Atelier du RIS
18 mars 2003

Intégration des justificatifs de sécurité (safety case) dans une démarche globale de mise en service

Par Yseult GARNIER

du Département de la Signalisation IG.SF

PLAN DE L ’EXPOSE

I - Présentation des différentes entités dans le cycle en V

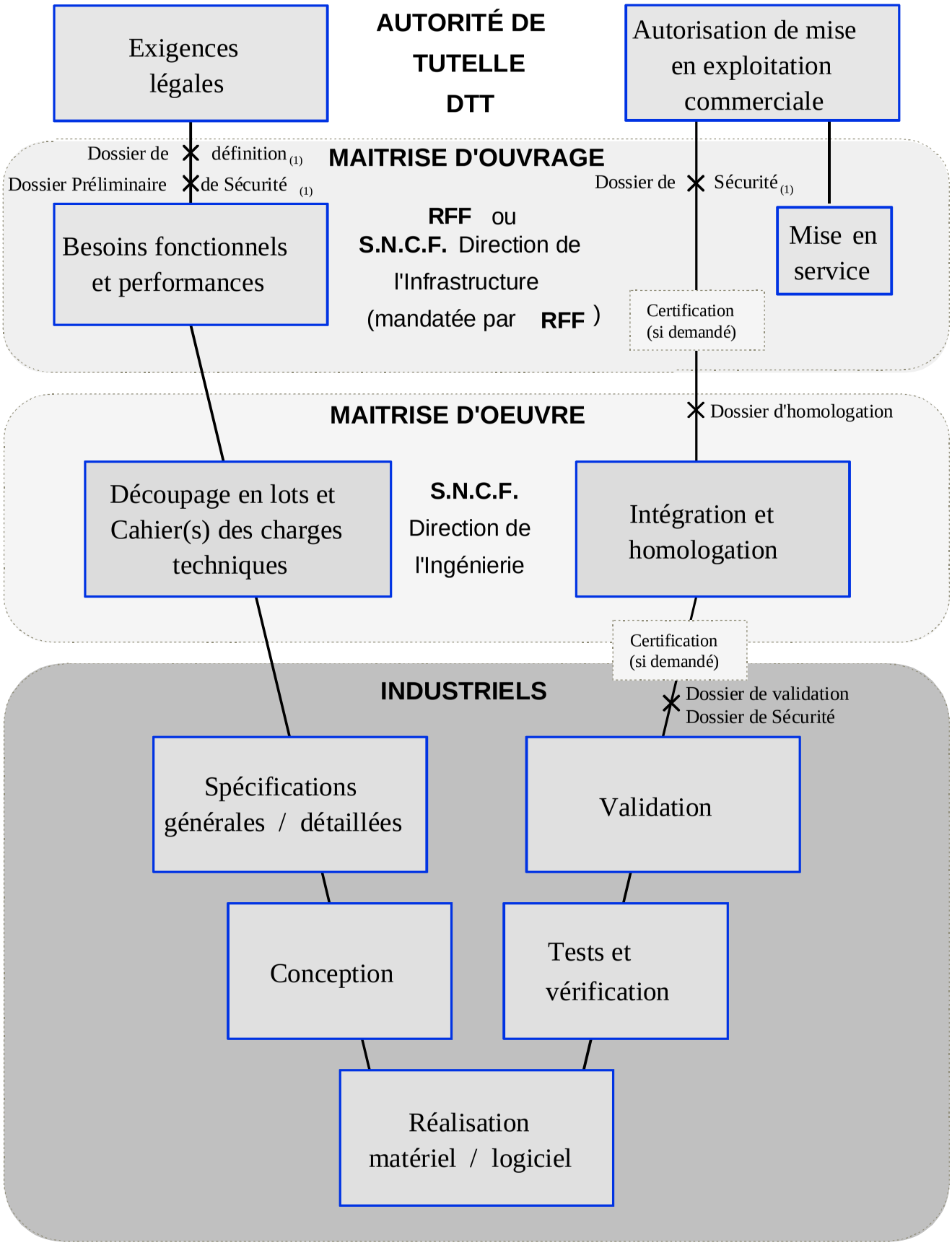
II- Rappel des exigences réglementaires nationales et européennes :

Décret 2000-286, décret 2001-129 de transposition de la directive 96/48, les normes du CENELEC (spécifique ferroviaire)

III - La démarche de "safety case" dans ce cycle en V

IV- Conclusion

Présentation des différentes entités dans le cycle en V



(1) Documents demandés par le Ministère des Transports (Bureau de Sécurité Ferroviaire).

SNCF
DIRECTION DE L'INGÉNIERIE

II - Rappel des exigences réglementaires nationales et européennes

1. Le Décret 2000-286 du 30 mars 2000 s'applique à la sécurité du Réseau Ferré National :

› Pour tout nouveau système ou tout système modifié :

- SNCF chargée pour le compte de RFF de la gestion du trafic et des circulations sur le réseau ferré national ainsi que du fonctionnement et de l'entretien des installations techniques et de sécurité de ce réseau et, le cas échéant, d'un mandat de maîtrise d'ouvrage
- application du principe Globalement Au Moins Equivalent (GAME remplace le principe GAMAB décrit dans la norme EN 50126) pour la sécurité
- conception et réalisation conformément aux règles, normes et prescriptions relatives à la SdF, à la qualité, à l 'accessibilité

II - Rappel des exigences réglementaires nationales et européennes (suite)

1. Le Décret 2000-286 du 30 mars 2000 s'applique à la sécurité du Réseau Ferré National (suite) :

› **Pour tout nouveau système ou tout système modifié (suite):**

- évaluation de la conception et de la réalisation et vérification de l'objectif de sécurité par un organisme ou service technique indépendant des concepteurs et constructeurs (OSTI).

Application : infrastructures, installations techniques et de sécurité, matériels roulants

II - Rappel des exigences réglementaires nationales et européennes (suite)

2. L'arrêté du 08 janvier 2002 pris pour l'application du décret 2000-286 s'applique à la sécurité du Réseau Ferré National :

Définition du contenu des documents suivants :

- Dossier de définition décrivant les principales caractéristiques techniques et fonctionnelles ainsi que les éléments concourant au respect des objectifs de sécurité,
- Analyse Préliminaire des Risques,

II - Rappel des exigences réglementaires nationales et européennes (suite)

2. L'arrêté du 08 janvier 2002 pris pour l'application du décret 2000-286 s'applique à la sécurité du Réseau Ferré National :

Définition du contenu des documents suivants (suite):

- Dossier Préliminaire de Sécurité précisant :
  - le système de référence pour la démonstration du GAME,
  - les données techniques et fonctionnelles ainsi que les objectifs de sécurité,
  - les principes garantissant le respect de l 'objectif de sécurité pendant l 'exploitation du système,
  - le nom de l'OSTI,
- Dossier de Sécurité.

Application : infrastructures, installations techniques et de sécurité, matériels roulants

II - Rappel des exigences réglementaires nationales et européennes (suite)

3. Les directives européennes :

Notamment, le décret 2001-129 de transposition de la directive 96/48 relative à l'interopérabilité du système ferroviaire transeuropéen à grande vitesse. S 'applique à :

- la définition, la construction, l 'aménagement, l 'exploitation, la maintenance des sous-systèmes
- la mise sur le marché des constituants d'interopérabilité

Elle impose en particulier la rédaction des Spécifications Techniques d'Interopérabilité (STI), qui précisent les exigences essentielles à respecter (Sécurité, Fiabilité, Disponibilité, compatibilité technique)

Application : LGV Est

II - Rappel des exigences réglementaires nationales et européennes (suite)

3. Les normes du CENELEC (spécifique ferroviaire) :

› Les normes ferroviaires européennes :

- NF EN 50126 : spécification et démonstration de la fiabilité, de la disponibilité, de la maintenabilité et de la sécurité (FDMS)
- NF EN 50128 : Logiciels pour systèmes de contrôle/commande et de protection ferroviaire

II - Rappel des exigences réglementaires nationales et européennes (suite)

Les normes ferroviaires européennes (suite):

- ENV 50129 : Systèmes électroniques de sécurité pour la signalisation
- pr EN 50129 : Diffère de l 'ENV 50129 par la méthode d 'allocation des THR et Niveaux d 'Intégrité de Sécurité (SIL)

Ces normes :

- spécifient le contenu d'un Dossier de Sécurité *"Safety Case"*,
- spécifient les exigences concernant le matériel selon le niveau de SIL du matériel,
- requièrent des méthodes et outils à utiliser à chaque étape du cycle de vie du système défini dans la NF EN 50126
- imposent une organisation pour la sécurité selon le niveau de SIL

III - La démarche de Safety Case dans ce cycle en V

Existence de 2 types de Dossier de Sécurité :

- Le Dossier de Sécurité transmis en final à la DTT : ce dossier de sécurité démontre le respect des exigences énoncées dans le DPS

- Le Dossier de Sécurité fourni par l'industriel au maître d'œuvre, appelé par la suite "Safety Case" : ce dossier est basé sur le plan de la norme pr EN 50129

III - La démarche de Safety Case dans ce cycle en V (suite)

Le Dossier de Sécurité fourni à la DTT :

- Il est basé sur l'arrêté du 08 janvier 2002 ; il doit contenir principalement les documents suivants :
  - documents descriptifs du système réalisé, liste des composants de sécurité,
  - objectifs de sécurité, justification de l'allocation par une démarche GAME
  - attestation du respect des méthodes et référentiels présentés dans le DPS,
  - attestation par la SNCF de la conformité de la réalisation aux engagements pris dans le DPS,
  - rapport de l'organisme ou service technique indépendant,

III - La démarche de Safety Case dans ce cycle en V (suite)

› Le Dossier de Sécurité fourni à la DTT (suite) :

- conclusion des études de sécurité réalisées et attestation de la couverture des risques identifiées dans l'APR,
- résultats des tests et essais,
- plan de documentation et de gestion des modifications,
- principes suivis pour la sélection, la formation ou l'habilitation du personnel,
- informations concernant la maintenance, l'exploitation et le suivi des de l'exploitation (ReX, …),
- garantie du maintien du niveau de sécurité dans le temps,
- Plan d'intervention et de sécurité

III - La démarche de Safety Case dans ce cycle en V (suite)

Le Safety Case :

- La preuve documentaire que les conditions d'acceptation de la sécurité ont été remplies doit faire partie d'un document structuré justificatif de la sécurité, appelé Dossier de Sécurité.
- Il doit contenir les parties suivantes :
  - 1 : Définition du système (ou du sous-système/équipement)

    Cette partie doit définir précisément ou référencer le système/sous-système/équipement correspondant au Dossier de Sécurité, en incluant les numéros de version et l'état des modifications de toute la documentation sur les exigences, la conception et l'utilisation.
  - 2 : Rapport de gestion de la qualité

    Cette partie doit contenir la preuve de la gestion de la qualité.

III - La démarche de Safety Case dans ce cycle en V (suite)

Le Safety Case (suite) :

- 3 : Rapport de gestion de la sécurité

  Cette partie doit contenir la preuve de la gestion de la sécurité.

- 4 : Rapport de Sécurité Technique

  Cette partie doit contenir la preuve de la sécurité fonctionnelle et technique

- 5 : Dossiers de Sécurité connexes

  Cette partie doit contenir les références des Dossiers de Sécurité de tous les sous-systèmes ou équipements dont le Dossier de Sécurité principal dépend.

- 6 Conclusion

  Cette partie doit résumer les preuves présentées dans les parties précédentes du Dossier de Sécurité, et justifier que le système/sous-système/équipement présente la sûreté requise, et est conforme aux conditions d'utilisation spécifiées.

III - La démarche de Safety Case dans ce cycle en V (suite)

Le Safety Case (suite) :

3 types de Safety Case :

- **Dossier de Sécurité pour les produits génériques (indépendants de l'application)**
  - Un produit générique peut être réutilisé pour diverses applications indépendantes.
- **Dossier de Sécurité pour une application générique (pour une classe d'applications)**
  - Une application générique peut être réutilisée pour une classe ou un type d'applications ayant des fonctions communes.
- **Dossier de Sécurité pour une application spécifique (pour une application spécifique)**
  - Une application spécifique est utilisée pour une seule installation particulière.

IV - Conclusion

- **Le Safety Case permet d'apporter la preuve documentaire que toutes les conditions d'acceptation de la sécurité ont été remplies**
- **Le Dossier de Sécurité fourni à la DTT :**
  - se base sur les résultats de l'industriel via le Safety Case
  - apporte la preuve que les activités de la MOE et la MOA sont conformes au DPS
  - apporte la démonstration du GAME / système de référence
- **En final : l'autorisation de mise en exploitation commerciale est prononcée sur la base de ces 2 dossiers**

F I N