# CYBERSECURITE DES SYSTEMES DE TRANSPORT APPLICATION A LA LIGNE 18 DU GRAND PARIS EXPRESS

Philippe Gaufreteau, Lilian Planche

# CYBERSECURITE DES SYSTEMES DE TRANSPORT APPLICATION A LA LIGNE 18 DU GRAND PARIS EXPRESS

# CYBERSECURITY IN TRANSPORTATION SYSTEMS APPLICATION TO GRAND PARIS EXPRESS LINE 18

**Auteurs :**
Philippe GAUFRETEAU et Lilian PLANCHE
EGIS Rail
170 avenue Thiers
69006 Lyon
+33 437 724 424 / philippe.gaufreteau@egis.fr
+33 437 724 294 / lilian.planche@egis.fr

## Résumé

Compte tenu des enjeux qui pèsent sur un système de transport, il est essentiel de prendre en compte les risques relatifs à la cybersécurité dès la phase de conception générale de ce type de système. La première étape de la démarche proposée consiste à réaliser une analyse préliminaire des risques relatifs à la cybersécurité du système de transport dans son ensemble. Les résultats de cette étude servent de base à la définition des exigences de cybersécurité applicables aux futurs titulaires des différents marchés qui seront passés dans le cadre du projet de la ligne 18 du Grand Paris Express. Ces exigences portent notamment sur les biens essentiels faisant l'objet du marché, et sur les mesures à prendre en compte pour le système afin de garantir la couverture des risques pour la cybersécurité.

## Summary

Given the challenges facing a transportation system, it is essential to consider cybersecurity risks from the design phase of this type of system. The first step in the proposed approach is to conduct a preliminary risk analysis regarding the cybersecurity of the transportation system as a whole. The results of this study serve as a basis for defining the cybersecurity requirements applicable to future holders of the various contracts to be awarded under the Grand Paris Express Line 18 project. These requirements include the essential assets that are the subject of the contract and the measures to be taken into account for the system in order to ensure the coverage of risks for cybersecurity.

## Introduction

Cette communication vise à rappeler l'importance des menaces pesant sur la sécurité des systèmes d'informations dans le secteur d'importance vitale qu'est le secteur des « Transports terrestres », et à développer les spécificités de la prise en compte de ces menaces et des mesures à mettre en œuvre dans ce contexte aux contraintes particulières. Le Grand Paris Express, en tant que nouveau réseau de transport pour la plus grande zone urbaine de France, se doit de prendre en compte cette problématique dès les phases préliminaires de conception. Cette communication présente la première étape de la démarche consistant en une analyse préalable des risques relatifs à la cybersécurité du système de transport dans son ensemble, réalisée en phase de conception générale de la future ligne 18 du Grand Paris Express.

Compte tenu du caractère confidentiel de l'analyse de risques pour la cybersécurité réalisée sur la future ligne 18, seules des illustrations partielles des résultats obtenus seront présentées dans le cadre de cette communication, notamment en ce qui concerne les scénarios de menaces et les mesures de sécurité associées.

*Nota : dans cette communication, le terme « sécurité » renvoie à la cybersécurité, sauf mention contraire.*

## Contexte et enjeux de la démarche

### 1. Enjeux de la cybersécurité pour les systèmes de transport

Les cyber-menaces qui pèsent sur le secteur des transports pourraient résulter en des atteintes graves à ces infrastructures critiques pour le bon fonctionnement de nos états modernes.

Parmi les attaques récentes, on peut citer celle subie par la San Francisco Municipal Transportation Agency fin novembre 2016. L'individu malintentionné qui a infecté plus de 2000 systèmes de l'opérateur de transport a pris l'institution par surprise : les cybercriminels exigeaient le paiement d'une énorme rançon de 100 bitcoins. L'attaque a mis hors service des bornes de vente de tickets du réseau de métro léger Muni et l'agence a été contrainte de laisser les usagers voyager gratuitement tandis que le service informatique tentait de résoudre le problème. Les individus malintentionnés ont utilisé une version de HDDCryptor qui a infecté 2112 systèmes, dont un poste de travail d'administrateur, des postes de travail CAD, des serveurs de messagerie électronique et d'impression, des bornes de vente de billets, des postes de travail d'employés, des terminaux du service des objets trouvés, des bases SQL et des systèmes de paiement.

Autre exemple, lors d'une attaque le 13 mai 2017, les passagers des gares de grandes lignes en Allemagne ont pu voir des messages inhabituels sur les écrans d'information. A la place des informations de départs et d'arrivées, un avis de ransomware demandait un paiement de 300 US $ en Bitcoin. Le virus WanaCry avait infecté 450 ordinateurs de la Deutsche Bahn (les chemins de fer allemands), rendant inopérants les systèmes d'information voyageurs, les distributeurs de billets et les réseaux de vidéosurveillance.

Les systèmes d'information des systèmes de transport sont à la croisée des mondes industriels (OT) et informatiques (IT), et ils doivent être pris en compte selon ces deux points de vue. Lors de la conception d'un nouveau système de transport, les enjeux de cybersécurité doivent être inclus dès le démarrage du projet. Par exemple, à partir d'un simple capteur, une succession de failles peut permettre de remonter jusqu'à un serveur et générer des nuisances importantes dans tout le système d'information. Inversement, un email

frauduleux peut introduire une menace à destination des systèmes embarqués.

### 2. La ligne 18 du Grand Paris Express

L'approche proposée est mise en œuvre par EGIS Rail en tant que Maître d'Œuvre des Systèmes de la ligne 18 du Grand Paris Express. La ligne 18 (voir Figure 1), longue d'environ 34 km, doit permettre de transporter entre Orly et Versailles-Chantiers plusieurs milliers de passagers en heure de pointe. L'exploitation de la ligne sera entièrement automatisée, avec un niveau d'automatisation GOA4 (Grade of Automation 4 – Exploitation sans personnel à bord des trains). Le système de transport inclut la ligne, les gares, les sites de remisage et de maintenance, les puits, les accès de secours et les Postes de Contrôle Centralisé (PCC). Il s'agit d'un système complet qui englobe les domaines suivants : systèmes courants forts (énergie), systèmes courants faibles (télécommunications, information voyageurs, contrôle d'accès, détection et extinction d'incendie, etc), façades de quais, automatismes de conduite des trains et commandes centralisées, matériel roulant et véhicules de maintenance, équipements industriels de maintenance, équipements des gares et de la ligne, voie ferrée et aménagements des tunnels/viaducs.

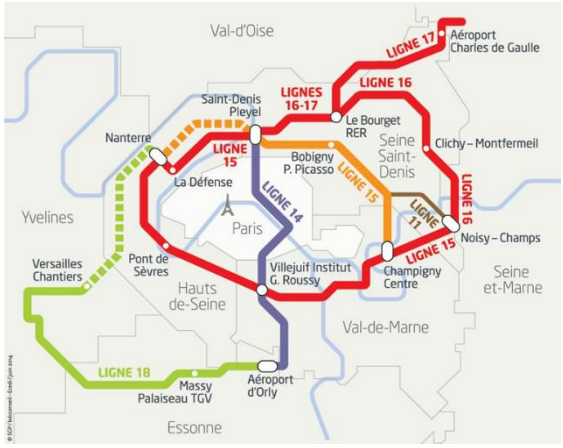


**Figure 1.** Carte du Grand Paris Express

## Objectifs à atteindre

L'approche proposée vise à faire converger les analyses de risques standards du monde IT avec les spécificités de la cybersécurité industrielle (en référence notamment à la norme IEC62443), dont la modélisation repose sur le modèle de référence pour les systèmes industriels (CIM - Computer Integrated Manufacturing). Le modèle CIM propose une organisation hiérarchique des systèmes numériques selon 5 niveaux, tel que l'illustre la Figure 2. Dans le cadre de notre étude, il permet de couvrir les différentes strates fonctionnelles, du niveau 4 : supervision générale du réseau (Poste de Contrôle Centralisé), au niveau 1 : contrôle du freinage ou de la traction des trains.

La démarche doit permettre d'intégrer les contraintes propres à un système de transport et à l'exploitation ferroviaire. Ces contraintes de cybersécurité impactent particulièrement :

- Les performances : augmentation des traitements (par exemple, liés au chiffrement),
- L'intégration des systèmes : cloisonnement des systèmes pour isoler les fonctions vitales,
- La durée de vie : mise à jour pour le maintien en sécurité.

Elle doit également prendre en compte les enjeux spécifiques aux nouveaux systèmes :

- Intégration de systèmes divers : numérisation, communications sans fil, interconnexion, rationalisation, etc,
- Intégration avec des systèmes externes : Autorité Organisatrice des Transports, exploitant, mainteneur, banques, développeurs d'applications, etc,
- Développement de l'offre de service, dans le but d'offrir plus qu'un service de transport : liens avec les terminaux mobiles, Wi-Fi, géolocalisation, contenus multimédia, etc,
- Mise en sécurité de systèmes anciens (produits déjà développés depuis plusieurs années) : la solidité d'une chaîne se jauge à son maillon le plus faible.

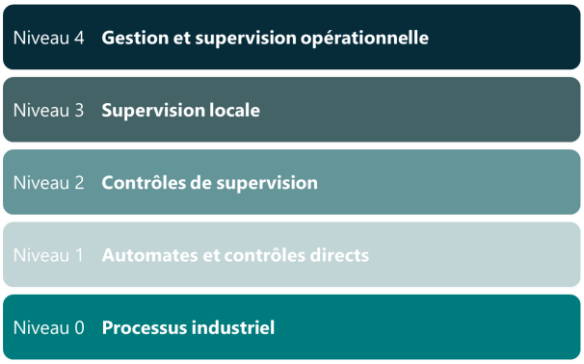


**Figure 2.** Modèle CIM

Les résultats de l'analyse préliminaire des risques pour la cybersécurité de la ligne 18 servent de base à la définition des exigences de cybersécurité applicables aux futurs titulaires des différents marchés qui seront passés dans le cadre du projet. Ces exigences portent notamment sur les biens essentiels faisant l'objet du marché, et sur les mesures à prendre en compte pour le système afin de garantir la couverture des risques identifiés dans l'analyse préliminaire de risques cybersécurité.

## Démarche mise en œuvre

### 1. Analyse des risques selon la méthode EBIOS

L'analyse des risques relatifs à la cybersécurité est réalisée en s'appuyant sur la méthode d'Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) créée par l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information). Cette méthode est conforme à la norme ISO 27005 sur la gestion des risques liés à la sécurité de l'information.

Elle se déroule en étapes successives (voir Figure 3) :

- L'étude du contexte consiste à cadrer le périmètre de l'étude en s'intéressant à la structure étudiée et à son environnement, en préparant des métriques et en identifiant les biens concernés.
- L'étude des évènements redoutés contribue à l'appréciation des risques par l'identification des besoins de sécurité applicables et leur hiérarchisation.
- L'étude des scénarios de menaces concerne les évènements susceptibles de mettre en cause la sécurité au sein du périmètre défini, les différentes mesures existantes et leur influence sur l'impact des évènements identifiés.
- L'étude des risques vise à cerner uniquement les scénarios qui doivent être traités en regard des problématiques spécifiques identifiées précédemment, à analyser l'impact des mesures

introduites en amont par la Maîtrise d'Ouvrage, et à définir les objectifs de traitement.
- L'étude des mesures de sécurité a pour objectifs de définir les mesures à mettre en œuvre, de contrôler leur application et d'évaluer leur efficacité.

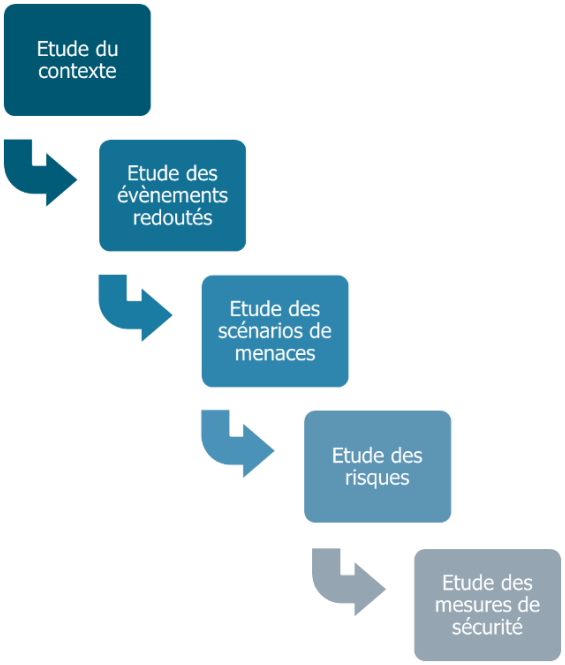


**Figure 3.** Démarche EBIOS

Cette étude est faite lors de la conception générale du système de transport, en amont de la phase d'exécution des marchés, à savoir en phase « Projet » au sens de la loi relative à la maîtrise d'ouvrage publique et à ses rapports avec la maîtrise d'oeuvre privée (dite « loi MOP »). Il s'agit donc d'une analyse préliminaire des risques relatifs à la cybersécurité, qui doit permettre l'identification des mesures à inclure dans les dossiers de consultations des entreprises qui seront établis pour les appels d'offre. Cette analyse n'a pas vocation à être exhaustive, mais vise avant tout à identifier les mesures générales qui devront être appliquées lors de la conception détaillée des différents sous-systèmes. Les futurs titulaires des marchés relatifs à ces sous-systèmes seront en charge de décliner ces mesures au travers d'analyses de risques détaillées sur leurs périmètres respectifs. Cette analyse cherche également à mettre en évidence, sous forme de points d'attention, plusieurs éléments de l'architecture sur lesquels la vigilance devra être maximale.

L'étude effectuée cherche à prendre en compte au plus tôt les principes de la défense en profondeur, de façon à assurer la sécurité intrinsèque du système et de ses composants, mais aussi d'intégrer des couches de sécurité en complément de la sécurité périmétrique. La sécurité périmètrique est la forme la plus classique de prise en compte de la sécurité dans un système, elle consiste à protéger le système à ses limites avec l'extérieur, en dressant des barrières robustes, en implémentant des contrôles systématiques et des mécanismes de détection adaptés. Cette première ligne dans la protection d'un système doit être suffisante pour écarter la plupart des attaquants, mais la sécurité absolue n'existant pas, elle ne peut être la seule protection mise en œuvre. Le principe de la sécurité en couches vient en complément de la sécurité périmètrique, il s'agit d'établir des remparts entre les différentes zones de sécurité (cf. IEC62443-1-1) d'un système, de manière à ralentir la progression d'un attaquant qui aurait réussi à pénétrer le système. Les zones de sécurité sont définies selon un périmètre qui regroupe de manière cohérente des composants en fonction du risque et de l'architecture du système d'information, par exemple les équipements centraux utilisés pour la supervision du trafic. Chaque couche nécessitant un effort conséquent pour être passée, la multiplication des couches entre l'attaquant et son objectif peut, selon la nature de l'attaquant, être dissuasive, ou le retarder suffisamment pour permettre sa détection. Le concept de sécurité intrinsèque, que l'on retrouve également sous l'expression « secure by design », consiste à prendre en compte la sécurité dès les premières étapes du développement d'un produit ou d'un système. En effet, il est toujours plus efficace d'intégrer les mesures nécessaires à la sécurisation lors de la conception, que de pallier à des manques plus tard dans le cycle de développement, ou lors de l'intégration. Son application conduit à la mise en oeuvre des principes de la sécurité périmètrique et de la sécurité en couches, mais également de règles de conception et de mesures techniques visant à durcir les composants et le système.

## 2. Définition du périmètre de l'étude

Etant donné la démarche globale dans laquelle s'inscrit l'analyse préliminaire, le périmètre d'étude s'est porté sur l'ensemble du système d'information du système de transport de la ligne 18, sur la base d'une architecture préliminaire simplifiée des réseaux informatiques du système de transport (voir Figure 4).

Ce système d'information gère des systèmes tels que : l'alimentation électrique, les télécommunications, l'information des voyageurs, la billettique et l'accès aux stations, la gestion du trafic, la protection incendie, la gestion de la maintenance, etc.

Dans la définition du contexte de l'étude, nous avons consolidé les éléments d'architecture technique issus des différents sous-systèmes pour obtenir une vue épurée de l'architecture globale offrant le bon niveau de définition au regard des objectifs de l'étude. Une attention particulière est portée sur les différents types de connectivités mis en œuvre : accès à des systèmes externes (ex : Wifi usagers), connexions sans fil, systèmes isolés, etc.

Les éléments structurants de l'analyse effectuée sur ce périmètre sont les suivants :
- Les enjeux au niveau du système de transport de la ligne 18 (ex : vitesse commerciale, niveau de régularité et de ponctualité des trains, niveau de disponibilité des systèmes, niveau de sécurité et de sûreté, qualité de l'information des voyageurs, évolutivité, etc).
- Les différentes parties prenantes du système de transport (l'exploitant du système de transport, les mainteneurs, la préfecture de Police, Ile de France Mobilités, les usagers, les industriels et leurs sous-traitants).
- Les contraintes réglementaires : obligations de la loi de programmation militaire (LPM) pour les Opérateurs d'Importance Vitale (OIV), obligations de la directive européenne 2016/1148 sur la sécurité des réseaux et des systèmes d'information (NIS) pour les Opérateurs de Services Essentiels (OSE),
- Le respect par les systèmes de traitement de l'information mis en œuvre, du règlement européen 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (enregistrements vidéo, enregistrements audio, données relatives aux abonnements et aux activités des opérateurs et usagers…) et à la libre circulation de ces données (GDPR),

- Diverses contraintes dont la définition précise n'est pas encore connue à ce stade du projet : contraintes relatives au personnel, contraintes d'ordre budgétaire, contraintes techniques, contraintes d'environnement, contraintes d'ordre calendaire.
- Les sources de menaces, selon la typologie proposée par la méthode EBIOS (ex : source humaine interne ou externe, malveillante ou sans intention de nuire, avec des capacités d'action plus ou moins importantes ; code malveillant d'origine inconnue ; etc). Une illustration des menaces identifiées est donnée au Tableau 1
- Les critères de sécurité et les métriques correspondantes permettant d'évaluer les besoins de sécurité des biens essentiels. Dans le cadre de l'analyse préliminaire du système de transport de la ligne 18, les critères de sécurité retenus sont : la disponibilité, l'intégrité, la confidentialité, la preuve (voir Tableau 2). Chaque critère est évalué selon 4 niveaux.
- Le niveau de chacun des risques identifiés permettant de les classer en risques modérés, significatifs, graves ou majeurs. Il est fonction de la gravité des évènements redoutés qui le déclenche et de la vraisemblance des scénarios de menace qui y conduisent. La gravité des événements redoutés est évaluée selon leurs impacts potentiels dans les différents domaines suivants : financier, juridique, organisationnel, commercial / image, social, accident. Les évènements redoutés sont classés par ordre croissant de gravité, l'impact le plus grave étant retenu pour chaque évènement. La vraisemblance des scénarios est appréciée selon une échelle à 4 niveaux : Minime, Significatif, Fort, Maximal, dont les définitions permettent aux contributeurs de l'analyse de discriminer clairement les différents niveaux. L'échelle de vraisemblance est présentée au Tableau 3 et celle de gravité au Tableau 4.

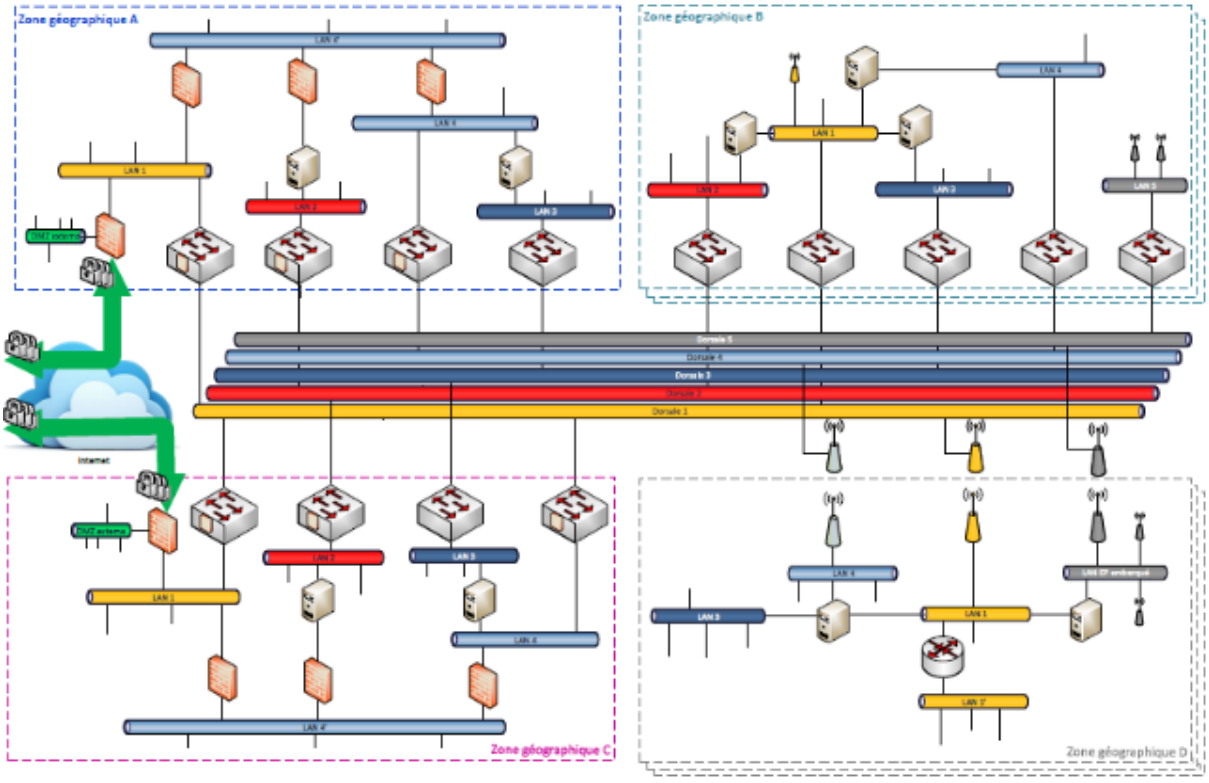


**Figure 4.** Architecture réseau simplifiée

| Type de source de menace | Source de menace |
|---|---|
| Source humaine interne, malveillante, avec de faibles capacités | Usager<br>Employé |
| Source humaine externe, malveillante, avec des capacités importantes | Fraudeur<br>Concurrent de l'exploitant<br>Organisation syndicale<br>Pirate<br>Ancien employé |
| Source humaine interne, sans intention de nuire, avec des capacités illimitées | Dirigeant négligeant |
| Source humaine externe, sans intention de nuire, avec de faibles capacités | Entourage d'un employé<br>Ile de France Mobilités |
| Code malveillant d'origine inconnue | Virus non ciblé ou ciblé |

**Tableau 1.** Sources de menaces identifiées (extrait)

| Critère de sécurité | Définition du critère |
|---|---|
| Disponibilité | Les utilisateurs doivent pouvoir accéder au système au moment voulu pour les traitements nécessaires au bon fonctionnement du système de transport. |
| Intégrité | Les informations ne doivent pas être modifiées indûment, altérées ou détruites. |
| Confidentialité | Une information doit être disponible et accessible uniquement aux personnes, composantes ou processus autorisés. |
| Preuve | les activités du système d'information doivent être identifiables et suivies. |

**Tableau 2.** Critères de sécurité

| Niveau de vraisemblance | Ordre | Description |
|---|---|---|
| **Minime** | 1 | Cela ne devrait pas se (re)produire. |
| **Significatif** | 2 | Cela pourrait se (re)produire. |
| **Fort** | 3 | Cela devrait se (re)produire un jour ou l'autre. |
| **Maximal** | 4 | Cela va certainement se (re)produire prochainement. |

**Tableau 3.** Echelle de vraisemblance

| Niveau de gravité | Ordre | Description des impacts | | | | | |
|---|---|---|---|---|---|---|---|
| | | **Financier** | **Juridique** | **Organisa-tionnel** | **Commercial / Image** | **Social** | **Accident** |
| **Modéré** | 1 | Incident de parcours sur le plan financier. | Infraction nécessitant une médiation | Nuisances | Mécontentement / Information à portée locale, ou spécialisée | Désaccord | Eventuellement une personne légèrement blessée |
| **Significatif** | 2 | Affecte Ile de France Mobilités ou l'exploitant sur le plan financier sur une année. | Infraction entraînant une amende | Perturbation forte | Perte de clientèle / Série d'informations à portée locale ou spécialisée | Absentéisme | Blessures légères et/ou menace grave pour l'environnement. |
| **Grave** | 3 | Affecte Ile de France Mobilités ou l'exploitant sur le plan financier entre 1 et 3 ans. | Infraction entraînant une indemnisation | Arrêt partiel | Intervention politique locale / Information à portée nationale | Départ de personnel, mouvement social | Un mort et/ou une personne grièvement blessée et/ou des dommages graves pour l'environnement |
| **Majeur** | 4 | Affecte Ile de France Mobilités ou l'exploitant sur le plan financier sur plus de 3 ans. | Infraction entraînant une sanction pénale | Arrêt total | Intervention gouvernementale / Information à portée internationale | Crise sociale, grève de longue durée | Des morts et/ou plusieurs personnes gravement blessées et/ou des dommages majeurs pour l'environnement. |

**Tableau 4.** Echelle de gravité

### 3. Biens essentiels et biens supports

Pour évaluer les risques relatifs à la cybersécurité qui pèsent sur la future ligne 18, il faut déterminer les biens essentiels (principales activités) qui auront des conséquences directes sur les missions et l'organisation de l'exploitant. Ces biens essentiels correspondent aux fonctions réalisées par le système d'information défini dans le périmètre de l'étude.

Pour les informations concernées par chacun des biens essentiels identifiés, nous avons choisi de travailler avec trois grandes familles d'informations : les informations d'exploitation qui permettent le bon fonctionnement du système de transport, les informations de sécurité qui permettent de garantir la sécurité de l'ensemble des personnes concernées par le système de transport et les informations personnelles qui concernent spécifiquement les activités des individus (voir Tableau 5).

Les biens essentiels reposent sur des biens supports (principaux équipements) qui sont exposés aux menaces potentielles en termes de cybersécurité. Leurs vulnérabilités nécessitent de mettre en place des mesures de sécurité adéquates. En analyse préliminaire, il ne s'agit pas de faire un inventaire exhaustif des biens supports concernés mais d'identifier, à une échelle macroscopique, les biens supports de plus haut niveau, et d'expliciter pour chacun d'eux les principaux biens supports de niveau inférieur qu'il inclut.

Ainsi, la typologie (simplifiée) des biens supports retenue dans le cadre de l'analyse préliminaire est la suivante :

- Les locaux du système de transport, aussi bien les bureaux dans lesquels sont installés les équipes que les gares, les centres de maintenance, la ligne, les trains, les puits, etc,
- L'organisation en charge de l'exploitation du système de transport,
- Les différents types de réseaux utilisés par le système d'information,
- Les différents acteurs en interface avec le système d'information, tels que : les mainteneurs, les entreprises en charge du développement et de la fourniture des divers équipements qui constituent le système de transport, les diverses autorités, etc.

Les liens entre biens essentiels et biens supports retenus sont ensuite établis.

| Bien essentiel | Information concernée |
|---|---|
| Gérer les télécommunications | Informations personnelles<br>Informations d'exploitation<br>Informations de sécurité |
| Gérer l'information des voyageurs | Informations d'exploitation<br>Informations de sécurité |
| Gérer les éclairages | Informations d'exploitation<br>Informations de sécurité |
| Gérer la protection incendie | Informations d'exploitation<br>Informations de sécurité |
| Gérer la maintenance | Informations d'exploitation |

**Tableau 5.** Correspondance entre biens essentiels et familles d'informations (extrait)

## 4. Etude des événements redoutés

L'analyse des évènements redoutés est effectuée en identifiant les risques encourus par les biens essentiels et en évaluant la gravité de leurs impacts. Ensuite, les scénarios de menaces sont étudiés en évaluant, pour chaque bien support, la vraisemblance des scénarios de menaces relatifs à chacun des critères de sécurité, sur la base des différentes sources de menaces retenues.

En raison de l'ampleur du périmètre de l'analyse et de son positionnement en phase de conception générale, nous avons décidé d'adopter une approche plus macroscopique afin de réduire le volume d'informations à traiter. Etant donné le périmètre couvert par l'analyse préliminaire des risques, le nombre de menaces relatives à la cybersécurité à prendre en compte est très important. Pour chacun des biens essentiels, nous évaluons d'abord le besoin de sécurité, puis la gravité de l'atteinte maximale envisageable pour chacun des critères. Le principe adopté a été de ne pas étudier systématiquement toutes les mesures applicables à un risque donné, mais de se focaliser sur les mesures qui seront nécessaires au futur exploitant de la ligne 18 dans le cadre de l'homologation du système « tel que réalisé ». Lors de la conception détaillée des sous-systèmes par les futurs titulaires de marchés, des choix de conception seront effectués et donneront lieu à l'identification de failles et de vulnérabilités différentes selon ces choix. Des mesures détaillées seront définies et viendront compléter, le cas échéant, les mesures identifiées lors de la conception générale par le maître d'œuvre. Ainsi, les mesures de réduction des risques pour la cybersécurité sont définies en correspondance avec les niveaux des différentes analyses de risques successives :

1) L'analyse préliminaire des risques au niveau système global effectuée par le maître d'œuvre,
2) Les analyses de risques détaillées réalisées au niveau des sous-systèmes par les entreprises titulaires des différents marchés,
3) L'analyse de risques conduite par l'exploitant dans le cadre de l'homologation de son système *(NOTA : à ce stade, le périmètre d'homologation n'est pas connu)*.

Pour chacun des biens essentiels, nous évaluons d'abord le besoin de sécurité, puis la gravité de l'atteinte maximale envisageable pour chacun des critères. Enfin, nous leur associons une classe parmi les 3 classes de systèmes industriels définies par l'ANSSI :

- Classe 1 : Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est faible. L'ensemble des mesures préconisées pour cette classe doivent pouvoir être appliquées en complète autonomie.
- Classe 2 : Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est significatif. Il n'y a pas de contrôle étatique pour cette classe de système industriel, mais l'entité responsable doit pouvoir apporter la preuve de la mise en place des mesures adéquates en cas de contrôle ou d'incident.
- Classe 3 : Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est critique. Dans cette classe, les obligations sont plus fortes et la conformité de ces systèmes industriels peut être vérifiée par l'autorité étatique ou un organisme accrédité.

L'analyse du besoin de sécurité des biens essentiels pour chacun des critères est illustrée au Tableau 6. Chaque besoin de sécurité est issu de la concertation avec les différents spécialistes métiers (ex : courants forts, sécurité incendie, automatismes, etc) et la Maîtrise d'Ouvrage.

| Bien essentiel | Besoin de sécurité | | | |
|---|---|---|---|---|
| | Disponibilité | Intégrité | Confidentialité | Preuve |
| Gérer les télécommunications | Moins de 1h | Maîtrisé | Privé | Authen-tique |
| Gérer l'information des voyageurs | Plus de 24h | Maîtrisé | Public | Formelle |
| Gérer les éclairages | Moins de 1h | Détec-table | Limité | Formelle |
| Gérer la protection incendie | Moins de 1h | Intègre | Limité | Authen-tique |
| Gérer la maintenance | Plus de 24h | Détec-table | Limité | Formelle |

**Tableau 6.** Analyse du besoin de sécurité des biens essentiels pour chacun des critères (extrait)

Les résultats de l'analyse de la gravité des impacts des critères de sécurité sur les biens essentiels sont illustrés au Tableau 7. La correspondance entre les classes de systèmes et la gravité des impacts est établie selon les principes suivants :

- Un niveau de gravité « modéré » conduit à affecter un système en classe 1,
- Un niveau de gravité « significatif » ou « grave » conduit à affecter un système en classe 2,
- Un niveau de gravité « majeur » conduit à affecter un système en classe 3.

Les classes associées aux biens essentiels sont affectées aux biens supports, en considérant que c'est la classe du niveau le plus haut qui s'applique à un bien support partagé entre plusieurs biens essentiels.

| Bien essentiel | Niveau de gravité | | | | Classe |
|---|---|---|---|---|---|
| | Disponibilité | Intégrité | Confidentialité | Preuve | |
| Gérer les télécom. | Majeur | Grave | Grave | Grave | 3 |
| Gérer l'info. voyageurs | Signi-ficatif | Grave | Modéré | Modéré | 2 |
| Gérer les éclairages | Majeur | Majeur | Modéré | Modéré | 3 |
| Gérer la protection incendie | Majeur | Majeur | Modéré | Modéré | 3 |
| Gérer la maintenance | Signi-ficatif | Signi-ficatif | Modéré | Signi-ficatif | 2 |

**Tableau 7.** Gravité des impacts des critères de sécurité sur les biens essentiels (extrait)

## 5. Etude des scénarios de menaces

Pour chaque bien support, on évalue la vraisemblance des scénarios de menaces relatifs à chacun des critères de sécurité, en prenant en compte les différentes sources de menaces retenues (voir Tableau 3).

L'application de ces principes aux menaces sur le réseau de communication du Système de Sécurité Incendie (SSI) est illustrée au Tableau 8.

| Scénario de menace | Source de menaces | Niveau de vraisemblance |
|---|---|---|
| Menace sur le réseau SSI causant une indisponibilité | Administrateur système<br>Organisation criminelle<br>Organisation terroriste<br>Virus non ciblé ou ciblé<br>Accident | Fort |
| Menace sur le réseau SSI causant une altération | Administrateur système<br>Organisation criminelle<br>Organisation terroriste<br>Agence gouvernementale étrangère<br>Virus non ciblé ou ciblé | Significatif |
| Menace sur le réseau SSI causant une compromission | Administrateur système<br>Pirates<br>Agence gouvernementale étrangère | Minime |
| Menace sur le réseau SSI causant une altération de la traçabilité | Sous-traitant<br>Administrateur | Minime |

**Tableau 8.** Niveau de vraisemblance des scénarios de menaces (extrait)

## 6. Etude des risques

Le croisement des évènements redoutés et des scénarios de menaces permet d'identifier des risques : au total, environ 60 risques ont été identifiés dans le cadre de l'analyse préliminaire effectuée à ce stade du projet.

Le niveau de chaque risque dépend de la gravité de l'évènement redouté, et des plus fortes vraisemblances parmi les scénarios de menaces associés aux biens supports dont dépend le bien essentiel à l'origine de l'évènement redouté. Les risques sont alors classés par niveau : intolérable, significatif, négligeable. A titre d'illustration, concernant le SSI évoqué plus haut, le risque de corruption d'opération de gestion de la protection incendie est considéré comme « intolérable », car il a un niveau de vraisemblance fort et un niveau de gravité majeur. Ou encore, le risque de perte de confidentialité sur l'opération d'information des voyageurs est « significatif », car il a un niveau de vraisemblance maximal et un niveau de gravité majeur.

A la suite, on représente la synthèse de l'évaluation des risques sans prise en compte de mesures de sécurité (voir Figure 5). C'est sur cette base que nous pourrons décider des options de traitement des risques, ce qui conduira à la définition des objectifs de sécurité, au sens de la méthode EBIOS qui propose quatre options possibles pour chacun des risques identifiés :

- l'éviter (ou le refuser) : changer le contexte de telle sorte qu'on n'y soit plus exposé,
- le réduire : prendre des mesures de sécurité pour diminuer l'impact et/ou la vraisemblance,
- le transférer (ou le partager) : partager les pertes occasionnées par un sinistre ou faire assumer la responsabilité à un (des) tiers,
- le prendre (ou le maintenir), voire l'augmenter : assumer les conséquences sans prendre de mesure de sécurité supplémentaire.

Dans le cadre de notre étude, il est décidé de réduire tous les risques significatifs et tous les risques intolérables, et pour tous les risques négligeables, de les prendre.

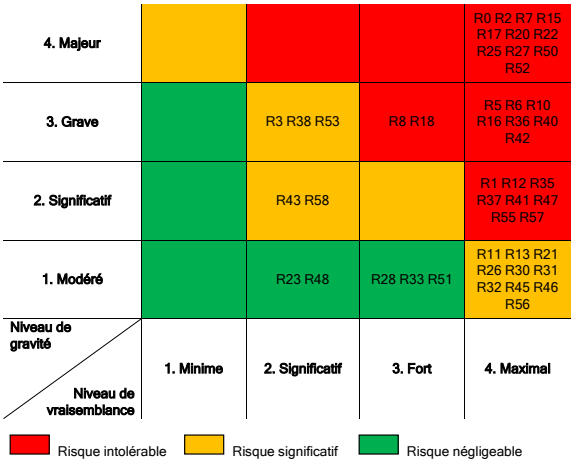


**Figure 5.** Synthèse des risques

## 7. Etude des mesures de sécurité

La prise en compte de l'ensemble des éléments d'analyse nous permet de classer les réseaux supports par niveau de sécurité, du moins sûr au plus sûr. Ce classement doit être pris en compte dans la définition des échanges entre les équipements : les échanges entre réseaux de niveau de sécurité différents doivent être réduits au strict nécessaire, et les systèmes des réseaux les plus

sécurisés doivent être les seuls à pouvoir initier des échanges avec les systèmes des réseaux moins sécurisés.

L'analyse générale de l'architecture a mis en évidence plusieurs éléments sur lesquels la vigilance devra être maximale. Ces points d'attention viennent en complément des équipements réseau et des équipements de protection : voir illustration à la Figure 6.

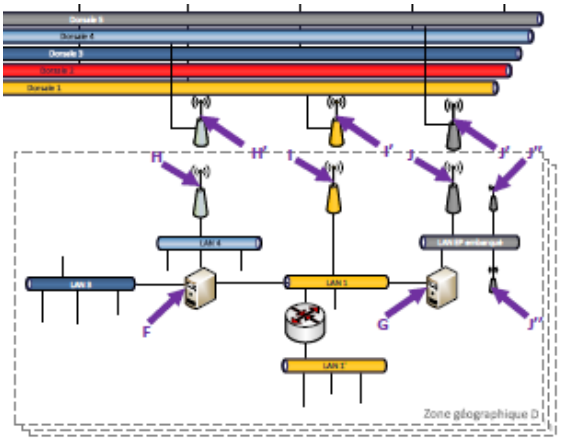


**Figure 6.** Points d'attention de l'architecture (extrait)

Pour les équipements permettant un accès réseau sans fil qui sont intrinsèquement moins sûrs que les équipements réseaux filaires, il faut s'assurer de la bonne prise en compte des mesures de sécurité par les équipements concernés. Pour ce faire, on peut demander à ce que les équipements soient conformes au profil de protection correspondant : borne sans-fil, défini par l'ANSSI (https://www.ssi.gouv.fr/guide/profils-de-protection-pour-les-systemes-industriels/), sur la base minimale d'une CSPN, ou d'une évaluation CC de niveau EAL3. Pour les équipements permettant d'effectuer des jonctions entre plusieurs réseaux de sécurité différente qui seront de ce fait particulièrement ciblés, il est recommandé de faire passer les échanges par une machine située dans la DMZ à la frontière entre ces deux réseaux. Cette approche est à généraliser pour les sous-réseaux utilisant des protocoles purement industriels, lorsqu'il n'est pas possible d'utiliser de simples passerelles protocolaires durcies.

L'étape suivante de l'analyse conduit à définir les mesures de sécurité préconisées pour couvrir les risques relatifs à la cybersécurité. Chaque mesure est caractérisée par :

- Son type (par exemple : Architecture, Authentification, Certification, Cloisonnement, Contrôle d'accès, Contrôle de cohérence, Détection, Durcissement, Sécurisation des protocoles, etc),
- La définition de la mesure,
- Le bien support sur lequel elle s'applique,
- Les critères de sécurité auxquels elle participe (disponibilité, intégrité, confidentialité, preuve),
- La ligne de défense à laquelle elle correspond (Prévention, Protection, Récupération).

Une centaine de mesures est identifiée, parmi lesquelles on distingue :

- les mesures techniques à caractère général couvrant les différentes catégories de mesures du guide de la cybersécurité des systèmes industriels de l'ANSSI, portant notamment sur les sujets suivants (liste non exhaustive) : architecture, authentification, cloisonnement, communication sans fil, contrôle de cohérence, détection, durcissement, sécurisation des protocoles,
- les mesures « métiers », portant sur des sujets analogues mais prenant en compte les spécificités des biens essentiels des systèmes d'information de la ligne 18 et des choix d'architecture faits lors de la conception générale de ces systèmes.

Un extrait de l'inventaire des mesures de sécurité identifiées dans l'analyse est donné à titre illustratif au Tableau 9.

La justification de couverture des différents risques identifiés, à l'aide d'une ou plusieurs mesures, est ensuite établie. Les risques sont alors réévalués en fonction de l'application des mesures, de façon à décider des options de traitement des risques à mettre en place.

| Type | Mesure de sécurité | Bien support sur lequel elle s'applique | Participe à | | | | Ligne de défense | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | Disponibilité | Intégrité | Confidentialité | Preuve | Prévention | Protection | Récupération |
| Fonctionnelle | M1 - Empêcher qu'une commande informatique unique puisse interrompre ou modifier l'extinction incendie ou toute autre opération critique, de telles opérations doivent nécessiter plusieurs échanges. | Réseau A<br>Réseau B<br>Réseau SSI | | X | | | X | | |
| Architecture | M2 - Disposer pour la protection incendie de moyens de contrôle alternatifs utilisant une infrastructure indépendante (cloisonnement physique). | Réseau A<br>Réseau B<br>Réseau SSI | X | | | | | | X |
| Cloisonnement | M3 - Un dispositif de filtrage réseau doit être installé à bord sur l'interconnexion entre le LAN A et le LAN B ou le LAN C afin de permettre de limiter l'exposition des équipements raccordés sur le LAN A, de compartimenter les sous-systèmes et d'isoler les flux au niveau L3/L4 (couches réseau/transport). A ce titre, un mécanisme de filtrage IP/port doit intégrer une fonction de contrôle de l'état de session (ex : stateful packet inspection) visant à maîtriser la provenance (anti-spoofing) et le sens des connexions réseau. | Réseau C<br>Réseau SSI | | X | X | | | X | |

**Tableau 9.** Inventaire des mesures de sécurité (extrait)

## Conclusion

### 1. Enseignements de l'analyse préliminaire des risques cybersécurité de la ligne 18

L'analyse préliminaire des risques relatifs à la cybersécurité menée dans le cadre du projet de la ligne 18 du Grand Paris Express est un premier élément dans la réponse à apporter aux enjeux de la cybersécurité pour les systèmes de transport. Le fait de prendre en compte la sécurité des systèmes d'informations aussi tôt dans la définition du système de transport doit permettre une défense en profondeur en incluant la sécurité dans la conception de chacun des composants. Cette approche permet de minimiser les vulnérabilités potentielles, en augmentant de manière coordonnée et homogène la sécurité de chacune de ces briques pour éviter l'apparition de maillons faibles.

Une des difficultés rencontrées dans ce type d'analyse réalisée en phase de conception générale d'un système de transport est l'étendue du périmètre traité. Tout en s'appuyant sur une démarche d'analyse reconnue et robuste (la méthode EBIOS), il est donc nécessaire de faire des choix du point de vue méthodologique pour optimiser le volume et le temps de réalisation de l'étude. Ce principe nous a conduits à ne pas étudier systématiquement toutes les mesures applicables à un risque donné, mais à nous focaliser sur les mesures qui seront nécessaires au futur exploitant de la ligne 18 dans le cadre de l'homologation de son système d'information. Ainsi, cette analyse préalable devra être complétée en phase d'exécution par une analyse dédiée réalisée par l'opérateur, indispensable à l'homologation des systèmes d'information critiques.

Un des principaux enseignements de cette étude est la nécessité de prendre en compte, lors de la définition des mesures de sécurité, les spécificités des biens essentiels des systèmes d'informations de la ligne 18 et des choix d'architecture faits lors de la conception générale de ces systèmes. Ces mesures « métiers » viennent compléter les mesures techniques à caractère général qui s'appliquent à la cybersécurité des systèmes industriels et qui sont transposées des référentiels de l'ANSSI.

### 2. Axes méthodologiques à développer

Parmi les points méthodologiques à développer dans ce type d'approche, un axe fort est celui de la prise en compte de la sûreté de fonctionnement dans une étude de la cybersécurité d'un système de transport, et réciproquement. Ce sujet a fait l'objet d'une attention particulière au cours de cette étude, notamment lors de l'estimation de la gravité des évènements redoutés et en particulier en termes d'atteinte à la sécurité des personnes et de dommages causés à l'environnement. Cependant, de nombreux développements restent à faire pour dérouler de façon concourante les processus de management et d'analyse propres à la cybersécurité d'une part et à la sûreté de fonctionnement d'autre part, et pour renforcer les « points de connexion » entre ces processus pour les systèmes industriels.

Les analyses de cybersécurité et de sûreté de fonctionnement partagent certaines problématiques communes, notamment celles relatives à la disponibilité et à l'intégrité. Elles s'appuient également sur des méthodes similaires en terme d'analyse des risques, qui se basent sur des éléments tels que la description des missions à remplir par le système étudié, la description des fonctions à mettre en œuvre pour assurer ces missions, la définition d'événements redoutés et des impacts de ces événements. Un des points fondamentaux de ces deux disciplines est de faire reposer les analyses sur une modélisation du système étudié : il nous semble nécessaire que cette modélisation soit commune et transversale aux deux domaines, tout en étant utilisée de manière spécifique à chaque discipline. En effet, à ce jour, il ne nous semble pas pertinent d'avoir une méthodologie unique pour traiter les problématiques de cybersécurité et de sûreté de fonctionnement, mais plutôt de travailler sur les points de convergence de ces deux disciplines dans les différentes phases du cycle de vie d'un projet.

## Références


1 ANSSI/ACE/BAC : Expression des Besoins et Identification des Objectifs de Sécurité EBIOS - Méthode de gestion des risques - Version du 25 janvier 2010

2 NF ISO/CEI 27001 : Technologies de l'information - Techniques de sécurité – Système de gestion de la sécurité de l'information - Décembre 2007

3 NF ISO/CEI 27005 : Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information - 13 Avril 2013

4 ANSSI/CSI/MSSISI/1.0 : Cybersécurité des systèmes industriels, Maîtriser la SSI pour les systèmes industriels - Version 1.0 de juin 2012

5 Loi de Programmation Militaire 2013-1168 CHAPITRE IV

6 Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Transports terrestres » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense

7 IEC 62443 (Série de normes) : Réseaux industriels de communication - Sécurité dans les réseaux et les systèmes ; Sécurité des systèmes d'automatisation et de commande industrielles

8 Cybersécurité des installations industrielles : défendre ses systèmes numériques - sous la D° de Yannick Fourastier (Airbus Group) & Ludovic Pietre-Cambacedes (EDF) – CEPADUES - Référence : 1168 - I.S.B.N. : 9782364931688 - Année de parution : 2015