

# Club SEE « Systèmes Informatiques de Confiance » (Club 63)

Cercle «Conception et validation pour la Sûreté de Fonctionnement»  
Journée du 23 mars 2000

Thème : Les normes et leur évolution

Sujet : Les normes du CENELEC dans le cadre du développement des systèmes informatiques critiques de Signalisation

par : Pascal BARAN

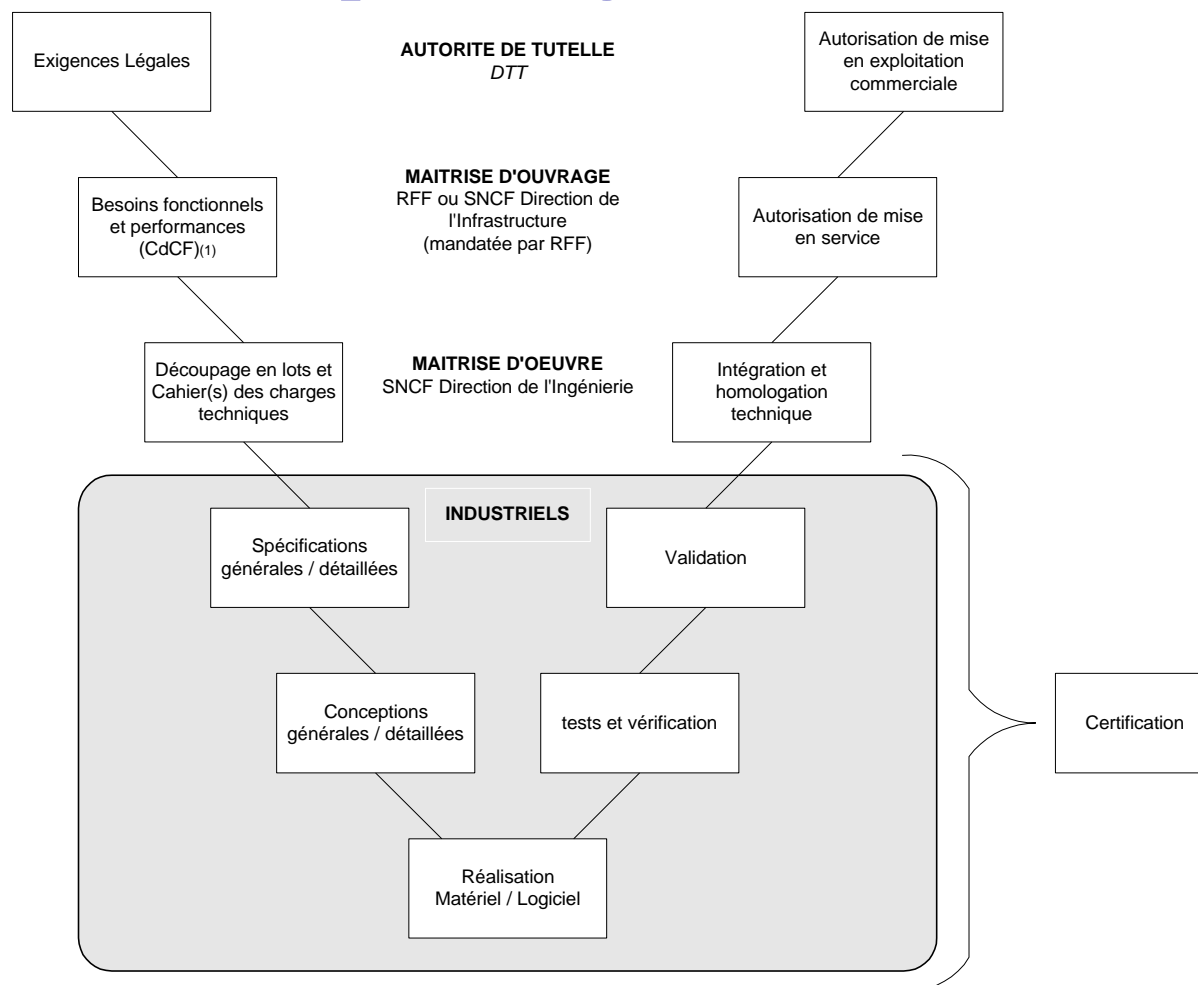
Département des Produits et Systèmes de Signalisation  
de la Direction de l'Ingénierie de la SNCF

Tel : 01.40.18.86.40 / Email : Pascal.BARAN@SNCF.fr



DIRECTION DE L'INGÉNIERIE  
DÉPARTEMENT IG.PS

# Présentation du contexte pour le développement d'un système critique de signalisation



(1) CdCF : Cahier des Charges Fonctionnel

# Exigences légales

## PROJET DE DECRET RELATIF A LA SECURITE DU RESEAU FERRE NATIONAL

- S'applique à la définition, la conception, la réalisation, l'exploitation et la maintenance de tous les systèmes constituant ou utilisant le réseau
- S'applique à tout nouveau système et à modification de systèmes existants
- Impose le principe **AMGE** (Au Moins Globalement Equivalent)
- Le projet de décret prévoit :
  - Un dossier d'initialisation élaboré par RFF avec SNCF
    - un dossier préliminaire de sécurité élaboré par SNCF et approuvé par le ministère des Transports
    - un dossier de sécurité élaboré par SNCF, présenté par RFF et tenu à jour pendant la vie du système
    - l'intervention d'un organisme technique compétent et indépendant pour le contrôle, le suivi et l'évaluation de la conception et de la réalisation
  - Le ministre délivre une autorisation de mise en exploitation du système

# Objet des normes du CENELEC

- Fournir un référentiel commun en Europe :
  - pour favoriser l'élargissement des marchés des constituants du ferroviaire
  - pour faciliter l'interopérabilité, l'interchangeabilité et la « **cross acceptance** » des constituants ferroviaires
- Répondre aux spécificités du domaine ferroviaire



DIRECTION DE L'INGÉNIERIE  
DÉPARTEMENT IG.PS

# Organisation de la normalisation du CENELEC

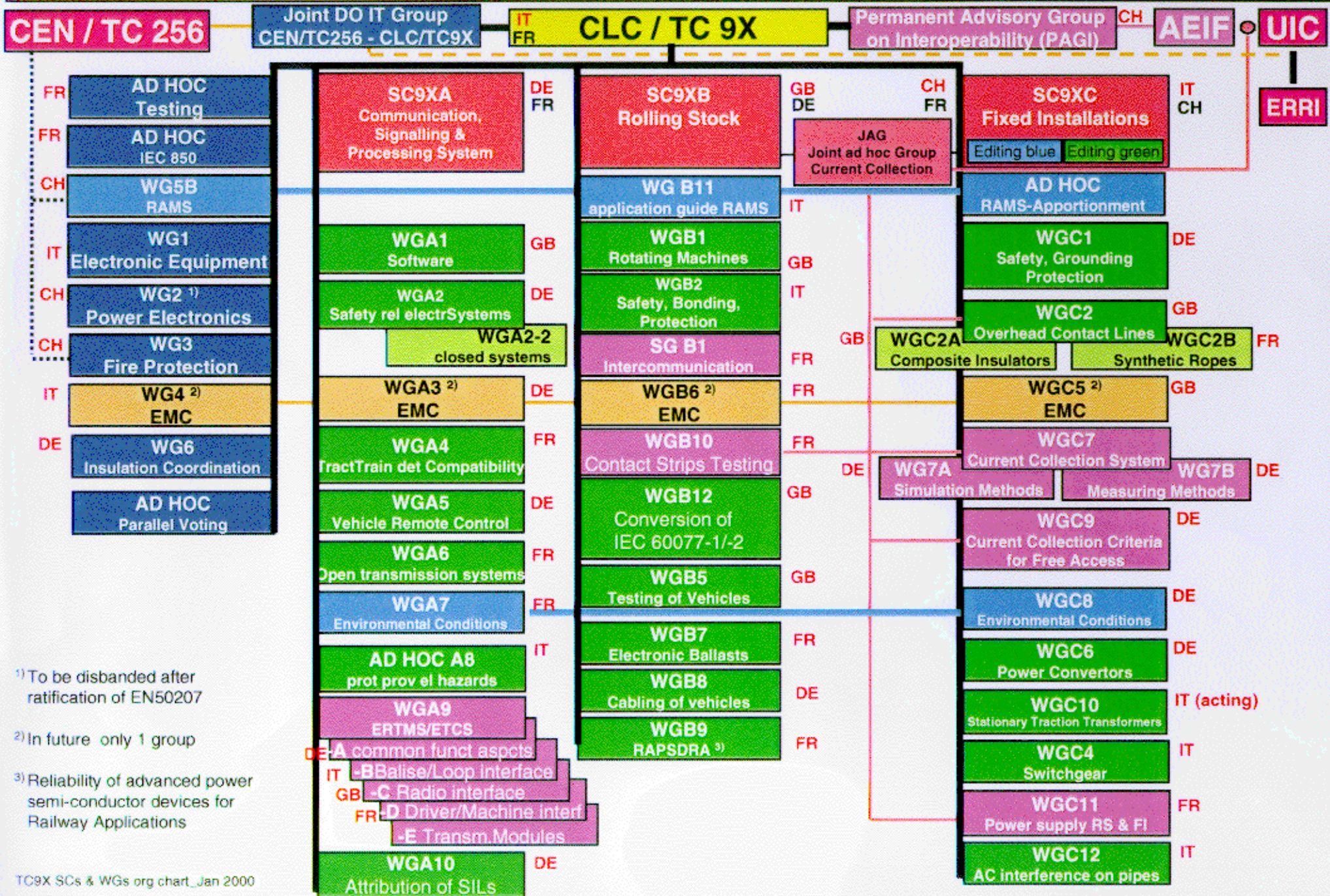
- **TC9X** : Applications ferroviaires - Normes communes  
Par exemple EN 50126
  - **SC9XA** : Signalisation et Télécommunications  
Par exemple EN 50128 et EN 50129
  - **SC9XB** : Matériel Roulant
  - **SC9XC** : Installations Fixes de Traction Electrique



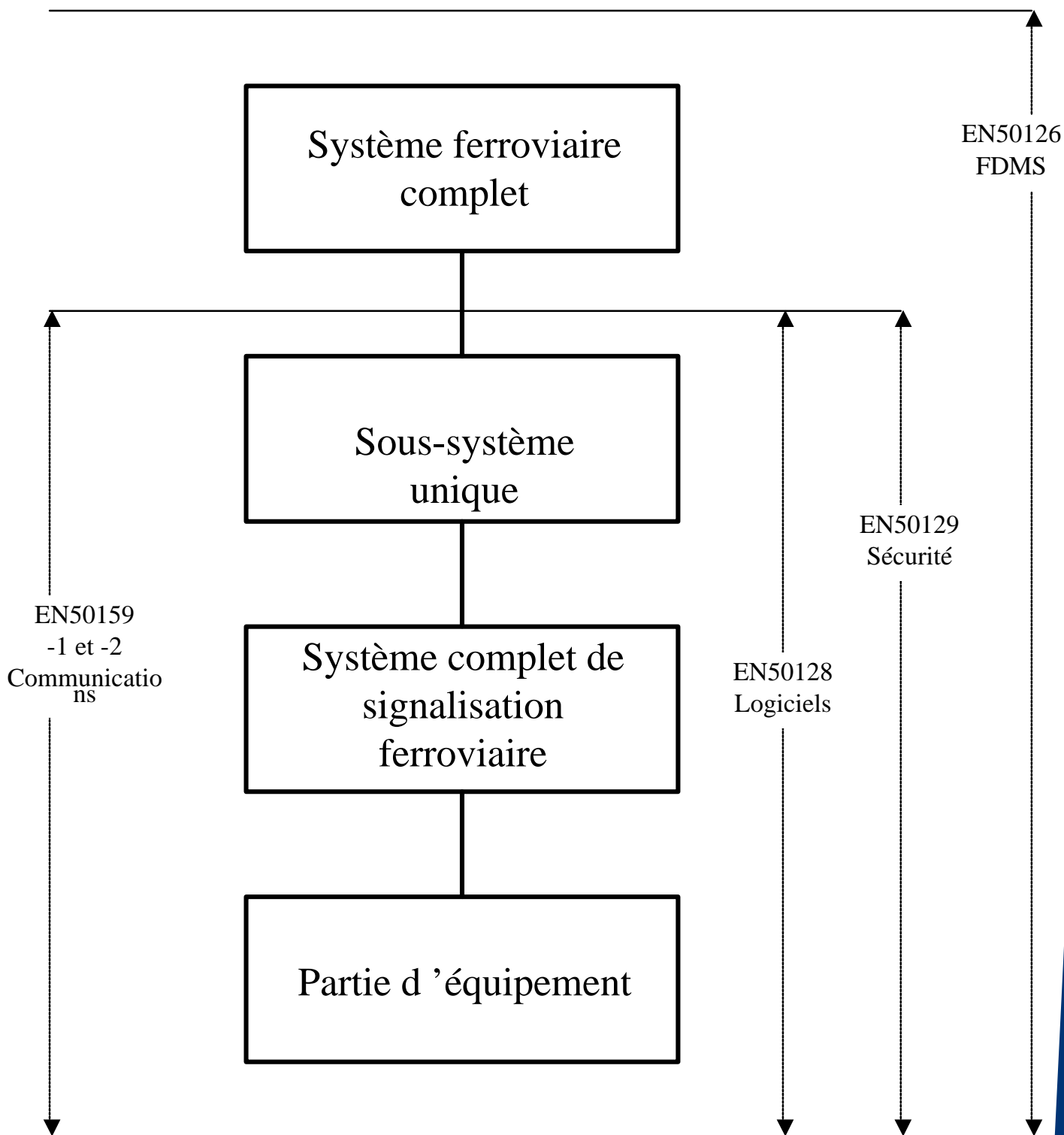
DIRECTION DE L'INGÉNIERIE  
DÉPARTEMENT IG.PS

# TC 9X - Railway applications

CLC/TC9X(Sec)169 - Jan 2000



# Domaine d'application des normes du CENELEC applicables pour le développement d'un système critique de signalisation



# L 'EN 50126 : Spécifications et démonstration de la Sûreté de Fonctionnement (FDMS)

## Objet :

- promotion d 'une approche commune pour la gestion de la FDMS

## Domaine d 'application :

- démarche de gestion de la FDMS sur tout le cycle de vie d 'un système (y.c. exploitation et maintenance)
- définition d'un processus systématique pour spécifier les exigences de FDMS et pour démontrer leur respect
- du simple équipement à une ligne complète
- nouveaux systèmes et systèmes modifiés
- par les sociétés d 'exploitation et les industriels

## Hors domaine d 'application :

- processus d 'approbation des autorités de tutelle
- objectifs quantifiés de FDMS
- règles et processus de certification

# Spécification des exigences de FDMS

- Analyse de Risques
- Matrice « Occurrence- Gravité »

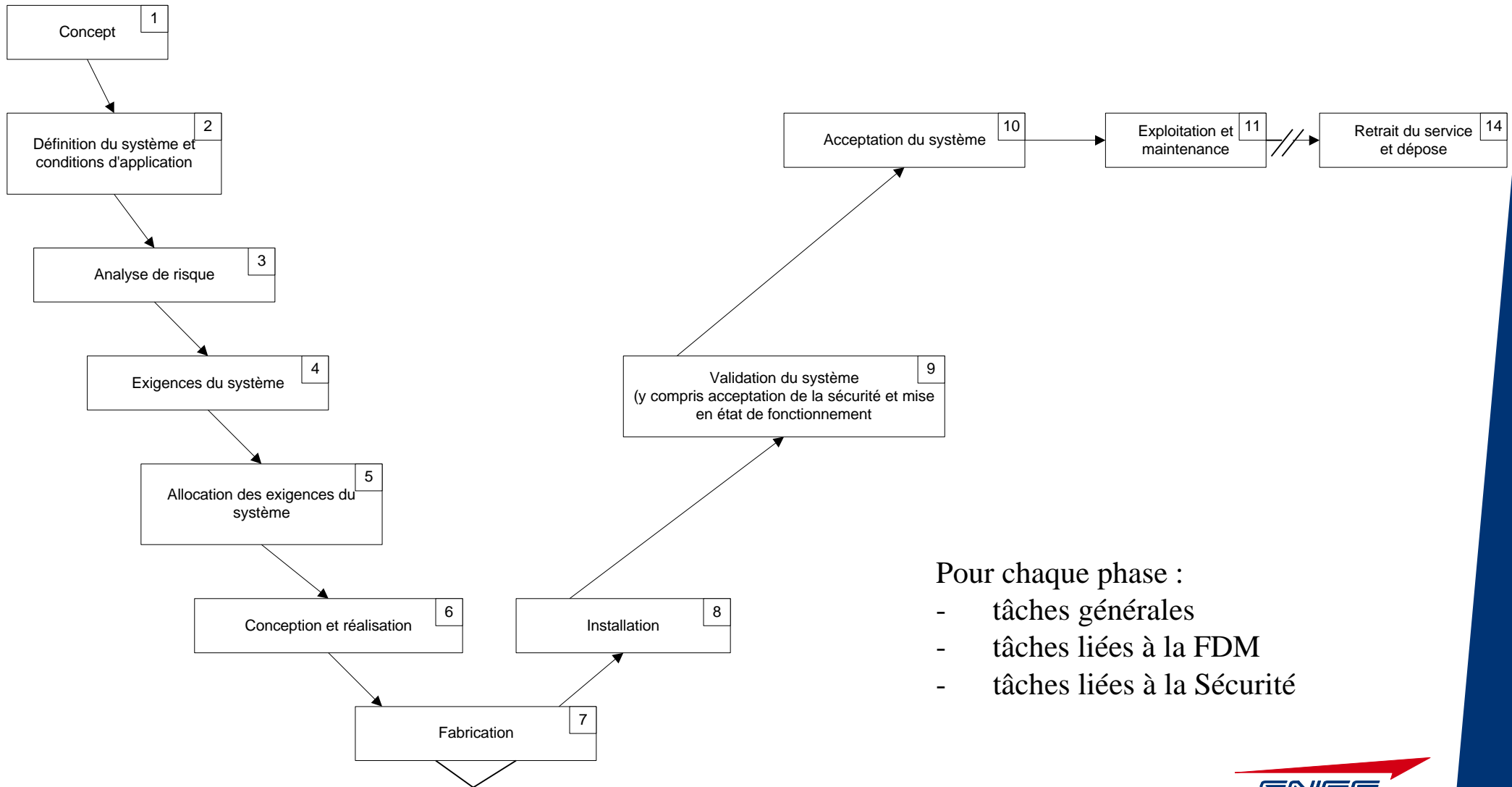
Fréquence de l'événement dangereux	Niveau de risque			
	Fréquent	Indésirable	Inacceptable	Inacceptable
Probable	Acceptable	Indésirable	Inacceptable	Inacceptable
Occasionnel	Acceptable	Indésirable	Indésirable	Inacceptable
Rare	Négligeable	Acceptable	Indésirable	Indésirable
Improbable	Négligeable	Négligeable	Acceptable	Acceptable
Invraisemblable	Négligeable	Négligeable	Négligeable	Négligeable
	Insignifiant	Marginal	Critique	Catastrophique
	Niveaux de gravité des conséquences d'une situation dangereuse			

- Principe d'Acceptation du risque « Au Moins Globalement Equivalent »



DIRECTION DE L'INGÉNIERIE  
DÉPARTEMENT IG.PS

# Tâches liées aux différentes phases du projet



Pour chaque phase :

- tâches générales
- tâches liées à la FDM
- tâches liées à la Sécurité



DIRECTION DE L'INGÉNIERIE  
DÉPARTEMENT IG.PS

# L 'ENV 50129 : Systèmes électroniques relatifs à la sécurité pour la signalisation

Objet : définition des exigences pour l 'acceptation des systèmes

Domaine d 'application :

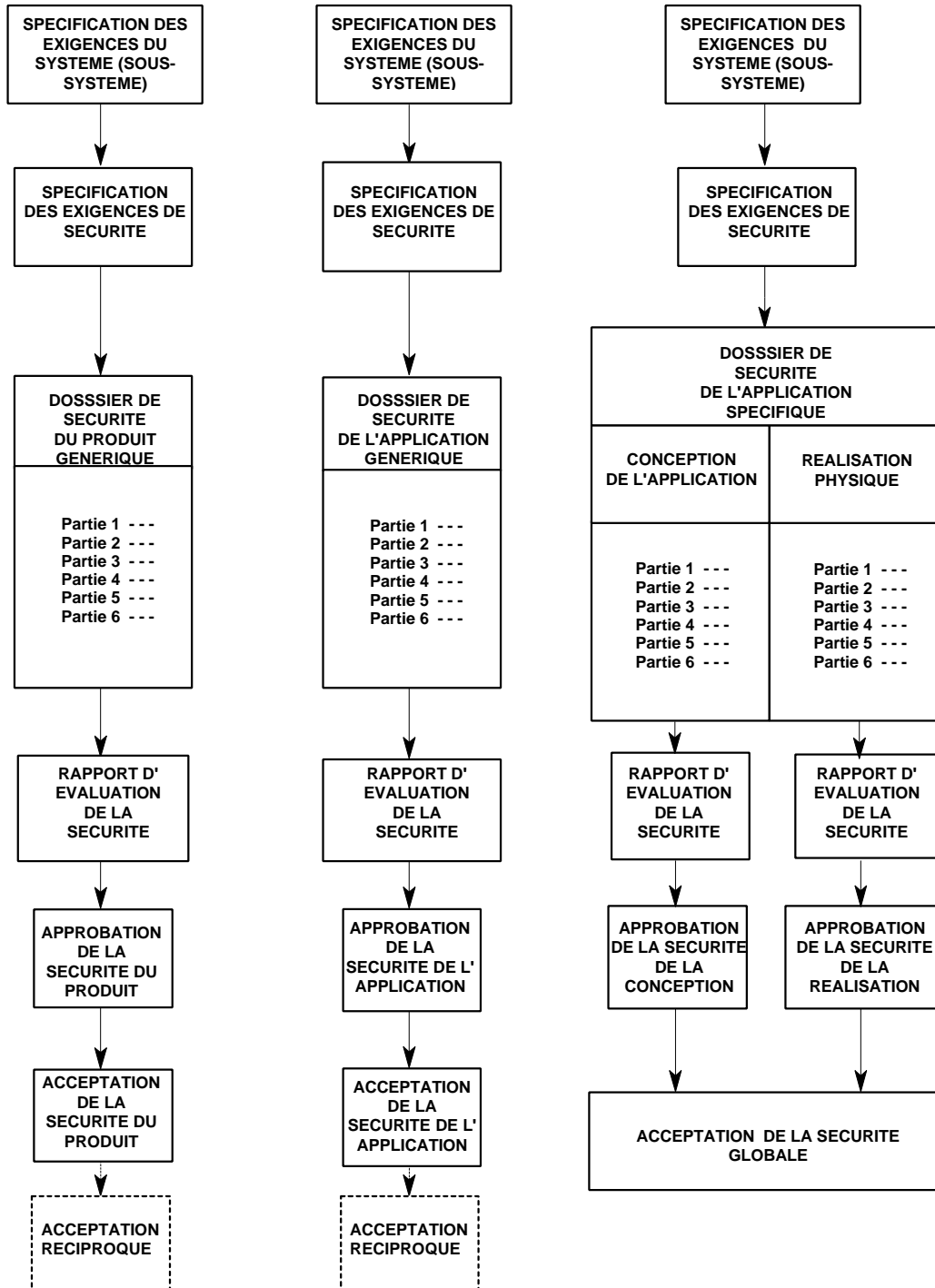
- démonstration du respect des exigences de sécurité pour toutes les phases du cycle de vie
- systèmes génériques et spécifiques

# Processus d'Approbation et d'Acceptation de la Sécurité

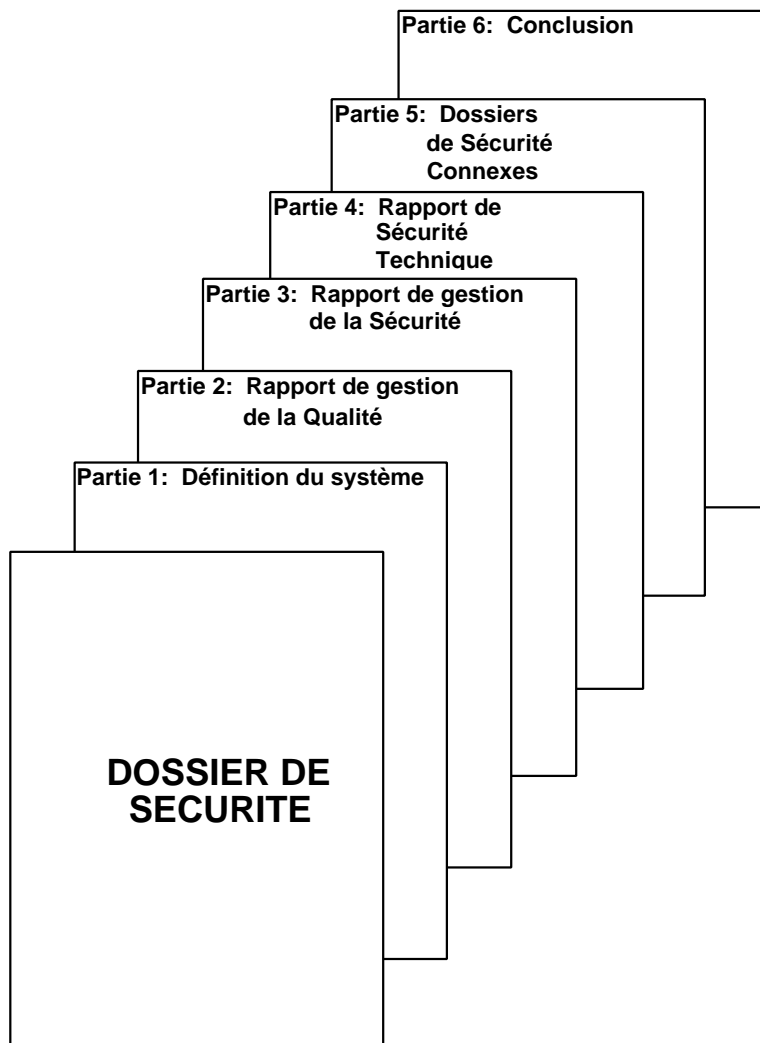
**PRODUIT GÉNÉRIQUE**  
(Indépendant de l'application)

**APPLICATION GÉNÉRIQUE**  
(Classe d'application)

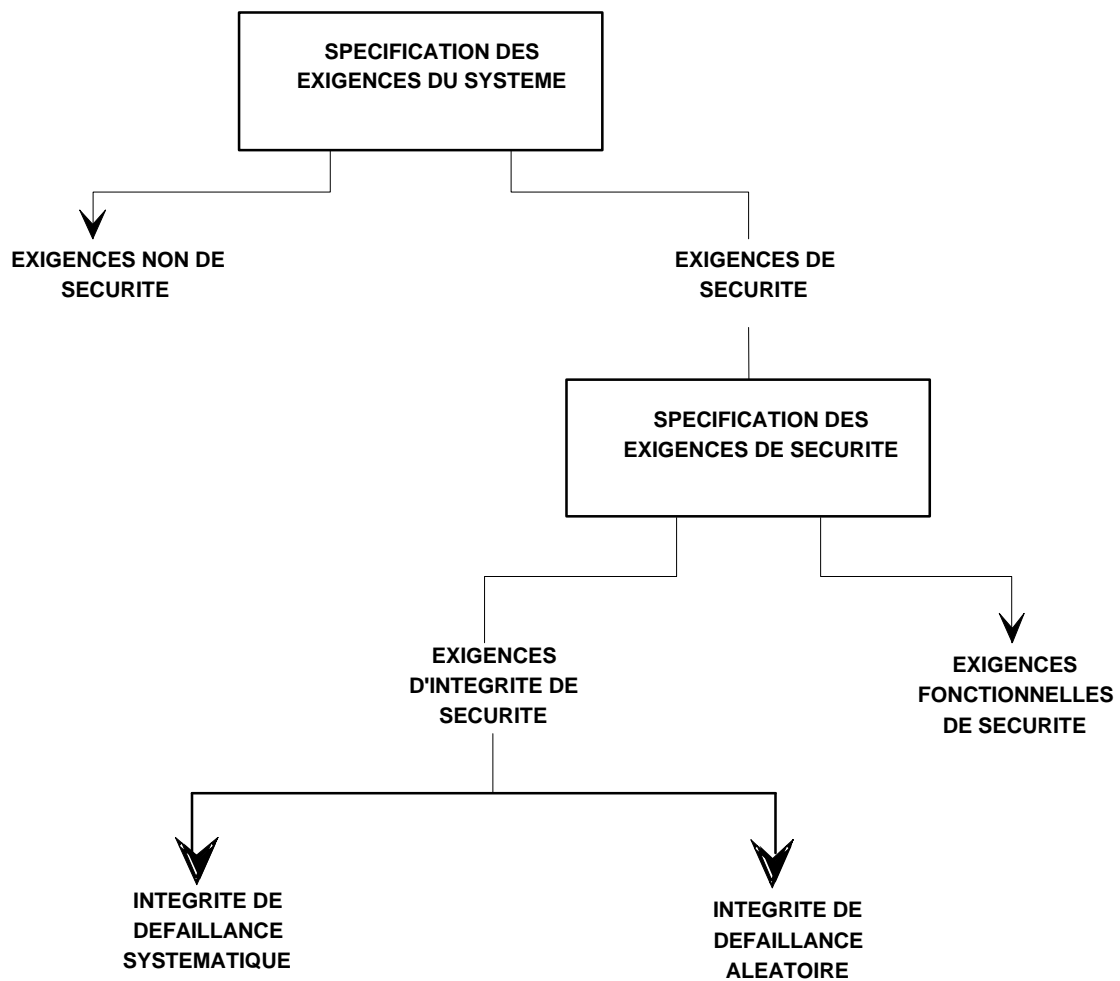
**APPLICATION SPÉCIFIQUE**



# Plan du Dossier de Sécurité



# Exigences de sécurité



# Processus d'allocation des SILs

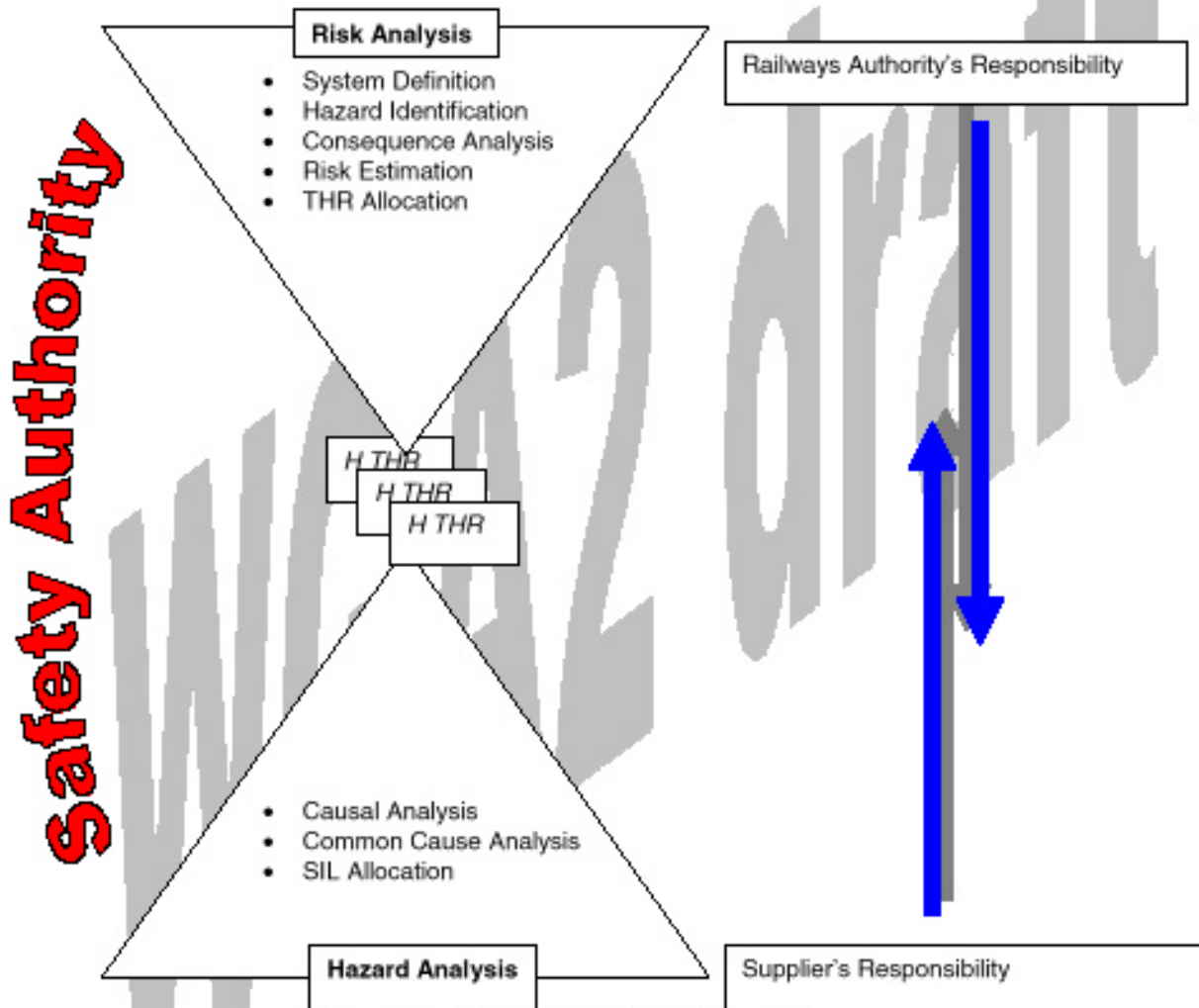
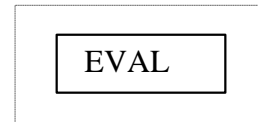
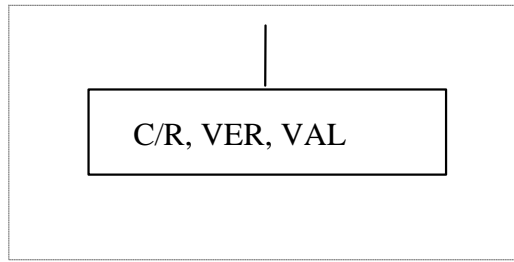


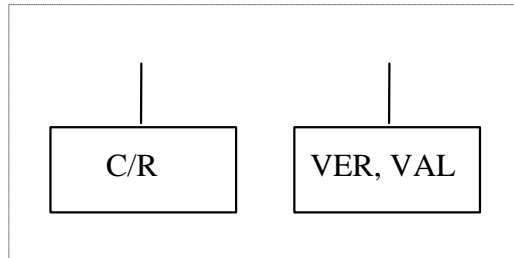
Figure A. 2: Global process overview

# Exigences d'indépendance

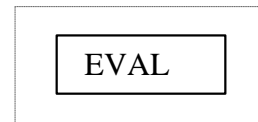
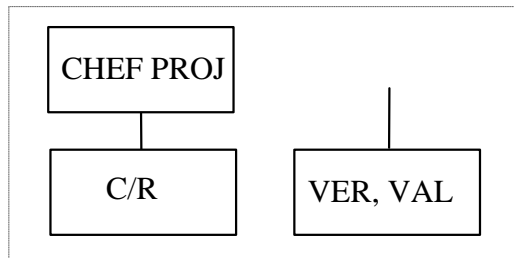
NIVEAU 0



NIVEAUX 1 & 2

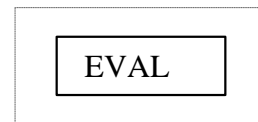
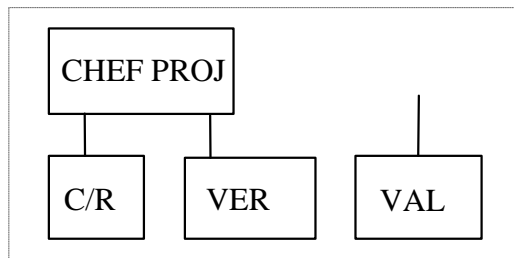


NIVEAUX 3 & 4

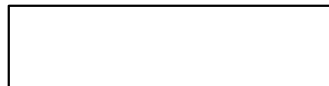


OU

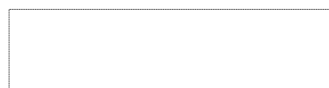
NIVEAUX 3 & 4



LEGENDE:



= Peut être la même personne



= Peut être la même société

C/R = Concepteur/Réalisateur      VER = Chargé de Vérification      VAL = Chargé de Validation

EVAL = Chargé d'Evaluation

CHEF PROJ = Chef de Projet

# L'EN 50128 : Logiciels pour systèmes de commande et de protection ferroviaires (1/2)

Objet : spécification des procédures et des exigences techniques applicables aux logiciels

Domaine d 'application :

- logiciels et interactions entre logiciel et système
- tous niveaux de sécurité (**SIL 1 à 4**)
- outils associés :
  - la programmation de l 'application
  - les systèmes d 'exploitation
  - les outils d 'aide
- les produits sur étagère (**COTS**)

# L'EN 50128 : Logiciels pour systèmes de commande et de protection ferroviaires (2/2)

## Contenu :

- définit les exigences pour chaque phase du cycle en V
- définit les moyens recommandés pour chaque phase en fonction du SIL :
  - Mandatory (Approche modulaire, tests fonctionnels, analyse d'impact en cas de maintenance, interface entièrement définie, ...)
  - Highly recommended (méthodes formelles, ...)
  - Recommended
  - Not recommended
  - Forbidden
- définit les exigences de l'évaluation
- définit les exigences de non régression (maintenance)
- définit les exigences des systèmes configurés par des données d'application



DIRECTION DE L'INGÉNIERIE  
DÉPARTEMENT IG.PS