Processus d'étude de sécurité pour la certification du système protection HGV de signalisation ferroviaire

Client : EUROTUNNEL

RIS – Atelier thématique n°5
Justification de sûreté de fonctionnement (safety case)
Journée du 18 MARS 2003 à Toulouse

Virgile LA LUMIA – Régis GIRKA

TECHNICATOME

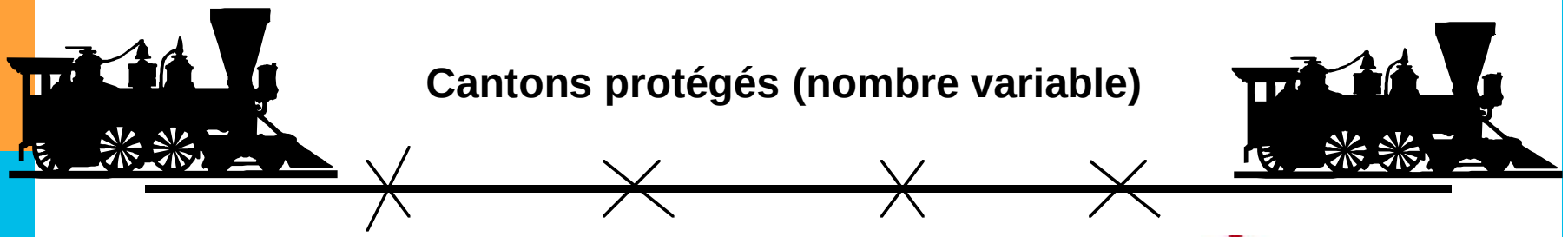
Présentation succincte du système de protection HGV (Heavy Goods Vehicule)

> Objectifs d'amélioration du système existant

- Optimisation du trafic dans le tunnel vis-à-vis des HGV
- Amélioration de la lutte anti-incendie : gestion des interdictions d'entrée et des évacuations en cas d'incendie

> Nouvel algorithme de protection :

- Définition dynamique du nombre de cantons protégés en fonction de la longueur réelle de chaque canton (TVM du train)

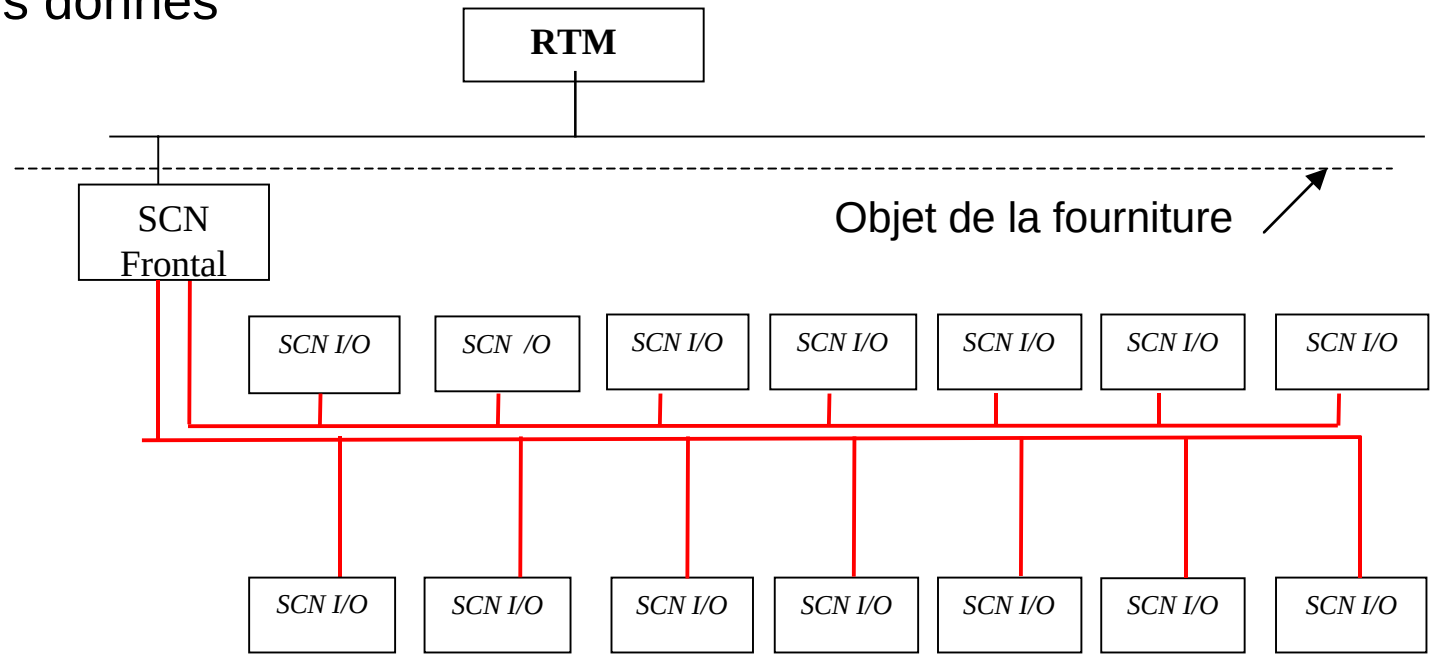


TECHNICATOME

Schéma simplifié du système protection HVG

- RTM (Railway Traffic Management) met en œuvre les algorithmes de protection : pilotage via le SCN Frontal (Safety Computer Network) des SCN I/O (Input/Ouput)

- Chaque SCN I/O gère la protection d'un certain nombre de cantons donnés



TECHNICATOME

Enjeux et objectifs de sécurité de la protection HGV

- Système protection HGV participe à la sécurité globale : **Classement SIL 2**
- Autorisation de mise en œuvre par la CIG (Commission Intergouvernementale de Sécurité du tunnel)
- EUROTUNNEL soumet le système à l'analyse de CERTIFER
- Base réglementaire principale pour la démonstration de sécurité : Norme XP ENV 50129 (Avril 2000) - Applications ferroviaires – Systèmes électroniques de sécurité pour la signalisation

TECHNICATOME

Processus étude de sécurité pour la certification du système protection HGV (partie SCN)

Norme XP ENV 50129 (Avril 2000) (Applications ferroviaires – Systèmes électroniques de sécurité pour la signalisation) distingue plusieurs aspects

- Démonstration de la gestion de la sécurité
- Atteinte de la sécurité technique (vérification des exigences ou justification vis-à-vis des contraintes techniques
- Satisfaction des objectifs de sécurité qualitatifs (robustesse / pannes) et quantitatifs (probabilité)

TECHNICATOME

Mise en œuvre du processus d'étude de sécurité en vue de la certification du système

> Problématiques génériques rencontrées dans tous les domaines (ferroviaire, nucléaire, etc.) :

- Aider le client : Intégration et prise en compte des interfaces du système analysé dans l'installation générale, etc.
- Satisfaire le client dans le service rendu (qualité du dossier de sécurité pour l'analyse par CERTIFER)
- Anticiper les attentes de autorité de sécurité / autorisation d'exploiter (définition du référentiel réglementaire, respect d'un processus d'analyse, etc.)

Démonstration de la gestion de la sécurité (partie SCN)

> Cycle de vie / sécurité du système

- Processus de gestion de la sécurité (planning des études et différentes phases de démonstration de sécurité) en conformité avec le cycle de vie du système

> Organisation de la sécurité

- Études et dossiers de sécurité établis sous la responsabilité du chargé d'études sécurité, hiérarchiquement indépendant des équipes de conception

Démonstration de la gestion de la sécurité (partie SCN) (Suite)

- Registre de situations dangereuses : Définition et suivi au titre de l'analyse préliminaire des risques
- Spécification des exigence de sécurité : données d'entrée explicites de responsabilité client
- Revues de sécurité : réalisées au titre de réunion générales ou particulières
- Justification de la sécurité réalisée au moyen des analyses et études de sécurité, soumises à l'acceptation du client

TECHNICATOME

Démonstration de l'atteinte de la sécurité technique (partie SCN)

> Vérification / exigences techniques de sécurité

- Montrer l'aptitude du système SCN à fonctionner en toute sécurité dans ses conditions d'exploitation (conditions climatiques, électriques) par essais d'identification et de qualification
- Respecter la spécification des exigences du système SCN par l'élaboration d'un plan de justification de la définition du système et l'établissement d'un dossier d'architecture ainsi que des interfaces

TECHNICATOME

Démonstration de l'atteinte de la sécurité technique (partie SCN) (Suite)

> Vérification de l'atteinte des objectifs de sécurité

- Réalisation d'une AMDEC sur les constituants du système SCN démontrant la capacité du système à respecter les exigence de sécurité
- A partir de l'AMDEC, identification des essais spécifiques de vérification de sécurité à réaliser en usine ou sur site
- Vérification du comportement attendu lors des essais

Démonstration de l'atteinte de la sécurité technique (partie SCN) (Suite)

> Vérification de l'atteinte des objectifs de sécurité

- Pour le logiciel et la carte CSG, niveau requis de sécurité SIL 2
- Réutilisation de la carte CSG déjà certifiée par CERTIFER pour le ferroviaire (analyse de sécurité générique de la carte CSG) mais avec identification et justification des différences ente le produit certifié et la définition utilisée sur SCN
- Sachant que CSG peut montrer un niveau supérieur à SIL 2 : marge de développement pour EUROTUNNEL

TECHNICATOME

Démonstration de l'atteinte des objectifs de sécurité par ER (partie SCN)

>Liste des ER (Évènements Redoutés)

Défaillances non observables par le RTM et conduisant à la non activation d'une protection (alors que l'information remontée au RTM est une protection activée) : **non pose d'une protection non vue par le RTM**

Défaillances non observables par le RTM et conduisant à la désactivation intempestive d'une protection (alors que l'information remontée vers le RTM indique une protection activée) : **levée intempestive d'une protection non vue par le RTM**

Défaillances du SCN conduisant à la **pose intempestive d'une protection**

TECHNICATOME

Démonstration de l'atteinte des objectifs de sécurité par ER (partie SCN)

> Analyse des ER par arbres de défaillances à partir des AMDEC et des données de fiabilité des constituants du Système SNC

- Objectif alloué pour une fonction SIL 2 :

  Taux d'occurrence global entre

  10^{-6}/heure et 10^{-7}/heure

- Taux d'occurrence démontré par ER pour système SCN :

  Inférieur à 10^{-7}/heure

TECHNICATOME

Parallèle des processus d'étude de sécurité Ferroviaire / Nucléaire

> Définition des exigences et des spécifications

- Ferroviaire : Norme NF EN 50126 (Applications ferroviaires – Spécifications et démonstration de fiabilité, de la disponibilité, de la maintenabilité et de la sécurité FMDS
- Nucléaire : CEI 61226 : Centrales nucléaires – Système d'instrumentation et de contrôle-commande importants pour la Sûreté -Classification

TECHNICATOME

Parallèle des processus d'étude de sécurité Ferroviaire / Nucléaire (suite)

> Processus d'étude et de réalisation des équipements de contrôle commande de sécurité

- Ferroviaire : Norme XP ENV 50129 (Applications ferroviaires – Systèmes électroniques de sécurité pour la signalisation)
- Nucléaire : Document TECHNICATOME : règles générales de développement et de qualification des équipements de contrôle commande et d'alimentation électrique

TECHNICATOME

Parallèle des processus d'étude de sécurité Ferroviaire / Nucléaire (suite)

- Processus d'étude et de réalisation des logiciels équipements de contrôle commande de sécurité
  - Ferroviaire : Norme XP ENV 50128 (Applications ferroviaires – Systèmes de signalisation, de télécommunication et traitement – Logiciels pour systèmes de commande et de protection ferroviaire)
  - Nucléaire : CEI 880 : Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires

TECHNICATOME