1 Recensement du système d'information de la SNCF.

Les systèmes informatisés sont exploités dans de nombreux domaines du secteur ferrovière

Il est possible de les regrouper dans les items suivants :

- Les trains ;
- Les communications train/réseau ;
- Gestion du réseau ferroviaire ;
- Gestion des gares ;

Ces items peuvent être déclinés en élément plus tangible.

1.1 Les trains.

Sous la dénomination des trains, il convient de discerner ce qui relève de la conduite du train en lui-même et les éléments, qui pourraient être considérer, de confort pour les clients.

Ces sous-éléments sont les suivants :

- ⇨ Contrôle commande du train pour la gestion :
  - de la motrice ;
  - des portes ;
  - des freins ;
  - de la climatisation.
- ⇨ Elément de confort :
  - WIFI proposé au client ;
  - Rechargement de batteries de Smartphone, ordinateur.
- ⇨ Dispositif de communication et de surveillance:
  - Diffusion audio de message;
  - Surveillance à bord via des caméras
  - Panneau d'affichage.
- ⇨ Dispositif de sécurité :
  - Déverrouillage manuel des accès ;
  - Gestion du signal d'alarme.

1.2 Train-réseau.

Cet item regroupe l'ensemble des interactions qui peut exister entre le train et son environnement immédiat.

- ⇨ Communication entre signalisation et le train ex : TGV ;
- ⇨ Communication train-centre de régulation ;
- ⇨ Communication entre le train et un passage à niveau.

1.3 Réseau.

Par réseau, il convient de considérer l'environnement du train de façon unitaire.
Cet environnement comprenant la gestion :

- ⇨ de la signalisation ;
- ⇨ des aiguillages ;
- ⇨ des passages à niveau.

1.4 Gestion des gares.

Les gares sont des endroits très intéressants car cumulant plusieurs fonctions. Ces fonctions sont :

- de nature technique par l'accueil et la gestion des trains ;
- de nature commercial par la vente de billets et de services ;
- ouvertes sur le monde :
  - Liberté d'accès ;
  - Accès à internet.

Les gares sont des points de convergence pour les métiers, la technique et le commerce.

Dans ce cadre, il est possible de décliner l'item comme suit :

- ⇨ Gestion des gares
  - ⇨ Affectation des quais à des trains.
  - ⇨ diffusion d'information aux clients ;
    - panneau d'affichage [Trains, horaires, dessertes] ;
    - dispositif de diffusion de message audio.
- ⇨ Gestion clientèle :
  - ⇨ SMS ;
  - ⇨ Panneau d'affichage ;
  - ⇨ internet [mail, site web, application mobile]
  - ⇨ Borne d'achat de billet.

2 Les attaques.

Trois types d'attaque sont identifiables selon le profil et les objectifs des attaquants :

- 1er profil d'attaque [PA1] : « just for fun », pour tester.
- 2ième profil d'attaque [PA2] : Porter atteinte à l'entreprise en recherchant à causer des pertes financières :
  - Rançon ;
  - Impact clientèle ;
- 3ième profil d'attaque [PA3] : Utiliser les plateformes de la SNCF pour atteindre un autre but.

2.1 Etude du profil PA1 :

Ce profil va regrouper les attaques concentrant les tentatives d'intrusion ou de blocage de service. Ce sont généralement des actions individuelles ou d'un groupe de copain. C'est la recherche de notoriété qui prévaut.

Les types d'attaque sont donc les suivants :

- Attaque type DDOS ;
- Tentative d'intrusion via le protocole http sur les composants suivants :
    - Application web et mobile ;
    - Elément connecté au réseau SNCF dans les gares ;
    - Train à quai.

2.2 Etude du profil PA2 :

Ce type de profil concentre sur des actions malveillantes, ciblées, motivée par la recherche de gain qui requièrent des connaissances techniques très élevées.

Concrètement, il peut être identifié les menaces suivantes :

- Prise de contrôle de panneau d'affichage et diffusion des informations erronées, fausses ou injurieuses ;
    - Obligation de mobiliser des ressources pour renseigner les voyageurs dans les gares;
- Rendre indisponible les panneaux d'affichage :
    - Obligation de mobiliser des ressources pour renseigner les voyageurs dans les gares;
- Rendre inopérant les trains :
    - Immobilisation d'actif financier ;
    - Perturbation du trafic ;
    - Remboursement voyageur ;
    - Augmentation du taux d'utilisation des trains en état de fonctionnement.
- Rendre indisponible ou aberrante la vente de billet [en ligne ou aux bornes] :
    - Obligation de mobiliser des ressources pour renseigner les voyageurs dans les gares;

2.3 Etude du profil PA3 :

Ce type de profil est la Menace la plus critique. Elle consiste à utiliser l'infrastructure pour atteindre un autre objectif.

Les scénarii plausibles sont les suivants :

- utiliser les composants réseau pour faire une attaque DDOS externe ou interne au réseau SNCF ;

- utiliser le WIFI dans les trains ou gare pour réaliser une activité malveillante tout en étant difficilement localisable [densité de personne dans une gare, personne dans un train en mouvement, etc.] ;

- Utiliser le réseau WIFI pour infecter les composants informatiques des clients

- provoquer le déraillement ou collision de trains :

    - si un accident : attentat « classique » ;

    - si plusieurs attentats simultanés : rechercher à submerger les services de secours pour désorganiser la force public et réaliser une autre activité en parallèle.

Les éléments à protéger sont les suivants :

- dispositif d'aiguillage ;
- système de signalisation [visuel ou par onde radio] ;
- passage à niveau ;
- contrôle commande des trains.

2.4 Synthèse du SI SNCF

Le SI de la SNCF peut être regroupé en trois groupes distincts :

- Le réseau et les trains;
- L'information dans les gares ;
- L'utilisation de système d'information au profit des clients.

Les figures ci-dessous représentent ces groupes.

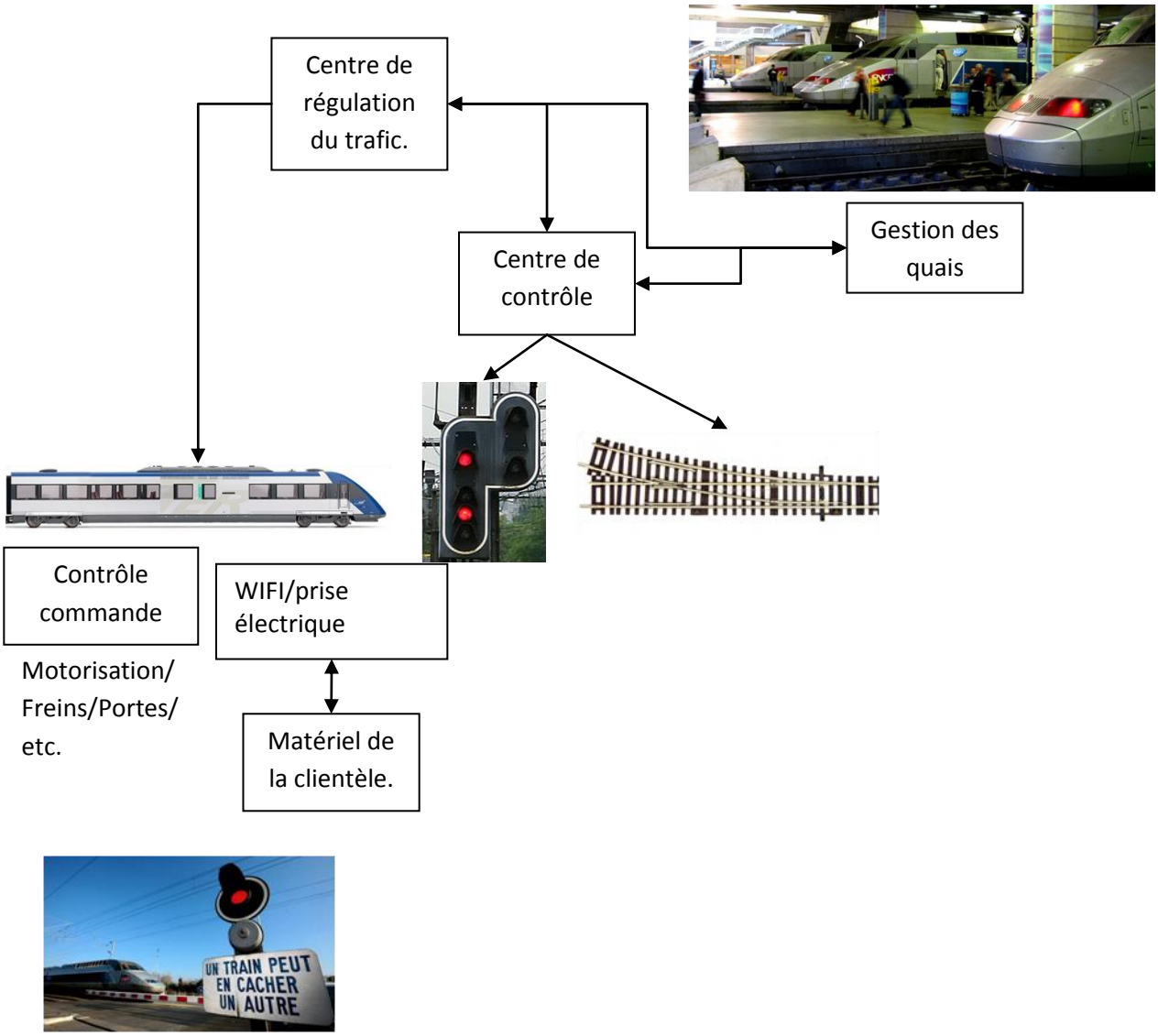


Figure 1 - Le réseau et les trains

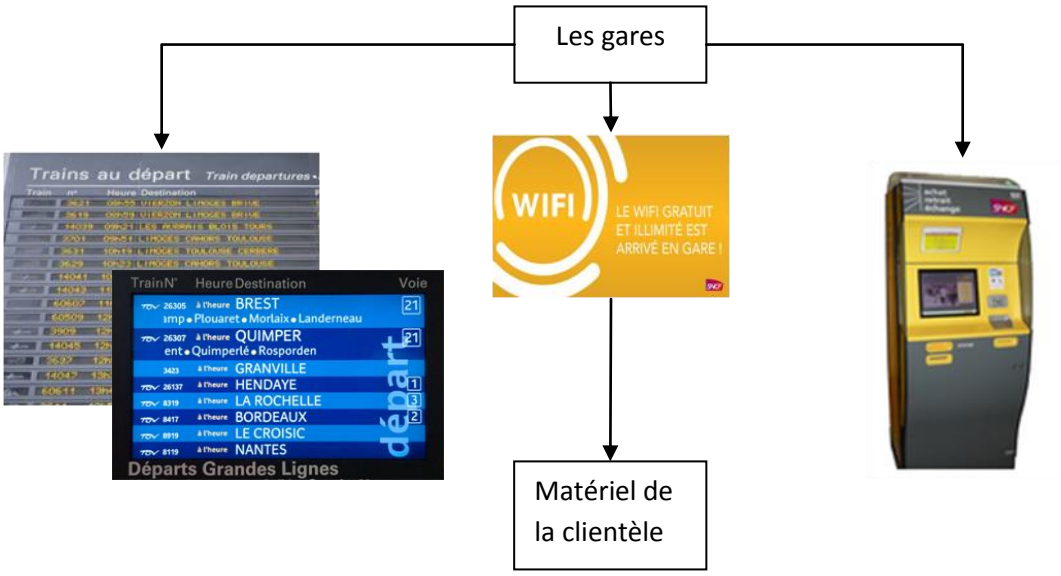


Figure 2 - L'information dans les gares

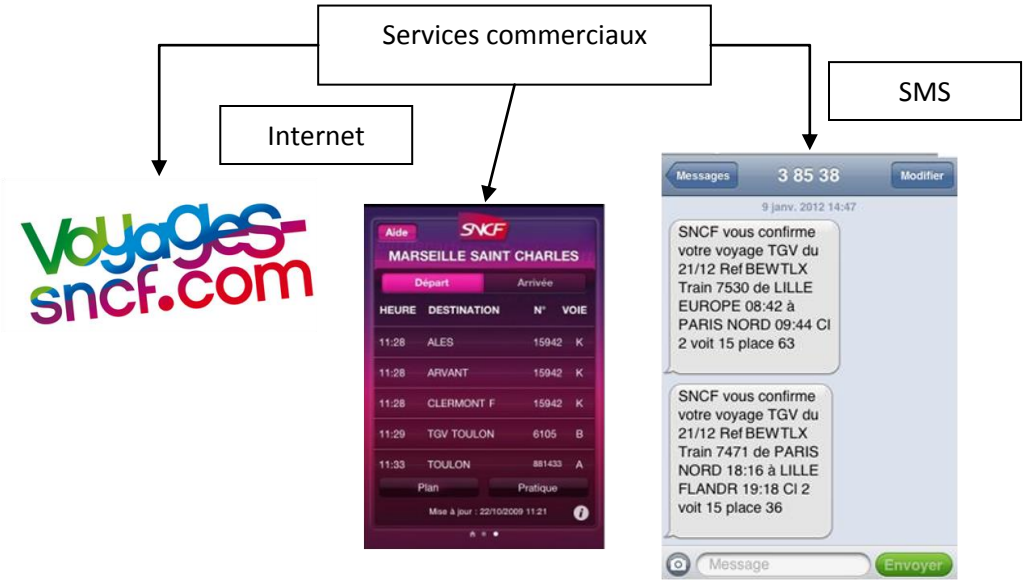


Figure 3 - L'utilisation des systèmes d'information au profit des clients.

3 La sureté versus la sécurité informatique.

D'une façon résumée, la sûreté peut être vue comme étant une confiance justifiée dans le comportement correct des fonctions requises du système concerné, dans des conditions d'utilisation données. Mais aussi l'aptitude à éviter des défaillances de service plus fréquentes.

Cela sous-entend qu'un système est considéré sûr s'il peut réaliser sa fonction dans les conditions d'exploitation exactement définies. Donc un système pourra fonctionner conformément à l'attendu si :
- son environnement d'exploitation est celui défini lors de sa conception ;
- si les systèmes l'utilisant respectent ses conditions d'emploi ;
- si sa conception a respecté les règles de l'art.

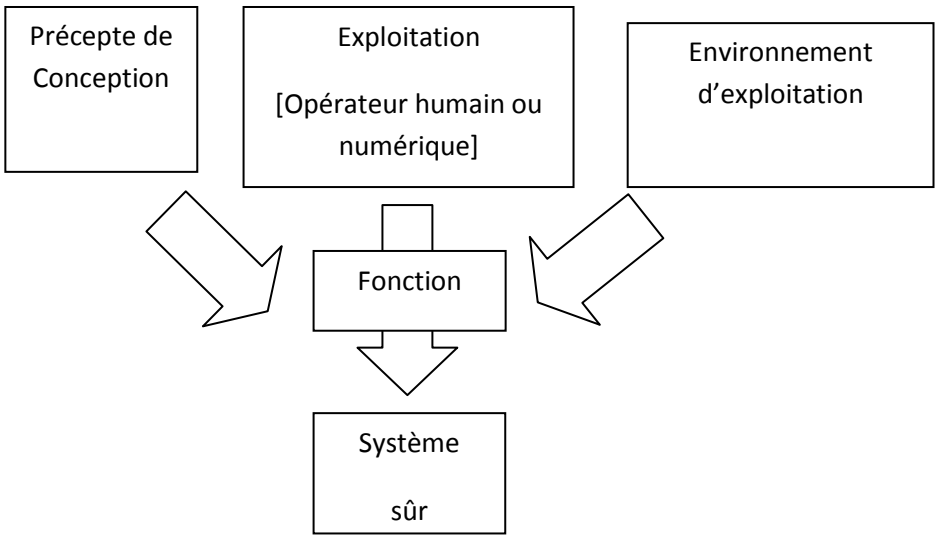


Figure 4 - Constitution d'un système sûr.

La notion de sécurité informatique telle qu'elle existe dans le corpus technique français ne permet pas de sortir du conflit sûreté versus sécurité informatique. Le terme « hacker » ou « hacking » est plus intéressant car il indique une notion de détournement d'un objet ou d'un système de sa fonction originelle pour lui faire faire autre chose.

Donc, la sûreté repose sur :
- des hypothèses de conception ;
- des hypothèses environnementales d'exploitation ;
- des hypothèses d'exploitation et de conduite ;

Si le hacking est la capacité à modifier la fonction alors, il va s'attaquer à ses paradigmes :
- de conception :
- de conditions environnementales ;

- d’exploitation et de conduite.

Donc le hacking va compromettre la sûreté en compromettant la base sur laquelle elle est fondée. Le hacking va donc, d’une façon générale, compromettre les hypothèses des études amont de conception.

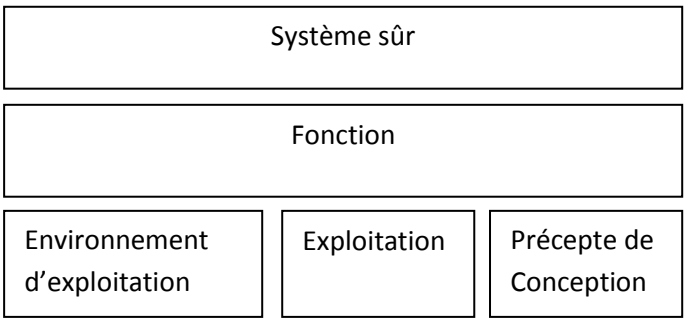
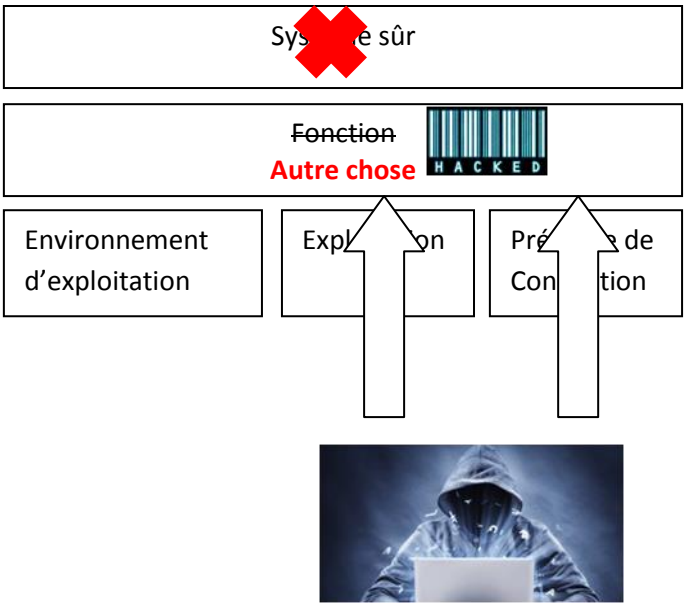


Figure 5 - Un système sûr ou l’appui d’une fonction sur des hypothèses

Les attaques de premier rang vont cibler préférentiellement les conditions d’exploitation et les préceptes de conception pour atteindre la fonction. Si ces deux items sont compromis alors la définition du système sûr est alors lui aussi compromis.



Compromission des hypothèses pour compromettre la notion de sûreté.

Le hacking impacte la pérennité de la sûreté d'une fonctionnalité. Ce constat nous permet donc de revenir sur le concept de la sécurité informatique vis-à-vis de la sûreté. La sécurité information doit donc permettre de contrer les effets du hacking. Donc la sécurité informatique doit garantir l'état physique et logique d'un système. La sécurité informatique doit donc figer l'état d'un système.

En conclusion, la sûreté d'un système repose sur son dimensionnement, les conditions d'exploitation, le respect de règle de son exploitation. La sécurité informatique va permettre d'assurer la pérennité de la sûreté d'un système en garantissant la pérennité des hypothèses émise lors des études amont de conception du système.

Donc la sécurité n'est pas contre la sûreté mais la garantie de sa pérennité dans le temps.

Peut-on aller jusqu'à affirmer que la sécurité est l'assurance vie d'un dispositif sûr ?

4 Proposition de pratique d'architecture.

Afin d'améliorer la sécurité informatique, il convient d'appliquer quelques règles de conception. Ces règles de conception sont déjà exprimées dans le référentiel normatif.

Les systèmes dits sûrs doivent être séparés des systèmes dits « normaux » et posséder leur propre capteur, automate et système de traitement et de présentation de l'information.

Il convient d'élaborer une cartographie des systèmes selon leur degré de sûreté. Cela induit donc la définition au préalable de la notion de degrés de sûreté.

Aucune interconnexion ne doit exister entre deux systèmes ayant des degrés de sûreté différents. Dans le cas où un système de moindre importance requière des informations d'un système ayant un classement de sûreté plus élevé, il convient d'instaurer des flux de communication monodirectionnels.

Afin de durcir un système, il convient de supprimer les composants et services inutiles, restreindre les droits d'exécution, désactiver les ports physiques non indispensables, etc.

Pour réduire la surface d'attaque d'un système, il convient de mettre en place deux principes :

- La segmentation : seule une partie du SI est accessible aux différents intervenants non privilégiés ;
- Mise en place d'une défense en profondeur par la mise en place de barrière physique et logique.

Pour cela, il faut donc :

- Séparer le SI industriel du SI de gestion ;
- Découper le SI industriel en « zones » ;
- Répartir les zones de manière à construire les « étages » de la défense en profondeur.

Pour les échanges entre composants, il convient de les chiffrer selon deux niveaux :

- Le premier niveau est l'utilisation d'un tunnel chiffré tel que SSL, ou autre ;
- Le second est le chiffrement du message lui-même.

Tous les échanges doivent être signés et le contenu certifié par un « checksum».

Toutes les informations doivent pouvoir être vérifiable selon un référentiel. C'est-à-dire que l'ensemble du SI communique selon un standard où les données sont organisées et possèdent un domaine de définition précis [au sens mathématique du terme].

Il doit exister un système détectant, de manière passive et sans interférence, des anomalies dans les échanges entre composants. Ce système doit permettre de lever des alertes sur un dispositif indépendant. La mise en place de ce système présuppose, la constitution d'une cartographie indiquant :

- Les interactions entre les systèmes ;
- La nature des messages :
    - contenu ;
    - séquence ;
    - etc.

Il conviendra de porter une attention particulière au dispositif de reconfiguration de réseau en cas de pannes. Certain système procède à la reconstitution automatique de parcelle de réseau permettant d'éviter de perdre durablement le contact entre deux sous-réseaux. Si ces dispositifs d'un point de vue opérationnel sont bénéfiques, ils présentent un problème dans le respect de la séparation des systèmes. Ils peuvent permettre des attaques en deux temps. Considérons un réseau où deux systèmes ne sont pas directement en contact. Une attaque ciblée conduit à perdre une zone du réseau. Le disposition de gestion lance une réorganisation du réseau et met en liaison deux systèmes qui ne doivent pas l'être. La machine compromisse peut donc accéder directement à la machine cible de l'attaque.

5 Limitation pratique à la sécurité.

Dans le monde industriel, de nombreux paramètres peuvent conduire à ne pas mettre en place une protection optimale.

Il peut être fait la liste suivante, sans être exhaustive :

- problème de perturbation entre le process industriel et le dispositif de surveillance ;
- longue durée d'exploitation des systèmes avec gestion de l'obsolescence et impossibilité de procéder au déploiement de mise à jour;
- opération de modernisation couteuse des systèmes et espacée de plusieurs années voire décennie ;
- impossibilité d'immobiliser des ressources matérielles pour les moderniser compte tenu de la charge d'exploitation ;
- augmentation de la latence des systèmes incompatibles avec le process industriel, suite à la cumulation des couches de protection et de chiffrement ;
- Augmentation des coûts de construction non acceptable vis-à-vis de la concurrence ;
- Difficulté de mettre en exergue les gains entre la conséquence d'une attaque et le coût pour se protéger d'un scénario d'attaque ;
- Problème de se protéger avec une technologie sur étagère [COTS] qui peut présenter des vulnérabilités spécifiques [SCADA, SSL, etc.];

- L’étendu du réseau qui peut être à l’échelle d’une ville, d’une région ou d’un pays [comment protéger un câble courant des dizaines de kilomètre le long des voies ferrées tout en garantissant sa maintenabilité ?].
- Protection physique versus facilité de maintenance