœuvre et à régler leur circulation. « Système de signalisation ferroviaire » Dans la présente directive, les installations sont celles nommées dans l'OCF chapitre 2, sections 6, 7 et 8.</p>
<p>IOP</p>	<p>Interopérabilité, interopérable</p>
<p>PAE</p>	<p>Procédure d'autorisation d'exploiter, autorisation d'exploiter proprement dite (décision de l'OFT)</p>
<p>PAP</p>	<p>Procédure d'approbation des plans</p>
<p>Phase « Planification »</p>	<p>Comprend toutes les activités jusqu'à la soumission des plans pour approbation : Dans la représentation en « V » généralement jusqu'à la phase 5. La phase « Planification » ne correspond pas tout à fait à la phase « Conception » selon la SN EN 50129 (voir aussi figure 1).</p>
<p>Phase « Réalisation »</p>	<p>Comprend toutes les activités depuis la phase « Planification » jusqu'à la mise en service : Dans la représentation en « V » généralement depuis la phase 6. La phase « Réalisation » ne correspond pas tout à fait à la phase « Réalisation Physique » selon la SN EN 50129 (voir aussi illustration 1).</p>
<p>Planification de la qualité</p>	<p>Terme de la norme ISO 9000, utilisé ici comme terme générique de toutes les exigences de mise en œuvre, conditions d'application, prescriptions de planification, d'examen et d'autres processus à respecter.</p>

Définition/ (source)	Définition / « autres désignations ou désignations équivalentes »
Principe des 4 yeux (ou du double regard)	<p>Principe qu'un travail est examiné par les chargés du projet (première paire d'yeux¹⁰) et par un expert indépendant, compétent et expérimenté dans le domaine (deuxième paire d'yeux).</p> <p>Attention: le principe des 4 yeux n'est pas un « contrôle double » ! L'examen par les chargés du projet doit être complet et terminé ; il ne saurait compter sur l'examen de l'expert suivant.</p> <p>Le rapport de sécurité, ou la preuve de la sécurité, documente la vision de la première paire d'yeux.</p> <p>Le rapport d'examen de l'expert documente la vision de la deuxième paire d'yeux indépendante.</p>
Rapport d'examen de l'expert (Dir. OCI-CF)	<p>L'expert effectue, indépendamment de l'auteur du projet, un examen orienté sur la sécurité. Il décrit le résultat de son examen dans un rapport conforme à la directive.</p> <p>« Rapport d'Evaluation de la Sécurité » dans la norme SN EN 50129.</p>
Rapport de sécurité (art. 8b OCF, art. 3, al. 2, let. k, OPAPIF, ch. 37 Dir. OPAPIF)	<p>Rapport fondé sur une analyse des risques, qui présente par quelles mesures il est remédié aux risques et comment s'assurer que le projet satisfasse aux prescriptions et que le dossier de sécurité visé à l'art. 8a OCF puisse être établi.</p>
Rapport de sécurité technique (SN EN 50129)	<p>Partie du dossier de sécurité conformément à la norme SN EN 50129.</p>
Rapport technique (Dir. OPAPIF)	<p>Le rapport technique comprend la description technique du projet et les conditions d'utilisation dont il faut tenir compte pour l'ensemble de l'installation.</p>
Validation (SN EN 50129) (SN EN 50126)	<p>Activité qui vise à démontrer, par des tests et des analyses, que le produit remplit intégralement ses exigences spécifiées.</p> <p>Confirmation par examen et apport de preuves tangibles que les exigences particulières pour un usage spécifique prévu ont été satisfaites.</p>
Vérification (SN EN 50129) (SN EN 50126)	<p>Activité qui vise à déterminer, par des tests et des analyses, à chaque phase du cycle de vie, que les exigences de cette phase à l'étude répondent aux sorties de la phase précédente et que le produit de la phase d'étude répond à ses propres exigences.</p> <p>Confirmation par examen et apport de preuves tangibles que les exigences spécifiées prévues ont été satisfaites.</p>

¹⁰ Plusieurs personnes travaillant ensemble sur le même projet (par ex. lors d'une division du travail dans une entreprise ou dans le cadre de *reviews* internes), forment ensemble une « paire d'yeux ». Cependant, la conclusion d'un travail doit être assurée personnellement par un responsable.

Annexe 2 Documents de référence

Appellation	Référence
SN EN 50126	SN EN 50126, Norme technique de l'ASE : Applications ferroviaires - Spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS = RAMS); SN EN 50126:1999 (F), © SEV 1999-09 ¹¹
SN EN 50128	SN EN 50128, Norme technique d'Electrosuisse : Applications ferroviaires - Systèmes de signalisation, de télécommunications et de traitement - Logiciels pour systèmes de commande et de protection ferroviaire; SN EN 50128:2011 (F), © Electrosuisse 2011-06 ¹¹
SN EN 50129	SN EN 50129, Norme technique d'Electrosuisse : Applications ferroviaires – Systèmes de signalisation, de télécommunications et de traitement - Systèmes électroniques de sécurité pour la signalisation; SN EN 50129:2003 (F), © Electrosuisse 2003-02 ¹¹
SN EN 50159	SN EN 50159, Norme technique d'Electrosuisse : Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Communication de sécurité sur des systèmes de transmission ; SN EN 50159:2010 (D), © Electrosuisse 2010-09 ¹¹
LCdF	Loi fédérale du 20 décembre 1957 sur les chemins de fer (état au 1 ^{er} juillet 2013); RS 742.101 ¹²
OCF	Ordonnance du 23 novembre 1983 sur les chemins de fer (état au 1 ^{er} novembre 2014); RS 742.141.1 ¹²
OPAPIF	Ordonnance du 2 février 2000 sur la procédure d'approbation des plans pour les installations ferroviaires (état au 1 ^{er} novembre 2014); RS 742.142.1 ¹³
Dir. OPAPIF	Directive de l'OFT concernant l'art. 3 de l'OPAPIF, Exigences relatives aux demandes d'approbation des plans, 1 ^{er} juillet 2013 ¹³
Dir. OCI-CF	Directive de l'OFT Organismes de contrôle indépendant Chemins de fer, 1 ^{er} juillet 2013 ¹³
Dir. IOP	Directive de l'OFT concernant l'art. 15a OCF, Exigences IOP imposées aux tronçons du réseau complémentaire, 1 ^{er} octobre 2013 ¹³
STI CCS	Spécification technique d'interopérabilité concernant le sous-système contrôle-commande et signalisation du système ferroviaire (annexe 7 OCF)
Règlement GSM	Règlement (CE) n° 352/2009 concernant l'adoption d'une méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques ¹⁴
Directive (CE) sur l'interopérabilité	Directive 2008/57/CE, mise à jour par les directives 2009/131/CE et 2011/18/CE ¹⁴ (« Directive sur l'interopérabilité »)

¹¹ En vente à l'Association Suisse de Normalisation (SNV), <http://www.snv.ch/fr/>, ou auprès d'Electrosuisse (Association reconnue dans le domaine de l'électronique, des technologies de l'énergie et de l'information), <https://www.electrosuisse.ch/fr/normalisation.html>

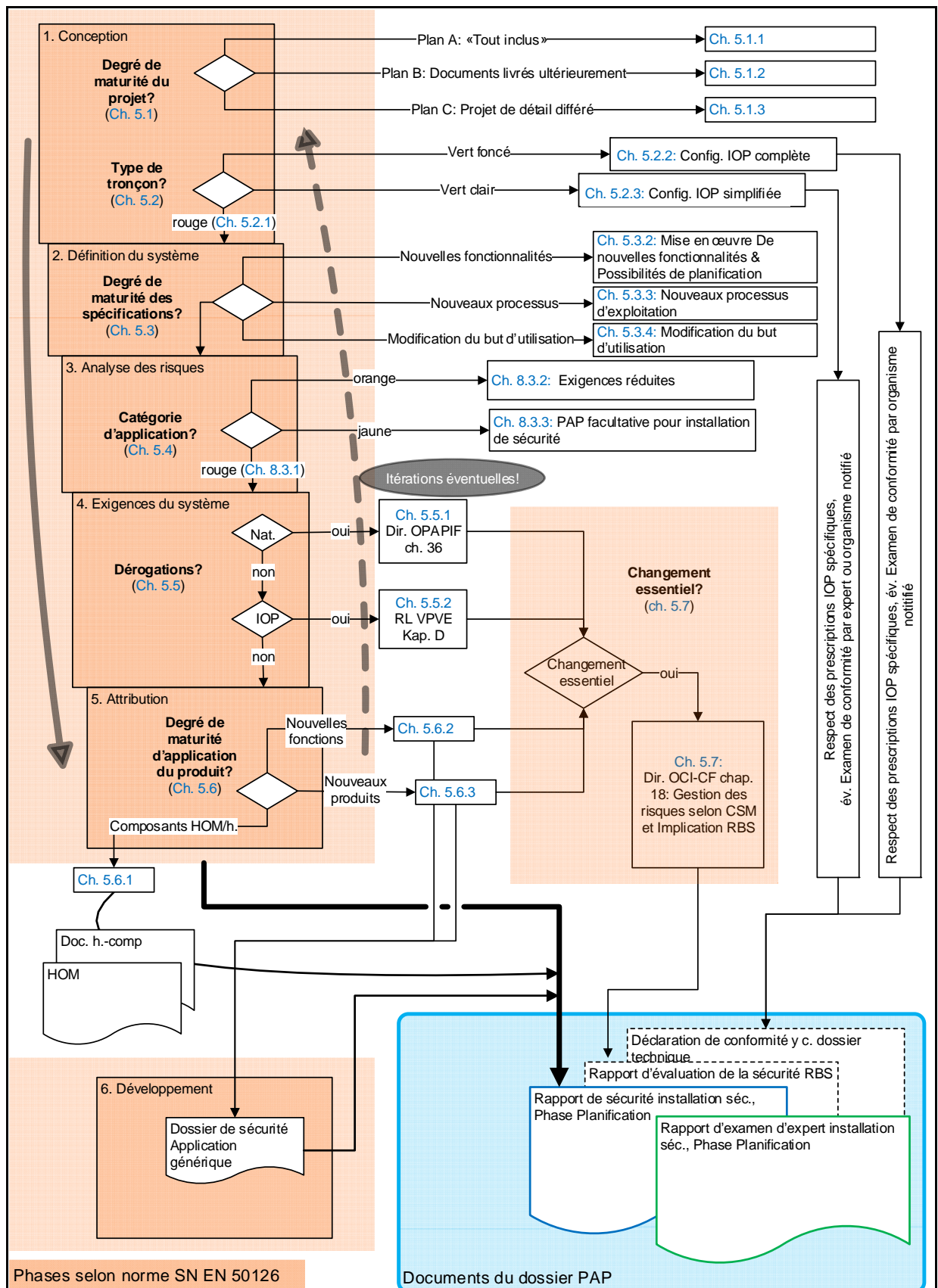
¹² Disponible au recueil systématique du droit fédéral, <https://www.admin.ch/gov/fr/accueil/droit-federal/recueil-systematique.html>

¹³ Disponible sur le site Internet de l'OFT, <https://www.bav.admin.ch/bav/fr/home/droit/bases-legales-prescriptions/directives.html>

¹⁴ Disponible sur <http://eur-lex.europa.eu>

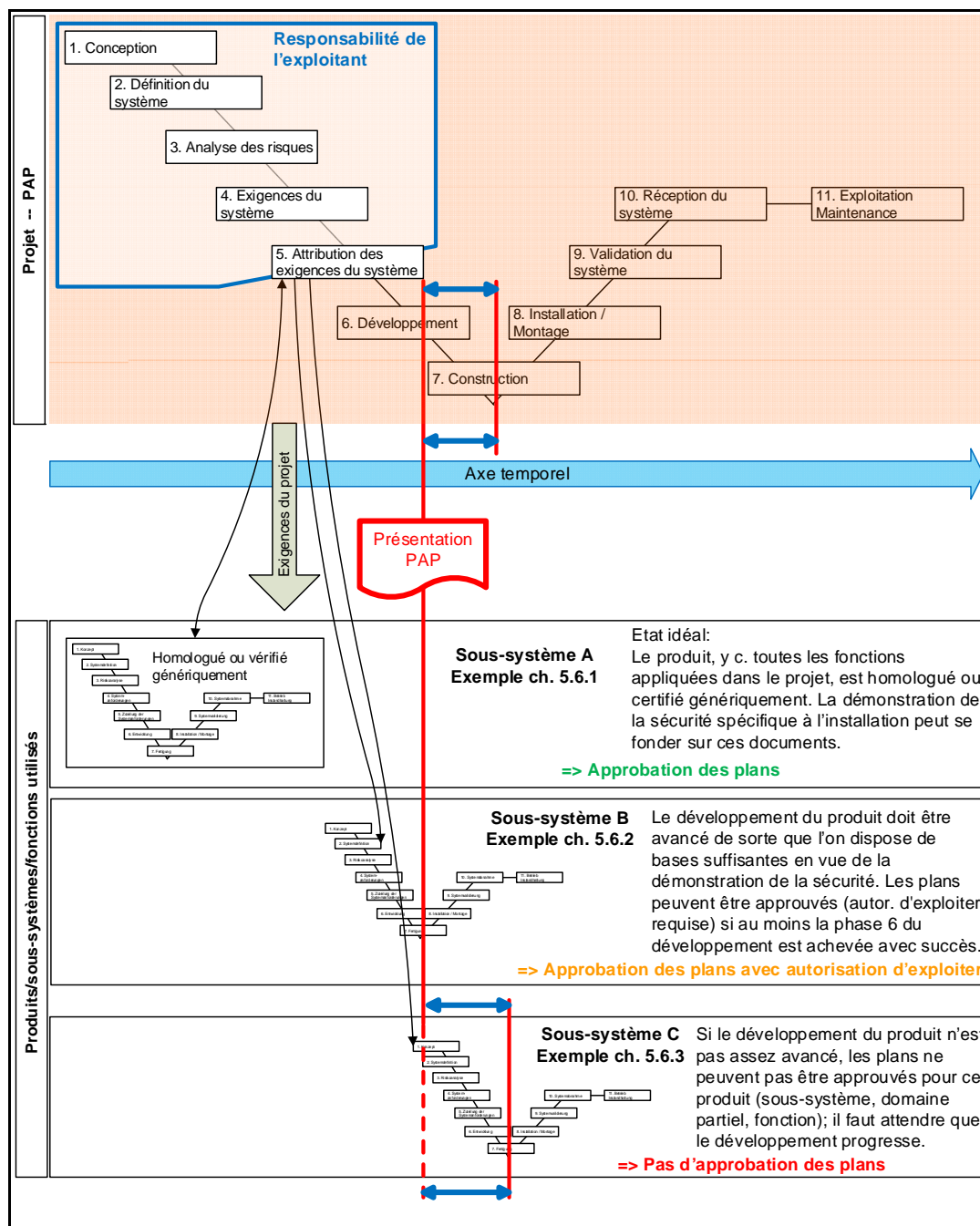
Annexe 3 Illustration du chap. 5

Figure 3 : Tableau décisionnelⁱ



Annexe 4 Illustration du ch. 5.6.4

Figure 4 : degré de maturité pour l'application du produit ⁱⁱ



ⁱ Remarque : la fig. 3 n'est **pas** un diagramme de flux (flow chart) proprement dit, mais une illustration sur la base d'éléments de diagramme. Les flèches sortant du déroulement normal (vertical) indiquent les points particuliers à prendre en compte. La fig. 3 a pour but de fournir une vue d'ensemble utilisable éventuellement en tant que liste de contrôle ; toutefois, elle n'indique **pas** toutes les tâches à accomplir dans les différentes phases.

ⁱⁱ Remarque : la fig. 4 n'est pas non plus un diagramme de flux mais une illustration des différents rapports entre l'état de développement du projet et du produit. Dans le cas du sous-système C, les flèches bleues horizontales montrent le progrès manquant dans le développement du produit.