TRANSPORT FERROVIAIRE INTELLIGENT ET SECURITE NUMERIQUE.

Enjeux et challenges dans l'espace Européen.

MRSIC8

Décembre 2021

EGE Ecole de Guerre Economique

AVANT-PROPOS

Nous tenons à remercier les enseignants de l'EGE et de la MRSIC8 pour les connaissances et expériences partagées. Merci également à nos collègues auditeurs de promotion pour cette belle année passée ensemble.

Nos pensées vont aussi à nos familles qui nous ont soutenu dans ce projet et ont supporté nos absences pendant cette année assez dense en travaux de production de connaissance et plus particulièrement lors des longues périodes de rédaction de ce mémoire.

Un grand merci à tous les experts et dirigeants qui nous ont accordé de leur temps et surtout de leur expertise terrain :

***Laurent Cébulski**, Directeur Général de l'EPSF - **Sadio Bâ** Coordinateur Sectoriel Transport de l'ANSSI - **Amal El Fallah Seghrouchni**, Professeur Émérite d'Intelligence Artificielle à Sorbonne Université et membre de la Commission mondiale sur l'Ethique des connaissances Scientifiques et des Technologie (COMEST) de l'UNESCO.– **Sophie Bouilland**, Global Chief Information Security Officer chez Transdev Group - **Antoine Ancel**, Directeur Cybersécurité du Groupe SNCF, **Eddy Thésée**, Vice-Président Cybersécurité chez Alstom - **Yseult Garnier** et **Quentin Rivette**, respectivement Responsable Cybersécurité Industrielle chez SNCF RESEAU et SNCF Voyageurs - **Jean-Baptiste Renault,** Responsable Cybersécurité Alstom France portfolio produits et Services - **Mihai Chirca**, Responsable Affaires Européennes chez Transdev Group - **Joel Noirot**, ancien RSSI SNCF et Responsable Sécurité Systèmes Informations des Infrastructures Techniques du Groupe SNCF, **Thomas Chatelet**, Chef de projet ERTMS à l'ERA (Agence Ferroviaire Européenne).*

*Les remarques ont été précieuses et nous ont permis de clarifier ou préciser certains propos**.***

Ce fût un privilège et immense plaisir d'échanger avec eux. Nous invitons d'ailleurs le lecteur à avoir une attention particulière sur les extraits des différents échanges / interviews que nous avons eus avec eux et qui apportent des éclairages et enseignement hautement précieux.

La thématique du Transport et particulièrement du ferroviaire fait partie des enjeux majeurs au sein de l'Union Européenne et dans le monde de manière générale. Nos capacités de mobilités, l'économie et la souveraineté des Nations en sont fortement dépendantes.

Appréhender l'environnement de ce vaste écosystème complexe, les articulations avec l'Europe et les grands challenges pour le ferroviaire du futur a motivé notre vif intérêt pour ce sujet.

Nous avons pris le parti de faire un focus sur les risques de cybersécurité pouvant avoir des impacts considérables sur les biens et les personnes.

Bonne lecture.

François Nguilla Kooh et Stéphane Doyen

François NGUILLA KOOH Dr. / PhD.

Chef de Division Sécurité Opérationnelle 1&2.
Direction Cybersécurité
e.SNCF - Groupe SNCF

Stéphane DOYEN

Cyber Risk Manager France

Direction Digitale France

TRANSDEV

Table des matières

Table des figures

Acronyme	Description
API	Application Programming Interface
APR	Analyse Préliminaire des Risques
AR	Appréciation des risques
BAL	Block automatique lumineux
BAPR	Block automatique à permissivité restreinte
CAPI	Cantonnement assisté par informatique
CCR	Centre de Contrôle et Commande
CERT	Computer Emergency Response Team
CMDB	Configuration Management Database
COTS	Composants sur étagères (Components Off The Shelf)
CSIRT	Cyber Security Incident Response Team si
CTI	Cyber Threat Intelligence
DMZ	Demilitarized Zone
EBIOS	Expression des Besoins et identification des objectifs de sécurité
ENISA	European Network and Information Security Agency
EPSF	Établissement public de sécurité ferroviaire
ERTMS	European Rail Traffic Management System
ETCS	European train control system (système européen de contrôle commande des trains)
EVC	European vital computer. (Ordinateur européen de sécurité) : calculateur de bord qui supervise la marche du train en fonction des données sol et bord
FMDS	Fiabilité, Maintenabilité, Disponibilité, Sécurité
FRMCS	Futur Railway Mobile Communication System
GAME	Globalement au moins équivalent (se dit du niveau de sécurité d'un nouveau système par comparaison avec celui d'un système déjà en exploitation)
GDPR	General Data Protection Regulation
GSM-R	Global system for mobile communication railways (Système de communication téléphonique pour mobile dédié aux chemins de fer)
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
IAAS	Infrastructure As A Service
ICS	Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IMS	Incident Management System
IOC	Indicator Of Compromise

Acronyme	Description
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAS	Maintenance Aid System
MILS	Multiple Independent Layers of Security
NAC	Network Access Control
NIDES	Système expert de détection d'intrusion de nouvelle génération
NIDS	Network-based Intrusion Detection System
NIS	Network and Information Security
OIV	Opérateurs d'Importance Vitale
OSE	Opérateurs de Services Essentiels
OSINT	Open-Source Intelligence
OT	Operational Technology / Technologie d'Exploitation
PAAS	Platform As A Service
PASSI	Prestataires d'Audit de la Sécurité des Systèmes d'Information
PDIS	Prestataires de Detection d'Incidents de Sécurité
PIV	Point d'Importance Vital
PLC	Programmable Logic Controler / Contrôleur logique programmable
PRIS	Prestataires de Réponses à Incidents de Sécurité
SAAS	Software As A Service
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SAIV	Sécurité des Activités d'Importance Vitale
SIIV	Système d'Information d'Importance Vitale
SIRP	Security Incident Response Platform / Plateforme de réponses aux incidents de sécurité
SL	Security Level
SOC	Security Operations Center
SSO	Single Sign On
STRMTG	Service technique des remontées mécaniques et des transports guidés
TAP	Test Access Point, système de détection réseau
VLAN	Virtual Local Area Network

EXEC SUMMARY

La préoccupation de la filière ferroviaire est de garantir le transport en toute sécurité. Les nouvelles mobilités, les nouveaux usages, l'ouverture de la circulation au sein de l'Union Européenne avec l'adoption de l'ERTMS (European Railway Trafic Management System) comme standard de gestion du trafic ferroviaire mondial rendent incontournables les nécessités de prise en compte de la cybersécurité pour garantir la sécurité des biens et de personnes, mais aussi pour servir de leviers de performance économique et de croissance des entreprises du secteur.

Dans le transport ferroviaire, et plus particulièrement dans le cas d'OIV (Opérateur d'Importance Vitale) ou d'OSE (Opérateur de Services Essentiels), le risque n'est pas limité aux vols de données, à l'indisponibilité des services ou à des questions de réputation, mais inclut la sécurité des vies humaines et d'infrastructures critiques indispensables à la bonne marche ainsi qu'à la souveraineté d'un pays.

La filière est plus que jamais entraînée dans une transformation digitale avec des bénéfices attendus sur trois axes :

- Efficience opérationnelle : qualité des services, meilleure ponctualité, dématérialisation des billets ;
- Sécurité des passagers à bord des trains, dans les gares, le long des rails, aux passages à niveau : caméras de surveillance connectées, annonces sonores automatiques ;
- Expérience passager améliorée, confort du voyage, utilisation d'applications mobiles, etc.

Opérationnellement, cela se traduit par une nécessité de collecte et de traitement en temps réel des informations sur la circulation ferroviaire et une collecte d'informations relatives à une connaissance des assets (à des fins d'amélioration de l'expérience client et à des fins de maintenance prédictive). Ces besoins nouveaux accélèrent la transformation digitale et par voie de conséquence l'augmentation de produits et services IT au sein des écosystèmes industriels d'une part et induisent une interconnexion entre briques IT et parfois des interconnexions via Internet. Même si la data est devenue de l'or, la connectivité constitue incontestablement le pouvoir. L'Or et le pouvoir attisent les convoitises et peuvent exposer les cœurs des systèmes critiques OT.

Selon Eddy Thésée, Vice-Président Cybersécurité chez Alstom, la digitalisation apporte des opportunités fantastiques en matière de création de valeur en rendant l'ensemble des transports ferroviaires et ses réseaux « intelligents », tant dans le développement que dans les besoins opérationnels et les exigences de maintenance. Mais ceci est néanmoins accompagné de fragilités, si la sécurité globale des systèmes numériques utilisés n'est pas prise au sérieux à l'instar de la culture de sûreté et de sécurité qui est une spécificité historique du monde ferroviaire[1].

Les innombrables apports de la digitalisation ont pour corollaire une augmentation de l'exposition des surfaces potentielles d'attaque, ce qui peut être perçu comme un revers. La sécurité des réseaux SI opérationnels du ferroviaire, basée sur le fait qu'ils étaient jusqu'à récemment encore cloisonnés grâce à des protocoles très souvent propriétaires, est aujourd'hui et plus que jamais remise en question. Bien que les attaques soient

[1] Alstom - *Cybersécurité - Pour une mobilité sûre et sécurisée*. [Livre Blanc En ligne]. [Réf. du 09 sept.2020]. Disponible https://www.alstom.com/sites/alstom.com/files/2020/09/15/Whitepaper Cybersecurity.pdf

heureusement rares, la surface d'exposition s'accroît de façon exponentielle. Ceci est dû à l'avènement de nouveaux usages et services aux passagers, à l'interconnexion croissante entre les systèmes IT traditionnels et les systèmes de production ferroviaire, ainsi qu'aux opportunités qu'offrent l'IoT, le Wifi, la 5G, le cloud. Les cybermenaces protéiformes progressent. D'autre part, les outils comme les groupes d'attaquants continuent de devenir plus puissants. De même, les cyberattaques d'origine étatique, marginales aujourd'hui sur le secteur des transports, seront les grandes menaces de demain de par leur efficacité coercitive en cas de contexte géopolitique tendu. Tout programme de sécurité qui ne tient pas compte de ces réalités est voué à l'échec.

Depuis plusieurs années déjà, la frontière entre IT et OT dans l'industrie s'est réduite progressivement et inéluctablement[2]. Alors que les écosystèmes informatiques ont des durées d'amortissements plus courtes autour de 3 à 5 ans, le monde industriel a quant à lui ses rythmes d'évolution sur 30 à 40 ans, voir 50 ans pour ses produits et matériels dédiés. Pouvoir concilier ces deux mondes lors des mises à jour d'assets ferroviaires embarquant de l'IT, ou patcher certaines vulnérabilités tout en garantissant le respect du principe de sécurité GAME (Globalement Au Moins Equivalent) qui prévaut dans l'OT, est une des problématiques majeures de la convergence IT-OT. La lourdeur de la démarche GAME peut-elle alors induire un risque cyber ?

Les écosystèmes industriels ferroviaires dits OT ont depuis quelque temps embarqué un certain nombre de composantes IT aussi bien à bord (informatique embarquée) que dans les systèmes de contrôle SCADA. Mais ces systèmes étaient fondamentalement isolés des systèmes d'information d'entreprise pour des raisons de conception et d'usage. Aujourd'hui, on parle de plus en plus de convergence ITOT pour signifier la tendance imposée par les besoins de faire dialoguer les systèmes bureautiques avec les SI industriels.

Pour Gartner, société de recherche et de conseil en technologie basée à Stamford, Connecticut, la sécurité OT se définit comme « *l'ensemble des pratiques et technologies utilisées pour (a) Protéger les personnes, les ressources et l'information, (b) surveiller et/ou contrôler les dispositifs, les processus et événements, et (c) initier des changements au sein des systèmes OT d'entreprise*. »[3]

Cette définition de Gartner semble assez restrictive. La cybersécurité est en effet trop souvent considérée comme un problème purement informatique, alors qu'elle devrait être un élément central de la stratégie d'entreprise. Trois aspects clés sont à prendre en compte dans la réflexion globale : les systèmes de commandement et de contrôle, qui se rapportent à la sécurité et à la signalisation ; le trafic et l'exploitation ferroviaires, qui mettent l'accent sur le maintien des trains dans les délais prévus ; et l'aspect bureautique de l'entreprise, qui se rapporte à l'interaction du système avec les clients[4].

Pour Antoine Ancel, Directeur Cybersécurité du groupe SNCF, on doit avoir une vision globale de la cybersécurité, d'autant plus qu'aujourd'hui le risque cyber se trouve, a minima dans les grands Groupes, classés dans le top des risques d'entreprise. Bien que la prise de conscience de son importance sur la pérennité des activités de beaucoup d'entreprises ait été tardive, la maîtrise du risque cyber et plus que jamais le renforcement de la posture en cybersécurité, doivent en conséquence être considérés comme de puissants leviers de

---

[2] Khobeib Ben Boubaker, *Réseaux IT-OT : les raisons d'une convergence délicate* [en ligne]. [Réf. du 18 nov. 2019]. Disponible sur https://www.stormshield.com/fr/actus/reseaux-it-ot-raisons-convergence-delicate/

[3] Earl Perkins, *Operational Technology Security – Focus on Securing Industrial Control and Automation Systems*. [En ligne]. [Réf. du 14 mars 2014]. Disponible sur https://blogs.gartner.com/earl-perkins/2014/03/14/operational-technology-security-focus-on-securing-industrial-control-and-automation-systems/

[4] Alstom - *Cybersécurité - Pour une mobilité sûre et sécurisée*. [Rapport en ligne]. [Réf. du 09 sept.2020]. Disponible https://www.alstom.com/sites/alstom.com/files/2020/09/15/Whitepaper Cybersecurity.pdf

croissance et d'opportunités. Selon lui, c'est un véritable levier de transformation des usages dans de bonnes conditions et une responsabilisation des acteurs, métiers IT et tout particulièrement utilisateurs[5].

Aujourd'hui les grandes ruptures se font grâce à l'apport de l'intelligence artificielle incontournable dans les mobilités de demain qui se veulent par ailleurs durables. La libre circulation au sein de l'Union Européenne avec les questions transfrontalières associées aux problématiques d'interopérabilité entre les différents réseaux ferroviaires nationaux sont autant de préoccupations qui viennent se rajouter à celles citées précédemment. Les questions relatives à la consommation énergétique, à l'intermodalité et la multimodalité[6], sujets majeurs des mobilités européennes et du ferroviaire de demain comme le rappelle Josef Doppelbauer, Directeur Général de l'ERA lors de la dernière table ronde[7] organisée par l'IMTD (Institut des Mobilités et des Transports Durables) en novembre 2021, viennent rallonger la liste des enjeux nécessitant indubitablement des ruptures organisationnelles et technologiques.

La question qui revient sans cesse est de savoir si l'Europe a pris la mesure des enjeux et est en ordre de marche pour garantir un transport ferroviaire de confiance et un modèle pour le monde ? Un vaste sujet, qui mérite que l'on s'y attarde un peu, car se posent des problématiques qui ne sont pas qu'au niveau technique, mais aussi au niveau gouvernance, normatif, juridique, réglementaire, sociétal et environnemental. Chacun de ses volets est une thématique majeure interdépendante des autres et qui nécessite une vision, une stratégie claire et des moyens financiers et humains en adéquation.

Les transports ferroviaires de demain seront dits « intelligents » grâce à l'intelligence qui sera conceptualisée et mise en œuvre dans :

- L'apport de nouveaux services d'agrément et faisant gagner du temps aux usagers, dans l'augmentation de l'offre de transport ainsi que la fluidification du trafic ;
- Les transformations digitales avec les technologies disruptives pour la plupart à base d'intelligence artificielle ;
- Les nouveaux modes de gouvernance transverse entre les directions IT et directions industrielles, en l'occurrence dans la perspective d'une convergence IT OT réussie pour une meilleure performance opérationnelle et économique ;
- Le processus et la mécanique de continuité numérique qui s'accompagne d'une maîtrise de la chaîne de valorisation des données métier. C'est un levier majeur de prise de décision pour réussir la transformation digitale, maîtriser les cycles de vie de produits, services et systèmes : un facteur clé pour réduire le time-to-market ;
- Le développement de la culture et l'approche d'analyse de risques, l'adoption du principe de proportionnalité dans le traitement de ces risques ;
- Les capacités de résilience ; on peut citer l'aptitude à pouvoir gérer les crises majeures auxquelles ils pourraient faire face demain ;
- La vision qu'aura l'Europe et les moyens mis en œuvre pour l'acculturation de l'industrie ferroviaire aux risques cyber systémiques et en pleine évolution ;
- Les politiques d'intégration territoriale et transnationale au sein de l'Union européenne ;
- La capacité de l'Europe à gérer les questions non seulement relatives à l'interopérabilité, à l'ouverture à la concurrence, mais aussi des problématiques,

[5] Annexes I - Interviews – Antoine Ancel, Directeur Cybersécurité du Groupe SNCF

[6] Rapporteurs Denis BAUPIN, député, et Fabienne KELLER, sénatrice. *La multimodalité et l'intermodalité. Nouvelles mobilités et véhicules écologiques* [en ligne]. [Réf. du 14 Janvier 2020]. Disponible sur http://blogs.senat.fr/nouvelles_mobilites/files/rapport1713-tome-III.pdf

[7] Dominique Riquet Député européen, Josef Doppelbauer, Directeur ERA, Nathalie Darmendrail de SNCF Didier Fernandes d'Alstom *Table ronde de l'IMTD (Institut des Mobilités et des Transports Durables). Le ferroviaire au cœur des grands enjeux des transports*. [En ligne]. [Réf. du 18 Févr. 2021]. Disponible sur En https://www.youtube.com/watch?v=kezTSFXzxSA

juridiques, réglementaires, législatives, de responsabilité sociétale et environnementale ;

- Le développement durable d'une manière générale avec un objectif ambitieux de réduction de l'empreinte écologique ;
- Le jeu d'influence aussi bien sur les normes que sur la dimension géopolitique mondiale ;
- La place donnée au ferroviaire comme un enjeu de souveraineté européenne aussi bien sécuritaire, économique et technologique.

Les enjeux et thématiques sont innombrables. Chacune de ces thématiques est déjà en soi un challenge auquel s'attèlent aussi plusieurs organisations internationales et nationales telles que l'ENISA, l'ERA, l'UNIFE au niveau européen, l'ANSSI, l'EPSF en France par exemple. Le présent document a pour ambition de capitaliser sur les différentes productions et de proposer une démarche pragmatique qui promeut une vision à 360° des enjeux de la sécurité numérique du ferroviaire tant au niveau du métier du ferroviaire que sur des aspects géostratégiques.

[8]

[8] Aménagement des espaces publics du nouveau pôle de transport multimodal de Morlaix (Bretagne) https://www.vinci.com/vinci.nsf/en/news-update/pages/new_multimodal_transport_hub_in_morlaix_france_112017.htm

Le document est organisé en deux parties :

Partie I : ENJEUX DU FERROVIARE A L'ÉCHELLE EUROPÉENNE : VISION INSTITUTIONNELLE, NORMATIVE, STRATÉGIQUE, GOUVERNANCE ET QUESTIONS DE SOUVERAINNETE

Nous présentons ici les parties prenantes de la filière : gestionnaires d'infrastructure, entreprises ferroviaires, acteurs de la chaîne d'approvisionnement, acteurs de la sécurité et de la maintenance ferroviaire et autres acteurs des sphères institutionnelles, étatiques, etc.

Il sera question d'exposer les enjeux en termes de gouvernance et d'établissement des normes sur lesquelles s'adosse la filière. Nous nous intéresserons en particulier aux grands programmes et projets européens en matière de transformation digitale et de Cybersécurité ferroviaire ainsi que du sujet de la place de l'Europe ferroviaire dans le monde et à sa démarche stratégique au regard de l'influence du ferroviaire dans les mobilités durables sur tous les continents. Nous ferons notamment un focus sur l'avancée concurrente croissante de la Chine dans le marché du ferroviaire mondial et européen en particulier.

Nous aborderons également les nombreux challenges du secteur ferroviaire qui animent actuellement les débats et différents échanges au sein de l'Europe et plus largement dans le monde.

Partie II : LE FERROVIAIRE : SYSTÈME INDUSTRIEL, TRANSFORMATION DIGITALE ET SÉCURISATION NUMÉRIQUE

Nous allons nous immerger dans l'industrie ferroviaire pour mieux cerner cet écosystème.

Nous essaierons d'appréhender la complexité de son organisation, de ses activités et des enjeux liés à la convergence entre les systèmes d'information dits d'entreprise (IT) et les systèmes d'information industriels (OT).

Le secteur vit un bouleversement sans pareil. On parle d'industrie du ferroviaire 4.0. Les arrivées du wifi, de la 5G, bientôt la 6G, de l'ERTMS, de l'Intelligence Artificielle, du Cloud, etc. augurent des lendemains qui façonneront le nouveau chemin de fer. Nous présenterons dans cette partie les apports certes hautement bénéfiques de ces technologies, mais aussi les menaces qu'elles embarquent et auxquelles il faudra faire face.

La question de la sécurité des personnes et des biens est une préoccupation principale au cœur de l'exigence de pilotage par les risques de l'industrie ferroviaire. C'est bien cette approche par les risques et surtout les impacts sur la sécurité qui servira de fil conducteur à notre réflexion sur toute la démarche de cyber-sécurisation des activités de la filière abordée dans les différents chapitres.

La lecture des interviews des spécialistes en annexe est vivement conseillée.

« Quand on s'attaque au monde du transport, on peut vite avoir des effets absolument dramatiques, y compris sur les vies humaines » Guillaume Poupard, Directeur général de l'ANSSI à l'occasion du Forum International de la Cybersécurité (FIC), à Lille en 2017

PARTIE I – LE FERROVIARE EN EUROPE : INSTITUTIONS, GOUVERNANCE, NORMES, ENJEUX ÉCONOMIQUES ET DE SOUVERAINETÉ

I. INTRODUCTION

Depuis plus de 30 ans, l'Union européenne a inscrit la politique des transports dans ces domaines d'action. La libre circulation de personnes et de biens grandissante, combinée à la hausse des émissions de gaz à effet de serre, devrait encore faire gagner » en importance[9] la « mobilité durable.

La Commission Européenne a fixé dans le livre blanc de 2011 de l'U.E intitulé « *Feuille de route pour un espace européen unique des transports — Vers un système de transport compétitif et économe en ressources* »[10], un objectif pour que la majeure partie du transport de passagers à moyenne distance se fasse par le train d'ici 2050. Déjà d'ici 2030, le réseau à grande vitesse devrait être triplé et en cible, un véritable réseau ferroviaire à grande vitesse pleinement européen de bout en bout. [11]

La création d'un espace ferroviaire unique et l'ouverture du secteur des transports ferroviaires à la concurrence, commencée en 2001, a donné lieu à quatre paquets ferroviaires dont le dernier adopté en 2016 rajoutait un volet technique et un volet relatif au « marché ».

Aussi, pour atteindre l'objectif d'ouverture du marché à la concurrence, éviter les distorsions à la concurrence et faciliter l'accès de nouvelles entreprises, l'UE a lancé un certain nombre d'initiatives pour une harmonisation des règles sur le plan organisationnel, administratif, réglementaire, technique, etc. indispensables à l'interopérabilité des différents systèmes ferroviaires nationaux.

Concernant le volet sécurité numérique, la directive NIS (Network and Information Security) a été adoptée le 6 juillet 2016 après trois années de négociations. Portée par la France et l'Allemagne, cette directive est le premier document législatif intégrant une approche européenne commune en matière de cybersécurité. Elle étend le champ d'application au secteur ferroviaire et a pour objectifs de renforcer le niveau de sécurité des réseaux et des systèmes d'information essentiels et d'améliorer le partage d'informations au niveau européen. Le 16 décembre 2020, la Commission Européenne a présenté sa stratégie en matière de cybersécurité pour la décennie, laquelle a pour ambition de « façonner l'avenir numérique de l'Europe »[12]. La directive NIS2 qui en découle (en cours d'approbation), étend la directive NIS L'objectif est de garantir non seulement un niveau commun en matière de cybersécurité sur le plan de la gouvernance, la protection, la défense, la résilience, mais intègre l'exigence de cybersécurité des chaînes d'approvisionnement. Un autre point important est la prise en compte de l'interdépendance croissante entre sécurité intérieure et sécurité extérieure.

Nous parlerons dans cette partie, des grands acteurs du ferroviaire en Europe, notamment institutionnelles, et ceux qui interviennent sur les aspects normatifs et de gouvernance globale. Les problématiques liées aux questions juridiques, environnementales et sociétales seront abordées. De même, nous nous intéresserons aux questions économiques et géopolitiques du ferroviaire Européen dans le monde et en particulier de la pénétration du ferroviaire Chinois dans l'espace européen.

---

[9] *La politique commune des transports* [En ligne]. [Réf. De mars 2022]. Disponible sur La politique commune des transports: généralités | Fiches thématiques sur l'Union européenne | Parlement européen (europa.eu)

[10] *Feuille de route pour un espace européen unique des transports – Vers un système de transport compétitif et économe en ressources* [En ligne]. [Réf. 28 mars 2011]. Disponible sur Feuille de route pour un espace européen unique des transports

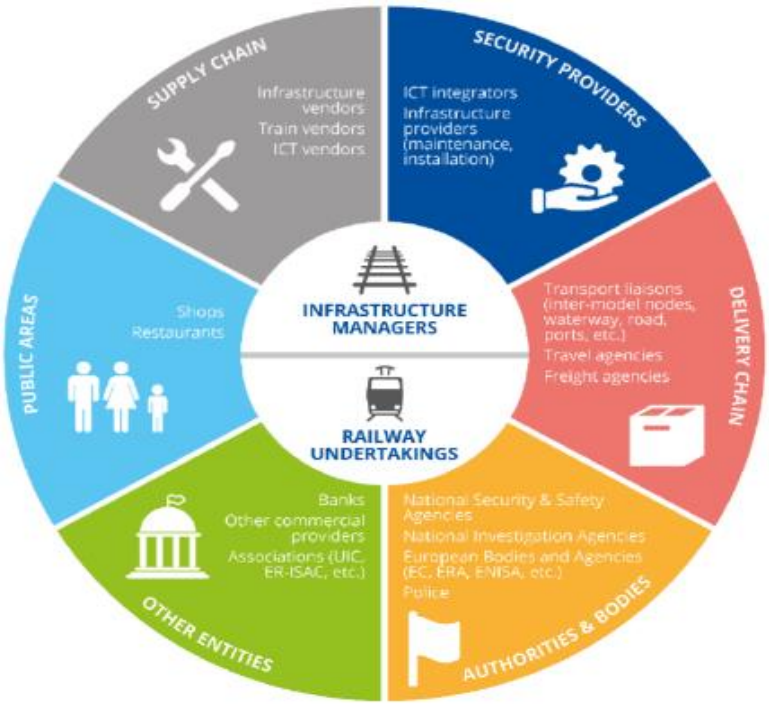
[11] *Transport Ferroviaire* [En ligne]. [Réf. De décembre 2016]. Disponible sur Transport ferroviaire (europa.eu)

[12] *Directive NIS : Quels enjeux juridiques - Orange Cyberdefense* [En ligne]. [Réf. Du 7 mars 2019]. Disponible sur Directive NIS

II. PANORAMA DES ACTEURS DU SECTEUR

Le secteur ferroviaire agrège un nombre impressionnant de métiers. On y trouve les opérateurs de transport, les gestionnaires d'infrastructure et les différentes entreprises du ferroviaire comme les industriels fournisseurs des systèmes ferroviaires.

Pour y voir clair, la directive 2012/34/UE de l'Union européenne, classe les acteurs principaux du secteur ferroviaire dans différentes grandes familles. On y retrouve comme le montre le schéma de l'ENISA[13] au centre de l'activité, les gestionnaires d'infrastructures (GI) et les entreprises ferroviaires (EF). Autour gravitent des parties prenantes aussi importantes les unes que les autres ; on peut citer les entreprises de la chaîne d'approvisionnement, celles assurant la sécurité et la maintenance, deux maillons forts du dispositif de production ferroviaire. On y retrouve aussi les autorités de régulation et organismes institutionnels divers, des acteurs étatiques, des services assurant des tâches régaliennes de sécurité ou de justice, et autres organismes financiers et bancaires pour ne citer que ceux-là avec lesquels interagissent le GI et les EF.



1 - Parties prenantes du secteur ferroviaire

Les gestionnaires d'infrastructure : regroupe des personnes ou entreprises chargées d'établir, de gérer et d'entretenir l'infrastructure ferroviaire, y compris la gestion du trafic, le contrôle-commande et la signalisation. En France SNCF RÉSEAU, Société Anonyme (SA) du groupe SNCF est le gestionnaire principal d'infrastructure du réseau ferré national. Il a pour missions essentielles de repartir les capacités disponibles de l'infrastructure, dont l'utilisation donne lieu à la perception de redevances qu'il détermine. SNCF RÉSEAU assure également l'entretien de l'infrastructure ferroviaire composée de 30 000 kms de lignes en service, le réseau ferroviaire national français compte également d'autres gestionnaires d'infrastructure. On en décompte une vingtaine environ ; on pourrait citer LISEA, gestionnaire de la ligne à grande vitesse Tours-Bordeaux, Getlink anciennement

[13] *Security measures in the Railway Transport Sector* [En ligne]. [Réf. De novembre 2020]. Disponible sur https://www.enisa.europa.eu/publications/railway-cybersecurity/at_download/fullReport

Eurotunnel, concessionnaire jusqu'en 2086, et gestionnaire d'infrastructure de la liaison fixe du tunnel sous la Manche[14], la Régie Autonome des Transports Parisiens (RATP), Chemins de fer de la Corse, Voie ferrée portuaire. On retrouve aussi dans ce bloc, les acteurs qui œuvrent au niveau des infrastructures ferroviaires, comme Egis Rail, Colas Rail ou NGE. Les autres gestionnaires d'infrastructure en Europe sont la DB Netz, filiale de la Deutsche Bahn pour l'Allemagne, Infrabel en Belgique, la Société nationale des chemins de fer luxembourgeois (CFL), AAIF - Adif Administrador de infraestructuras ferroviarias en Espagne, RFI - Rete ferroviaria italiana en Italie, RFN - Rede ferroviaria nacional au Portugal.

Les entreprises ferroviaires : on retrouve ici des entreprises publiques ou privées agréées conformément à la directive, dont l'activité principale est de fournir des services de transport de marchandises et/ou de voyageurs par chemin de fer avec l'obligation pour l'entreprise d'assurer la traction. Cela inclut également les entreprises qui n'assurent que la traction ». On peut citer : en France, la SNCF et Transdev Rail anciennement la Société Générale de Chemins de fer et de Transports Automobiles (CFTA), Deutsche Bahn (Allemagne) ; Renfe (Espagne) ; ÖBB (Autriche), DSB (Danemark) ; SNCB (Belgique), NS (Pays-Bas), CD (République tchèque).

Les exploitants ferroviaires : ce sont les gestionnaires d'infrastructures et les entreprises ferroviaires en charge de la mise en œuvre de leurs équipements, la formation de leurs personnels, la définition des consignes et instructions opérationnelles dans le respect de la réglementation[15].

La chaîne d'approvisionnement : les acteurs de la chaîne d'approvisionnement fournissent des actifs ferroviaires et IT/OT aux EF et aux GI. Ils peuvent être des vendeurs de trains, de systèmes ICS, de systèmes informatiques, etc. Le secteur ferroviaire est dépendant de ces fournisseurs et leur collaboration est vitale pour assurer la cybersécurité dans le secteur ferroviaire. On retrouve dans cette catégorie, les constructeurs et fournisseurs des infrastructures et matériels roulants (Alstom Transport, Bombardier Siemens, Hitachi), ainsi que les mainteneurs RAMFER, ETF, AZURAIL, SFERIS, ETF, etc.

- Les compagnies ferroviaires et opérateurs qui transportent des passagers ou du fret (tels que la RATP, la SNCF, mais aussi les sociétés étrangères comme la Deutsche Bahn) ;
- Les constructeurs et équipementiers en charge du développement et de la conception du matériel roulant exploité par les opérateurs tels que Alstom Transport, Siemens, Bombardier, Hitachi…

Les prestataires de services : ce sont les tiers engagés par des EF ou des GI pour effectuer tout ou partie d'un service, qui peut être un service commercial (par exemple, une entité en charge de la maintenance des trains) ou un service IT/OT (par exemple, la surveillance informatique). Les prestataires de services comprennent les conseillers, les entreprises de travaux, les consultants en gestion de projet, les fournisseurs de systèmes, les intégrateurs.

La Chaine de livraison : elle comprend toutes les parties prenantes impliquées dans la fourniture du service de transport aux clients, pour le fret (par exemple, les agences de fret, les entreprises de logistique) ou les passagers (par exemple, les agences de voyages, les courtiers touristiques). Il couvre également les tiers qui interagissent avec le chemin de fer pour la prestation de services (par exemple, les entreprises de transport routier).

---

[14] *Les opérateurs ferroviaires de transport de voyageurs et de fret, Les gestionnaires d'infrastructures* [En ligne]. [Réf. De septembre 2019]. Disponible sur Acteurs | UTP - Union des Transports Publics et Ferroviaires

[15] *POSITIONNEMENT DE L'EPSF PARMI LES ACTEURS DU SYSTÈME FERROVIAIRE FRANÇAIS* [En ligne]. Disponible sur Positionnement de l'EPSF parmi les acteurs du système ferroviaire | EPSF (securite-ferroviaire.fr)

Les Autorités et organismes : ce sont toutes les parties prenantes chargées d'appliquer les politiques et réglementations dans le secteur ferroviaire (par exemple, les régulateurs ferroviaires (cas de l'EPSF[16] en France), les autorités nationales et européennes pour la sécurité ou la cybersécurité (l'ANSSI[17] en France), les organismes d'évaluation de la conformité, en tant qu'organisme notifié et organisme désigné. La majorité des opérateurs de services essentiels (OSE) collaborent sur les questions de cybersécurité avec des organismes nationaux, par exemple les agences gouvernementales, de sécurité ou de cybersécurité, les ministères des Transports ou des Infrastructures, les équipes nationales d'intervention en cas d'incident de sécurité informatique (CSIRT) ou les équipes d'intervention d'urgence informatique (CERT), les autorités responsables de la gestion des crises ou des urgences, de la gestion des catastrophes, de la sécurité nationale, de la lutte contre le terrorisme ou de la protection des données. Au niveau européen les organismes phares traitant de ces problématiques sont : L'ENISA[18] : l'ERA23, la DG CONNECT24, la DG MOVE25, le CENELEC26 et l'European Rail ISAC27.

Le secteur public : ici sont regroupés les tiers qui utilisent les locaux ferroviaires pour livrer des biens ou des services (plus précisément dans les gares). Il s'agit notamment des prestataires de services aux passagers (par exemple, des espaces de repos, des salons), ainsi que des restaurants ou des points de vente dans les gares.

Les autres entités : on y retrouve les autres entités (ex : banques, assurances fret) qui entretiennent des relations avec les acteurs ferroviaires. Il s'agit d'associations, groupes de travail (tel que l'UIC[19], le CER[20], ERFA[21], RailNetEurope[22], COLPOFER[23], autour de certains thèmes du secteur ferroviaire.

De ces grandes familles découlent un nombre impressionnant de parties prenantes ainsi que de métiers autour de ce secteur. Mais tout ceci requiert un minimum de gouvernance et de régulation au travers, organisations, institutions et autres organismes ou agences sur le plan national, mais surtout européen.

III. INSTITUTIONS

III.1. L'UIC – UNION INTERNATIONALE DES CHEMINS DE FER

L'Union Internationale des Chemins de fer créée en 1922 à Paris regroupe 46 compagnies ferroviaires, dont 27 pays avec quasiment tous les pays de l'Union européenne (excepté la Finlande). Cette organisation, avec des membres en majorité européens, a pour objectif de répondre efficacement aux défis actuels et futurs liés à la mobilité et au développement durable. Les capacités de recherche et d'innovation de l'UIC sont mobilisées pour accompagner le rail mondial pour le positionner comme « dorsale » durable d'un système de transport compétitif, efficace en ressources et intelligent. Et cela vaut d'autant plus pour

[16] *Etablissement Public de Sécurité Ferroviaire* [En ligne]. Disponible sur EPSF
[17] *Agence Nationale de la Sécurité des Systèmes d'Information* [En ligne]. Disponible sur ANSSI
[18] *ENISA –Sécuriser la société de l'information en Europe* [En ligne]. Disponible sur ENISA - En français — ENISA (europa.eu)
[19] *UIC, l'association professionnelle mondiale représentant le secteur ferroviaire et promouvant le transport ferroviaire* [En ligne]. Disponible sur Home | UIC - International union of railways
[20] *Le rôle du CER est de représenter les intérêts de ses membres sur la scène politique de l'UE.* [En ligne]. Disponible sur CER:Home | The Voice of European Railways
[21] *ERFA today represents 30 members, who operate across the European network* [En ligne]. Disponible sur ERFA - European Rail Freight Association - ERFA - European Rail Freight Association (erfarail.eu)
[22] *RNE compte 38 membres titulaires issus de plus de 30 pays différents et 11 membres associés* [En ligne]. Disponible sur Home - Railnet Europe, Rail Net Europe (rne.eu)
[23] *La mission de COLPOFER est d'améliorer la protection des personnes, des locaux, des trains et des informations au sein du système ferroviaire grâce à une coopération étroite entre les forces de police ferroviaire et les organisations de sécurité des entreprises ferroviaires.* [En ligne]. Disponible sur COLPOFER

le rail européen. Pour l'UIC, le rail qui représente 45% des transports publics, est un atout de grande valeur pour l'Europe[24].

Le secteur ferroviaire a une collaboration de longue date avec tous les autres secteurs pour gérer la cybersécurité. Les cyberattaques sont reconnues à un stade précoce et traitées dans le cadre d'un effort intersectoriel commun. Une industrie ferroviaire digitalisée disposant de solutions de cybersécurité avancées pour assurer entièrement sa protection et une infrastructure TIC robuste et résiliente, associées à de solides processus de continuité des activités, garantissant la haute disponibilité du système et des services ferroviaires : telle est la vision de l'UIC à horizon 2050[25] avec une déclinaison plus pragmatique de l'ERRAC à un horizon plus proche 2030[26] .

III.2. L'ERA – EUROPEAN UNION AGENCY FOR RAILWAYS

L'Agence de l'Union européenne pour les Chemins de fer (ERA) établis en France, contribue à l'intégration des réseaux ferroviaires européens en renforçant la sécurité des trains et en leur permettant de traverser les frontières au sein de l'UE comme s'ils circulaient dans leur pays d'origine. L'ERA fait intervenir les autorités nationales, les institutions européennes et d'autres organismes, à l'élaboration de normes techniques, de mesures et d'objectifs de sécurité communs et économiquement viables[27]. L'Agence est très orientée sûreté de fonctionnement, systèmes de commande et de contrôle. Elle s'occupe aussi des questions relatives à la signalisation et les problématiques autour de la digitalisation. L'ERA collabore étroitement avec l'ENISA sur les travaux relatifs à la cybersécurité ferroviaire.

L'ERA délivre, outre les autorisations internationales pour les matériels roulants, mais aussi les certificats de sécurité internationaux pour les entreprises ferroviaires dans l'ensemble de l'Union européenne. Toutefois, les autorités nationales restent pleinement compétentes en matière de contrôle.

Comme nous le précise Thomas Chatelet Chef de Projet ERTMS à l'ERA, l'ERA a, selon le 4ème paquet ferroviaire (réglementation ferroviaire votée par le Parlement européen et le Conseil européen), la compétence exclusive de délivrer les autorisations pour les véhicules circulant dans au moins 2 états membres, en vérifiant la conformité au cadre réglementaire ferroviaire européen (Directives d'interopérabilité et de sécurité ferroviaire [(EU) 2016/797 - (EU) 2016/798], Spécifications Techniques d'Interopérabilité (TSI), Méthodes Communes de Sécurité (CSM)). Les vérifications de l'ERA se font par rapport au cadre législatif européen ; les vérifications des agences nationales peuvent prendre en compte certaines normes nationales si elles sont justifiées et acceptées par l'Agence. En outre, l'Agence surveille les performances et le processus de décision des autorités nationales de sécurité par le biais d'audits et d'inspections, au nom de la Commission.[28]

L'ERA a comme mission prioritaire d'accélérer l'interopérabilité. Les directives européennes NIS et le règlement européen ont renforcé son rôle, le 16 juin 2019 dans le cadre du «4ème paquet ferroviaire[29] ». Il revient à l'ERA, par une harmonisation progressive des règles et des normes, à œuvrer pour lever les barrières techniques dressées entre les États au cours

[24] *UIC, l'association professionnelle mondiale représentant le secteur ferroviaire et promouvant le transport ferroviaire* [En ligne]. Disponible sur Home | UIC - International union of railways
[25] *RAIL 2050 VISION RAIL - THE BACKBONE OF EUROPE'S MOBILITY - ERRAC* [En ligne]. [Réf. De décembre 2017]. Disponible sur 122017_errac_rail_2050_vision.pdf (uic.org)
[26] *Rail 2030 – Research and innovation priorities -ERRAC* [En ligne]. [Réf. De septembre 2019]. Disponible sur ERRAC_2030.pdf
[27] *Agence de l'Union européenne pour les chemins de fer – ERA* [En ligne]. Disponible sur Agence de l'Union européenne pour les chemins de fer (ERA) | Union Européenne (europa.eu)
[28] Annexes | - Interview de Thomas Chatelet, ERA
[29] *Ouverture à la concurrence du transport ferroviaire - les paquets ferroviaires et la création de l'ARAFER* [En ligne]. [Réf. Du 22 mars 2017]. Disponible sur Ouverture à la concurrence du transport ferroviaire - les paquets ferroviaires et la création de l'ARAFER | Ministère de la Transition écologique (ecologie.gouv.fr)

de leur histoire. À titre d'exemple, un train souhaitant relier Berlin à Madrid devrait aujourd'hui être en mesure de circuler sous quatre tensions électriques, six systèmes de signalisation et deux écartements de rails différents. Josef Doppelbauer lors de la conférence sur les enjeux du ferroviaire tenue en novembre 2021[30] a rappelé s'il était encore besoin de ce qu'il appelle les difficultés de l'Europe des règles et réglementations ferroviaires « *En septembre dernier, un Train dénommé Connecting Europe Express*[31]*, a quitté Lisbonne et effectué 20.000km à travers 267 pays européens. En raison des 600 règles différentes - on en avait 14632 il y a quelque temps, le trajet de ce train a duré 36 jours et a nécessité 3 trains et 55 changements de locomotives en raison des multiples types d'écartement de rail et des règles disparates des différents pays* »

Les autorisations de circulations entre pays et les échanges d'informations entre acteurs ferroviaires des différents pays sont encadrés par des accords bilatéraux entre autorités ferroviaires des pays respectifs : c'est le cas des accords de coopération entre la France et l'Italie[32]. Mais selon Thomas Chatelet, Chef de projet ERTMS à l'ERA « ces accords bilatéraux n'ont pas vocation à perdurer étant donné que l'ERA a les compétences exclusives pour les Certificats Uniques de Sécurité des Entreprises Ferroviaires opérant dans deux états membres ou plus et cela devrait suffire[33] ». De plus le respect des exigences reposant sur les données (cas du PGIC de SNCF RÉSEAU[34]) sont des obligations réglementaires que doivent respecter les parties prenantes de l'activité de l'opérateur concerné.

III.3. L'UNIFE - UNION DES INDUSTRIES FERROVIAIRES EUROPEENNES

L'UNIFE est l'organisme européen représentant les **Industriels de la chaîne d'approvisionnement européenne du ferroviaire**. L'UNIFE pèse lourd avec ses 400.000 employés environ en Europe et toutes les sociétés qui relèvement d'elle. L'UNIFE regroupe des fabricants de matériel roulant, des fournisseurs d'infrastructures et de signalisation, d'intégrateurs, de systèmes et de sociétés d'ingénierie. Chacune de ces entreprises à une responsabilité dans la conception, la fabrication, la maintenance et la remise à neuf des systèmes, sous-systèmes et équipements de transport ferroviaire[35] qui rendent possibles les mobilités par le rail. L'UNIFE participe à plusieurs projets de recherche du programme Shit2Rail, d'ERRAC et plusieurs projets innovants regroupés sous l'appellation Horizon2020[36]. Certains concernent la sécurité du ferroviaire et en particulier la maintenance basée sur l'IA[37].

---

[30] Table ronde de l'IMTD (Institut des Mobilités et des Transports Durables). Le ferroviaire au cœur des grands enjeux des transports. [vidéo en ligne]. [Réf. du 18 Févr. 2021]. Disponible sur En direct de l'IMTD, table ronde Le ferroviaire au cœur des grands enjeux des transports

[31] *Connecting Europe Express": promouvoir le rail en Europe* [Vidéo en ligne]. [Réf. 2021]. Disponible sur "Connecting Europe Express" : promouvoir le rail en Europe

[32] *Accord de coopération EPSF/ANSFISA* [En ligne]. [Réf. De mai 2021]. Disponible sur Accord de coopération EPSF/ANSFISA - Mai 2021 | EPSF (securite-ferroviaire.fr)

[33] Annexes - Interview Thomas Chatelet - ERA

[34] *PGIC - Cartographie Capacité,Traification, Facturation, Réclamations, Régularité, Accidents Incidents, Essai de matériel* [En ligne]. [Réf. 2021]. Disponible sur Annexe2bis.pdf (autorite-transports.fr)

[35] *THE EUROPEAN RAIL SUPPLY INDUSTRY* [En ligne]. Disponible sur The European Rail Supply Industry - UNIFE

[36] *Le portail français du programme européen pour la recherche et l'innovation* [En ligne]. [Réf. Du 15 janvier 2019]. Disponible sur Horizon2020.gouv.fr.

[37] *Project coordinated by UNIFE* [En ligne]. Disponible sur HORIZON2020 Projects - UNIFE

IV. ORGANISMES DE CYBERSÉCURITÉ ET DES TECHNOLOGIES FERROVIAIRES

IV.1. L'ENISA - EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

L'ENISA (Agence de l'Union européenne pour la cybersécurité) est le **centre d'expertise sur la cybersécurité en Europe**. Elle aide l'Union européenne (UE) et les États membres à être mieux équipés et préparés pour prévenir et détecter les problèmes de sécurité de l'information et y répondre.

C'est un organisme central dont les travaux bénéficient à toutes les parties prenantes dans l'Union européenne : organismes du secteur public tels que les gouvernements des pays de l'UE; les institutions de l'UE ; les entreprises de télécommunications, fournisseurs d'accès à internet et sociétés d'information et de communication, les entreprises, en particulier les petites et moyennes entreprises; les spécialistes de la sécurité des réseaux et de l'information, telles que les équipes d'intervention en cas d'urgence informatique; les universités; le grand public.

L'ENISA fournit des conseils pratiques et des solutions aux secteurs publics et privés des États membres et aux institutions de l'UE. Dans la liste de ces missions, on retrouve :

- L'organisation des exercices de cybersécurité dans toute l'Europe[38];
- La contribution à l'élaboration des stratégies nationales en matière de cybersécurité;
- La coordination entre les équipes (CSIRT)[39] d'intervention en cas d'urgence informatique et le renforcement des capacités.

L'ENISA[40] contribue également à l'élaboration de la politique et la législation de l'Union sur la sécurité des réseaux et de l'information.

Concernant ses liens avec les autres organismes européens : l'UIC collabore étroitement avec l'ENISA et l'ERA sur plusieurs thématiques de stratégie, gouvernance, opérationnelle et and Recherche et Innovations. En 2018, l'UIC a lancé plusieurs événements et publications pour aborder les questions de cybersécurité dans le secteur ferroviaire (Guidelines for Cybersecurity in Railways[41]). L'UIC appuie d'ailleurs l'ENISA dans le cadre du grand programme commun Shift2Rail qui constitue aujourd'hui le principal mécanisme de mise en œuvre de l'innovation ferroviaire.

IV.2. L'ERRAC – EUROPEAN RAIL RESEARCH ADVISORY COUNCIL

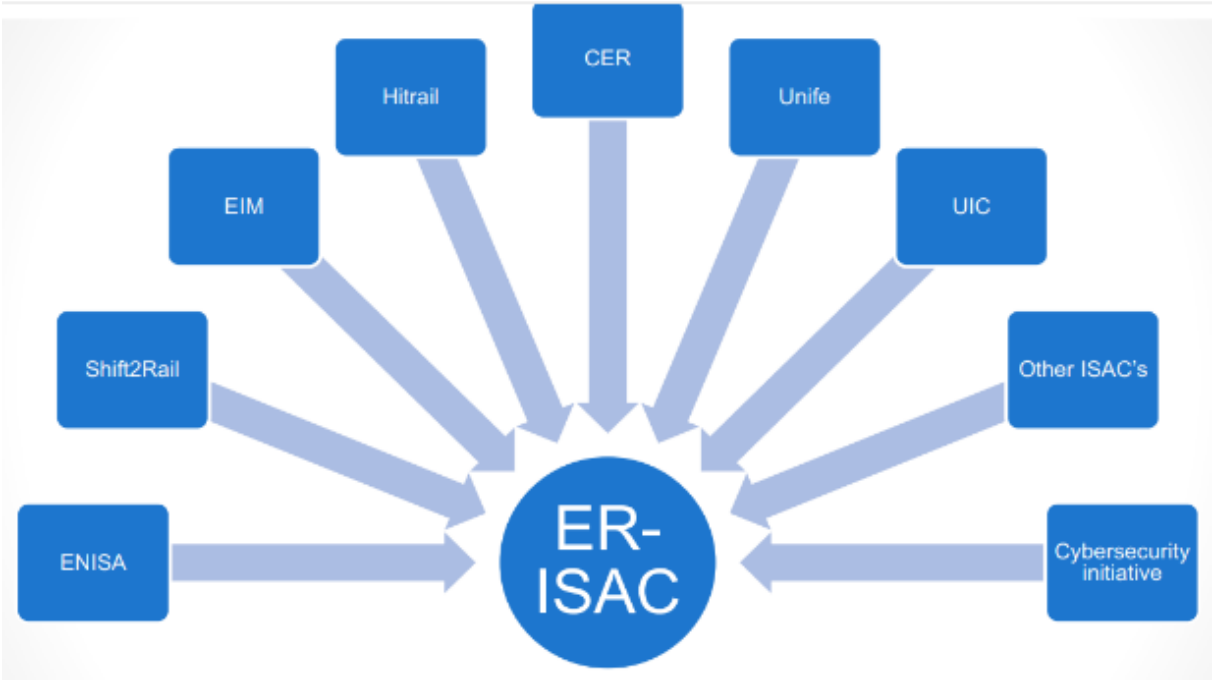
ERRAC[42] est la **plateforme technologique européenne pour le secteur ferroviaire**, réunissant toutes les parties prenantes - opérateurs ferroviaires, gestionnaires d'infrastructure, constructeurs de trains et autres fournisseurs, fournisseurs de transport urbain, universitaire et experts scientifiques et bien d'autres qui s'intéressent à la recherche ferroviaire. C'est la plateforme privilégiée pour s'accorder afin d'exprimer d'une

[38] *L'ENISA mène un large éventail d'activités dans le domaine des cyber-exercices.* [En ligne]. Disponible sur Cyber Exercises — ENISA (europa.eu)
[39] *CSIRTs in Europe* [En ligne]. Disponible sur CSIRTs in Europe — ENISA (europa.eu)
[40] *ENISA –Sécuriser la société de l'information en Europe* [En ligne]. Disponible sur ENISA - En français — ENISA (europa.eu)
[41] *Guidelines for Cyber-Security in Railways* [En ligne]. [Réf. Du 1 juin 2018]. Disponible sur Guidelines for cyber security in railways
[42] *European Rail Research Advisory Council* [En ligne]. Disponible sur ERRAC

seule voix qui se veut forte, aux institutions européennes les besoins du secteur en matière de recherche et d'innovation.

IV.3. LES ISACS - INFORMATION SHARING AND ANALYSIS CENTERS

Les **centres de partage et d'analyse de l'information** (ISAC[43]) sont des organisations à but non lucratif. Ils mettent à disposition un point central pour la collecte d'informations sur les cybermenaces (dans de nombreux cas pour les infrastructures critiques) et le partage bidirectionnel d'informations entre le secteur privé et le secteur public. Ces informations concernent les causes profondes, les incidents, les vulnérabilités, les menaces, ainsi que le partage d'expériences, de connaissances et d'analyses. Dans de nombreux États membres de l'UE, il existe des initiatives ISAC ou similaires.



2 - Parties prenantes des ISAC du secteur ferroviaire européen (Source ISAC/ENISA)

Les ISACs sont en grande partie pilotés par l'industrie avec un soutien gouvernemental notamment en termes de facilitation administrative et partage de connaissances professionnelles (lutte contre la cybercriminalité, partage d'informations pertinentes pour l'industrie)[44].

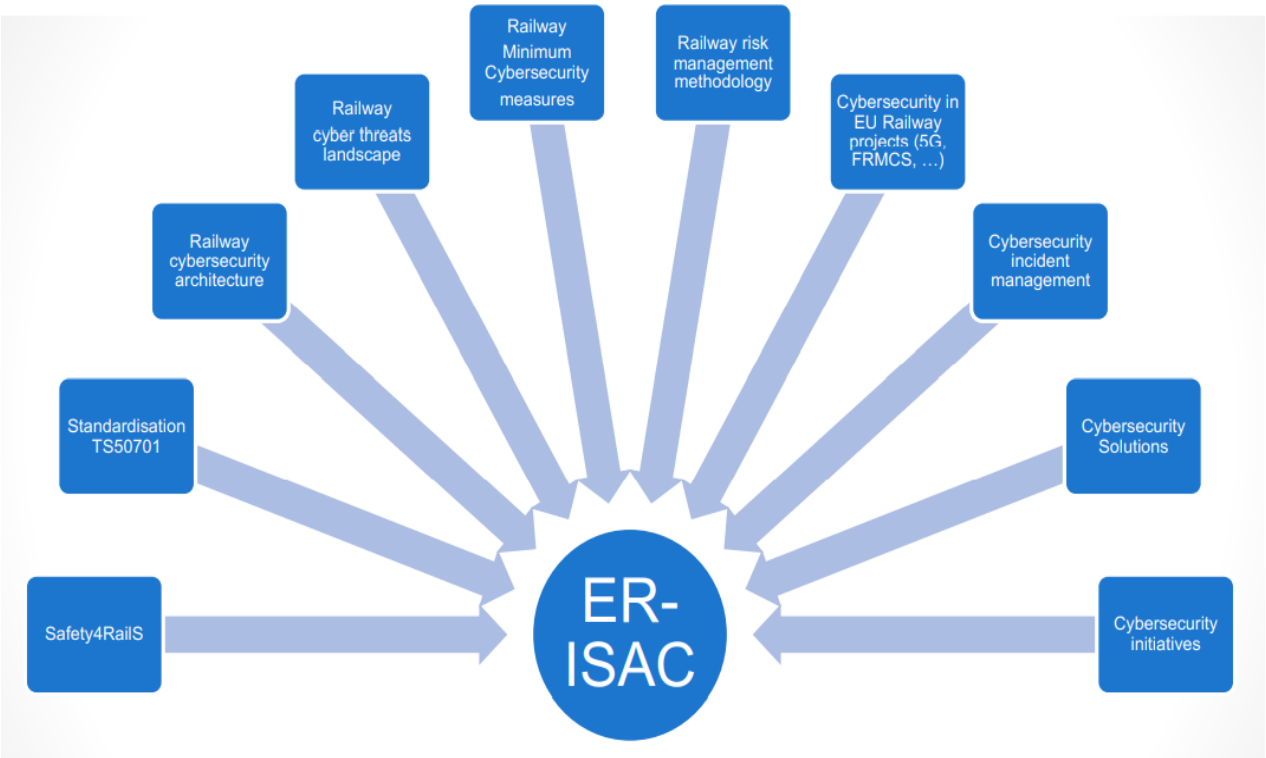
Les ISAC en Europe, adaptés au secteur des transports ferroviaires, sont organisés en 3 modèles : le modèle axé sur les pays ; le modèle sectoriel ; le modèle de collaboration internationale.

Comme on peut le voir dans la figure csuit, les ER-ISAC couvrent un large panel de thématiques : gouvernance, spécifications, méthodologie de management de risques, standards tels que la TS50701, Architecture de cybersécurité, communications avec la 5G et le protocole FRMCS (qui remplacera le GMS-R), cartographie des menaces de cybersécurité, gestion d'incidents de cybersécurité, solutions de cybersécurité, etc.

---

[43] *Information Sharing and Analysis Centers (ISACs)* [En ligne]. [Réf. 2021]. Disponible sur Information Sharing and Analysis Centers (ISACs) — ENISA (europa.eu)

[44] *Information Sharing and Analysis Centres (ISACs) Cooperative models* [En ligne]. [Réf. 2017]. Disponible sur https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models



3 - Thématiques couvertes par les ER-ISAC[45]

Les membres et experts de l'ISAC sont unanimes, la clé du succès des ISACs est la confiance, et le meilleur outil pour gagner la confiance reste les relations personnelles et les « cercles de confiance ». Certaines informations (par exemple, des détails techniques sur les menaces et les incidents) peuvent être largement partagées avec tous les membres. En outre, il y a aussi le cercle interne où les informations partagées sont plus détaillées et transitent via d'autres moyens sécurisés.

L'UIC offre aussi du support à ER-ISAC (European Railway – Information Sharing and Analysis Center), groupe de partage et de confiance entre différents acteurs ferroviaires sur le sujet cyber.

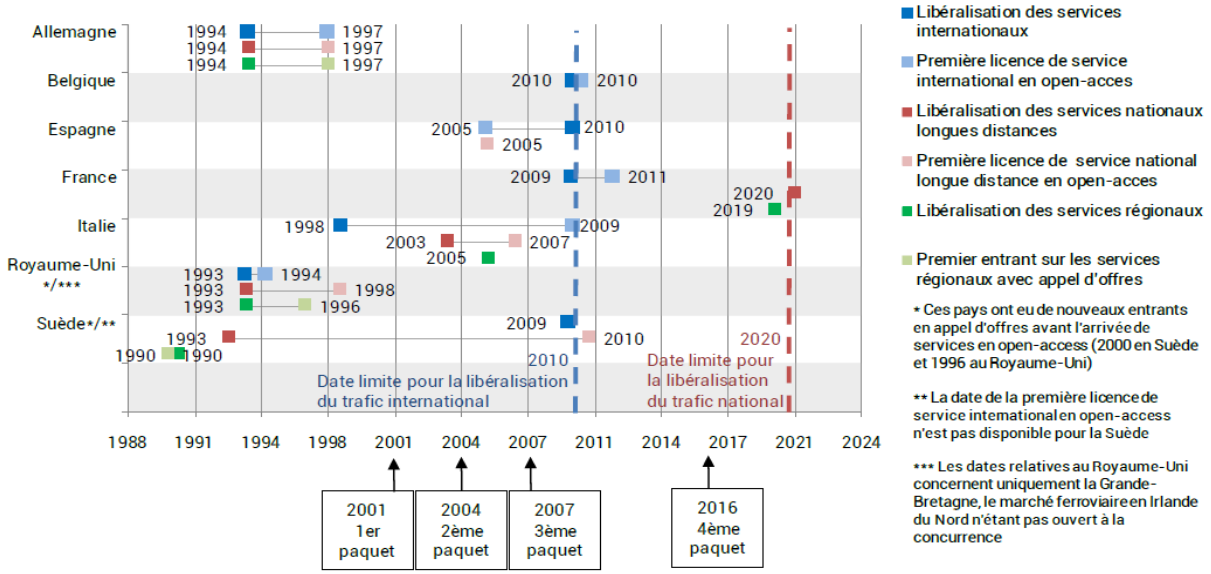
Pour Thomas Chatelet de l'ERA, la complémentarité de ces 3 acteurs UIC, ENISA et les ER-ISAC et l'ERA est nécessaire pour avoir un niveau de recommandation commun en direction des acteurs ferroviaires pour prendre en compte la menace cyber et les solutions à y apporter[46].

[45] *European Railway Information Sharing & Analysis Center* [En ligne]. [Réf. Mars 2021]. Disponible sur 8-initiatives-of-the-er-isac-devisscher.pdf (europa.eu)
[46] Annexes I - Interview Thomas Chatelet - ERA

V. PAQUETS, GOUVERNANCE ET NORMES FERROVIAIRES EUROPÉENNES

V.1. PAQUETS FERROVIAIRES

La politique européenne des transports ferroviaires est régie par un ensemble de directives constituant les quatre « paquets ferroviaires »[47] actuellement adoptés. La Commission Européenne a initié en 1991 une première directive pour ouvrir les activités ferroviaires à la concurrence. Cette directive, fondée sur la séparation entre le gestionnaire de l'infrastructure et l'opérateur historique, a ensuite été modifiée par quatre paquets ferroviaires.



4 – Dates clés des paquets ferroviaires et d'ouverture à la concurrence du trafic de voyageurs[48]

- **Le 1er paquet ferroviaire** vise à définir les fonctions essentielles et l'ouverture à la concurrence du fret transeuropéen, il est adopté le 26 mars 2001. Ces directives abordent l'ouverture à la concurrence du fret sur le réseau transeuropéen, les licences des entreprises ferroviaires, la répartition des capacités d'infrastructure ferroviaire, la tarification de l'infrastructure ferroviaire et la certification en matière de sécurité.

- **Le 2ème paquet ferroviaire** est relatif à l'ouverture à la concurrence du fret, il est adopté en avril 2004 suivi de la création d'une agence ferroviaire européenne (ETRA) à Valenciennes, dont la mission est de proposer des mesures d'harmonisation progressive des règles de sécurité et d'élaborer des spécifications techniques d'interopérabilité (STI).
  Les directives de ce paquet abordent la sécurité des chemins de fer, l'institution dans chaque État membre d'une autorité nationale de sécurité (l'Établissement Public de Sécurité Ferroviaire (EPSF) pour la France), d'un organisme permanent d'enquête sur les accidents (Le BEA-TT Bureau d'Enquêtes sur les Accidents de

[47] *Le transport ferroviaire – du 1er au 4e paquet ferroviaire* [En ligne]. [Réf. 2019]. Disponible sur Du 1er au 4e paquet ferroviaire - ART (autorite-transports.fr)
[48] *COMPARAISON FRANCE - EUROPE DU TRANSPORT FERROVIAIRE* [En ligne]. [Réf. 2018]. Disponible sur comparaison-france-europe-transport-ferroviaire.pdf (autorite-transports.fr)

Transport terrestre en France[49]), l'interopérabilité du système ferroviaire transeuropéen à grande vitesse et conventionnel et l'ouverture à la concurrence, le transport de marchandises sur l'ensemble du réseau ferroviaire international au 1er janvier 2006 et sur le marché national au 1er janvier 2007.

- **Le 3ème paquet ferroviaire** met en place l'ouverture à la concurrence du transport international de voyageurs, y compris le cabotage[50], il est adopté en 2007.Les directives associées sont relatives à l'ouverture à la concurrence du transport international de voyageurs, à la certification des conducteurs de train alors que les règlements sont relatifs aux services publics de transport de voyageurs par chemin de fer et par route. Pour le règlement 1371, il est dit « Obligations de service public » et institue un régime unifié des droits et obligations des voyageurs ferroviaires au sein de la Communauté européenne.

- **Le 4ème paquet ferroviaire** est relatif à l'ouverture des transports nationaux de voyageurs, adopté mi-décembre 2016. Il s'agit d'une proposition législative de la Commission sur la possibilité des compagnies de chemin de fer d'opérer partout dans l'Union européenne.

V.2. GOUVERNANCE AUTOUR DE LA SECURITE FERROVIAIRE

La transposition de la directive 2004/49/CE du Parlement européen et du Conseil concernant la sécurité des chemins de fer communautaires instaure dans son article premier la création obligatoire, dans chaque État membre, d'une autorité de sécurité ferroviaire[51]. En France, c'est l'EPSF (Établissement Public de Sécurité Ferroviaire) qui tient ce rôle. Cette dernière veille au principe de base de la sécurité ferroviaire à savoir : *« **il est interdit** **de dégrader le niveau de sécurité global du système (par l'introduction de nouveaux items ou de changements de l'existant).** »*

L'article L2221-1 du Code des transports précise que l'Établissement public de sécurité ferroviaire veille au respect des règles relatives à la sécurité et à l'interopérabilité des transports ferroviaires. Il est l'autorité nationale de sécurité au sens de la directive (UE) 2016/798 du Parlement européen et du Conseil du 11 mai 2016 relative à la sécurité ferroviaire. Il exerce ses missions au sein du système ferroviaire français (les réseaux urbains de métros et tramways relevant de la compétence des préfets). Sous réserve des missions dévolues à l'Agence de l'Union européenne pour les chemins de fer prévues par le règlement (UE) 2016/796 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour les chemins de fer, l'EPSF est notamment chargé de délivrer les autorisations requises pour l'exercice des activités ferroviaires et d'assurer des activités de surveillance portant en particulier sur les entreprises

Le transport ferroviaire est un mode complexe dont la sécurité est maîtrisable pour autant que la responsabilité de chacun des nombreux acteurs, ainsi que leurs rôles respectifs soient clairement identifiés.

- *L'État* fixe les objectifs de sécurité et la façon de les atteindre. Il est responsable de la réglementation nationale et veille à son application. Lien vers le site du ministère chargé des Transports
- L'*Agence de l'Union européenne pour les chemins de fer (ERA)* prépare la réglementation européenne sur mandat de la Commission, délivre les autorisations

[49] *Le Bureau d'Enquêtes sur les Accidents de Transport terrestre* [En ligne]. [Réf. Du 24 aout 2014]. Disponible sur Le Bureau d'Enquêtes sur les Accidents de Transport Terrestre - BEA-TT
[50] *Le cabotage ferroviaire* [En ligne]. [Réf. 2021]. Disponible sur Le cabotage ferroviaire - Autorité de régulation des transports
[51] *Prise en compte des enjeux de cybersécurité au sein de la sécurité ferroviaire - EPSF* [En ligne]. [Réf. Du 21 avril 2022]. Disponible sur Prise en compte des enjeux de cybersécurité au sein de la sécurité ferroviaire | EPSF

pour lesquelles elle est compétente et assure le contrôle des activités des autorités nationales de sécurité. Lien vers le site de l'Agence

- *L'EPSF* délivre les autorisations qui relèvent de son domaine de compétence dans le cadre de la répartition définie par les directives européennes entre l'Agence de l'Union européenne pour les chemins de fer et les autorités nationales de sécurité. Il veille au respect des conditions de maintien de ces autorisations, moyennant des contrôles, des audits et des inspections. Il suit par ailleurs l'évolution du niveau de sécurité en France, grâce notamment à la traçabilité et à la classification des événements de sécurité survenant sur le système ferroviaire français. Il participe à l'élaboration des règles de sécurité et d'interopérabilité, tant au niveau européen que national[52].

5 - Organisation du contrôle en phase opérationnelle dans le secteur du transport ferroviaire (Source EPSF)

À titre indicatif en 2021, l'EPSF a attribué des certificats nationaux de sécurité ferroviaire à 22 entreprises ferroviaires. Parmi elles 7 sont détentrices d'un certificat de sécurité unique délivré par l'agence de l'Union européenne pour les chemins de fer en cours de validité sur tout ou partie du réseau du système ferroviaire français[53] : CAPTRAIN ITALIA SRL - CFL (Chemins de fer luxembourgeois) - EUROSTAR France - FRET SNCF - SNCF VOYAGEURS – LINEAS - THI FACTORY / THALY. Pour les Gestionnaires d'Infrastructure (GI) on en décompte 14 sur le territoire français qui disposent d'un agrément en cours de validité, même si SNCF RÉSEAU reste le principal GI : CAPTRAIN ITALIA SRL - CFL (Chemins de fer luxembourgeois) - EIFFAGE RAIL EXPRESS – EUROTUNNEL - Grand Port Maritime de Marseille - LINEA FIGUERAS PERPIGNAN SA - LISEA - OC'VIA - RFI - SNCF RÉSEAU - COLAS RAIL - TRANSDEV RAIL – SFERIS – SOCORAIL.

- *Les exploitants ferroviaires* (les gestionnaires d'infrastructures et les entreprises ferroviaires) mettent en œuvre leurs équipements, forment leurs personnels, définissent leurs consignes et instructions opérationnelles dans le respect de la réglementation. Ils en contrôlent l'application.
- *Le Bureau d'Enquêtes sur les Accidents de Transport terrestre (BEA-TT)* réalise des enquêtes en cas d'accidents ferroviaires graves ou potentiellement graves. Il exerce un rôle distinct, mais complémentaire de celui de l'EPSF. La mise en œuvre pratique des recommandations du BEA-TT est suivie par l'EPSF. Lien vers le site du BEA-TT

[52] *POSITIONNEMENT DE L'EPSF PARMI LES ACTEURS DU SYSTÈME FERROVIAIRE FRANÇAIS – EPSF* [En ligne]. [Réf. Du 26 mars 2021]. Disponible sur Positionnement de l'EPSF parmi les acteurs du système ferroviaire
[53] *OPérateurs ferroviaires autorisés - EPSF* [En ligne]. [Réf. 2021]. Disponible sur OPÉRATEURS FERROVIAIRES AUTORISÉS | EPSF (securite-ferroviaire.fr)

- Par ailleurs, dans le cadre de ses multiples fonctions, *l'Autorité de régulation des transports (ART)* peut être saisie à l'encontre des décisions prises par l'EPSF.[54]

V.3. ORGANISMES DE NORMALISATION

V.3.1. EN FRANCE

Par délégation de l'Association Française de NORmalisation (**AFNOR**), le Bureau de Normalisation Ferroviaire (BNF) assure la normalisation des matériels roulants, des installations fixes et des autres assets spécifiques dans le ferroviaire. Il participe aux travaux de normalisation dans le domaine ferroviaire au niveau européen et international. Il traduit les normes européennes ou internationales élaborées dans ce cadre.

Le bureau de normalisation ferroviaire assure essentiellement les trois missions suivantes :

- Il organise et anime l'élaboration des Normes Françaises (**NF**) ;
- Il organise et anime la participation française à l'élaboration des normes européennes (EN) du Comité européen de Normalisation (CEN) et du Comité européen de Normalisation en Électrotechnique (CENELEC), ainsi que des normes internationales (ISO et IEC). Pour certains travaux, il assure le secrétariat ;
- Il met à disposition des versions françaises des normes européennes ou internationales.

V.3.2. ORGANISMES ET NORMES FERROVIAIRES AU NIVEAU EUROPÉEN

Le CEN ou Comité européen de normalisation est l'un des trois organismes européens de normalisation (avec le CENELEC[55] et l'ETSI) habilités officiellement par l'Union européenne et par l'Association Européenne de Libre-Echange (**AELE**) à l'élaboration et de la définition de normes volontaires au niveau européen. Le CENELEC (Comité européen de Normalisation Electrotechnique), est une association qui regroupe les Comités Electrotechniques Nationaux de 34 organismes nationaux de normalisation (ONS) des 27 pays de l'Union européenne, le Royaume-Uni, la République de Macédoine du Nord, la Serbie et la Turquie, ainsi que trois pays de l'Association européenne de libre-échange (Islande, Norvège et Suisse). Il y a un membre par pays, le Royaume-Uni, la République de Macédoine du Nord, la Serbie et la Turquie, ainsi que trois pays de l'Association européenne de libre-échange (Islande, Norvège et Suisse). Il y a un membre par pays[56]. Tous les membres de ces organismes sont également membres de l'Organisation internationale de normalisation (ISO). CEN et CENELEC travaillent de pair pour la publication de certains travaux.

Il n'existe pas moins de 500 normes ferroviaires et un nombre important à l'état de projet. Ces normes abordent tous les aspects de l'infrastructure ferroviaire (voies ferrées et matériel roulant) ; elles traitent des thématiques telles que la sécurité, l'interopérabilité, les capacités, les communications, l'efficacité énergétique, l'ergonomie, etc. Elles visent

[54] EPSF [En ligne]. [Réf :2022] Disponible sur Page d'accueil - Autorité de régulation des transports (anciennement Arafer) (autorite-transports.fr)
[55] *Le Comité européen de normalisation est l'un des trois organismes européens de normalisation.* [En ligne]. [Réf. 2021]. Disponible sur About CEN - CEN-CENELEC (cencenelec.eu)
[56] *Membres du conseil d'administration* [En ligne]. [Réf. 2022]. Disponible sur CEN Community - List of members

tous les types de train, voyageurs et marchandises, les trains à grande vitesse et les trains régionaux.

Ci-dessous, quelques familles de normes significatives du secteur :

- ISO/TC 269/SC 1 « Infrastructure » ;
- ISO/TC 269/SC 2 « Matériel roulant » ;
- IEC/TC 9 « Matériels et systèmes électriques ferroviaires » ;
- CENELEC/TC 9X « Applications électriques et électroniques dans le domaine ferroviaire »
- CLC/TS 50701[57]. En juin 2021, CEN-CENELEC a publié la CLC/TS 50701 issue des travaux du groupe de travail WG26 réunissant des grands acteurs majeurs du secteur. Cette norme prend en considération les aspects pertinents liés à la sécurité (EN 50126) et s'inspire de différentes sources (IEC 62443-3-3, CSM-RA), en les adaptant au contexte ferroviaire. Elle couvre de nombreux sujets clés tels que la vue d'ensemble du système ferroviaire, la cybersécurité au cours du cycle de vie d'une application ferroviaire, l'évaluation des risques, la conception de la sécurité, l'assurance et l'acceptation de la cybersécurité, la gestion des vulnérabilités et la gestion des correctifs de sécurité[58].

V.4. GOUVERNANCE ET DIRECTIVES EN CYBERSECURITE FERROVIAIRE

La gouvernance de la cybersécurité européenne est régie par :

- Une organisation autour des entités telles que l'AED, l'ENISA ;
- Des directives et dispositions juridiques et réglementaires, telles que les directives NIS, le Règlement Général sur la Protection des Données (RGPD), le cybersecurity Act[59]
- Un cadre normatif pour garantir la confiance dans les produits et services

V.4.1. SÉCURITÉ NUMERIQUE ET RENFORCEMENT DE LA CYBERDÉFENSE EUROPÉENNE

L'Agence Européenne de Défense (AED), en collaboration avec l'ENISA, Agence de l'UE pour la cybersécurité et Europol[60] est responsable de la coopération de l'UE en matière de défense dans le cyberespace. Les États membres sont aidés par l'AED pour se constituer une main-d'œuvre militaire qualifiée dans le domaine de la cyberdéfense et pour développer des technologies de cyberdéfense proactives et réactives. La stratégie de cybersécurité de l'UE adoptée en décembre 2020 par la Commission européenne et le Service européen pour l'Action Extérieure (SEAE) renforce la coordination de la cyberdéfense, la coopération et la constitution des capacités de cyberdéfense.

C'est à l'ENISA qu'a été confiée la mission de coordination entre les États membres, les institutions de l'UE et d'autres parties prenantes pour lutter contre les cyberattaques. L'ENISA, qui contribuait déjà à la cyberpolitique de l'UE, a vu ses prérogatives renforcées par la loi de l'UE sur la cybersécurité (Cybersecurity Act)[61].

---

[57] *Railway applications - Cybersecurity* [En ligne]. [Réf. 2021]. Disponible sur CLC/TS 50701:2021 - Railway applications - Cybersecurity - European Standards (en-standard.eu)
[58] *Une étape importante pour la cybersécurité des chemins de fer : la nouvelle norme CLC/TS 50701* [En ligne]. [Réf. Du 10 juin 2021]. Disponible sur A major step for railways cybersecurity: the new CLC/TS 50701 - CEN-CENELEC (cencenelec.eu)
[59] Adoption définitive du Cybersecurity Act : un succès pour l'autonomie stratégique européenne [En ligne]. [Réf. Du 11 juin 2019]. Disponible sur adoption-definitive-du-cybersecurity-act-un-succes-pour-lautonomie-strategique-europeenne/
[60] *European Cybercrime Centre - EC3* [En ligne]. [Réf. Du 1er mars 2022]. Disponible sur European Cybercrime Centre - EC3 | About Europol | Europol (europa.eu)
[61] *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA* [En ligne]. [Réf. Du 17 avril 2019]. Disponible sur certification de cybersécurité des technologies de l'information et des communications

La gouvernance autour de la cybersécurité ferroviaire est alignée avec celle de la cybersécurité Européenne. L'UE a bien pris la mesure des menaces qui pèsent et vont peser en Europe et globalement dans le monde, vu la projection de 22,3 milliards d'appareils dans le monde qui devraient être connectés à l'internet des objets d'ici à 2024. Le secteur critique que représentent les transports sera effectivement, comme l'énergie, la santé et la finance dans le top des secteurs ciblés par les cybermalveillants[62].

Le 22 mars 2021, le Conseil européen a adopté des conclusions sur la stratégie de cybersécurité, soulignant que la cybersécurité est essentielle à l'édification d'une Europe résiliente, verte et numérique. Le Conseil au travers de ses États membres a initié une plateforme pluridisciplinaire européenne contre les menaces criminelles (Empact[63]) dans le but d'identifier, de hiérarchiser et de combattre les menaces que représentent la criminalité organisée internationale et les cyberattaques.

Une attention particulière a été portée sur les cybermenaces liées aux objets industriels connectés (IIoT) et à la 5G. Concernant les IIoT, le Conseil a adopté en décembre 2020, des résolutions pour le respect de la vie privée, la sécurité de l'information et la cybersécurité. Il est prévu la mise en place d'une législation horizontale à long terme pour traiter tous les aspects pertinents de la cybersécurité des dispositifs connectés, tels que la disponibilité, l'intégrité et la confidentialité ainsi que les conditions requises à la mise sur le marché. Concernant la 5G, le Conseil a adopté en janvier 2020, une boîte à outils pour des mesures communes en matière de cybersécurité des réseaux 5G et fournir des orientations.

Les mesures stratégiques recensées dans la boîte à outils renforcent les pouvoirs réglementaires des autorités nationales pour contrôler le déploiement et l'usage des réseaux. D'autres mesures spécifiques permettant de faire face aux risques liés aux vulnérabilités non techniques (par exemple, le risque d'interférence par des Acteurs étatiques ou soutenus par l'État non membre de l'UE) et l'évaluation du profil de risque des fournisseurs ont été aussi prévues à cet effet.

D'une manière générale, les États membres doivent veiller à la mise en place des mesures spécifiques afin de réagir de manière appropriée et proportionnée en cas de survenue d'incidents. Autre point, il a été demandé aux États membres de renforcer les exigences de sécurité pour les opérateurs de réseaux mobiles (par exemple, contrôles d'accès stricts, règles d'exploitation et de surveillance sécurisées, limitations de l'externalisation de fonctions spécifiques, etc.) [64]. Autre point marquant, au regard de son règlement sur la cybersécurité, l'UE a mis en place un cadre de certification de cybersécurité unique pour l'UE fondé sur les risques. L'objectif est d'augmenter la confiance sur la sécurité des produits et services importants pour le monde numérique[65].

Toutefois et comme nous le précise Thomas Chatelet de l'ERA[66], le cadre réglementaire ferroviaire européen ne comporte, pour le moment, pas de prérequis spécifique à la cybersécurité à l'exception :

- D'une référence indirecte dans les CSM (Common Safety Methods)[67] à la norme CENELEC EN 50126 dans laquelle le « Safety Case » est lié à la prise en compte du risque cyber ;

[62] *Cybersécurité: comment l'UE lutte contre les cybermenaces* [En ligne]. [Réf. Du 29 avril 2022]. Disponible sur Cybersécurité: comment l'UE lutte contre les cybermenaces - Consilium (europa.eu)
[63] *Cycle politique de l'UE - EMPACT* [En ligne]. [Réf. Du 20 janvier 2022]. Disponible sur Empact
[64] *Réseaux 5G sécurisés : Questions et réponses sur la boîte à outils de l'UE* [En ligne]. [Réf. Du 29 janvier 2020]. Disponible sur Secure 5G networks: the EU toolbox (europa.eu)
[65] *Le cadre de certification de l'UE en matière de cybersécurité* [En ligne]. [Réf. Du 22 février 2022]. Disponible sur Cybersecurity certification framework | Shaping Europe's digital future (europa.eu)
[66] Annexes I – Interview Thomas Chatelet - ERA
[67] *Que sont les méthodes de sécurité communes (CSM-RA) et quand s'appliquent-elles ?* [En ligne]. [Réf. Du 2 décembre 2019]. Disponible sur What Common Safety Methods (CSMs-RA) are and when do they apply? (leedeo.es)

- Des règles de base pour les TSI (Technical Specification for Interoperatbility) TAP/TAF (Télématique Passager/Fret) et des règles plus spécifiques pour la TSI CCS (Contrôle-Commande et Signalisation) pour assurer l'authenticité et l'intégrité des messages ETCS (European Train Control System) ainsi que la PKI y étant associée. Ces TSI s'appliquent à tous nouveaux sous-systèmes « contrôle-commande et signalisation au sol », modernisés ou renouvelés et aux « sous-systèmes de contrôle-commande et de signalisation embarqués du système ferroviaire tel que définis à l'annexe II, points 2.3 et 2.4, de la directive (UE) 2016/797 du Parlement européen et du Conseil.[68]

V.4.2. DIRECTIVE NIS NETWORK AND INFORMATION SYSTEM SECURITY (SRI – SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION)

La directive européenne NIS répond aux 4 enjeux majeurs ci-dessous :

La directive Network and Information System Security (NIS) poursuit un objectif : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Elle vise à l'émergence d'une Europe forte et de confiance, qui s'appuie sur les capacités nationales des États membres en matière de cybersécurité, la mise en place d'une coopération efficace et la protection des activités économiques et sociétales critiques au sein d'un État et entre États, pour faire face collectivement aux risques de cyberattaques. Le processus pour aboutir à l'établissement d'une telle directive est long et fastidieux d'autant plus qu'il faut faire accorder aussi bien les États que les courants de pensée parfois transnationaux avec des avis parfois divergents, voire antagonistes. Il a fallu quatre années de négociations pour aboutir à une adoption en juillet 2016 par les institutions européennes d'une directive partagée. Tous les pays avaient jusqu'à avril 2018 pour la transposer dans leurs législations nationales. Ce fut le cas pour la France en février 2018. La figure qui suit présente la chronologie des événements liés à la directive NIS jusqu'à la transposition dans le droit national notamment pour le cas de la France.

[68] *Spécifications techniques pour l'interopérabilité - ERA* [En ligne]. [Réf. 2016]. Disponible sur Technical Specifications for Interoperability | ERA (europa.eu)

6 - Dates clés de la directive NIS[69]

Sur le plan politique, la Directive NIS et les mises en œuvre nationales font l'objet d'un examen continu. La Commission européenne et les États membres, avec l'aide de l'ENISA, s'efforcent de relever un certain nombre de défis, en particulier ceux qui ont trait au contexte politique et réglementaire. Dans le même temps, la mise en œuvre des mesures de sécurité minimales par les sociétés relevant du statut d'OSE, fait l'objet d'un suivi par les États membres dans le but d'identifier les améliorations potentielles et les domaines dans lesquels ces OSE auraient besoin d'un soutien supplémentaire.

V.4.3. LA NOUVELLE DIRECTIVE NETWORK INFORMATION SECURITY (NIS2)

Le 16 décembre 2020, le Parlement européen et le Conseil européen proposent une évolution de la directive NIS dans le cadre de la nouvelle stratégie de cybersécurité de l'Union. Cette nouvelle version vise à renforcer davantage la résilience des entités publiques et privées européennes face aux cybermenaces, dans un contexte de numérisation et d'interconnexion croissante des activités, en Europe et dans le monde. À cet effet, et dans le cadre de la NIS 2 (SRI 2) les États membres sont tenus de :

- **Désigner des CSIRT** ;
- **Mettre en place des cadres nationaux de gestion de crise dans le domaine de la cybersécurité**, en désignant les autorités nationales compétentes chargées de gérer les incidents et crises de grande ampleur en matière de cybersécurité ;

[69] *La directive Network and Information System Security (NIS) ,assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne - ANSSI* [En ligne]. [Réf. 2021]. Disponible sur Directive Network and Information Security

- **Désigner une autorité nationale compétente en matière de cybersécurité**, à laquelle seront confiées des missions de surveillance au titre de cette directive. Chaque État doit désigner également un point de contact national unique pour toutes les questions de cybersécurité. Ce point de contact exercera une fonction de liaison pour assurer la coopération transfrontalière entre les autorités compétentes des États membres.

V.4.4. RÈGLEMENT GÉNÉRAL DE PROTECTION DES DONNÉES – RGPD

« *La réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 est une obligation légale de conformité pour toute entité traitant des données à caractère personnel*. »

Au vu du volume de données à caractère personnel traité, qu'il s'agisse de données des clients, mais aussi des collaborateurs, des opérateurs de mobilité, la mise en place d'un délégué à la protection des données (DPO, Data Protection Officer) est nécessaire voire obligatoire. Il représente le pilote de la gouvernance des données personnelles. Soumise à une stricte obligation de confidentialité, il est chargé d'apporter, à tous, des renseignements sur les questions relatives à la protection des données personnelles. Le secteur industriel ferroviaire manipule une quantité impressionnante de données des clients, des usagers qui utilisent les services d'agrément et aussi des données d'interlocuteurs divers. Ces données peuvent revêtir un caractère personnel. Les informations sur les conducteurs sur les badges ou autres identifiants utilisés par des collaborateurs ou les différents prestataires sont à manipuler avec la plus stricte des précautions d'usage. La protection des données au regard des droits fondamentaux des respects de la vie privée demande une obligation de leur sécurisation, elle est nécessaire, mais non suffisante.

Le cadre général de la RGPD requiert la mise en œuvre d'un certain nombre d'obligations reposant sur des bases légales et de mise en conformité[70].

Le RGPD est basé sur des règles externes :

- La charte des droits fondamentaux (art 8) du 7 décembre 2020 ;
- La Déclaration des droits de l'homme et du citoyen (art.2), du 26 août 1789 ;
- L'article 9 du Code civil, du 18 mars 1803 ;
- La Loi « Informatique et Libertés » (« LIL »), du 6 janvier 1978 ;

V.5. PROCESSUS DE NORMALISATION

L'initiative d'une nouvelle norme européenne provient le plus souvent d'un organisme national de normalisation ou alors de la Commission européenne par le biais d'un mandat de normalisation pour une directive CE. Une fois ratifiée, toute norme européenne (EN) doit être adoptée à l'identique au niveau national. Un moyen efficace d'influer sur le contenu des normes européennes consiste à participer au comité miroir du pays respectif. Cette instance délègue des experts au sein des organismes de normalisation européens, décide, au niveau national, de la position à prendre sur les projets de normes européennes, et accompagne le processus de normalisation dans ses différentes étapes. Participer

[70] *Règlement européen sur la protection des données personnelles - CNIL* [En ligne]. [Réf. 2018]. Disponible sur RGPD en 6 étapes

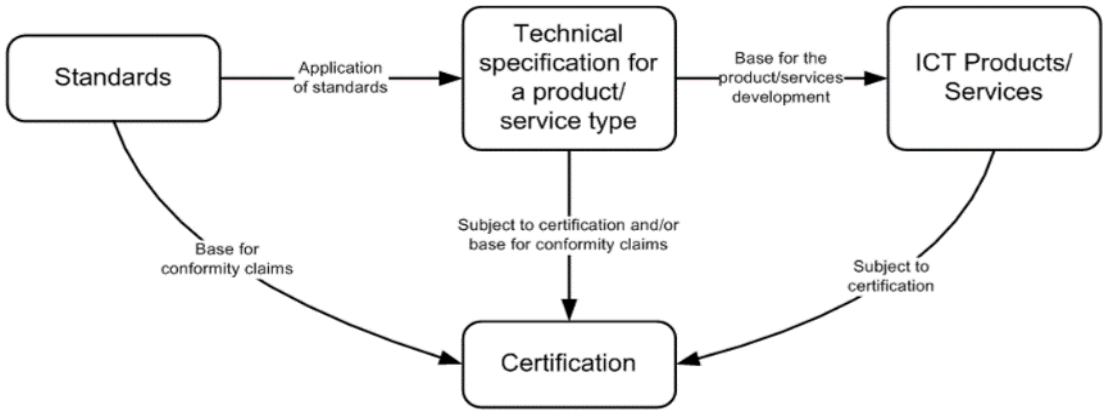
activement, et de préférence à une phase précoce, au travail de normalisation est le meilleur moyen d'influer sur le contenu des normes européennes.[71]

Concernant la cybersécurité en particulier, la normalisation joue un rôle important, comme stipulé dans le Cybersecurity Act[72] :

« Il est nécessaire de renforcer la coopération internationale afin d'améliorer les normes de cybersécurité, notamment par la définition de normes de comportement communes, l'adoption de codes de conduite, l'utilisation de normes internationales et le partage d'informations, la promotion d'une collaboration internationale plus rapide en réponse aux problèmes de sécurité des réseaux et de l'information et la promotion d'une approche mondiale commune de ces problèmes ».

Concernant la certification

Le règlement (UE) 2019/881 (loi sur la cybersécurité), établit un cadre européen de certification de la cybersécurité pour les produits, services et processus TIC. L'ENISA participe à ce nouveau cadre, en préparant des systèmes de certification candidats à la demande de la Commission européenne ou du Groupe européen de coordination de la cybersécurité (représentation des États membres)[73].



7 - Processus de certification à l'ENISA (Source ENISA)

La tâche de certification de la cybersécurité nécessite l'implication et le soutien des parties prenantes appropriées.

L'objectif du cadre de certification de la cybersécurité de l'UE est d'établir et de maintenir la confiance et la sécurité dans les produits, services et processus de cybersécurité. Chaque système spécifiera un ou plusieurs niveaux de garantie (de base, substantielle ou élevée), sur la base du niveau de risque associé à l'utilisation envisagée du produit, du service ou du processus.

L'importance des normes et de la certification occupent une position importante aussi bien pour garantir la maîtrise des exigences en cybersécurité des produits et services utilisés ou délivrés au sein de l'Union européenne et aussi pour parer aux « portes dérobées » (backdoors) éventuelles.

[71] L'élaboration d'une norme européenne - KAN [En ligne]. [Réf. 2021]. Disponible sur L'élaboration d'une norme européenne - KAN

[72] *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013* [En ligne]. [Réf. Du 17 avril 2019]. Disponible sur certification de cybersécurité des technologies de l'information et des communications

[73] *EU Cybersecurity Certification Framework* [En ligne]. [Réf. 2019]. Disponible sur Certification — ENISA (europa.eu)

VI. INITIATIVES ET GROUPES DE TRAVAIL AU NIVEAU EUROPÉEN

Plusieurs initiatives et groupes de travail ont été lancés et accélérés depuis cinq ans environ. Dans le ferroviaire Européen, SHIFT2RAIL est le grand programme phare de transformation de l'industrie ferroviaire. Il regroupe un certain nombre de projets comme nous le verrons dans la suite. L'UIC et l'ENISA en sont les principaux sponsors.

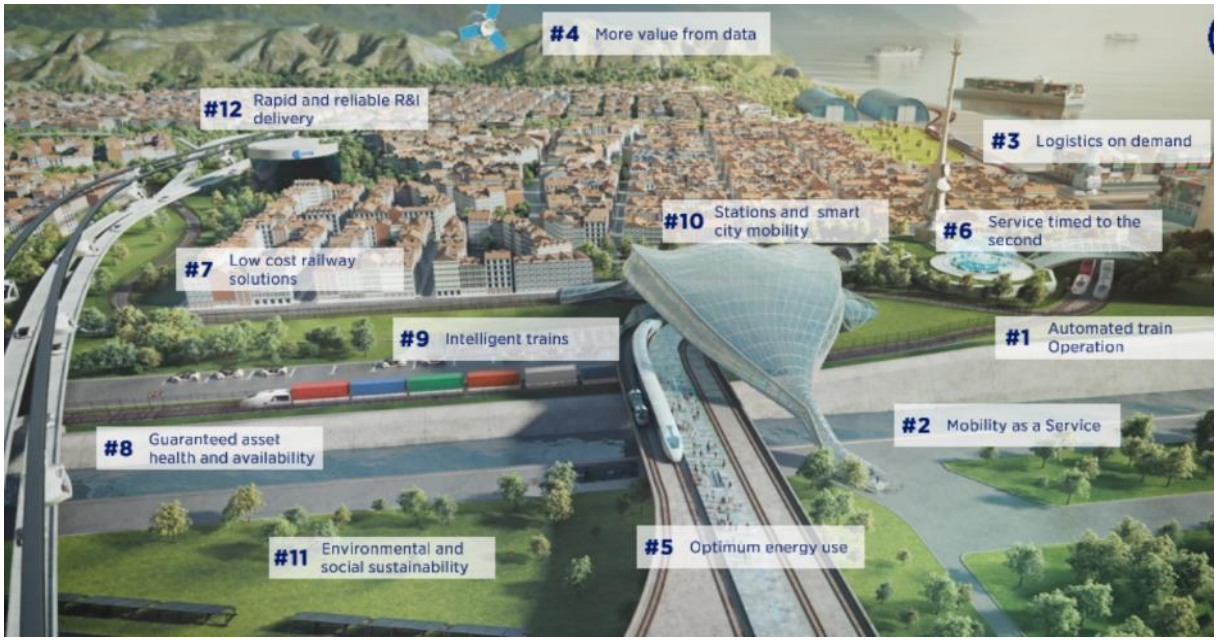
VI.1. SHIFT2RAIL

Shift2Rail[74] est l'initiative majeure dans le domaine ferroviaire en Europe pour construire le système ferroviaire de demain. Elle regroupe 21 États membres actifs : Allemagne, Autriche, Belgique, Bulgarie, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Italie, Lettonie, Lituanie, Luxembourg, Pologne, Portugal, République tchèque, Roumanie, Suède et Norvège.

L'initiative Shift2Rail a été lancée dans le cadre du programme Horizon 2020 pour rechercher des solutions ciblées en recherche et innovation (R&I) axées sur le marché. Elle vise aussi à promouvoir la compétitivité dans l'industrie ferroviaire européenne. Les problématiques de cybersécurité dans le secteur ferroviaire sont largement abordées par exemple, dans le cadre du projet CYRAIL (CYbersecurity in the RAILway sector), ou dans le cadre des projets X2Rail-113 et X2Rail-314.

Shift2rail promeut l'accélération de l'intégration des technologies nouvelles et avancées dans des solutions et produits ferroviaires de pointe[75]**,** avec pour ambition de :

- Réduire jusqu'à 50 % le coût du cycle de vie des transports ferroviaires ;
- Doubler la capacité ferroviaire, augmenter la fiabilité ainsi que la ponctualité à hauteur de 50 %.



8 - Les 12 ambitions du programme Shif2Rail[76]

[74] *Shift2Rail est la première initiative européenne dans le domaine du rail avec une recherche et une innovation ciblées.* [En ligne]. [Réf. 2021]. Disponible sur À propos - Shift2Rail

[75] *Shift2Rail : l'entreprise commune pour construire le système ferroviaire de demain- UNIFE* [En ligne]. [Réf. 2021]. Disponible sur Shift2Rail - UNIFE

[76] *Shift2Rail Capacités* [En ligne]. [Réf. 2021]. Disponible sur Shift2Rail | Capabilities

VI.2. CYRAIL

Cyrail[77] est un Projet du programme Shift2Rail

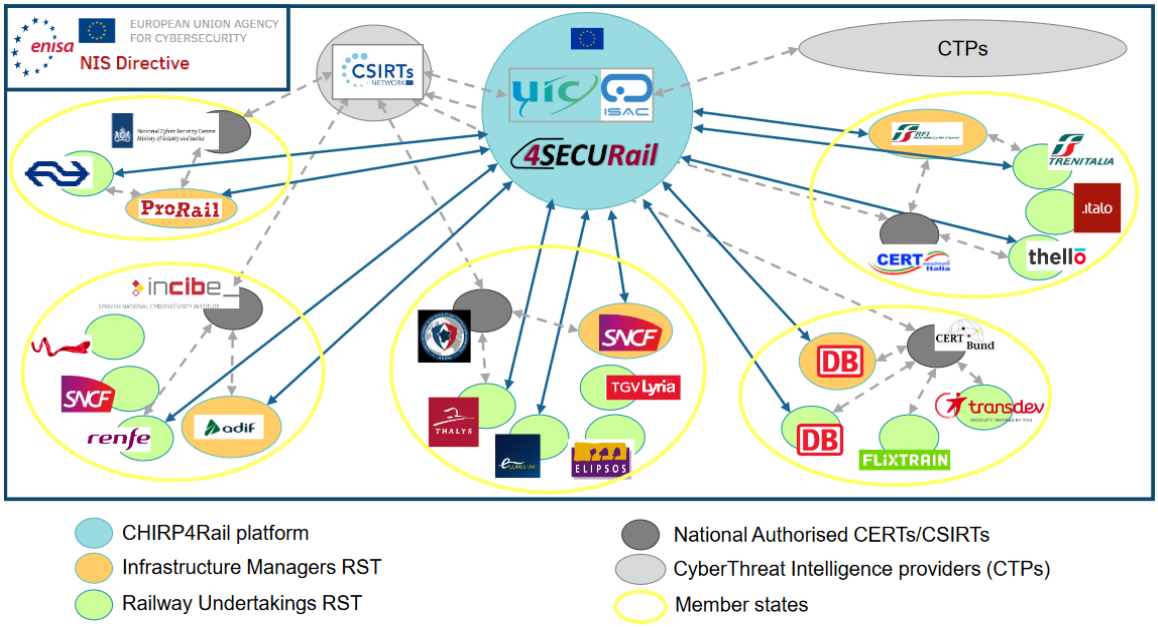
Ce projet a pour objectif de définir à l'échelle européenne :

a) Un **système de détection et d'analyse des menaces** pesant sur les infrastructures ferroviaires
b) Un **dispositif de gestion d'incident et d'alerte en cas d'attaques**.
c) Des **plans d'atténuation et des contre-mesures adaptées** sur la base des impacts potentiels identifiés.
d) Des **profils de protection pour l'évaluation du niveau de cybersécurité des applications de contrôle et de signalisation ferroviaires**.

Cyrail permettra également d'intégrer le concept de Security-by-design pour les nouvelles infrastructures ferroviaires.

VI.3. 4SECURAIL

4SECURail est un projet du grand programme Horizon 2020 visant à la protection de la liberté et la sécurité de l'Europe et de ses citoyens. Le projet 4SECURAIL[78], doté d'un budget de 1,695 milliard d'euros et financé par l'UE, est spécifique à l'environnement ferroviaire et œuvre pour la mise en œuvre d'une équipe de réponse aux cyberattaques (CSIRT). Il s'appuie sur un démonstrateur et définira les exigences des parties prenantes pour une activité collaborative. Un environnement collaboratif CSIRT[79] a été mis en œuvre à cet effet sur la forme d'un modèle de plateforme collaborative dénommé Chirp4Rail avec l'articulation indiquée dans le schéma qui va suivre. Cette plateforme contribuera à mettre en commun les renseignements sur les menaces et d'autres types d'informations entre autres, les modes opératoires, les signatures des cybermalveillants.

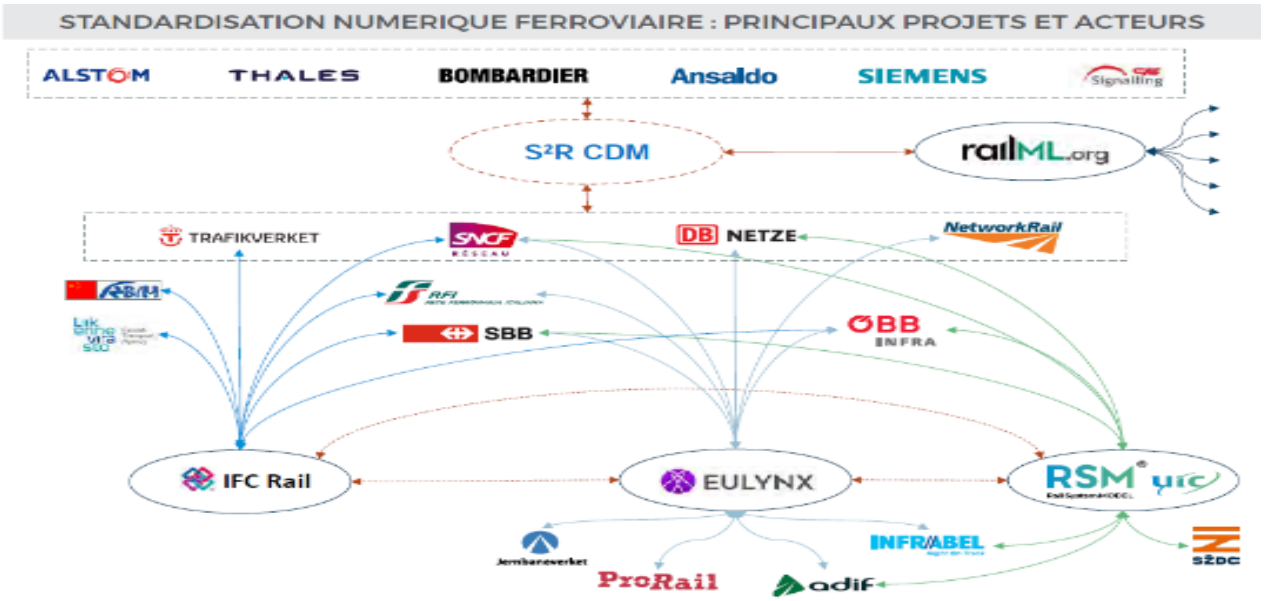


9 - Interactions du projet UIC 4SECURail (Source ENISA)

[77] *CYRail Project - La cybersécurité dans le secteur du chemin de fer.* [En ligne]. [Réf. 2020]. Disponible sur CYRail project
[78] *EU-CSIRT collaborative environment dedicated to rail - ENISA* [En ligne]. [Réf. 16-17 March 2021]. Disponible sur 4SECU Rail
[79] *Un sous-système de signalisation pour les voies ferrées – EUROPA.EU* [En ligne]. [Réf. 2019]. Disponible sur MÉTHODES FORMELLES ET CSIRT POUR LE SECTEUR FERROVIAIRE

VI.4. LINX4RAIL

Courant 2021, Shift2Rail a lancé le projet LinX4Rail avec pour but de consolider les différentes initiatives **de standardisation numériques au sein des compagnies ferroviaires**[80]. Le schéma ci-dessous donne une idée des acteurs et des interactions et des synergies autour de ce projet comme c'est le cas dans la plupart des projets Shift2Rail.



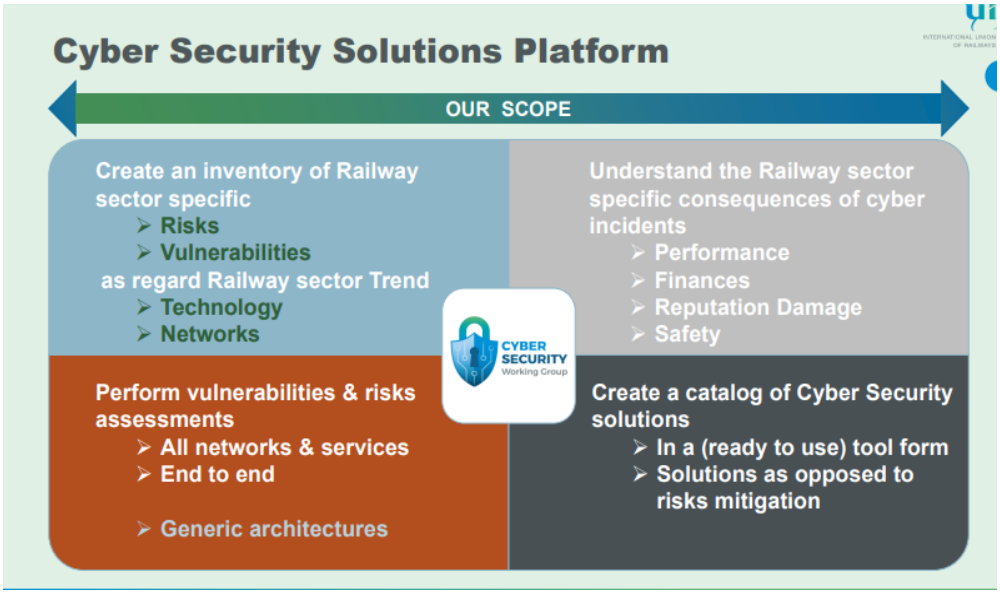
10 - Quelques acteurs du transport ferroviaire au sein de l'Union européenne[81]

VI.5. CYBER SECURITY SOLUTIONS PLATFORM PROJECT

Le projet « Cyber Security Solutions Platform Project », lancé en 2020 et dans le cadre du groupe de travail Cyber Security de l'UIC, vise à développer d'ici 2025 une Plateforme adressant les problématiques très opérationnelles de cybersécurité propres au transport ferroviaire au sein de l'U.E.

Le projet a pour mission de consolider l'inventaire des risques et vulnérabilités, les impacts des incidents cyber (cf. schéma ci-dessous). À cela s'ajoutent une démarche d'évaluations des risques et un catalogue de solutions cyber spécifiques au secteur ferroviaire.

[80] UIC, *Solutions techniques pour le rail opérationnel.* [En ligne]. [Réf. du 10 mai 2021]. Disponible sur https://uic.org/IMG/pdf/uic-solutions-techniques-pour-le-rail-operationnel.pdf
[81] UIC, *Solutions techniques pour le rail opérationnel.* [En ligne]. [Réf. du 10 mai 2021]. Disponible sur https://uic.org/IMG/pdf/uic-solutions-techniques-pour-le-rail-operationnel.pdf



11 - Périmètre de la Cybersecurity Platform (Source ENISA)[82]

VI.6. GROUPE DE TRAVAIL WG 26 RAILWAY APPLICATIONS – CYBERSECURITY

CENELEC est le Comité européen de normalisation en électronique et en électrotechnique

Le comité CENELEC TC 9X « Applications électriques et électroniques dans le domaine ferroviaire » dispose d'un groupe de travail dédié « CLC/TC 9X/WG 26: IT-Security / Cybersecurity in the railway sector[83]».

Ce groupe de travail regroupe environ 90 experts de 13 pays avec l'ERA et l'ENISA en tant qu'observateurs. Il a été chargé d'établir des spécifications techniques pour la gestion de la cybersécurité dans l'ensemble du secteur ferroviaire ; spécifications qui doivent se baser sur les normes et standards de sécurité et de cybersécurité industrielle déjà existantes (notamment la EN 50126 relatives à la Fiabilité, la Disponibilité, la Maintenabilité et de la Sécurité (FDMS) des appareils et systèmes ferroviaires [84]et l'IEC 62443 pour la prise en compte de l'évaluation des risques, des exigences de cybersécurité en milieu industriel)

Le challenge fixé à ce groupe de travail est de résoudre le double paradoxe :

a) Proposer des solutions répondant aux exigences de sûreté, mais suffisamment ouvertes pour accepter les évolutions du marché ;
b) Concilier les durées de vie assez longue pour rentabiliser le coût de possession des matériels ferroviaires avec un cycle de vie adapté pour être en mesure de fixer les vulnérabilités IT émergentes au plus tôt.

Ce groupe de travail WG26[85] a été missionné pour dégager une démarche normative CENELEC unifiant les deux processus sur les thématiques suivantes[86] :

- Modèle d'architecture ferroviaire et exemple de zonage ;

---

[82] *CYBER SECURITY SOLUTION PLATFORM PROJECT* - UIC [En ligne]. [Réf. du 22 mars 2021]. Disponible sur Cyber Security Solution Platform (europa.eu)
[83] *Les réseaux ferroviaires, qui font partie intégrante des infrastructures critiques, continuent de faire l'objet de cyberattaques. - IEC E-TECH* [En ligne]. [Réf. Du 15 mars 2018]. Disponible sur Protecting railway networks from cyber threats
[84] *Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Generic RAMS Process* [En ligne]. [Réf. Du 6 décembre 2017]. Disponible sur Railway Applications. The Specification and Demonstration of Reliability
[85] *Security measures in the Railway Transport Sector – ENISA* [En ligne]. [Réf. De novembre 2020]. Disponible sur RAILWAY CYBERSECURITY
[86] *Railway CyberSecurity challenges* [En ligne]. [Réf. 2021]. Disponible sur 4 status update on cenelec wg 26 benoliel schlehuber

- Exigences de sécurité ;
- Principes de conception de la cybersécurité ;
- Interface Cybersécurité & Sécurité ;
- Prise en compte des systèmes patrimoniaux ;
- Méthodes d'acceptation des risques.

Lancé en juillet 2017, ce groupe de travail a rendu publics les résultats de ses travaux sous la forme d'une Spécification Technique, la TS 50701 publiée en juillet 2021. C'est la première étape vers son adoption comme norme internationale.

VI.7. LE PROJET HONEYTRAIN

Ce projet lancé en 2015 s'inscrivait dans le cadre du programme Shift2Rail et vise à **simuler virtuellement l'écosystème IT et industriel ferroviaire, y attirer les cybermalveillants et observer leurs techniques tactiques et procédures**. Il a été lancé pour 6 semaines. Et en seulement 6 semaines, le système a enregistré près 2,7 millions d'attaques[87]. Un des attaquants a réussi à accéder à la configuration des composants industriels et, dans un cas, à la signalisation, qui comme on le sait est essentielle pour la sécurité. Ce type d'attaque ne pouvait être possible qu'avec une connaissance approfondie des systèmes SCADA utilisés dans l'infrastructure ferroviaire[88]. Cela permet de comprendre selon Israël Baron, ancien RSSI d'Israël Railways que de nombreux attaquants cherchent à s'infiltrer dans au cœur de l'infrastructure industrielle des systèmes ferroviaires[89].

VII. CYBERSÉCURITÉ/CYBERDÉFENSE : ORGANISATION A L'ÉCHELLE EUROPÉENNE

VII.1. DEVELOPPEMENT DE COMPETENCE ET SENSIBILISATION

Assurer la sécurité numérique de presque 747 millions d'Européens n'est possible qu'avec le partage de connaissances, la sensibilisation de toutes les parties prenantes et grâce au renforcement des capacités. Nous pensons ici, aussi bien aux compétences humaines qu'aux infrastructures[90].

Le Conseil et le Parlement européen sont parvenus en décembre 2020 à un accord informel pour un Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité. Ce Centre,[91] soutenu par un réseau de centres nationaux de coordination, aura pour vocation parmi d'autres missions à[92] :

- Soutenir les jeunes entreprises et les PME du secteur de la cybersécurité ;
- Renforcer la recherche et l'innovation en matière de cybersécurité ;
- Contribuer à combler le déficit de compétences en matière de cybersécurité.

---

[87] *KeTech – Connected Driver Advisory System* [En ligne]. [Réf. Du 4 décembre 2019]. Disponible sur Signalling and Telecoms – Rail Engineer (rssing.com)
[88] *La cybersécurité des chemins de fer et des métros - Où en est l'industrie ?* [En ligne]. [Réf. 2021]. Disponible sur Rail and Metro Cybersecurity - The First Global Cyber Security Observatory (cyberstartupobservatory.com)
[89] *Questions et réponses sur la cybersécurité ferroviaire - Israel BARON* [En ligne]. [Réf. 2021]. Disponible sur The First Global Cyber Security Observatory
[90] *Qu'est-ce que l'Agence européenne de cybersécurité ? - ENISA* [En ligne]. [Réf. Du 20 avril 2021]. Disponible sur Qu'est-ce que l'Agence européenne de cybersécurité ? - Oodrive
[91] *Le Centre de compétences en matière de cybersécurité, basé à Bucarest, obtient le feu vert du Conseil* [En ligne]. [Réf. Du 20 avril 2021]. Disponible sur Le Centre de compétences en matière de cybersécurité, basé à Bucarest, obtient le feu vert du Conseil - Consilium (europa.eu)
[92] *Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination* [En ligne]. [Réf. Du 4 décembre 2019]. Disponible sur ST-5628-2021-INIT

Le directoire général en charge des questions des mobilités et des Transports (DG MOVE) au sein de la Commission Européenne s'est engagé dans le développement d'une boîte à outils pour améliorer la sensibilisation et la préparation des parties prenantes du secteur des transports aux menaces cyber[93]. Cette boîte à outils fournit des moyens pour mieux maîtriser les menaces cyber et contenir leurs impacts sur les services de transport, les systèmes et les opérations y afférentes.[94]

Ce développement de compétences et surtout la sensibilisation des populations européennes sont la priorité des priorités quand on sait que le premier maillon à même de garantir la cybersécurité est l'humain. Sa moindre baisse de garde peut être une faille (même minime) pouvant être exploitée en vue d'une attaque de grande ampleur.

VII.2. LE RESEAU CYCLONE

Lors de la 12e édition du Forum International de la Cybersécurité (FIC) en janvier 2020, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) a appelé au développement d'une souveraineté européenne en matière de cybersécurité ainsi qu'à la promotion, au niveau international, des valeurs européennes pour la paix et la stabilité du cyberespace[95].

Bien que disposant de solides bases en matière de sécurité numérique en Europe, l'organisation d'une gestion de crise cybernétique au niveau international est essentielle. Le caractère transnational du cyberespace des cyberattaques impose une organisation commune des dispositifs nationaux, européens et internationaux.

Au travers de la future NIS 2, la directive crée un réseau européen pour la préparation et la gestion des crises cyber par les États membres appelé UE-CyCLONe (Cyber Crises Liaison Organisation Network). CyCLONe représente :

- Un groupe de coopération pour soutenir et faciliter la coopération stratégique et l'échange d'informations entre les États membres ;
- Un réseau des CSIRT afin de promouvoir une coopération opérationnelle rapide et effective.

UE-CyCLONE contribuera à la gestion coordonnée des incidents et crises de grande ampleur en matière de cybersécurité, et de garantir au travers d'une communication multimodale d'échanges réguliers d'informations entre les États membres et les institutions, organes et agences de l'Union.

La Commission devra mettre en place un système d'évaluation, permettant de valider les politiques de cybersécurité des États membres et un examen collégial régulier pour en contrôler l'efficacité.

La directive CyCLONe c'est aussi :

- Un renforcement des obligations en matière de gestion et de signalement des risques de cybersécurité ;
- Une extension des obligations des organismes assujettis ;
- Un régime pour les entités dites essentielles et celles dites importantes.

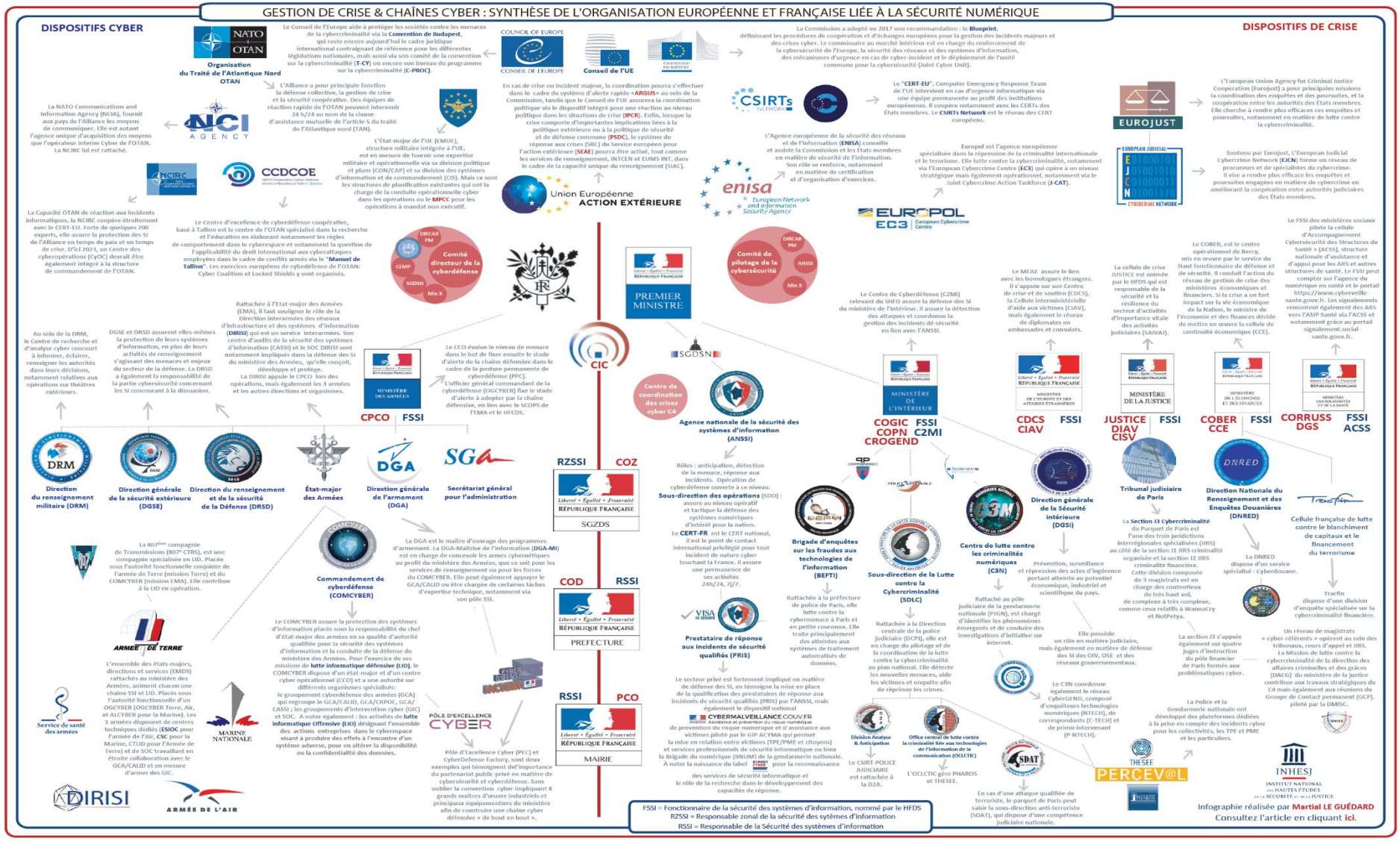
---

[93] *La Commission européenne publie une "boîte à outils de cybersécurité"* [En ligne]. [Réf. Du 16 décembre 2020]. Disponible sur cybersecurity-toolkit_fr.pdf

[94] *NOUVEAU Kit d'outils de cybersécurité de la CE pour les transports* [En ligne]. [Réf. Du 18 décembre 2019]. Disponible sur NEW EC Cybersecurity Toolkit for transport - UETR

[95] *FIC 2020 : L'ANSSI PLAIDE POUR UNE SOUVERAINETÉ EUROPÉENNE EN MATIÈRE DE CYBERSÉCURITÉ - ANSSI* [En ligne]. [Réf. Du 28 au 30 janvier 2020]. Disponible sur FIC 2020 : souveraineté européenne en matière de cybersécurité

L’ENISA (European Network Information Security Agence) sera tenue, en coopération avec la Commission, de réaliser un rapport tous les six mois sur l’état de la cybersécurité dans l’Union.



12 - Cartographie des acteurs de la communauté étatique cyber française et européenne – juillet 2020[96]

[96] *L'infographie originale réalisée par Martial LE GUEPARD – IHEMI* [En ligne]. [Réf. 2021]. Disponible sur L'infographie originale

VII.3. GESTION D'INCIDENTS ET DE CRISE A L'ECHELLE EUROPEENNE

Le projet HoneyTrain a montré s'il en était encore besoin l'attrait du secteur ferroviaire par les cybermalveillants. Au-delà des capacités de protection, de détection, cette cyber-résilience passe par une force de réaction aux incidents et d'un dispositif éprouvé de gestion de crise au niveau des entreprises et des États. Les cas de cyberattaque d'ampleur pouvant affecter les Opérateurs de Services Essentiels (OSE) ne sont plus légion.

L'Union européenne s'est dotée de capacités de réponses afin de faire face aux cybermenaces et à la cybercriminalité. Un modèle de réponse a clairement été élaboré pour donner aux États les moyens d'apporter une réponse forte en cas de crise majeure d'origine cyber. Néanmoins, ce modèle n'apporte pas toutes les réponses et des interrogations existent. Le périmètre de chacune des institutions n'est pas suffisamment défini et est rarement partagé de tous, réduisant malheureusement la capacité d'une intervention commune et forte.

La cartographie[97] (voir plus loin la figure « *Cartographie des acteurs formant la communauté étatique cyber française et européenne* ») amorcée en 2019 a été complétée par un tableau d'acteurs qui peuvent avoir un rôle dans la gestion et le traitement d'une crise ou d'un incident d'origine cyber. Il est intéressant de bien identifier les liens entre la chaîne de commandement territorial, les différentes chaînes de commandement ministériel et le secteur privé.

VII.4. CRISE CYBER ET ARTICULATION DES CHAINES DE COMMANDEMENT

Nous allons prendre le cas de la France. De manière globale, il est nécessaire de noter qu'en dehors des spécificités liées à chaque ministère, une organisation générale permet à chaque ministère de garder la responsabilité de la sécurité de ses systèmes d'information. L'organisation repose alors sur les HFDS (Haut Fonctionnaire de Défense et de Sécurité), accompagnant chaque ministre, assisté d'un FSSI (Fonctionnaire de Sécurité des Systèmes d'Information), responsable de la politique SSI du ministère. En parallèle chaque ministère désigne des AQSSI (Autorités Qualifiées en Sécurité des Systèmes d'Information), responsables de la sécurité des SI au sein de leur périmètre.

Au niveau des différents échelons administratifs, des RZSSI (Responsable Zonal de la Sécurité des Systèmes d'Information) et des RSSI (Responsable de la Sécurité des Systèmes d'Information) sont nommés et appuient le préfet de zone ou de département, en charge des risques cyber sur leur territoire.

Le dispositif institutionnel de gestion des incidents cyber a particulièrement été structuré, mettant en place des espaces de discussions interministérielles, un plan dédié, des périmètres d'intervention parfaitement définis en fonction des responsabilités de chacun. Il est néanmoins à noter que la connaissance dans la gestion de crise de ses différents acteurs est prégnante et pose problème dans la mise en œuvre d'une réponse optimale à la crise. Comment alerter, lorsque l'on ne connaît pas les différentes parties prenantes possédant la capacité de vous soutenir ?

La réalisation d'un document unique de cartographie des acteurs est nécessaire, apportant une aide aux différentes parties prenantes impliquées dans la gestion de crise.

---

[97] *Gestion de crise et chaînes cyber : organisation européenne et française* [En ligne]. [Réf. Du 3 juillet 2020]. Disponible sur Gestion de crise et chaînes cyber : organisation européenne et française | IHEMI

Afin d'évaluer les capacités de réponse à incident cybercriminel des services de l'État sur l'ensemble du territoire, impactant notamment des systèmes industriels de contrôle et commande, il a été développé des scénarios de crise majeure et multiacteurs, auxquels l'ensemble des acteurs se verraient mobilisés.

Plusieurs éléments sont à prendre en compte au niveau territorial :

Il est nécessaire de prendre en compte les attaques ayant pour origine extérieure aux frontières, mais aussi les conséquences potentielles d'une attaque impactant plusieurs pays. Pour toutes les nations ayant signé le traité de Lisbonne du 13 décembre 2007 et entré en vigueur le 1er décembre 2009, l'Union européenne a mis à disposition les capacités de réaction coordonnée face aux incidents et crises cyber. Chaque organisation gouvernementale a l'obligation de s'appuyer sur son MEAE (Ministère de l'Europe et des Affaires étrangères) et sa cellule de crise CDCS (Centre de Crise et de Soutien, Crisis and Support Centre), afin d'assurer les échanges avec les centres de crises des gouvernements étrangers et des organisations internationales (Union européenne, Organisation du Traité de l'Atlantique Nord, etc.).

L'ANSSI ne possède pas, à ce jour, de maillage territorial en région hors l'existence de 13 délégués territoriaux. Elle concentre son activité sur les OIV, OSE et FSN (Fournisseurs de Services Numériques). En cas de crise majeure impliquant des services de l'État et/ou des SIE (Systèmes d'Information Essentiels) d'un OIV, mais potentiellement des sites non classés OIV, OSE ou Seveso, comme des salles de spectacles ou de cinéma, c'est l'ensemble des chaînes de commandement présentées dans la cartographie dont l'ANSSI qui seraient mises à contribution pendant et après la crise en fonction de leur périmètre respectif.

Ce serait le cas notamment si l'on était confronté à une attaque d'ampleur mettant en danger la vie de citoyens comme cela peut être le cas dans le ferroviaire, ou affectant d'importantes parties du tissu économique.

VIII. GUERRE ÉCONOMIQUE À L'ÉCHELLE MONDIALE

Le cyberespace est devenu de nos jours un espace d'opportunités de développement, mais aussi de guerre économique et de conflictualités de tous ordres.

VIII.1. LE FERROVIAIRE, PUISSANT LEVIER DE DEVELOPPEMENT

Le chemin de fer est un puissant levier de développement. Il est considéré comme le moyen de transport de choix pour réduire la facture climatique. C'est aussi un moyen de conquête et d'influence dans le monde.

Malgré ces bienfaits, on ne relève pas un engouement et des investissements conséquents dans de nombreux pays en développement. Le rapport de la banque mondiale révèle que les services de transports ferroviaires sont délaissés pour des raisons diverses et variées[98] :

- Service ferroviaire non compétitif et mal intégré aux autres formes de transport ;
- Prix élevés et manque de fiabilité poussant les clients potentiels à utiliser d'autres modes de transport.

Et pourtant plusieurs actions ont été menées par la Banque Mondiale, dans le but d'inciter les pays en développement à attirer le plus de personnes et permettre au fret ferroviaire

[98] *Railways* [En ligne]. [Réf. Du 2022]. Disponible sur Railways (worldbank.org)

d'être plus efficace et bien géré. La Banque Mondiale a par ailleurs financé un certain nombre de projets, par exemple :

- En Chine, le projet ferroviaire de GuiGuang reliant les régions moins développées du sud-ouest au delta de la rivière des Perles. Douze nouvelles lignes ont été construites dans le but d'améliorer la connectivité ferroviaire des régions les plus pauvres de Chine et favoriser la croissance économique, cette liaison a contribué grandement à faciliter pour les populations la recherche et l'obtention de meilleurs emplois et développé aussi bien le tourisme interne qu'externe.
- En Inde, la Banque mondiale finance un corridor dédié au fret pour répondre à la demande croissante du pays en matière de transport économe en énergie. Au cours des 30 prochaines années, le projet réduira de 67 millions de tonnes les émissions de gaz carbonique.

D'autres projets, notamment ceux relatifs aux travaux de recherches et d'analyses, ont également fait l'objet de financement de la Banque mondiale pour le développement du ferroviaire dans plus de 20 pays. En Afrique, en Asie, au Moyen-Orient et en Europe de l'Est, la Banque soutient 16 projets d'investissement d'une valeur de 6,9 milliards de dollars américains.

La Banque mondiale participe également dans le développement des connaissances en matière de gouvernance du secteur ferroviaire, en développant des liens multimodaux ayant un impact sur la pauvreté dans le monde entier. Le document intitulé « *Transport et TIC. 2017. Réforme des Chemins de fer : Toolkit pour améliorer la performance du secteur ferroviaire. Washington, DC : Banque mondiale, licence : Creative Commons Attribution CC by 3.0* »[99] est un recueil fort intéressant de multiples travaux dirigés en la matière par la Banque Mondiale.

VIII.2. ENJEUX ECONOMIQUES ET DOMAINES DE CROISSANCE

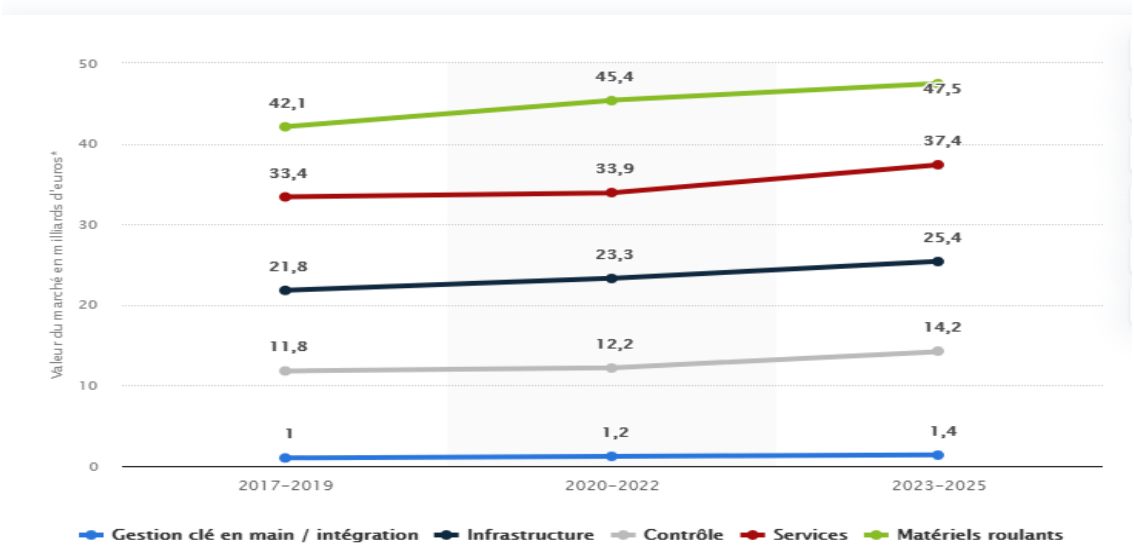
Une étude récente montre que dans le monde, la marge de progression du marché du secteur est considérable. **Pour se faire une idée, on ne serait qu'à environ 10% de ce que sera le secteur ferroviaire dans les 30 ans à venir**. Beaucoup de choses dans le domaine du transport ferroviaire restent encore à faire. Le potentiel de développement est considérable. Le ferroviaire est un vivier d'opportunités aux États-Unis, en Asie, en Amérique latine ou encore en Russie, sans oublier l'Europe bien entendu[100].

Depuis 2018, le réseau ferroviaire mondial a été étendu de 23 300 kilomètres et le nombre de véhicules a augmenté de 20 000 unités. Les experts s'attendent à un taux de croissance annuel moyen de 2,3% jusqu'en 2025. Le volume total du marché devrait atteindre 204 milliards d'euros d'ici 2025 contre 177 milliards d'euros à la fin de 2019[101] . Ce marché couvre tous les secteurs du schéma qui suit :

[99] *Manuel pour l'Amélioration de la Performance du Secteur Ferroviaire* [En ligne]. [Réf. Du septembre 2017]. Disponible sur La Réforme des Chemins de Fer

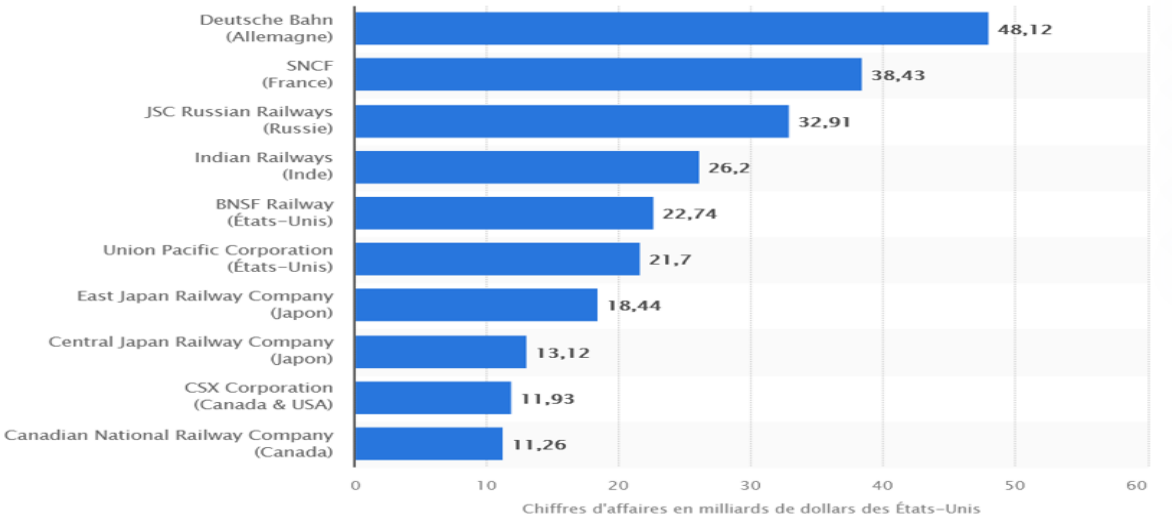
[100] *Le secteur ferroviaire en France et dans le monde: un exceptionnel potentiel de croissance* [En ligne]. [Réf. Du 9 septembre 2020]. Disponible sur Le secteur ferroviaire en France et dans le monde

[101] *Le marché mondial du rail devrait croître d'ici 2025 - l'UNIFE* [En ligne]. [Réf. Du 2 octobre 2020]. Disponible sur Global railway market is expected to grow until 2025



13 - Valeur du marché ferroviaire mondial en milliards d'euros de 2017 à 2025[102]

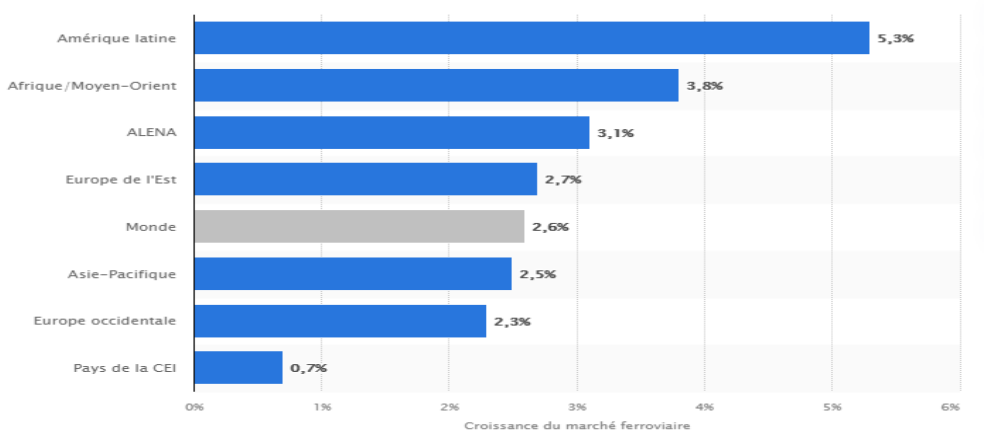
Ces chiffres sont trompeurs, car le marché accessible est largement moindre, étant donné que certains pays comme la Chine et le Japon réservent souvent les contrats aux seules entreprises locales. En termes de répartition du marché ferroviaire, la CRRC (China Railway Rolling Stock Corp)[103] arrive avec 30 milliards d'euros de chiffre d'affaires environ (dont 4 ou 5 milliards à l'international) et donne de fortes raisons d'inquiétude à Alstom et Siemens[104]. Depuis deux ans, CRRC a gagné quasiment tous les contrats de métro et de tramway aux États-Unis à l'exception de celui de Washington[105]. La CRCC se déploie de plus en plus à travers le monde et est présente dans 104 pays et régions avec 83 % des pays équipés de lignes ferroviaires. Derrière on retrouve en termes de poids financiers, les constructeurs Alstom Transport, Siemens Mobility et le canadien Bombardier.



14 - Chiffre d'affaires des plus grandes sociétés ferroviaires du monde (2019)

[102] *Valeur du marché ferroviaire mondial accessible de 2017 à 2025, selon le produit – STATISTA* [En ligne]. [Réf. Du 4 aout 2021]. Disponible sur Marché ferroviaire mondial par produit 2025 | Statista
[103] *China Railway Rolling Stock Corp* [En ligne]. [Réf. 2022]. Disponible sur CRRC - Company Profile
[104] *CRRC, le géant chinois qui fait peur à Alstom et Siemens – LES ECHOS* [En ligne]. [Réf. Du 6 février 2019]. Disponible sur Le géant chinois qui fait peur à Alstom et Siemens
[105] *CRRC a signé le contrat de voitures du métro de Los Angeles aux Etat-Unis* [En ligne]. [Réf. Du 19 avril 2017]. Disponible sur CRRC a signé le contrat de voitures du métro

Avant 2020, une grande partie de la croissance ferroviaire avait lieu dans la région Asie-Pacifique et en Europe occidentale.



15 - Prévision de croissance du marché ferroviaire mondial 2021-2023 à 2015-2017[106]

VIII.2.1. DOMAINE DE CROISSANCE DE L'EUROPE

L'Europe a son grand marché ferroviaire avec Rail Baltica, l'un des grands projets d'infrastructure ferroviaire en Europe dont on parle si peu. Premier projet européen avec des voies à écartement standard UIC de bout en bout, il est destiné à relier la Finlande, l'Estonie, la Lettonie, la Lituanie à la Pologne en passant par la Lettonie et la Lituanie. Ce projet a émergé depuis 1994, mais a mûri très lentement. Le rapport de la Cour des comptes européenne, publié en juin 2020, épingle les délais et coûts de financement du projet : quatre ans de retard prévu pour une finalisation en 2030 au lieu de 2026 et un dépassements de budget, sept milliards d'euros au lieu de cinq initialement.

16 - Le projet Rail Baltica[107]

Un potentiel de développement énorme existe aussiaux États-Unis. Bien que disposant du réseau ferroviaire le plus étendu du monde en termes de kilomètres de voies (bien plus que la Chine), les États-Unis sont confrontés à une demande importante affectant certains nœuds ferroviaires. Un marché ouvert aux trains autonomes pour désengorger certains

[106] *Prévision de la croissance du marché ferroviaire mondial, selon la zone géographique – STATISTA* [En ligne]. [Réf. Du 4 aout 2021]. Disponible sur Variation du marché ferroviaire mondial par régions
[107] *Le projet Rail Baltica* [Réf. D'aout 2020]. Disponible sur tent-t corridors - Railway Technology (railway-technology.com)

maillons de la chaîne d'approvisionnement du pays en raison d'une activité inédite dans les ports[108].

VIII.2.1. DOMAINE DE CROISSANCE DES AMÉRIQUES

L'Amérique latine a les prévisions de croissance les plus élevées sur le marché du contrôle ferroviaire en raison d'investissements importants dans le secteur du fret. Le marché de l'offre ferroviaire devrait également connaître une demande soutenue de la part de marchés matures comme l'ALENA (accord de libre-échange en USA-Canada-Mexique) et l'Europe occidentale. Dans l'ensemble, le contrôle et l'infrastructure ferroviaires devraient croître au rythme le plus élevé, tandis que le matériel roulant et les services resteront probablement les segments les plus importants[109].

VIII.2.2. DOMAINE DE CROISSANCE ASIE-PACIFIQUE

La croissante sur la partie Asie-Pacifique est en grande majorité portée par la Chine

« Présent dans 104 pays et régions, couvrant 83 % des pays équipés de lignes ferroviaires, CRRC frappe à la porte de l'Europe. La Chine a échoué par deux fois à s'offrir une entreprise .. pour se constituer sur le Vieux Continent une tête de pont - certains diront un cheval de Troie. » . Aujourd'hui, il est clair que le chinois CRRC frappe à la porte de l'Europe et vise le marché mondial.[110] et s'apprête à "'avaler" l'Europe[111]. L'acquisition en mai 2020 par la CRRC du groupe allemand Vossloh, spécialisé dans les infrastructures ferroviaires est un signal qu'on ne fera pas semblant d'ignorer. *"L'exemple d'Alstom-Siemens doit être un exemple emblématique de ce qu'il ne faut plus faire, c'est-à-dire nous empêcher de nous rassembler pour peser face aux géants chinois ou face aux géants américains"[112].* Quels échos à ces mots du ministre Français des finances Bruno le Maire ?

VIII.3. CROISSANCE IMPARABLE DU FERROVIAIRE CHINOIS ET SON INFLUENCE MONDIALE

Nous nous intéressons spécifiquement à l'industrie ferroviaire chinoise pour plusieurs raisons :

- La fulgurance de son développement en 12 ans ;
- Sa pénétration grandissante dans l'espace et le marché européen ;
- La stratégie de la Chine qui utilise le ferroviaire comme levier de développement, d'influence économique en Asie, en Europe et dans le monde.

Lors de la crise de 2008, la Chine a fait le choix d'investir massivement dans les infrastructures pour la circulation de trains à grande vitesse dans le but de stimuler sa croissance.

---

[108] *Les trains autonomes sont sur la bonne voie pour accroître le fret aux États-Unis – Economie - L'Opinion* [En ligne]. [Réf. Du 14 octobre 2021]. Disponible sur Les trains autonomes

[109] *Le marché ferroviaire mondial continue de croître malgré la baisse des volumes de transport due au COVID-19 - Andreas Schwilling* [En ligne]. [Réf. Du 2 octobre 2020]. Disponible sur Marché mondial ferroviaire unife 2020

[110] *L'Europe, terre de conquête pour les acteurs du ferroviaire – LES ECHOS* [En ligne]. [Réf. Du 6 février 2019]. Disponible sur L'Europe, terre de conquête pour les acteurs du ferroviaire

[111] CRRC, Le géant chinois du ferroviaire prêt à avaler l'europe. Thomas Leroy avec Jean-Baptiste Huet [En ligne]. [Réf. Du 19 février 2020]. Disponible sur https://www.bfmtv.com/economie/entreprises/industries/crrc-le-geant-chinois-du-ferroviaire-pret-a-avaler-l-europe_AV-202002190220.html

[112] *Bruno Le Maire fustige le rachat de Vossloh Locomotives par CRRC après l'échec de la fusion Alstom-Siemens* , Simon Chodorge [En ligne] [Réf. d 02 Septembre 2019]. Disponible sur https://www.usinenouvelle.com/article/bruno-le-maire-fustige-le-rachat-de-vossloh-locomotives-par-crrc-apres-l-echec-de-la-fusion-alstom-siemens.N879390

Le rapport de la banque mondiale montre, pour le cas de la Chine, une expansion spectaculaire de son réseau ferroviaire au cours des 30 dernières années. La moitié de l'ensemble du réseau LGV ferroviaire mondial se trouve désormais en Chine.

« En 1949, la Chine n'avait que 22 000 km de lignes de chemin de fer mal entretenues et endommagées par la guerre, dont moins de 1000 km doublés et aucune ligne n'étaient électrifiés. Depuis, le gouvernement chinois a élargi le réseau ferroviaire de plus que cinq fois et a totalement transformé la qualité et la capacité de son secteur ferroviaire. Le réseau à grande vitesse a particulièrement connu une croissance extraordinaire et représente maintenant environ la moitié de toutes les lignes ferroviaires à grande vitesse dans le monde. » [113]

17 - Les plus grands réseaux ferroviaires LGV du monde[114]

Le développement rapide du transport ferroviaire chinois se poursuit aussi bien dans le transport de marchandises que celui de passagers dans le cadre d'une structure fortement centralisée. À noter toutefois que, le secteur n'est pas complètement monolithique et fait participer plusieurs grandes entreprises de chemins de fer, des réseaux industriels et des entreprises de chemins de fer locaux dans le cadre d'une Joint-Venture. À la fin de 2015, le réseau chinois avait déjà atteint 121 000 km, avec 50% du réseau doublé et plus de 60% électrifié. À la mi-2016, la Commission Nationale chinoise de Développement et de Réforme (CNDR) a publié le plan quinquennal de développement pour les chemins de fer chinois, révisant son objectif à 175 000 km de lignes d'ici 2025. Toutefois, le rapport révèle une faible utilisation du transport intermodal de la chaîne d'approvisionnement malgré le succès des itinéraires long-courriers des réseaux de fret ferroviaire réussis. En douze ans après l'ouverture de sa première ligne à grande vitesse (LGV) lors des JO de Pékin en 2008, la Chine prévoyait de doubler la taille de son réseau Grande Vitesse (GV) au cours des quinze prochaines années. Les temps de trajet ont diminué, l'économie du pays a explosé avec plus de 800 millions de Chinois sortis de la pauvreté. Entre 2000 et 2018, 47% de la population est passée de la pauvreté à la classe moyenne.

La croissance du ferroviaire chinois est impulsée par des objectifs et des agendas politiques et géostratégiques. Elle bénéficie aussi de leviers économiques très avantageux, notamment les coûts de main-d'œuvre et d'acquisition de terrains qui sont moins chers en Chine. À titre de comparaison, 1 km de TGV coûte en Europe entre 25 et 39 millions de dollars, aux USA environ 59 millions de dollars et en Chine 17 millions de dollars. Aussi, d'autres chiffres sont assez parlants, en 1980 le PIB chinois était à 43% du PIB français et 11% du PIB américain. En 2020, le PIB chinois est monté à 5.8 fois le PIB global français et est à hauteur de 71% du PIB américain avec une tendance en continuelle hausse même si le PIB par habitant reste 3 fois moins par ailleurs par rapport à la France.

---

[113] *Manuel pour l'Amélioration de la Performance du Secteur ferroviaire* [En ligne]. [Réf. De septembre 2017]. Disponible sur RR Toolkit FR

[114] *Les plus grands réseaux ferroviaires à grande vitesse – STATISTA* [En ligne]. [Réf. Du 26 juin 2020]. Disponible sur Les plus grands réseaux ferroviaires à grande vitesse

VIII.3.1. CHINA RAILWAY EXPRESS, LA NOUVELLE ROUTE DE LA SOIE

Lancée par le président Xi Jinping en 2013, la *Belt and Road Initiative* (BRI) vise à bâtir des réseaux commerciaux et d'infrastructures reliant l'Asie et l'Europe[115]. Ce projet chinois repose sur une stratégie de « cinq connectivités » (*wu tong*), dans lesquelles **les infrastructures de transport représentent un domaine prioritaire juste après la connectivité politique, et devant les connectivités commerciale, financière et interpersonnelle**[116] . À travers les corridors ferroviaires finalisés ou planifiés vers l'Union Européenne, via l'Asie centrale, l'Iran et la Turquie, la stratégie chinoise vise à raccourcir le délai de transport des biens commerciaux et à faciliter les relations économiques entre les régions asiatiques et européennes. L'idée de développer des liaisons ferroviaires transcontinentales reliant l'Asie et l'Europe n'est pas nouvelle et date déjà des années 60. Politiquement, bien que la Chine souligne que les connexions ferroviaires ne visent que des retombées économiques, les considérations géopolitiques de Pékin accompagnant la mise en œuvre de ces projets ne doivent pas être négligées. Il est clair que les réseaux de transport sont porteurs d'influence tant économique que politique. La construction de nouvelles voies ferrées reliant la Chine et la région centrasiatique et un prolongement jusqu'en Iran facilite à la Chine l'accès aux ressources énergétiques[117]. En effet ces régions recèlent d'immenses réserves énergétiques, hydrocarbures, charbon, mais aussi potentiel hydroélectrique. La Chine poursuit ainsi ses objectifs d'asseoir sa suprématie géopolitique avec la construction de chemins de fer au travers des Républiques caucasiennes et des corridors multimodaux vers la Birmanie[118,119]. D'autres enjeux politiques se jouent aussi avec ce mode de transport ; c'est le cas de la construction d'une connexion ferroviaire de l'Iran jusqu'à la Chine en passant par l'Afghanistan[120,121]

Le chemin de fer est un levier puissant de la stratégie chinoise aussi bien pour son influence en Asie que pour contourner le contrôle des voies maritimes par les américains et la politique d'encerclement des États-Unis et ses alliés dans la région. Ces tracés de chemins de fer sont aussi utilisés pour construire et contrôler ses propres réseaux de télécommunications utilisés par ailleurs par les pays traversés.

La montée en puissance de la Chine et ses projets logistiques continentaux redonnent une importance centrale à l'Eurasie. La Russie coopère de plus en plus avec la Chine. Le rôle de l'Allemagne en regard de la stratégie de l'Europe vis-à-vis de la Russie et de la Chine interpelle. L'Allemagne est très présente économiquement en Russie et est favorable à la coopération avec la Chine en mettant en avant bien légitimement la défense de ses intérêts propres en Asie centrale.

Henri de Grossouvre, pense qu'avec cette percée du ferroviaire Chinois en Europe, l'Eurasie intègre la globalisation, jusque-là, principalement maritime, en lui donnant une nouvelle dimension et en proposant une alternative politico-économique diversifiée. Un jeu de clés,

---

[115] *La stratégie ferroviaire chinoise en Asie centrale dans le cadre de la Belt and Road Initiative: concurrences, conflits et coopérations* [En ligne]. [Réf. 2020]. Disponible sur La stratégie ferroviaire chinoise en Asie centrale

[116] *« belt and road » a une riche connotation et une signification profonde - xinhuanet* [En ligne]. [Réf. 29 mars 2015]. Disponible sur « belt and road » a une riche connotation et une signification profonde - xinhuanet

[117] *LA STRATÉGIE FERROVIAIRE CHINOISE EN ASIE CENTRALE DANS LE CADRE DE LA BELT AND ROAD INITIATIVE:* [En ligne]. [Réf. Du 4 décembre 2019]. Disponible sur La stratégie ferroviaire chinoise en Asie centrale dans le cadre de la Belt and Road Initiative: concurrences, conflits et coopérations

[118] *Du Sichuan à la Birmanie, la Chine s'offre une ouverture sur l'océan Indien – COURIER INTERNATIONAL* [En ligne]. [Réf. 1 septembre 2021]. Disponible sur Du Sichuan à la Birmanie

[119] *La Chine tisse les «nouvelles routes de la soie» en Birmanie – RFI* [En ligne]. [Réf. Du 16 janvier 2020]. Disponible sur La Chine tisse les «nouvelles routes de la soie» en Birmanie (rfi.fr)

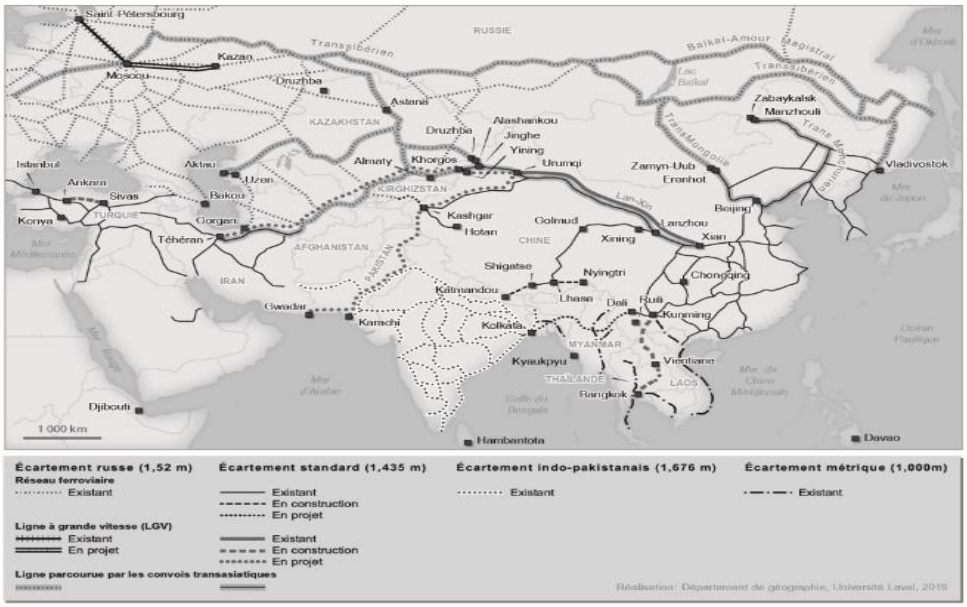
[120] *Connexion ferroviaire de l'Iran à la Chine par l'Afghanistan – ISNA* [En ligne]. [Réf. Du 16 mai 2021]. Disponible sur Connexion ferroviaire de l'Iran à la Chine par l'Afghanistan - ISNA

[121] *Un train chinois arrivé en Iran fait revivre la route de la soie – EUROPE 1* [En ligne]. [Réf. Du 15 février 2016]. Disponible sur Un train chinois arrivé en Iran fait revivre la route de la soie (europe1.fr)

selon lui permettant de faire émerger une globalisation multipolaire et diversifiée face à une globalisation uniformisée présentant des velléités de centralisation[122].

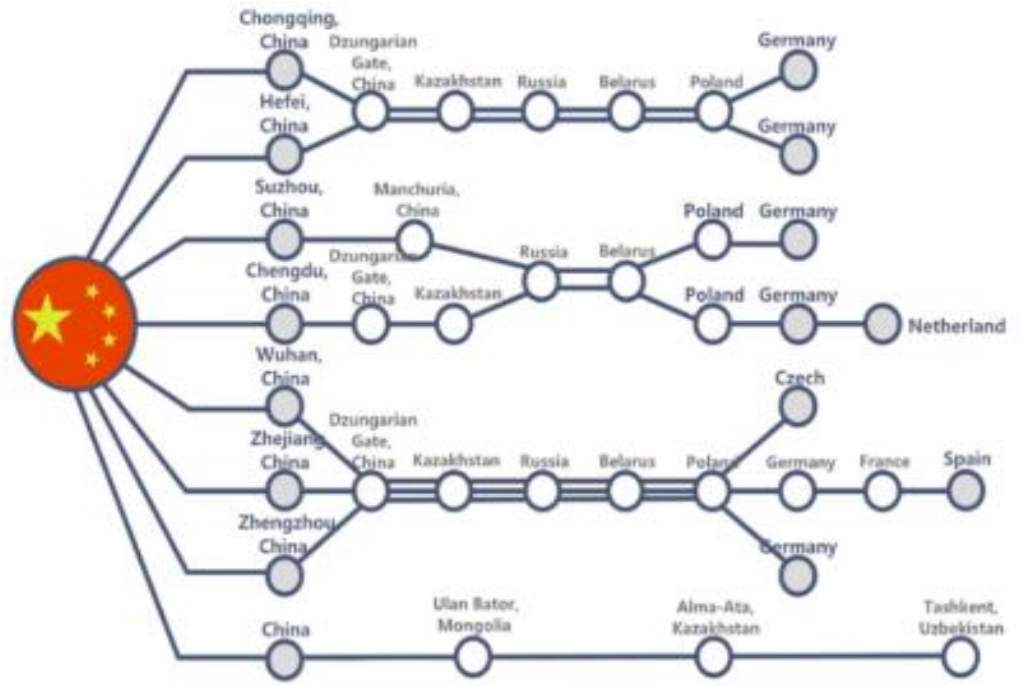
Entre la Chine et l'Europe, s'est ainsi constituée une nouvelle route de la soie comme le montrent les 2 schémas qui suivent,[123] longue de 11 000 km de rail pour 22 jours de trajet environ.

« ***En janvier 2017****, une petite nouvelle un peu confidentielle a retenu l'attention des spécialistes : un train long rempli de marchandises en provenance de Yiwu (province de Zhejiang) s'est arrêté, après 16 jours de voyage, dans la station de Barking à* ***Londres****. Le tunnel sous la Manche permet à Londres, capitale tournée vers la mer, d'être une des extrémités du fret ferroviaire continental eurasiatique*. »[124]

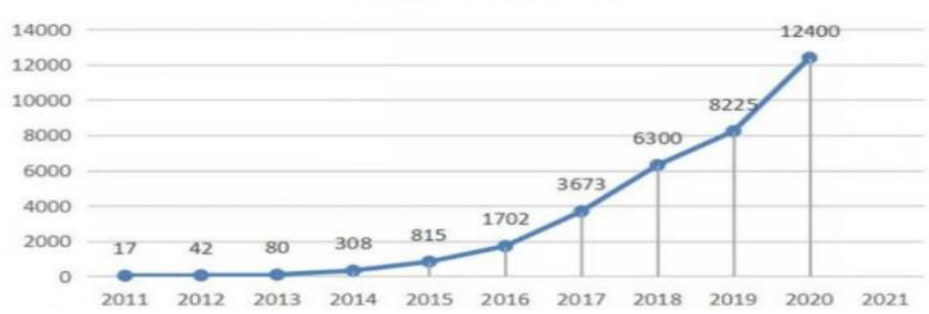


18 - Routes et Dessertes de la China Railway Express

[122] *CHINE-EUROPE, le boom passé inaperçu du fret ferroviaire et ses conséquences économiques et géopolitiques - AgoraVox* [En ligne]. [Réf. Du 12 mai 2021]. Disponible sur CHINE-EUROPE, le boom passé inaperçu du fret ferroviaire
[123] *China Railway Express* [En ligne]. Disponible sur China Railway Express-Suzhou Sohologistics CO., LTD.
[124] *CHINE-EUROPE, le boom passé inaperçu du fret ferroviaire et ses conséquences économiques et géopolitiques - Henri de Grossouvre* [En ligne]. [Réf. Du 12 mai 2021]. Disponible sur CHINE-EUROPE, le boom passé inaperçu du fret ferroviaire



19 - Projets Développement d'infrastructures et services ferroviaires en Asie[125]



20 - Évolution des trains affrétés par an depuis 2011 (Source AGORAVOX)

La pandémie du COVID19 qui a sévi en Europe en 2O20 et 2021 a vite montré l'ampleur de la pénétration du fret ferroviaire de la Chine en Europe. La China Railways Express entre l'Europe et la Chine initialement motivée pour le transport de matériel informatique moins cher de la Chine vers l'Europe s'est transformée en une vaste autoroute à voies et embranchements multiples transportant des marchandises de tout ordre. La fréquence des liaisons entre la Chine et l'Europe a atteint un niveau sans précédent (Voir l'évolution du trafic sur le graphique ci-dessus). En 2020, leur nombre s'est cumulé à plus de 12,4 K trains par an, soit 340 trains par jour. Le train le plus long peut atteindre aujourd'hui une longueur de 1,5 kilomètre !

Le leadership mondial de l'industrie ferroviaire européenne est mis à l'épreuve par de nouveaux entrants sur le marché. C'est le cas de l'Asie et en particulier la Chine qui outre les produits traditionnels se positionne de plus en plus dans le segment ferroviaire. Tout récemment, le rachat par Hitachi de la branche Signalisation ferroviaire de Thalès. [126]

[125] *La stratégie ferroviaire chinoise en Asie centrale dans le cadre de la Belt and Road Initiative: concurrences, conflits et coopérations* [En ligne]. [Réf. 2020]. Disponible sur La stratégie ferroviaire chinoise en Asie centrale

[126] *Thales vend sa signalisation ferroviaire au japonais Hitachi – LE MONDE* [En ligne]. [Réf. Du 4 aout 2021]. Disponible sur Thales vend sa signalisation ferroviaire au japonais Hitachi

Le 20 décembre 2020, après sept ans de négociation, un accord d'investissement UE / Chine a été signé par la présidente de la Commission Européenne l'Allemande Ursula von der Leyen. Cette dernière déclarait qu'il serait dans l'intérêt géopolitique et économique de l'Union pour son autonomie stratégique d'accompagner activement le développement logistique eurasiatique et non de le subir. Reste à savoir si cet accord global, qui ambitionne de faciliter l'accès du marché chinois pour les entreprises européennes, permettra aux opérateurs ferroviaires européens et du monde, de pouvoir profiter pleinement des opportunités liées à l'émergence de plusieurs projets de chemin de fer suburbains en Chine.

La meilleure réponse à ce défi concurrentiel passe par l'innovation pour améliorer la qualité et la fiabilité des produits en réduisant les coûts du cycle de vie. Les investissements publics et privés dans Shift2Rail ont également un effet multiplicateur sur les efforts indispensables à l'industrie pour mettre ces produits sur le marché et conquérir d'autres opportunités tant en Europe qu'à l'étranger. Avec une démarche commune, l'Europe pourra mutualiser les forces et moyens de production, renforcer la collaboration et le partenariat dans l'ensemble de l'industrie ferroviaire.

« Il faut être proactif, se concentrer sur la technologie, regarder ce qui se fait ailleurs dans le monde et dans d'autres secteurs, et innover en dépit des lenteurs réglementaires. La réglementation, curative, suivra. Ce sont ceux qui se lancent qui gagneront sur le plan économique et qui, de plus, arriveront à des niveaux de sécurité plus élevés. »[127]

VIII.4. BATAILLE TECHNOLOGIQUE

VIII.4.1. POSITIONNEMENT STRATEGIQUE de L'EUROPE POUR DES SOLUTIONS FERROVIAIRES TIC

D'après le rapport de la Commission Européenne, l'Europe dans son ensemble occupe le top du marché de la cybersécurité d'une manière générale dans le monde comme le montre l'encart ci-contre[128].

Le marché européen de la cybersécurité

- Les pays européens occupent 18 des 20 premières places de l'indice de cybersécurité dans le monde
- La valeur du marché européen de la cybersécurité est estimée à plus de 130 milliards d'euros et progresse à un rythme de 17 % par an
- L'UE compte plus de 60 000 entreprises dans le secteur de la cybersécurité et plus de 660 centres d'expertise en cybersécurité

Cette place est flatteuse ; mais la dépendance de l'Europe vis-à-vis des nouvelles technologies et dont le monopole est sous d'autres continents interpelle. Lors de l'atelier sur « *la sécurité ferroviaire du futur* » organisé en mars 2021 par la FONdation pour une Culture de SéCurité Industrielle (Foncsi) le constat partagé suite à une question relative à la souveraineté était le suivant: *« Les nouvelles technologies sont essentiellement fournies par des entreprises implantées en dehors de l'Europe, on peut aisément imaginer qu'en cas de relations diplomatiques tendues, celles-ci puissent leurrer le système pour provoquer un arrêt des trains par exemple. »*[129]

---

[127] *ATELIER SÉCURITÉ FERROVIAIRE DU FUTUR – FONCSI* [En ligne]. [Réf. Du 23 mars 2021]. Disponible sur Synthèse atelier ferroviaire futur

[128] *Comment l'UE lutte contre les cybermenaces* [En ligne]. [Réf. 2022]. Disponible sur Cybersécurité: comment l'UE lutte contre les cybermenaces - Consilium (europa.eu)

[129] *Atelier sécurité ferroviaire du futur - FONCSI* [En ligne]. [Réf. Du 23 mars 2021]. Disponible sur synthese-atelier-ferroviaire-futur (foncsi.org)

VIII.4.2. BATAILLE DANS L'INNOVATION

D'une manière générale le niveau de digitalisation en Europe est significativement inférieur à celui de l'Amérique du Nord et la France est en retard par rapport à d'autres pays européens comme le Royaume-Uni. Alors que l'Europe avait pris une longueur d'avance il y a 20 ans lors de l'invention du GSM ou le déploiement du DSL, l'Amérique du Nord a su rattraper l'Europe et investir chaque année bien plus dans ses infrastructures numériques – un ratio de 1 à 2 par habitant entre les US et l'Europe depuis 2006. Les résultats sont sans appel : 80% des principaux sites web sont originaires des États-Unis alors que 81% des utilisateurs sont hors des États-Unis (voir Illustration 1). Parmi les 25 grandes sociétés digitales au monde, 85% de la valeur de marché est américaine, 13% asiatique et seulement 2% européenne !
Dans le domaine ferroviaire, l'Europe est encore en bonne place. Le véritable enjeu et donc de toujours avoir plusieurs longueurs d'avance. Et la Chine est un concurrent redoutable.
Des projets futuristes émergent, on peut par exemple citer le projet Hyperloop. Hyperloop est un nouveau moyen de transport des personnes et des marchandises à des vitesses comparables à celles du transport aérien pour le prix d'un ticket de bus. Il s'agit d'un mode de déplacement à la demande, écologique et sûr. Le système se sert de moteurs électriques pour faire accélérer (jusqu'à 1200km/h) et décélérer une capsule reposant sur coussin d'air aimanté dans un tube à basse pression ou sous vide. Le véhicule glisse silencieusement sur des kilomètres sans aucune turbulence. Avec cette technologie de pointe, le trajet entre Paris et Madrid ne prendrait pas plus de 90 minutes et Toulouse Montpellier en 24 minutes.[130]

Train futuriste imaginé par Elon Musk et porté aujourd'hui par 3 grandes entreprises.[131]

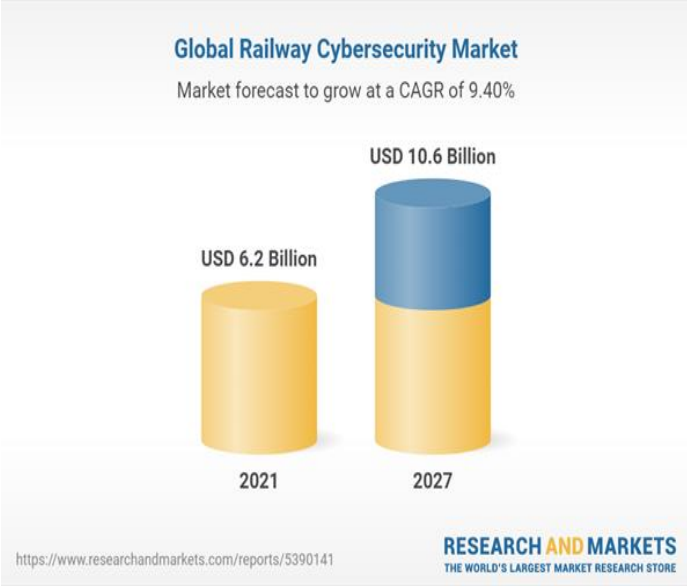
Le choix de la France et de la ville de Toulouse est un signe illustrant entre autres du très haut niveau technologique de la France en la matière et de la qualité de ses ingénieurs. Mais la vigilance est de mise pour ne pas perdre cette bataille stratégique.

VIII.4.3. SOLUTIONS FERROVIAIRES EN CYBERSÉCURITÉ ET INTELLIGENCE ARTIFICIELLE

Que fait l'Europe face aux stratégies des pays qui tiennent aujourd'hui les devants en matière de matériels et solutions ferroviaires en cybersécurité et IA ? Qu'en est-il des stratégies européennes quant aux solutions européennes face à la concurrence asiatique

[130] *Le projet Hyperloop au sud de Toulouse voit moins grand que prévu* [En ligne]. [Réf. Du 23 décembre 2021]. Disponible sur le-projet-hyperloop-au-sud-de-toulouse-voit-moins-grand-que-prevu
[131] *Hyperloop* [En ligne]. [Réf. Du 20 janvier 2020]. Disponible sur Hyperloop • Les Horizons

ou israélienne ? D'après l'étude 2021 de ResearchAndMarket[132] bien que la croissance de la zone Asie-Pacifique soit la plus rapide avec une projection de la plus grande part du marché d'ici 2027, les équipementiers tels que Thales Group (France), Siemens AG (Allemagne), Alstom (France), Wabtec (États-Unis) et Nokia Networks (Finlande) et leurs investissements dans la cybersécurité ferroviaire sont les principaux moteurs de la croissance de ce marché à l'échelle mondiale. L'offre diversifiée de leur gamme de produits et de solutions et leurs solides réseaux de distribution dans le monde entier en font des acteurs majeurs malgré la poussée de la Chine ou des pays tels que Israël, comme le confirme Jean-Baptiste Renault (voir Annexes I - Interviews (JBR, Alstom)), responsable Cybersécurité France chez Alstom « *de plus l'expertise du ferroviaire et la connaissance de nos clients que nous avons nous donnent tout de même encore une longueur d'avance* ».



21 - Marché Mondial de la Cybersécurité ferroviaire en

Il y a par ailleurs au travers de partenariat des leaders comme Airbus Cybersecurity et Alstom[133] une volonté de capitalisation des fortes expériences, respectivement sur la cybersécurité industrielle et sur le ferroviaire afin de monter des offres de service à très haute valeur ajoutée.

La bonne pénétration d'Alstom ou de Thalès sur les marchés asiatiques est un bon signe même si cela passe très souvent par des joint-ventures avec des entreprises locales Chinoises comme nous le confirme Eddy Thésée, Vice-Président Cybersécurité Alstom Portfolio Produits et Services[134] . Thalès est reconnu comme acteur majeur du secteur du transport en Thaïlande, Thales a déployé pour la première fois sa technologie ETCS en 2017 sur l'East Coast Line du réseau thaïlandais, et est engagée dans plusieurs transformations majeures dans le ferroviaire Thaïlandais. Les systèmes de haute technologie de Thales couvrent 17 000 km de grandes lignes dans 38 pays[135].

Alstom est présent depuis plusieurs dizaines d'années en Asie avec plus de 4000 personnes employées et 10 à 15% de son chiffre d'affaires dans cette région[136]. En septembre 202, un contrat de 720 millions d'euros a été signé portant sur le développement d'un système intégré de métro automatisé pour la ligne ceinturant la ville de Taïpei, à Taïwan[137].

---

[132] *Railway Cybersecurity Market* [En ligne]. [Réf. De juillet 2021]. Disponible sur Railway Cybersecurity Market by Type (Infrastructural & On-board), Offering, Security Type

[133] *Airbus CyberSecurity et Alstom signent un partenariat en matière de cybersécurité* [En ligne]. [Réf. Du 13 septembre 2021]. Disponible sur Airbus CyberSecurity and Alstom sign cyber-security partnership

[134] Annexes I – Interview Eddy Thésée – VP Cybersécurité Asltom

[135] *LA THAILANDE RENFORCE LA SÉCURITÉ FERROVIAIRE DANS 48 GARES GRÂCE À THALES* [En ligne]. [Réf. Du 18 septembre 2019]. Disponible sur La Thailande renforce la sécurité ferroviaire dans 48 gares grâce à Thales | Thales Group

[136] *ECONOMIE – L'Asie-Pacifique, moteur de la stratégie de croissance d'ALSTOM, Cécile Brosolo* [En ligne]. [Réf. Du 25 avril 2017]. Disponible sur https://lepetitjournal.com/singapour/actualites/economie-lasie-pacifique-moteur-de-la-strategie-de-croissance-dalstom-46219

[137] *Alstom pousse ses feux en Asie-Pacifique, Véronique Guillermard* [En ligne]. [Réf. Du 30 septembre 2021]. Disponible sur https://www.lefigaro.fr/societes/alstom-contrat-de-430-millions-d-euros-pour-un-metro-a-taipei-20210930

- **Solutions technologiques et en cybersécurité pour le secteur du transport ferroviaire**

Société	Pays	Continent	Spécialisée Cyber ferroviaire	Poids des solutions cyber pour le ferroviaire	Poids des solutions pour le ferroviaire	Commentaires
ABB	Suède	Europe	NON	Faible	Fort	Acteur majeur des technologies de l'énergie et de l'automation
AIRBUS CYBERSECURITY	France	Europe	NON	Moyen	Faible	Cybersécurité Solutions intégrées de sécurisation IT/OT. Cyber résilience des systèmes industriels de manière générale et dans l'accompagnement pour la cybersécurité ferroviaire. Partenariat en septembre 2021 avec Alstom pour développer la cybersécurité ferroviaire.
ALSTOM	France	Europe	NON	Fort	Fort	Construction matériel roulant - Transport et cybersécurité ferroviaire Expertise en management de risques ferroviaires IT/OT
BAE SYSTEMS	Royaume-Uni	Europe	NON		Faible	Défense et Aérospatiale
CAPGEMINI (SOGETI)	France	Europe	NON	Faible	Faible	Solutions digitales / numérisation et contrôle des trains, conceptions de train & innovations, manufacturing 4.0
CERVELLOSEC	Israël	Asie	OUI	Fort	Faible	Solutions de cybersécurité ferroviaires. Conseils et produits (Plateforme - protection contre les cybermenaces internes et externes, segmentation avancée du réseau, la ségrégation, l'authentification et la surveillance seule entreprise offrant une technologie brevetée pour l'authentification de la signalisation ferroviaire. Cervello et Expandium partenariat stratégique visant à combiner la cybersécurité avec la maintenance prédictive pour les systèmes de signalisation ferroviaire et de télécommunications.
CISCO	USA	Amérique	NON	Fort	Faible	
CRITIFENCE	Israël	Asie	OUI	Fort	Faible	Cybersécurité IT/OT Solutions de cybersécurité conçues pour les infrastructures critiques, les systèmes SCADA et de contrôle industriel qui permettent de surveiller et de contrôler le réseau OT facilement et de manière totalement passive. -SCADADome® 2200T - Solution de cybersécurité pour l'industrie du transport
CYLUS	Israël	Asie	OUI	Fort	Faible	
ENSCO INC.	USA	Amérique	OUI	Faible	Fort	L'aérospatiale, sécurité nationale, du transport de surface et de la cybersécurité
EUROMICRON GROUP	Allemagne	Europe	NON	Faible	Fort	Spécialisé dans l'IoT
HITACHI LTD.	Japon	Asie	NON	Moyen	Fort	Electronique Rachat par Hitachi de la branche Signalisation ferroviaire de Thalès

Société	Pays	Continent	Spécialisée Cyber ferroviaire	Poids des solutions cyber pour le ferroviaire	Poids des solutions pour le ferroviaire	Commentaires
HUAWEI	Chine	Asie	NON	Fort	Faible	Solution de communications opérationnelles ferroviaires. Les solutions Huawei couvrent trois aspects de communications ferroviaires : la régulation cruciale des trains, le réseau dorsal et les dispositifs haut débit le long des voies.
IBM	USA	Amérique		Fort	Faible	Matériels et solutions informatiques « Nos locomotives sont essentiellement devenues des actifs numériques, vu la quantité d'informations dont elles disposent et les réseaux de capteurs » Mark Schulze vice-président de la sécurité, des opérations, BNSF
ICSS	France	Europe	NON	Faible	Faible	Entreprise individuelle expert dans les systèmes industriels
RAYTHEON TECHNOLOGIES (COLLINS AEROSPACE)	USA	Amérique	NON	Fort	Faible	Aérospatial, Défense militaire (IOT)
RAZORSECURE	Royaume-Uni	Europe	OUI	Fort	Faible	Produits et services pour améliorer la cybersécurité ferroviaire pour le matériel roulant, la signalisation et les systèmes d'infrastructure.
SELECTRON SYSTEMS AG	Suisse	Europe	NON	Moyen	Fort	Solutions ferroviaires Solutions système dans le cadre de l'automatisation de véhicules ferroviaire, plus communément connues sous le nom Train Control and Monitoring System - TCMS.
SHIFT5	USA	Amérique	OUI	Fort	Faible	Cyber Maintenance prédictive, planification ferroviaire de précision, détection d'intrusion, tests de vulnérabilités
THALES GROUP	France	Europe	NON	Fort	Fort	Innovation disruptive pour le ferroviaire à base d'intelligence Artificielle
TOSHIBA	Japon	Asie	OUI	Faible	Fort	Solutions numériques Le « service de surveillance à distance » pour les véhicules ferroviaires utilise les technologies IoT *1 pour surveiller l'état de fonctionnement des véhicules ferroviaires en temps quasi réel.
WATERFALL SECURITY	Israël	Asie	OUI	Fort	Faible	Cybersécurité ferroviaire Safety and Security for Rail Systems Operations Passerelles de sécurité unidirectionnelle, systèmes de contrôle industriel (ICS), infrastructure critique, communication unidirectionnelle, intégration IT/OT pour infrastructure critique, cybersécurité industrielle, sécurité du périmètre réseau, cybersécurité SCADA et cyberattaques Certification: Critère Commun EAL4+, ANSSI-CSPN, NITES Singapour Conformité Directives et réglementation mondiale des systèmes industriels, ANSSI, NERC CIP, IEC 62443, NRC 5.71, NIST 800-82r2, CFATS, ISO, IIC SF, et autres ferroviaires à la norme IEC 62443, CENELEC TS-50701.. Partenaires: FIREEYE, SPLUNK; DRAGOS;FORECOUST; Indegy; CyberX
RAILNOVA	Belgique	Europe	NON	Faible	Faible	Exploitation des systèmes ferroviaires
PILZ						SecurityBridge a été conçu selon le process de développement de la sûreté conformément à la norme CEI 62443-4-1. Par conséquent, il tient compte du principe de « zones et conduits ». SecurityBridge contrôle le trafic de données du process et surveille l'intégrité du système de sûreté.
STIMIO	France	Europe	NON	Faible	Fort	Solutions d'IoT pour la maintenance prédictive et l'optimisation de l'exploitation ferroviaire

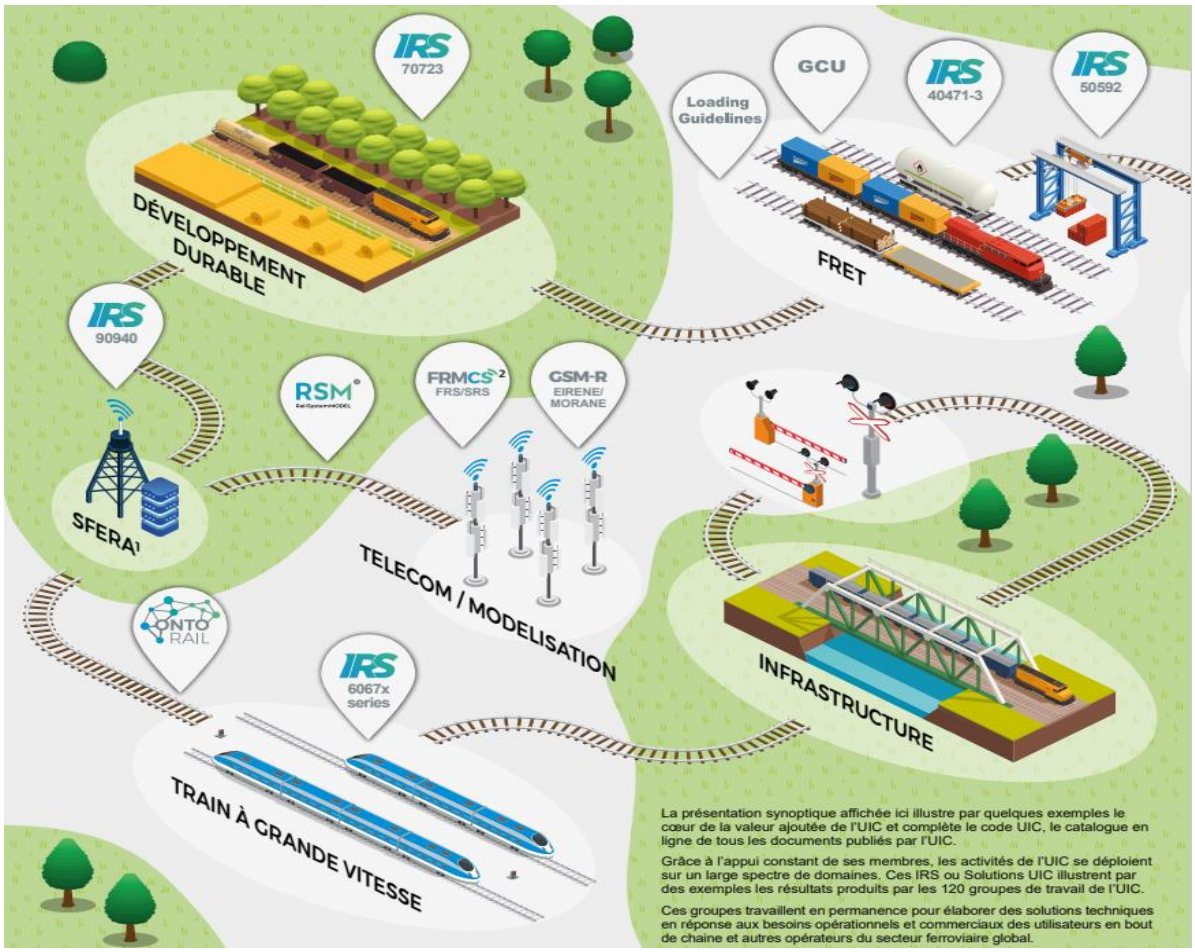
IX. LES CHALLENGES

Parmi les préoccupations encore prégnantes au sein de l'UE, on retrouve :

- Une standardisation et harmonisation des normes techniques et des règles de sécurité ferroviaire et celles relatives à la cybersécurité des différents pays traversés.
- La mise en œuvre de la RGPD, la Privacy-By-Design : l'utilisation des IoT va amplifier la problématique ;
- Les certifications des produits et solutions de cybersécurité ferroviaire ;
- L'évaluation de la maturité en cybersécurité des SII.

Les challenges à venir dans l'UE ne sont pas seulement techniques, on peut citer par exemple :

- Les problématiques de Responsabilité Sociétale et Environnementale ;
- Les questions autour de l'éthique et les responsabilités juridiques lors d'usage de trains faisant usage d'Intelligence Artificielle et les trains autonomes ;
- Le développement de la coopération inclusive et la confiance.

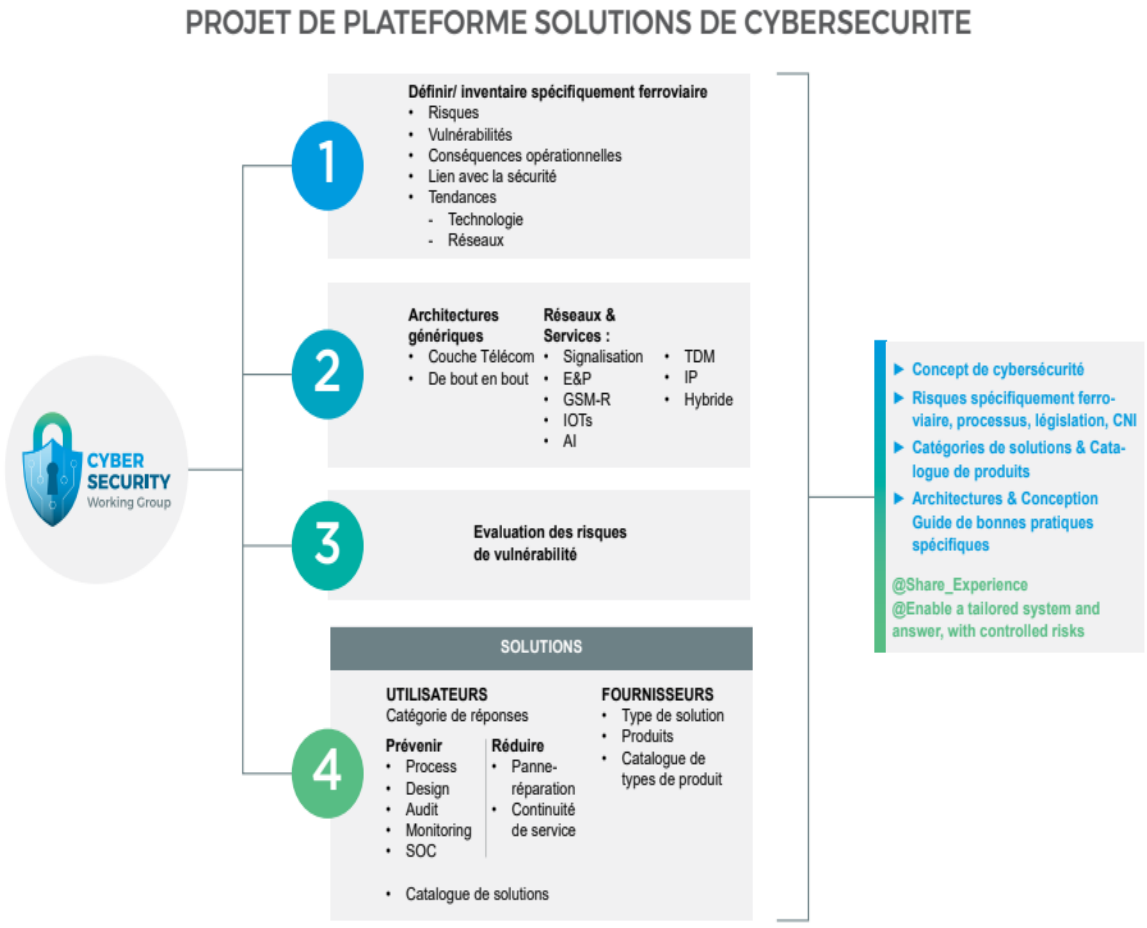


22 - Un écosystème qui se veut opérationnel et durable[138]

[138] UIC, *Solutions techniques pour le rail opérationnel.* [En ligne]. [Réf. du 10 mai 2021]. Disponible sur https://uic.org/IMG/pdf/uic-solutions-techniques-pour-le-rail-operationnel.pdf

IX.1. STANDARDISATION ET HARMONISATION DES NORMES TECHNIQUES ET SOLUTIONS

Les intégrations transrégionales et transnationales ne peuvent être accélérées sans une harmonisation des normes techniques et règles nationales. Il en va de même de la nécessité de certification ou labellisation européenne de certains produits et solutions qui revêtent par ailleurs un enjeu de souveraineté. L'Union Internationale des Chemins de fer (UIC) travaille activement dans la mise en place d'une plateforme de solutions en cybersécurité avec un label européen[139].



23 - Projet de plateforme solutions de Cybersécurité (Source UIC)

IX.2. ÉVALUATION DU NIVEAU DE MATURITÉ EN CYBERSECURITE

Il est difficile d'évaluer la maturité du niveau de cybersécurité même pour les SI d'entreprise actuels. L'imaginer pour des systèmes industriels semble être une gageure. Amorcer une démarche d'évaluation est un processus vertueux de volonté d'amélioration continue.

Plusieurs modèles d'évaluations de maturité ont été proposés pour des domaines techniques et en particulier celui de la cybersécurité parmi lequel le C2M2 (Cybersecurity

[139] UIC, *Solutions techniques pour le rail opérationnel.* [En ligne]. [Réf. du 10 mai 2021]. Disponible sur https://uic.org/IMG/pdf/uic-solutions-techniques-pour-le-rail-operationnel.pdf

Capability Maturity Model [140]). Le C2M2 est un programme du Bureau de la cybersécurité, de la sécurité énergétique du ministère de l'Énergie des États-Unis. Il dérive du modèle d'évaluation de la maturité de cybersécurité du sous-secteur de l'électricité (ES-C2M2) dans sa version 1.0 datant de 2012 sous l'impulsion de la Maison-Blanche et du Département américain de la Sécurité intérieure. Le but de ce modèle est d'améliorer la cybersécurité des organisations d'infrastructures critiques.

Le modèle C2M2 est similaire au modèle CMMI avec ses 5 niveaux de maturité. Le niveau 5 est le niveau de calcul de l'efficience.

C2M2 organisé en dix domaines :

- Gestion des risques (GR) ;
- Gestion des modifications et de la configuration des actifs (ACM) ;
- Gestion des identités et des accès (IAM) ;
- Gestion des menaces et des vulnérabilités (TVM) ;
- Connaissance de la situation (AS) ;
- Partage de l'information et communications (ISM) ;
- Intervention en cas d'événement et d'incident ; continuité des opérations (RI) ;
- Gestion de la chaîne d'approvisionnement et des dépendances externes (EDM) ;
- Gestion de la main-d'œuvre (WM) ;
- Gestion du programme de cybersécurité (CPM).

George E.P. Box, un statisticien britannique, a inventé une expression qui est souvent utilisée lorsqu'on parle de modèles de maturité et de cadres de contrôle. Il a dit *: « Tous les modèles sont faux, mais certains sont utiles. »*[141]

Un autre challenge est la capacité à mesurer l'efficience des mesures de cybersécurité.

IX.3. ÉVALUATION DU COUT DE LA CYBERSECURITE

Une autre difficulté et pas des moindres est l'estimation du coût de la cybersécurité. C'est une opération très complexe (coûts directs, indirects) au regard de la dimension holistique qu'elle doit couvrir. Il est difficile de pourvoir de manière exhaustive à quantifier et à chiffrer.

IX.4. RESPONSABILITE SOCIALE ET SOCIETALE D'ENTREPRISE (RSE)

La responsabilité sociétale des entreprises représente l'intégration, dans le monde de l'entreprise, des principes du développement durable et de ses trois piliers sur les plans Environnemental, Social et Sociétal[142] , Économique.

Telle que définie dans des standards internationaux, la RSE est composée de sept champs d'action :

Gouvernance - Droits de l'Homme - Social - Environnement - Loyauté des pratiques - Enjeux liés aux clients / consommateurs - Développement des territoires.

[140] Energy.gov, *Modèle de maturité des capacités en matière de cybersécurité*. [En ligne]. Disponible sur Cybersecurity Capability Maturity Model (C2M2) | Department of Energy

[141] Security Bloggers Network, Modèles de maturité et cadres de sécurité, [Réf. du 29 avril 2021] Disponible sur A Timeline of Frameworks for Cybersecurity and Compliance - Security Boulevard

[142] *RSE : Une dimension Sociale ou sociétale* [En ligne]. [Réf. 2012]. Disponible sur RSE : Une dimension Sociale ou Sociétale - Le Blog RH

24 - Les 17 objectifs du développement durable (source Ecologie.gouv.fr) [143]

Le ferroviaire ne déroge pas à l'obligation morale, du respect des exigences liées aux sept champs d'action cités plus haut. Les usagers et collaborateurs sont de plus en plus sensibles à ces valeurs.

Si on prend le cas de la chaîne logistique ou d'approvisionnement, on peut mesurer la difficulté du respect de cette exigence sur toute la chaîne. Le référentiel RSE en logistique répond à l'objectif d'établir un lien robuste entre la RSE telle qu'elle est définie dans les standards internationaux et les réalités de la filière logistique. La logistique couvre, dans l'ensemble de ce référentiel, l'ensemble des opérations assurées sur les flux physiques de marchandises, notamment : le transport, le stockage, l'entreposage, la manutention et l'emballage.

IX.4.1. LES OPÉRATEURS DU MARCHE ET LA RSE

Quelques entreprises françaises se démarquent et font figure d'exemples en Europe.

SNCF avec la note maximale A1+, est un exemple d'opérateur ferroviaire à citer au niveau européen. Elle est classée à la 5e place des entreprises les plus performantes au niveau mondial, tous secteurs confondus, parmi les 4 879 sociétés auditées sur leurs performances dans les domaines sociaux, sociétaux, environnementaux et de gouvernance.

Construite à partir des travaux stratégiques du projet « *Tous SNCF* » avec l'ensemble des sociétés et activités du groupe, la stratégie RSE (Responsabilité sociale et sociétale d'entreprise) fixe le cap et donne un cadre cohérent et commun pour faire de la RSE un levier de compétitivité et de performance globale. Mikaël Lemarchand explicite les six axes structurants qui composent cette stratégie RSE pour la décennie 2020-2030[144] pour SNCF :

- Développer la part du ferroviaire et des mobilités durables ;
- Réduire l'empreinte environnementale des activités ;
- Améliorer l'adaptation et la résilience des activités au changement climatique ;

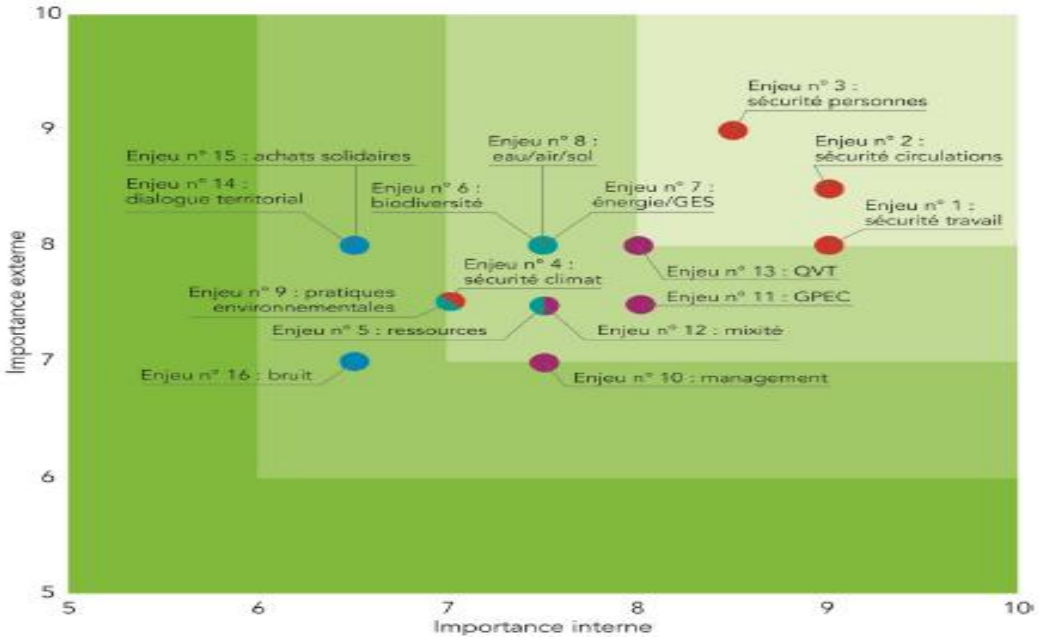
[143] *Référentiel RSE en logistique* [En ligne]. [Réf. 2018]. Disponible sur Référentiel RSE en logistique
[144] *LA STRATÉGIE RSE DU GROUPE SNCF EN DÉTAILS* [En ligne]. [Réf. Du 13 septembre 2021]. Disponible sur La stratégie RSE | SNCF

- Agir pour la cohésion sociale et l'économie écologique et solidaire dans les territoires ;
- Faire des salariés SNCF les principaux acteurs et bénéficiaires de la transition écologique et sociale ;
- Développer une éthique irréprochable et une gouvernance ouverte.

« *La stratégie RSE 2020-2030 validée par le Conseil d'administration le 23 juin inscrit le groupe SNCF dans des trajectoires de progrès, cohérentes avec les attentes de nos parties prenantes. Toute la société est en train de basculer dans la transition écologique. La prise de conscience des citoyens, des consommateurs, des collectivités comme des entreprises, s'accélère et se généralise. Le groupe SNCF, par la nature de ses activités et par les valeurs qui nous réunissent, a un rôle et une responsabilité dans la réussite de ces transitions sociale, écologique et économique. Les projets, tous SNCF, ont déjà permis de définir les actions concrètes et prioritaires pour chaque entité et établissement, au plus près du terrain. Nous sommes déjà lancés !*», conclut Mikaël Lemarchand - SNCF.

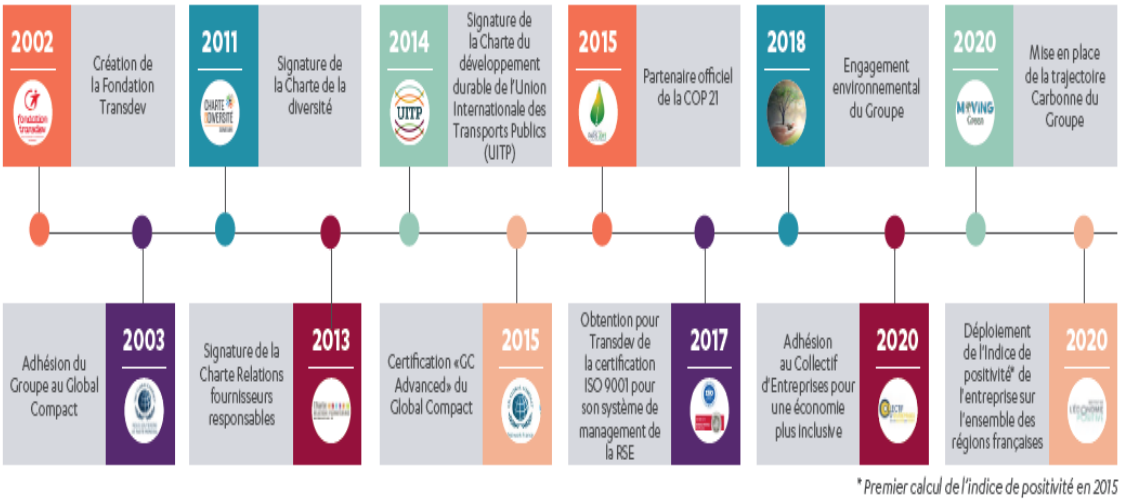
Les enjeux définis par la SNCF recouvrent 4 grandes thématiques qui peuvent être applicables dans toute l'Europe :

- Sécurité
  - ✓ Assurer une production en toute sécurité ;
  - ✓ Offrir un réseau sûr aux entreprises ferroviaires ;
  - ✓ Réduire la dangerosité du réseau vis-à-vis des personnes ;
  - ✓ Sécuriser les infrastructures face au changement climatique ;
- Environnement
  - ✓ Optimiser les ressources et valoriser les matières dans le cadre de la démarche d'économie circulaire ;
  - ✓ Respecter les écosystèmes naturels en tant que bien commun ;
  - ✓ Réduire les émissions de gaz à effet de serre et améliorer l'efficacité énergétique ;
  - ✓ Minimiser l'empreinte des activités sur l'eau, l'air et les sols, et maîtriser les rejets ;
  - ✓ Intégrer la performance environnementale dans les pratiques métiers ;
- Social
  - ✓ Mettre le management de proximité au cœur de la production ;
  - ✓ Développer l'employabilité ;
  - ✓ Valoriser l'accès des femmes à tous les emplois et lutter contre les discriminations ;
  - ✓ Garantir le bien-être au travail de chacun ;
- Territoire
  - ✓ Inscrire le dialogue territorial au cœur des pratiques ;
  - ✓ Contribuer activement au développement économique et social des territoires, à travers l'achat solidaire et les PME.



25 - Les 16 enjeux de la politique RSE SNCF Réseau[145]

Un autre exemple, celui de Transdev. En 2020, **Transdev** a rejoint le Collectif d'Entreprises pour une économie plus inclusive qui rassemble des entreprises françaises emblématiques dans leur secteur. Transdev s'est également engagé auprès de l'ONU Femmes pour lutter contre les violences faites aux femmes dans les transports. Transdev accélère son engagement environnemental à travers la formalisation de la stratégie MOVING Green prévue être déployée dans le Groupe à partir de 2021.



26 – Chronologie de l'Engagement RSE chez Transdev [146]

Alstom en France a obtenu le label « engagé RSE » niveau 3, confirmé. L'évaluation a été conduite par l'AFNOR, sur le modèle ISO 26 000. Alstom devient ainsi le premier constructeur ferroviaire à obtenir ce label dans le monde.

COLAS Rail annonce que 93% de leurs activités sont certifiés ISO 14001 (management des impacts environnementaux) dans le monde en 2020. Une certification qui leur permet de garantir la maîtrise de leur impact sur l'environnement.

---

[145] *Responsabilité sociétale d'Entreprise – SNCF* [En ligne]. [Réf. 2016]. Disponible sur Rapport RSE SNCF 2016 Def
[146] *Déclaration de performance extra-financière – TRANSDEV* [En ligne]. [Réf. Du 31 décembre 2020]. Disponible sur 2020-dpef_fr_version-seule_finale.pdf (transdev.com)

IX.5. INTELLIGENCE ARTIFICIELLE POUR L'INDUSTRIE FERROVIAIRE

L'Intelligence Artificielle (IA) est partout et est une réalité dans plusieurs applications pratiques du monde ferroviaire[147]. À la SNCF, on estime que les premiers trains autonomes de voyageurs circuleront sur les lignes régionales dès 2023[148].

Sur le site de l'organisation de standardisation ISO, des 132 cas d'usage d'IA soumis par des experts entre juillet 2018 et fin novembre 2019149, seuls, deux évoquent des expérimentations relatives une à la signalisation et l'autre aux trains autonomes[150]

- ✓ Cas d'usage de 49.AI : Solution d'optimisation des feux de circulation basée sur la fusion de données multisources. On parle bien d'optimisation ;
- ✓ Cas d'usage 113 (trains autonomes (exploitation de trains sans surveillance (UTO)) : offrir une fiabilité et une sécurité supplémentaires et de prévenir les accidents sur les chemins de fer, l'optimisation de la consommation d'énergie, à l'augmentation de la capacité de transport ;

Quelques instructions sont en cours, par exemple l'ISO/TR 22100-5:2021 (en relation avec l'ISO 12100) qui n'aborde que les aspects-conseils pour le développement d'applications d'apprentissage automatique de l'intelligence artificielle. La sécurité peut être compromise en raison de la complexité importante de l'introduction de l'apprentissage automatique de l'IA sur les machines. Les machines ou les systèmes à base d'IA ne peuvent agir que dans des limites spécifiques et cela doit être pris en compte dans le processus d'évaluation des risques[151].

Terry Wykle Responsable Programme Intelligence Artificielle chez Infrabel, (Gestionnaire d'Infrastructure Belge) affirme qu'« *on est encore loin de dire que l'IA va permettre à tous nos trains d'être à l'heure* ». Les expériences menées au sein de TUC Rail filiale d'Infrabel montrent à quel point les challenges pour que les algorithmes d'IA s'alignent aux exigences de qualité et de sécurité industrielle sont encore devant nous[152]. Pour Terry Wykle, l'IA ne pourra être utilisée directement dans la gestion des flux de circulation et restera pour l'instant en assistance des processus industriels.

Plusieurs défis sont à relever :

- Démontrer la causalité pour pouvoir prétendre atteindre les niveaux de sûreté requis dans le ferroviaire. On n'est encore loin de démontrer des niveaux de sécurité assimilables aux sûretés de fonctionnement SIL1[153]. Pouvoir gérer la circulation ferroviaire qui est de niveau SIL4 avec des algorithmes d'IA semble à date inatteignable : les algorithmes d'apprentissage d'IA fonctionnant en « boîte noire » dans le sens où l'on peut juger des données qui entrent dans la boîte et des résultats qui en sortent, mais sans savoir ce qui se passe à l'intérieur[154] ;

---

[147] Thales**,** *Thales augmente l'intelligence des trains pour optimiser le trafic ferroviaire et économiser 30% de leur consommation énergétique* [En ligne]. [Réf. du 25 Nov. 2020]. Disponible sur https://www.thalesgroup.com/fr/monde/transport/news/thales-augmente-lintelligence-des-trains-optimiser-le-trafic-ferroviaire

[148] *Ce que l'intelligence artificielle va changer pour les transports ferroviaire et aérien – L'OPINION* [En ligne]. [Réf. Du 28 janvier 2019]. Disponible sur Ce que l'intelligence artificielle va changer pour les transports ferroviaire et aérien - l'Opinion (lopinion.fr)

[149] *Information technology — Artificial intelligence (AI) — Use cases* [En ligne]. [Réf. 2021]. Disponible sur ISO/IEC TR 24030:2021(en), Information technology — Artificial intelligence (AI) — Use cases

[150] *Cas d'usage* [En ligne]. [Réf. 2021]. Disponible sur Use+cases-v05_electronic_attachment_022021.pdf (iso.org)

[151] *Sécurité des machines — En relation avec l'ISO 12100 — Partie 5: Implications de l'intelligence artificielle pour l'apprentissage automatique* [En ligne]. [Réf. De janvier 2021]. Disponible sur ISO - ISO/TR 22100-5:2021

[152] *Terry Wykle - séminaire IA et infrastructure ferroviaire* [Vidéo en ligne]. [Réf. 10décembre 2019]. Disponible sur Terry Wykle - séminaire IA et infrastructure ferroviaire

[153] *Qu'est-ce que le système de signalisation SIL des chemins de fer?* [En ligne]. [Réf. Du 14 janvier 2020]. Disponible sur What is Railway SIL Signaling System

[154] *LES DEFIS DE L'INTELLIGENCE ARTIFICIELLE – Benoit GEORGES* [En ligne]. [Réf. Du 27 aout 2018]. Disponible sur Les boîtes noires du « deep learning » | Les Echos

- Avoir une bonne gouvernance des données. Les données sont le carburant de l'IA. Pour le Pr Amal El Fallah Seghrouchni, on est sur le triptyque : données – objets connectés – Automatismes. L'un des soucis majeurs est lié la collecte des données et les problématiques de la Data Privacy. Concernant le domaine du développement durable et notamment dans le domaine industriel des transports, l'utilisation massive des IoT et aussi de l'IA pose la question de la consommation énergétique qui en découle[155]
- Disposer d'énormes puissances de calcul et gérer le problème de latence. Des SI critiques ne peuvent, en aucun cas, attendre les résultats d'une exécution longue d'un cycle d'apprentissage ;
- Établir des normes, des certifications ou labels sur l'IA. Le monde industriel est notoirement encadré par les normes, certifications, labels, standards, etc. On sait que les transformations de rupture ne peuvent s'opérer à date sans IA. Comment faire rentrer l'IA dans le moule des normes et autres processus de standardisation, sachant qu'aujourd'hui on ne certifie que ce qu'on connait complètement et ce dont le comportement peut être déterminé en fonction des entrées. Si on prend le cas de la conduite autonome, les algorithmes de machine learning sont déterministes. Les règles qui vont guider ces algorithmes sont créées au fur et à mesure de l'apprentissage par la machine elle-même sans qu'on en ait une quelconque maîtrise en fonction des données en entrée. À ce jour, personne ne sait qualifier le niveau de performance de ces types d'algorithmes en dehors du domaine d'entrée exactement équivalent à celui des données utilisées pour fabriquer le modèle. Ne plus pouvoir qualifier la performance dès que l'on sort du domaine de fonctionnement prévu à la conception représente un sérieux problème de sécurité[156] . Si on ne peut certifier l'IA, il existe tout de même des méthodes indirectes pour la contrôler. On peut utiliser d'autres systèmes qui fonctionnent sans IA pour la contraindre à son domaine de conception ;

IX.6. ASPECTS REGLEMENTAIRES ET JURIDIQUES

Lors de l'atelier de mars 2021 du FONCSI autour des enjeux de la sécurité ferroviaire de demain, le panel de participants s'est accordé qu'il faut se résoudre à « *Accepter que le temps de la réglementation soit plus long que celui des avancées technologiques : se focaliser sur la technologie et faire confiance au législateur qui adaptera le cadre réglementaire* ». Et qu'il fallait trouver des astuces pour faire avancer l'innovation par exemple en développant des espaces de conduite autonome isolés physiquement et réglementairement du reste du système. Il fallait aussi tourner la page de l'époque où le système ferroviaire avait son régime juridique d'exception, sa propre police[157].

Le cadre réglementaire européen est décrit dans le règlement d'exécution n°402/2013 de la Commission Européenne concernant la méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques applicable dans le secteur ferroviaire. Laurent Cébulski, (LC), Directeur Général de l'EPSF, lors de son interview[158], le confirme avec quelques exemples illustratifs : ce cadre indique notamment trois principes d'acceptation des risques :

- **L'application de règles de l'art** : en premier lieu les spécifications réglementaires et les normes dont il est admis que leur respect garantit un niveau de sécurité acceptable. Autrement dit, selon Laurent Cébulski, « *Si je suis conforme à la règle*

[155] Annexes I – Interview de Pr. Amal El Fallah Seghrouchi – COMEST UNESCO
[156] *White Paper Machine Learning in Certified Systems* [En ligne]. [Réf. Du 22 mars 2021]. Disponible sur White Paper Machine Learning in Certified Systems (archives-ouvertes.fr)
[157] *ATELIER SÉCURITÉ FERROVIAIRE DU FUTUR – FONCSI* [En ligne]. [Réf. Du 23 mars 2021]. Disponible sur synthese-atelier-ferroviaire-futur
[158] Annexe I: Interview Laurent Cebuslki, DG EPSF

européenne, ça vaut la présomption de sécurité. Par exemple, si mon frein est conçu selon la norme, je sais que mon train va freiner. Je n'ai donc pas besoin de faire de démonstration supplémentaire » ;

- **Une comparaison avec un système similaire** : dans la mesure où ce système a démontré au travers de son fonctionnement qu'il garantit un niveau de sécurité acceptable ; LC : « *mon matériel est conçu exactement de la même façon qu'un autre matériel, qui est autorisé, donc je préjuge que ce matériel va se comporter de la même façon, donc ça vaut également de barrière* » ;
- **Une estimation explicite des risques** : notamment nécessaire lorsque les deux premiers principes ne peuvent pas être utilisés, et lorsqu'on fait référence aux techniques de sûreté de fonctionnement. Ce principe est particulièrement utilisé dans le cadre d'innovations disruptives pour lesquelles aucun cadre réglementaire n'est défini et qu'il n'existe aucun système similaire. L'introduction croissante de nouvelles technologies tend à augmenter l'utilisation de ce principe. LC : « *la règle n'existe pas, le système de référence n'existe pas, donc je fais une démonstration basée sur la sûreté de fonctionnement* ».

Cette réglementation ferroviaire ne prévoit pas, à ce jour, de dispositions spécifiques à la cybersécurité ni d'interfaces avec les autorités et organismes compétents en la matière. Deux cas spécifiques où un besoin de cadre juridique est attendu ardemment : il s'agit d'une législation claire en cas d'attaque d'un opérateur ferroviaire avec des impacts humains et une réglementation en cas de défaillance liée à l'usage de produits, solutions, systèmes utilisant l'IA.

IX.6.1. CADRE EUROPÉEN EN CAS D'ATTAQUE DU FERROVIAIRE

Dans un marché unique européen où les entreprises sont de plus en plus interdépendantes, les impacts de l'agression d'un opérateur peuvent dépasser le territoire d'un seul État. La France a donc soutenu et largement contribué aux efforts de l'Union européenne pour développer le Programme européen de protection des infrastructures critiques.

Élément majeur du programme européen, la directive du Conseil sur la désignation et la protection des infrastructures critiques européennes du 8 décembre 2008 constitue un cadre pour l'amélioration de la sécurité des grandes infrastructures à vocation transnationale. C'est aussi un encouragement à développer et à améliorer les dispositifs nationaux de sécurité des activités d'importance vitale dans chacun des États membres. Cela permet d'éviter des distorsions de concurrence et de contribuer à une meilleure sécurité des activités économiques et des citoyens, c'est-à-dire à une résilience à l'échelle de l'Union européenne.[159]

IX.6.2. INTELLIGENCE ARTIFICIELLE, TRAINS AUTONOMES ET RESPONSABILITÉS JURIDIQUES

La problématique sur le contrôle de l'IA n'est pas spécifique au monde ferroviaire, mais exige une très haute attention au regard de la gravité des impacts qu'elle peut engendrer.

« Les victimes tolèrent moins les accidents lorsqu'ils sont provoqués par un automatisme plutôt que par l'erreur d'un opérateur humain." [160]

[159] *La sécurité des activités d'importance vitale* [En ligne] [Réf. Octobre 2016]. Disponible sur plaquette-saiv.pdf (sgdsn.gouv.fr)
[160] *ATELIER SÉCURITÉ FERROVIAIRE DU FUTUR – FONCSI* [En ligne]. [Réf. Du 23 mars 2021]. Disponible sur synthese-atelier-ferroviaire-futur

La filière ferroviaire européenne semble partagée, concernant la question relative du positionnement de l'intelligence dans le système : l'IA pour la conduite ou l'IA dans les systèmes à des fins d'assistance ?

La prédilection est pour une intelligence répartie dans le système, avec un arbitrage à faire sur la répartition entre les différentes entités (constructeur, opérateur, gestionnaire d'infrastructure…).

Les conséquences en matière de rôle, de compétence et de responsabilité des acteurs du ferroviaire seront drastiquement différentes selon le choix fait. Qui va endosser la responsabilité civile et pénale s'il y a un problème dans le logiciel que personne n'a su voir ? Le juge va s'attacher à ce qui était humainement vérifiable. La directive européenne concernant le secteur ferroviaire est très claire : la responsabilité pèse sur l'exploitant dudit matériel et il semble politiquement difficile d'envisager un changement de cadre législatif tout au moins à l'horizon 2030-40 ». Cette directive va sensiblement bouger, car on s'oriente suite à une proposition d'Alstom et appuyée par plusieurs acteurs à un déport de responsabilité sur les fournisseurs de services et solutions en raison de la certification qui sera plus sur les services et solutions que sur tout le train en lui-même et partant une responsabilité de l'exploitant dégagée.

IX.7. COOPERATION INCLUSIVE ET BESOIN DE CONFIANCE

Plusieurs groupes de travail et initiatives existent sous l'égide de l'UIC et/ou l'ENISA. Arriver à faire émerger les intérêts communs, mutualiser les forces en la matière et ne pas évoluer en blocs isolés et disparates est un gros challenge.

Comme indiqué dans le rapport de l'ENISA[161]

« *La mise en place d'un écosystème ISACs soutiendrait le renforcement des capacités de sécurité en Europe. Certains États membres comprennent déjà à quel point il est utile pour renforcer la résilience au niveau national (ISACs sectoriels et axés sur les pays). D'autre part, le secteur privé déclare souvent qu'il est utile de construire des partenariats transfrontaliers (ISAC internationaux) et d'échanger des informations sur les menaces à l'échelle européenne.*

Les ISAC pourraient également être un mécanisme utile dans la mise en œuvre de la directive NIS, car ils offrent un « niveau intermédiaire » entre les opérateurs de services essentiels et les CSIRT au niveau national. En recueillant des informations sur les menaces et les incidents et en soutenant leurs membres dans l'analyse de la vulnérabilité et des menaces, ils peuvent également contribuer de manière significative au processus de gestion des risques (en particulier l'évaluation des risques) aux niveaux national et international. »

Cette coopération nécessite une formation et mobilisation de ressources expertes dans le domaine, des ressources logistiques et financières et des canaux de communication. D'après l'enquête sur les CSIRT réalisée par l'ENISA en 2013, les obstacles techniques au partage paraissent plus nombreux, mais sont plus faciles à surmonter. Le plus difficile demeure les obstacles légaux et réglementaires.

Toutefois, quelques règles de base ont notamment été spécifiées pour encadrer la politique de partage d'information, notamment pour les « CSIRT ». C'est ce qui en ressort du rapport

[161] *Information Sharing and Analysis Center (ISACs) - Cooperative models* [En ligne]. [Réf. Du 14 février 2018]. Disponible sur Information Sharing and Analysis Center (ISACs) - Cooperative models — ENISA (europa.eu)

des différents travaux de l'ENISA[162]. Vu la sensibilité des informations manipulées et traitées par les CSIRT (SOC/CISRT) des mesures appropriées doivent être mises en place pour s'assurer que la portée des données fournies à des organisations externes est strictement contrôlée. Il en est de même de la catégorisation des informations, des destinataires, les modes et les circuits de distribution qui doivent faire l'objet d'une cartographie et parfaitement maîtrisée.

Concernant les transports ferroviaires de demain avec les transformations de rupture qui s'opèrent grâce à l'apport de l'IA, la coopération avec les universitaires et le monde de la recherche sont plus que fondamentaux.

Face aux menaces et sources de menaces multiples et protéiformes, l'Europe a tout intérêt à consolider ses forces. Cela passe par l'engagement des acteurs de l'UE, la confiance mutuelle et le partage d'informations, facteurs clés d'une Europe forte en cybersécurité.

X. BILAN ET RECOMMANDATIONS

X.1. BILAN

Le rapport de l'ENISA de novembre 2020 dresse une liste des principaux constats et des difficultés parmi lesquels :

- **La faible sensibilisation au numérique et à la cybersécurité dans le secteur ferroviaire**.
- **La complexité de la réglementation en matière de cybersécurité** :
  Plusieurs entreprises signalent qu'au-delà de la directive NIS, elles doivent se conformer à d'autres lois nationales, telles que celles relatives à la sécurité nationale ou aux infrastructures critiques ; il y a nécessité de lignes directrices opérationnelles plus souples pour s'adapter aux spécificités et à l'organisation du secteur ferroviaire.
- **La difficulté à concilier les mondes de la sécurité et de la cybersécurité** :
  Dans le secteur ferroviaire, l'importance des exigences de sécurité est incontestable. Pour que chaque mise à jour introduise des dispositions en matière de cybersécurité, les équipes de sécurité doivent s'assurer que les mécanismes de sécurité restent intacts. Cela nécessite plus de temps et d'argent que les décisionnaires doivent prendre l'habitude de prévoir.
- **La transformation numérique du cœur de métier ferroviaire** :
  Ces changements introduisent de nouvelles vulnérabilités et soulignent la nécessité pour les systèmes OT de se conformer aux mêmes dispositions de cybersécurité, voire à des dispositions plus élevées, que les systèmes informatiques. Les actifs réseau, les périphériques connectés au réseau, les développements logiciels doivent être traités avec le même soin (ou plus) dans le domaine opérationnel. Comme les systèmes informatiques, les systèmes OT doivent être livrés avec des outils de surveillance, de supervision et d'administration intégrés. En outre, les nouveaux systèmes OT doivent désormais intégrer les exigences de sécurité et de cybersécurité dès leur conception (security by design).

[162] *Actionable information for security incident response – ENISA* [En ligne]. [Réf. Du 19 janvier 2015]. Disponible sur Actionable information for security incident response — ENISA (europa.eu)

- **La dépendance à l'égard de la chaîne d'approvisionnement pour la cybersécurité** :
  Les opérateurs ferroviaires dépendent fortement de leurs fournisseurs et autres tiers (y compris cloud) pour les mises à jour du système, la gestion des correctifs et la gestion du cycle de vie des composants. Les dispositions applicables aux fournisseurs ne sont pas définies dans le cadre de la directive NIS, de sorte qu'ils ont des exigences légales moins strictes pour appliquer la cybersécurité. Les normes CEI 62443 ou la TS 50701 sortis en juillet 2021, bien qu'intégrant des exigences de suivi de la chaîne d'approvisionnement, ne sont pour autant pas prescriptives. Il reste donc aux entreprises à s'assurer comme l'indiquent Jean-Baptiste Renaud, Yseult Garnier et Quentin Rivette[163] de le prévoir dans les appels d'offres et surtout dans les contrats.
- **La maintenance prédictive au service de la performance économique** :
  La maintenance prédictive à base d'algorithmes d'IA et de données collectées par des capteurs permet de fiabiliser les données relatives à l'état d'usure (normale ou anormale) d'un composant. Elle permet ainsi d'éviter des coûts inutiles liés aux remplacements préventifs systématiques qui prévalent de nos jours. En effet, pour se prémunir d'une dégradation qui pourrait s'avérer inacceptable, il arrive souvent de remplacer des matériels qui fonctionnent encore.
- **L'étendue géographique de l'infrastructure ferroviaire** :
  Le déploiement géographique du système ferroviaire est en lui-même un critère qui rend difficiles et coûteuses la mise en œuvre ou la mise à jour des mesures de sécurité.
- **La nécessité d'établir un équilibre entre sécurité, compétitivité et efficacité opérationnelle** :
  La sécurité et la cybersécurité dans le ferroviaire ont un coût proportionnel à la dimension géographique. Il s'agit donc de trouver le bon équilibre entre sécurité (sensible ici puisqu'il s'agit de sécurité de personnes) et compétitivité et efficience opérationnelle. Le principe de GAME (Globalement Au Moins Équivalent) sur lequel repose le ferroviaire et qui voudrait qu'à chaque évolution, on démontre que le niveau de sécurité du nouveau système est au moins équivalent au niveau de sécurité du système précédent est considéré par ailleurs comme un frein à l'innovation. Pour plusieurs experts du secteur, ce critère (basé sur des données antérieures) est difficile à utiliser pour établir une analyse de risques de bout en bout lorsqu'il s'agit d'une modification systémique ; ils estiment qu'il faudrait dépasser cette logique comparative basée sur l'expérience et un contexte passé, et utiliser des méthodes d'évaluation du taux de panne plus modernes[164].

[163] Annexes I - Interviews (JBR, Alstom, YGR & QRE de SNCF)
[164] *ATELIER SÉCURITÉ FERROVIAIRE DU FUTUR – FONCSI* [En ligne]. [Réf. Du 23 mars 2021]. Disponible sur synthese-atelier-ferroviaire-futur

X.2. RECOMMANDATIONS

Elles sont relatives à la filière ferroviaire au sein de l'UE.

- ✓ **Améliorer, visibiliser et fluidifier la gouvernance ;**
- ✓ **Développer une véritable coopération inclusive avec toutes les parties prenantes ;**
- ✓ **Développer une plateforme solide et sécurisée de partage d'informations ;**
- ✓ **Investir massivement dans la recherche et l'innovation :**
  - Développer les expérimentations notamment autour de l'IA ;
  - Développer des labels européens en cybersécurité ;
- ✓ **Harmoniser les normes nationales avec les normes européennes en cybersécurités ;**
- ✓ **Développer une stratégie offensive européenne en cas de cyberattaque étatique ;**
- ✓ **Développer une Intelligence en cybersécurité :**
  - Partager les menaces et les impacts de cyberattaques dans le ferroviaire ;
- ✓ **Mettre en place une législation européenne et internationale relative aux attaques de SI industriels critiques ;**
- ✓ **Définir des législations adaptées aux cas d'usage des technologies à base d'IA et les chaînes de responsabilités idoines ;**
- ✓ **Accélérer les programmes de développement durable.**
- ✓ **Mettre en place des programmes communs pour acculturer tout le personnel à la cybersécurité et en particulier celui du domaine de sécurité et d'exploitation.**

PARTIE II – LE FERROVIAIRE, SYSTÈME INDUSTRIEL ET ENJEUX DE TRANSFORMATION DIGITALE ET SÉCURISATION NUMÉRIQUE

I. INTRODUCTION

Avec ses 472 milliards de passagers-kilomètres, 216.000 km de voies ferrées actives et 430 milliards de tonnes-kilomètres pour le transport de marchandises, le secteur ferroviaire joue un rôle clé en Europe. Ce rôle clé l'oblige par ailleurs à se conformer aux lois et réglementations en matière de cybersécurité, aux normes internationales et meilleures pratiques qui protègent les clients et les employés.

Des bouleversements majeurs s'opèrent dans le monde ferroviaire. La digitalisation, l'automatisation[165] et la transformation[166] du modèle économique de ce secteur amènent avec elles des flots d'opportunités et des leviers pour accroître la compétitivité des entreprises du secteur[167]. A cela s'ajoute, les enjeux du transport en commun et le nombre croissant d'interconnexions avec des systèmes externes et multimodaux. Ce secteur évolue et s'ouvre aussi progressivement à la concurrence. Cela conduit à une redistribution des responsabilités et à la séparation des systèmes et des infrastructures ferroviaires, avec un impact direct sur les systèmes informatiques correspondants.

À l'instar d'autres secteurs il y a quelques années, comme le bancaire en particulier, les transformations digitales qui s'opèrent dans le secteur ferroviaire font naitre de nouvelles menaces protéiformes par l'augmentation des surfaces d'exposition aux cyberattaques. Le secteur attire comme dans beaucoup d'autres secteurs, des cybercriminels avec une motivation financière, des activistes et groupes avec des visées géopolitiques et des manœuvres de déstabilisation, des agents et groupes parrainés par des États malveillants, des terroristes, mais aussi potentiellement des employés mécontents ou licenciés ayant encore accès aux systèmes[168]. Les entreprises, les organisations, les États et l'Union européenne se doivent de se doter d'outils de la Cyber Intelligence et de moyens pour assurer la souveraineté, la sécurité, la compétitivité ainsi que le développement durable de leurs industries ferroviaires. L'ampleur du marché de la cybersécurité dans ce secteur est un indicateur fort des enjeux que porte ce secteur et aussi de l'attractivité qu'il peut susciter de la part des cybermalveillants. Le marché de la cybersécurité ferroviaire va plus que doubler d'ici 2027 et passer de 6Mds$ en 2019 à 12,6 Mds$[169].

Dans cette partie nous présentons dans un premier temps le système industriel ferroviaire, ses enjeux, notamment ceux relatifs à la convergence IT, OT et les transformations digitales sans précédent qui s'opèrent en son sein.

Nous aborderons la problématique de cybersécurité, un pilier incontournable de la pérennité de l'activité ferroviaire. Il sera question au regard de l'état de l'art et des différents retours d'expérience de partager les fondamentaux d'une véritable posture de cybersécurité notamment sur les aspects non seulement techniques, mais aussi transverses comme la gouvernance, les questions juridiques et réglementaires, la sensibilisation et la formation.

---

[165] Jana Pieriegud**,** *Digital transformation of railways* [En ligne]. [Réf. du 12 avril 2018]. Disponible sur https://files.stample.co/browserUpload/1ec2baf0-38da-4b52-9150-f7b9651ee3a9

[166] *Globalrailwayview, Digitalisation and rail's future: Q&A with Siemens Mobility's Gerhard Kreß.* [En ligne]. [Réf. du 19 juin 2019]. Disponible sur gerhard-kress-siemens-mobility-interview/

[167] European Parliament, *Digitalisation in railway transport. A lever to improve rail competitiveness*. [Rapport en ligne]. [Réf. du 20 Févr. 2019]. Disponible sur https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635528/EPRS_BRI(2019)635528_EN.pdf

[168] *Railway cybersecurity training. Cybersecurity training for railway undertakings (RU) and infrastructure managers (IM)* [En ligne]. Disponible sur https://www.railway-cybersecurity.com/

[169] Marketsandmarkets Report. *Cybersécurité ferroviaire : d'énormes opportunités avec la diversification du marché* [En ligne]. [Réf. du 03 février 2021]. Disponible sur https://www.marketsandmarkets.com/Market-Reports/railway-cybersecurity-market-128598673.html

Un chapitre sera par ailleurs consacré à la gestion des risques avec une vue systémique et holistique au regard de l'ampleur de la couverture des activités et des personnes qui portent la filière.

II. LA FILIÈRE FERROVIAIRE : MISSIONS, ENJEUX ET MÉTIERS

II.1. MISSIONS

Les missions principales du secteur sont les suivantes :

- Le transport de voyageurs par les différents matériels roulants : TGV, trains régionaux, tramways, métros, RER, etc.
- Le transport de marchandises (le fret)

Pour assurer ses missions principales, le secteur doit assurer l'installation, l'exploitation et la maintenance dans le temps de l'ensemble des infrastructures ferroviaires (lignes, matériels roulants). De plus il lui revient de veiller à la sécurité des trains voyageurs, trains de travaux, trains de marchandises (fret).

Maintes fois, le transport ferroviaire a démontré qu'il était un secteur d'activité d'intérêt vital pour la France. Ainsi après la seconde guerre mondiale, à la Libération, il a été l'un des vecteurs essentiels de la reconstruction du pays, permettant son approvisionnement en matières premières et en denrées vitales. Durant la sécheresse de l'été 1976, grâce à des affrètements spéciaux, les éleveurs de troupeaux ont été livrés en fourrage, avec près de 650 k tonnes de paille acheminées par trains entre juillet et décembre 1976. Cette même opération a été renouvelée en 2003 et en 2011.

Aujourd'hui, avec la crise sanitaire, liée à la pandémie du SARS-CoV-2, dit COVID19, l'intérêt vital des autoroutes ferroviaires n'est plus à démontrer. Elles ont assuré durant le confinement l'approvisionnement du territoire en denrées alimentaires, produits essentiel, mais ont également permis le fonctionnement des industries nécessaires à la vie quotidienne des citoyens en les approvisionnant en matières premières essentielles.

Trois catégories de train ont permis de réaliser ces missions :

- Les *trains vitaux Nation* (environ 10 % du trafic nominal) ont permis le transport du chlore permettant l'assainissement de l'eau courante, le transport du gaz de pétrole liquéfié, les granulés de bois nécessaires aux centrales urbaines pour le chauffage, notamment à destination des hôpitaux ;
- Les *trains vitaux pandémie* (environ 20 % du trafic nominal) ont permis le transport des denrées essentielles pour la population, mais aussi les céréales nécessaires à la production des pâtes, les fruits et légumes, la poudre de lait, ou encore la chimie et le PVC nécessaires aux industries pharmaceutiques et médicales (fabrication des seringues, des poches médicales, confection des masques, etc.) ;
- Les *trains de continuité industrielle* (15 à 30 % du trafic nominal) ont permis aux usines stratégiques de continuer à fonctionner. Ils ont permis de contenir le ralentissement de l'activité du fait de manque de matière ou de la baisse des demandes.

Si le transport des voyageurs durant le confinement était en sommeil, les trains ont permis dans des conditions optimales, les transferts des malades atteints de la COVID19 entre les établissements de santé des grandes villes, permettant de désengorger les centres hospitaliers des zones saturées par la pandémie en les délestant sur les zones moins touchées.

Outre les missions que nous venons de citer, le train est le levier par excellence de la transformation et du dynamisme de l'économie d'un État. Seulement pour la France, on dénombre environ deux milliards de passagers transportés en 2019. Ce qui illustre la place prépondérante du transport ferroviaire dans la mobilité moderne et cela va en croissant. La bonne tenue de cette place passe la conception des trains « propres », sûrs, confortables, connectés, offrant une qualité de service optimale, et circulant sur une infrastructure moderne. Ce qui s'accorde bien avec les objectifs de l'observatoire de la métallurgie[170].

II.2. ENJEUX ECONOMIQUES, SOCIETAUX ET ENVIRONNEMENTAUX

Le secteur ferroviaire est tiré par des besoins de performance économique et d'accroissement de parts de marché dans un contexte de concurrence de plus en plus prégnante. Cette concurrence est notamment accentuée en France par l'ouverture du marché, alors que cette ouverture est une réalité depuis plusieurs années dans d'autres pays européens. De plus le secteur est réglementé par des directives et les réglementations européennes et a une pression liée aux inéluctables évolutions sociétales qui requièrent entre autres : une augmentation de la capacité de transport et un accroissement de la fréquence des trains nationaux et internationaux.

Pour accompagner ces bouleversements, il est essentiel de :

- Garantir la sécurité dont une part prépondérante du volet cybersécurité ;
- Diversifier les offres aux clients (avec différents services multimodaux) ;
- Proposer une expérience usager optimale et adaptée ;
- Réduire l'impact environnemental : du fait de l'augmentation des volumes engendrant des besoins énergétiques supplémentaires. Dans la logique du remplacement progressif des énergies fossiles par des énergies plus vertes, le domaine du transport ferroviaire se place parmi les meilleurs élèves de la Quatrième révolution industrielle. Le challenge est de conserver ce statut en imaginant le transport du futur avec la composante énergétique. Il y a une réelle réflexion à mener concernant l'usage d'énergies alternatives comme l'hydrogène, les hybrides, le tout électrique ou au bio-GNV[171]. La digitalisation combinée à l'optimisation de la consommation d'énergie, par exemple avec l'ajustement de l'éclairage ou de l'air conditionné en fonction des conditions extérieures et du taux d'occupation réel des trains, est un bon exemple de cas d'usage.
- Accélérer l'innovation et l'ouverture à la concurrence du transport de voyageurs incite les différents opérateurs et acteurs de la filière à augmenter leur productivité, améliorer leurs performances du réseau, à investir dans l'innovation et améliorer la qualité du service des clients finaux, en cherchant à progresser sans cesse en fiabilité, à augmenter la sécurité et la ponctualité, à répondre aux besoins d'information et de communication, et enfin à améliorer le confort ressenti.

Tout ceci ne peut se faire sans une véritable stratégie du maintien des compétences dans les différents domaines historiques et la montée en compétences dans les nouveaux domaines comme la cybersécurité, l'intelligence artificielle, la data et la data analyse sont essentiels et structurants.

Une réduction des coûts globaux d'utilisation, enjeux importants, sera une des clés de réussite. Aborder les sujets par une vue limitante de réduction des coûts globaux (certes

[170]Observatoire Prospectif et Analytique des Métiers et Qualifications de la Métallurgie Secteur Ferroviaire [En ligne]. Disponible sur https://www.observatoire-metallurgie.fr/secteurs/ferroviaire
[171] Gaz-mobilite.fr [En ligne]. Disponible sur https://www.gaz-mobilite.fr/dossiers/biognv-definition-biogaz/

un enjeu crucial) sans vision globale et un investissement massif risque s'avérer à la longue comme une erreur stratégique majeure.

II.3. PANORAMA DES ACTIVITES METIERS

Le transport ferroviaire est un secteur qui innove constamment pour transformer les voies ferrées, les gares ou les trains afin d'accueillir et accompagner les voyageurs. Il se veut un des moyens de transport les plus sûrs et les plus écologiques. Il existe aujourd'hui plus de 160 métiers dans le secteur du ferroviaire[172] autour des activités suivantes :

- Accueil en gare et accompagnements des voyageurs ;
- Billetterie ;
- Préparation et conduite des trains ;
- Organisation et gestion de la circulation des trains ;
- Entretien et sécurisation du réseau ferré et des matériels ;
- Sécurité des gares et à bord des trains ;
- Gouvernance, développement et management du ferroviaire.

Pour faire circuler un train, plusieurs composantes sont sollicitées : le train lui-même, les rails, les systèmes de distribution d'électricité, les feux de signalisation, les ponts, les tunnels et viaducs, les systèmes d'aiguillage, les passages à niveau, les croisements, les télécommunications, la sécurité, les nouvelles technologies (innovantes et modernes)[173], les stations de remisage, les équipements industriels de maintenance[174],[175].

Le champ de couverture des activités est vaste. La compréhension des segments d'activité et des métiers est un préalable pour mieux appréhender les enjeux métiers et les enjeux de sécurité inhérents.

Les principaux segments d'activité relevant de l'exploitation industrielle sont[176] :

- La gestion des infrastructures ferroviaires ;
- La gestion du matériel roulant ;
- La gestion de la circulation : c'est une activité d'importance capitale qui nécessite :
  - ✓ Une bonne gestion des horaires : la conception et l'adaptation des plans de transport permettent à des milliers de trains de circuler quotidiennement, de faire cohabiter toutes les entreprises ferroviaires sur le réseau et gérer aussi des demandes de circulation de dernière minute impliquant différents gestionnaires ;
  - ✓ Une maîtrise de la signalisation : ce point est au cœur du modèle ferroviaire de manière générale comme on le verra dans le chapitre suivant. Pour transmettre au conducteur des ordres et informations liées à la sécurité des circulations, il est en effet fait usage de signaux[177];
  - ✓ Un système d'aiguillage (mécanique ou électrique) sous contrôle. L'aiguillage permet de donner une direction au train, de l'orienter sur une voie ou une

---

[172] *Les métiers du ferroviaire Collection : Zoom sur les métiers*. Onisep. Juillet 2021. [En ligne]. [Réf. De 2017]. Disponible sur https://www.utp.fr/system/files/Dpt_social/UTP_SOC_290817_Les_metiers_du_ferroviaire_-_ONISEP_ADFPMF.pdf

[173] *SNCF Réseau et ses métiers de la maintenance, des travaux et de la circulation ferroviaire.* [Vidéo en ligne]. Disponible sur https://www.youtube.com/watch?v=wqwdAeh98Mk

[174] SNCF, *SNCF Réseau et ses métiers de la maintenance, des travaux et de la circulation ferroviaire*. [En ligne]. [Réf. du 28 mai 2020]. Disponible sur https://www.youtube.com/watch?v=wqwdAeh98Mk

[175] Philippe Gaufreteau, Lilian Planche, *Cybersécurité des systèmes de, transport application à la ligne 18 du Grand Paris express* [en ligne]. [Réf. du 20 mars 2019]. Disponible sur https://hal.archives-ouvertes.fr/hal-02074202/document

[176] Jean-François Lecole. *Étude prospective sur la filière matériel roulant ferroviaire horizon 2015 –2025*. Rapport novembre 2015 [En ligne]. Disponible sur https://www.observatoire-metallurgie.fr/secteurs/ferroviaire

[177] EPSF - *Les signaux. Les régimes d'exploitation des lignes. Les systèmes d'espacement des trains* [En ligne]. [Réf. du 05 juillet 2017]. Disponible sur https://securite-ferroviaire.fr/sites/default/files/users/reglementations/pdf/document-pedagogique-signaux-regimes-exploitation-v1.pdf

autre[178]. Une erreur dans l'aiguillage a pour conséquence des retards voire des accidents de trains ;

- La supervision, la surveillance :
  - ✓ La surveillance du réseau ferré est une fonction de veille sur les installations de signalisations électriques ou mécaniques, les aiguillages, les caténaires ainsi que les installations informatiques et de télécoms. Détecter rapidement la panne du système d'aiguillage causée par un morceau de ballast, un bloc de glace ou un quelconque autre objet coincé dans l'aiguille accélèrera sa réparation ou son remplacement et préviendra une éventuelle collision par mauvais aiguillage d'un train ;
- ➢ La maintenance : la maintenance des installations du système ferroviaire est un élément vital de la continuité des activités[179]. On l'abordera amplement dans le document, la maintenance prédictive est au cœur des enjeux aussi bien environnementaux que financiers.

III. LE FERROVIAIRE INDUSTRIEL ET LA CONVERGENCE IT-OT

Avant d'aborder les problématiques de gouvernance ou purement opérationnelles, il est primordial de mieux appréhender les systèmes au cœur de la machinerie ferroviaire, à savoir son écosystème industriel : une machinerie lourde et d'une complexité hors normes.

III.1. LE MODELE FERROVIAIRE

Le modèle ferroviaire actuel se fonde sur le principe non négociable de Sûreté dit *Safety* : les trains doivent circuler en toute sécurité. Tous les modèles mathématiques et l'ingénierie lourde et complexe sur lesquels se base l'industrie ferroviaire ont pour finalité ultime de résoudre les problématiques suivantes :

- ➢ La survitesse et le déraillement ;
- ➢ Les collisions de tout ordre : latérales (prise en écharpe), frontales (nez à nez), avec un obstacle (animaux…) ou avec des véhicules routiers. Pour cela, il est interdit aux trains d'occuper une section de voie (le canton) quand il y a déjà un train dans cette section[180].

Le système industriel ferroviaire repose en grande partie sur son système de signalisation. Son rôle est d'une importance de tout premier plan dans l'orchestration de toute la machinerie industrielle qui se doit d'être bien huilée. Au fil du temps, la signalisation a évolué pour passer des signaux manuels jusqu'aux systèmes de contrôle commande informatisés, avec toujours l'exigence de garantir une utilisation non conflictuelle de ressources d'infrastructure pouvant conduire à un accident[181].

Maîtriser la signalisation ferroviaire est, en conséquence, la condition sine qua none à la sécurité ferroviaire. Les vies humaines étant directement en jeu, la SAFETY est inscrite en lettre d'or. Tout est mis en œuvre pour une vigilance sur les risques relatifs à la sûreté de fonctionnement au regard des niveaux d'exigences SIL (Safety Integrity Level) attendu.

---

[178] SNCF - *L'aiguillage sous toutes ses coutures*. [en ligne]. [Réf. du 23janvier 2019]. Disponible sur https://www.sncf.com/fr/itineraire-reservation/informations-trafic/reportages/systeme-aiguillage

[179] UIC*, Solutions techniques pour le rail opérationnel.* [En ligne]. [Réf. du 10 mai 2021]. Disponible sur https://uic.org/IMG/pdf/uic-solutions-techniques-pour-le-rail-operationnel.pdf

[180] Christian Chaumette, *Le contrôle/commande ferroviaire* [En ligne]. [Réf. du 10 décembre 2020]. Disponible sur https://www.techniques-ingenieur.fr/base-documentaire/ingenierie-des-transports-th14/materiel-roulant-ferroviaire-42630210/le-controle-commande-ferroviaire-trp3075/contexte-trp3075niv10001.html?lectureFacile=true

[181] Maurizio Palumbo, *La signalisation ferroviaire depuis la naissance jusqu'à ERTMS***.** [En ligne]. [Réf. novembre 2015]. Disponible sur http://www.railwaysignalling.eu/wp-content/uploads/2015/07/White_Paper_Signalisation_Ferroviaire.pdf

On parle de sécurité du système ferroviaire dans sa globalité : le train avec l'ensemble de ses différentes composantes qui concourent à sa bonne marche. Comme nous le confirme Quentin Rivette, Responsable Cybersécurité Industrielle, chez SNCF Voyageurs[182], une série d'analyse de sécurité ferroviaire et sûreté de fonctionnement est menée pour démontrer la robustesse globale du système. Tous ces tests ont pour objectif d'aboutir à un risque résiduel acceptable avec pour principe général : le risque résiduel ne doit pas excéder le risque tolérable. Au final, c'est à l'exploitant de l'installation d'accepter et/ou d'assumer le risque résiduel[183].

Le système ferroviaire est doté de plusieurs systèmes de sécurité, de système de contrôle de vitesse par balise appelée KVB[184], système de Transmission Voie MachineTVM[185], et du Système européen de Régulation du Trafic ferroviaire (ERTMS) en plus des systèmes de répétitions des signaux et le DART (Dispositif Automatique D'Arrêt de Train).

D'autres mécanismes de protection viennent s'ajouter aux autres dispositifs de sécurité. C'est le cas des systèmes de protection des trains (ATP : Automatic Train Protection) introduits en Europe dans les années 80, afin d'améliorer la sécurité en surveillant en permanence la vitesse du train. En France, dans les réseaux historiques, c'est le système KVB de contrôle de vitesse par balise qui en assure la fonction avec des alertes sonores pour informer le conducteur en cas de franchissement d'un signal fermé (non-autorisation de rouler) ou de dépassement de la limitation de vitesse. Aussi ce système prévoit un freinage automatique avec un système de type VACMA (Veille Automatique à Contrôle du Maintien d'Appui), si le conducteur ne réagit pas dans un délai donné aux avertissements.

Outre les problématiques de survitesse et de collision précédemment évoquées, se pose également le problème d'interopérabilité. Jusqu'ici chaque pays voire certaines régions d'un même pays avait des implémentations spécifiques de système ATP. En France, par exemple, au moins deux systèmes coexistent à ce jour. Permettre un déplacement transnational d'un train nécessite de disposer du système ATP du pays traversé. On se retrouve dans certains cas avec neuf équipements de sécurité dans les trains ! Pour pallier à cette problématique et permettre une libre circulation des trains dans l'espace européen, une version interopérable et normalisée du système de contrôle/commande (ATP/ATC) sous la dénomination ETCS (European Train Control System) a été choisie pour le standard ERTMS.

Dans les deux prochaines sections, nous aborderons les deux paradigmes clés du système ferroviaire à savoir la signalisation et le système de contrôle commande.

III.2. LE SYSTEME DE GESTION DU TRAFIC FERROVIAIRE EN EUROPE - ERTMS

À la fin de l'année 1990, sous l'impulsion de l'Institut européen de la Recherche Ferroviaire (ERRI, European Rail Research Institute), a été développé un système ATP commun aux pays européens. Ce système, reconnu aujourd'hui sous la dénomination ERTMS/ETCS, est le standard actuel de la signalisation Européenne.

---

[182] Annexes I - Interview Quentin Rivette – RCS-I SNCF Voyageurs

[183] Endress+Hauser, *Sécurité fonctionnelle – SIL Les systèmes instrumentés de sécurité dans l'industrie des process* [En ligne]. [Réf. du 18 février 2014]. Disponible sur https://bdih-prod-assetcentralapi-assetcentral-rest-srv.cfapps.eu10.hana.ondemand.com/files/DLA/0600F01300141EE3A6906064952DFD94/CP01008Z11FR_0313_SIL-BD.pdf

[184] F. Lisiecki, *Système de signalisation de classe B : Contrôle de Vitesse par Balises (KVB) – Equipement bord. SAM S 707* [En ligne]. [Réf. du 17 avril 2017]. Disponible sur https://securite-ferroviaire.fr/reglementations/systeme-de-signalisation-de-classe-b-controle-de-vitesse-par-balises-kvb-equipemen-0

[185] P. Houcho, *Système de signalisation de classe B : Transmission Voie Machine (TVM 430 et bi-standard ERTMS/TVM) Équipement bord SAM S 706* [En ligne]. [Réf. du 23 mai 2016]. Disponible sur https://securite-ferroviaire.fr/sites/default/files/users/reglementations/pdf/sam-s706-v2-mac.pdf

L'ERTMS (European Railway Traffic Management System) est destiné à remplacer les 27 systèmes de signalisation ferroviaire en service en Europe. C'est un projet industriel majeur développé par huit membres de l'UNIFE (Union des industries ferroviaires européennes) composé d'Alstom Transport, AZD Praha, Bombardier Transport, CAF, Hitachi Rail STS, Mermec, Siemens Mobility et Thales, en étroite coopération avec l'Union européenne, les acteurs ferroviaires et les membres de l'industrie du Système mondial de communications mobiles des Chemins de fer (GSM-R)[186].

Son déploiement est progressif, et il doit se faire sur les infrastructures au sol et sur le matériel roulant.

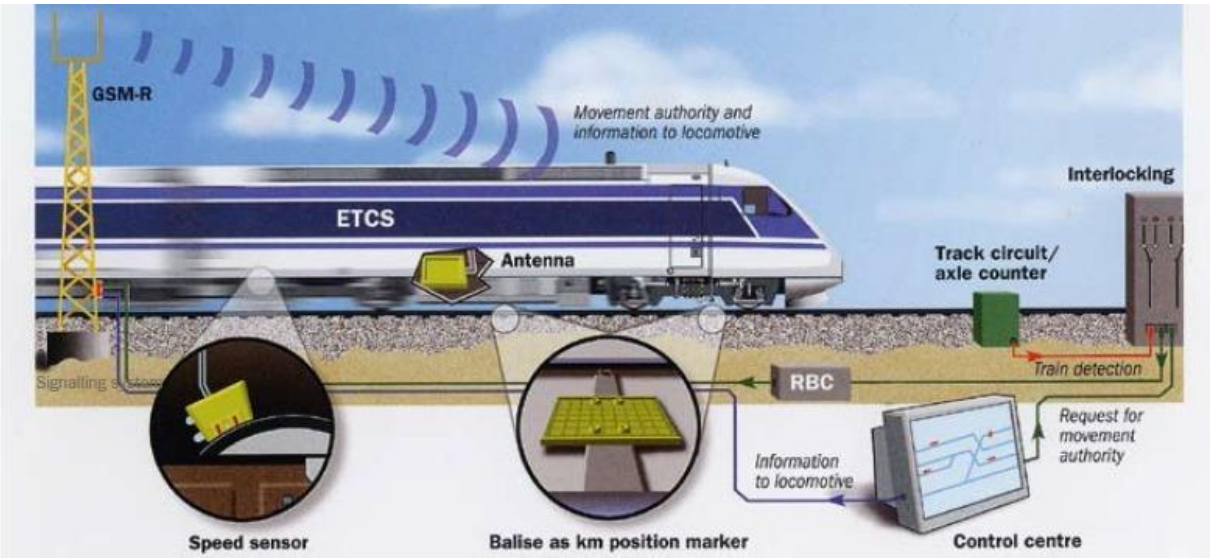
Il est composé pour la partie « commande contrôle » des trains, du système, ETCS. Il se base du GSM-R pour la communication par support radio. Il existe 4 niveaux de système de contrôle[187] :

- Avec le niveau 0, aucune supervision du train n'est assurée, seul un contrôle de vitesse est effectué ;
- Avec le niveau 1, le contrôle est opéré grâce à la transmission ponctuelle des signaux à l'aide de balises : c'est lors du passage au-dessus de la balise que le train obtient l'autorisation de se déplacer sur le canton suivant ;
- Le niveau ETCS 2 repose sur la radiocommunication numérique. Les installations de signalisation extérieures (balises) deviennent donc superflues, à l'exception de quelques indicateurs ;
- Pour le dernier niveau, l'ETCS 3, la signalisation latérale ainsi que les équipements de voie ne sont plus nécessaires. Comme avec l'ETCS niveau 2, les trains se localisent au moyen de balises de positionnement. Cependant l'ETCS 3 n'est pas encore complètement adopté et se déploie petit-petit à titre expérimental. L'aspect économique est aussi rédhibitoire : l'ETCS3 nécessite le remplacement de tous les systèmes de signalisation actuels. Il est prévu que cette technologie soit déployée sur la ligne Marseille-Vintimille et sur la ligne à grande vitesse Lyon-Paris, sans interruption du trafic, à partir de l'année 2025[188].

[186] Matthias Ruete, *Le Système européen de gestion du trafic ferroviaire* [En ligne]. Disponible sur https://transport.ec.europa.eu/transport-themes/infrastructure-and-investment/trans-european-transport-network-ten-t/european-rail-traffic-management-system_pt

[187] Annexe II - Les systèmes ETCS

[188] Morand Fachot**,** *Protecting railway networks from cyber threats. Rail networks, as integral parts of critical infrastructure, continue to come under cyberattack*. [En ligne]. [Réf. du 15 mars 2018]. Disponible sur https://etech.iec.ch/issue/2018-02/protecting-railway-networks-from-cyber-threats



27 - ERTMS / ETCS – Niveau 2 sur la ligne de Botnie[189]

La technologie ETCS de l'ERTMS donne au conducteur des informations en temps réel : occupation de la ligne, sa vitesse limite, la capacité de décélération et de freinage qui dépend également du poids du train. Les données ainsi transmises au conducteur lui permettent d'ajuster sa vitesse et d'adopter les bonnes mesures en cas d'urgence[190]. Cette technologie a été adoptée de facto comme un standard international.

III.3. LA COMMANDE CENTRALISEE DU RESEAU (CCR) ET LE SYSTEME DE CONTROLE ET DE GESTION DES TRAINS (TCMS)

Le CCR et le TCMS sont des dispositifs critiques dans la machinerie de l'exploitation ferroviaire. Ces deux dispositifs embarquent déjà de l'IT. Leurs interconnexions grandissantes avec une multiplicité de composants IT va par construction, augmenter leurs niveaux d'exposition aux attaques.

En France, par exemple, 1500 postes d'aiguillage gèrent les itinéraires sur le réseau principal avec 277 secteurs de circulation. Pour moderniser la gestion de ces flux, la commande de ces postes d'aiguillage est centralisée dans un CCR pour une fluidification du trafic offrant un meilleur service aux voyageurs et une meilleure exploitation ferroviaire.

Le TCMS (Train Control and Monitoring System) est quant à lui un dispositif central dans la coordination du contrôle et de la surveillance entre des systèmes disparates. On le désigne souvent comme étant le « cerveau du train »[191]. Il permet d'intégrer des données de plusieurs systèmes, fournissant des services aux conducteurs, aux responsables de la maintenance et aux passagers. Il est actuellement déployé sur la totalité des applications ferroviaires françaises. Un TCMS est un système de contrôle distribué embarqué dans le train et conçu dans le but de contrôler et de surveiller une liste d'équipements et de processus fonctionnels des trains. Basé sur une architecture de contrôle et de surveillance,

[189] [En ligne] https://www.researchgate.net/profile/Mats-Baeckstroem/publication/228863349/figure/fig4/AS:667775970328577@1536221606423/The-European-Rail-Traffic-Management-System-ERTMS-level-2-for-the-Bothnia-line-in.png

[190] SNCF, *Le réseau du futur* [En ligne]. Disponible sur https://www.sncf-reseau.com/fr/entreprise/newsroom/sujet/entreprise-ambition-reseau-futur

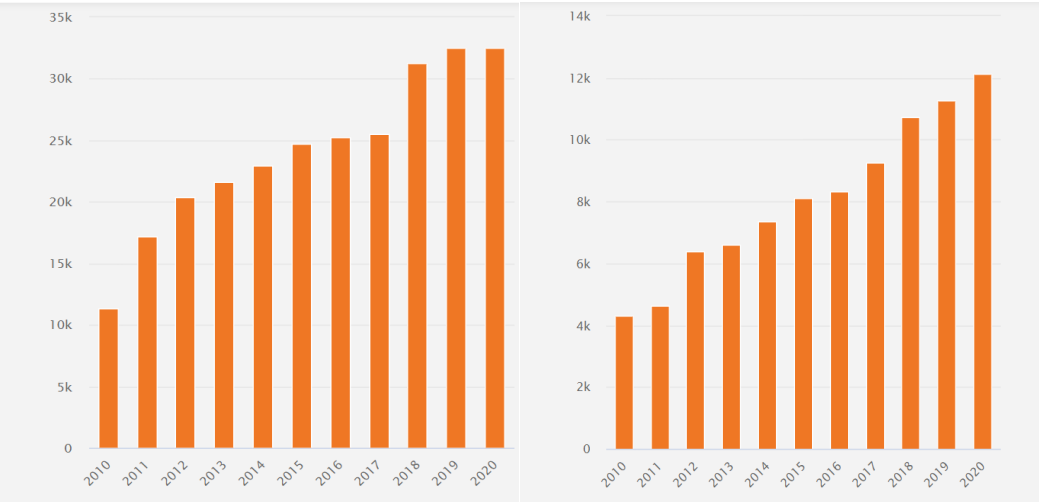
[191] Railengineer, What is TCMS. *Train Control & Management System (TCMS) is a train-borne distributed control system.* [En ligne]. [Réf. du 11 août 2015]. Disponible sur https://www.railengineer.co.uk/what-is-tcms/?nowprocket=1

le TCMS centralise toutes les informations relatives à l'état de fonctionnement de tous les équipements ferroviaires dits « intelligents[192] ».

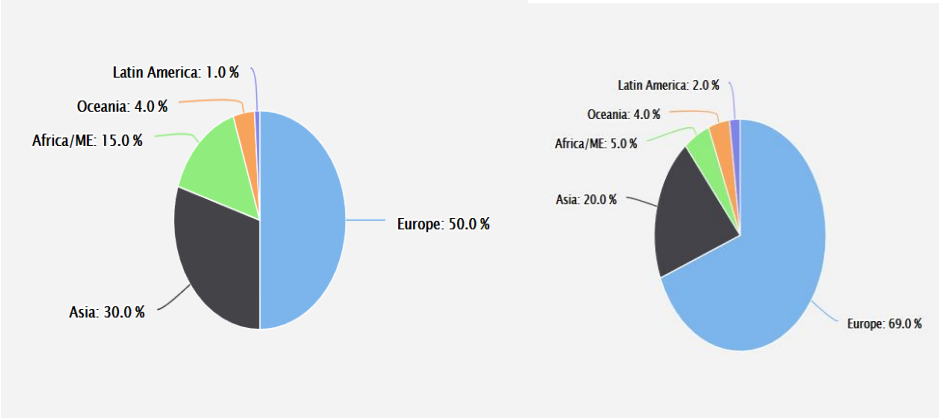
Les fonctions physiques à contrôler ou à surveiller peuvent aller de la température de la rame à la part de l'effort de traction entre les voitures dans une unité multiple.

Et de plus en plus, ces contrôles et ces surveillances se font au travers de NTIC et dans certains cas s'opèrent à distance : un aspect de la convergence IT-OT.

Hors-UE, c'est la République Populaire de Chine (essentiellement sur sa partie orientale) qui domine l'ensemble des pays européens cumulés en termes de kilomètres d'infrastructures sous ERTMS. Concernant le nombre de véhicules implémentant l'ERTMS l'Allemagne arrive à rivaliser avec la Chine. Il est à noter qu'en date de l'écriture de ce document l'ERTMS n'est pas encore déployé aux États-Unis, Canada, Russie, en dehors de quelques expérimentations.



28 - Évolution mondiale du déploiement de l'ERTMS sur voies (graphique gauche) et dans les véhicules (graphique droit) [193]



29 - Répartition mondiale du déploiement d'ETCS 1 & 2 sur les voies (graphique gauche) et dans les véhicules (graphique droit)

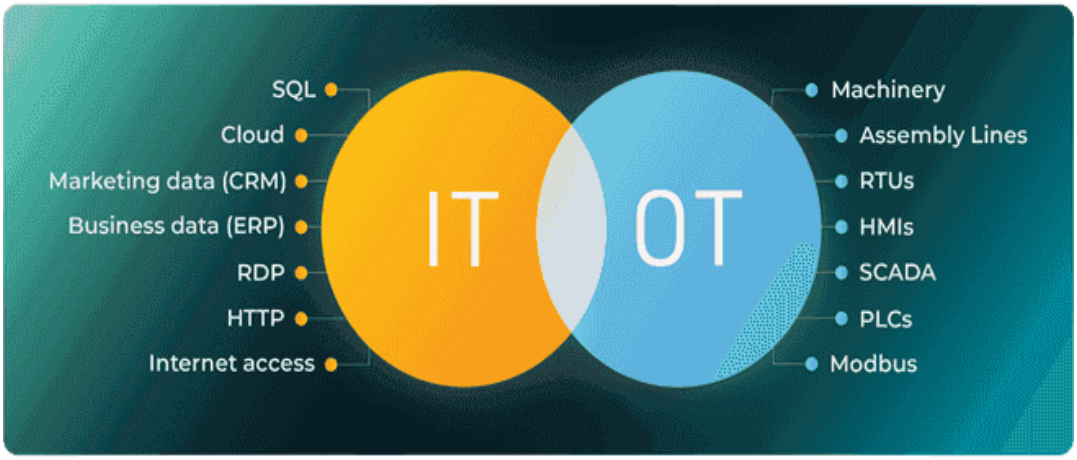
[192] railwaysignalling.eu, *What is a Train Control and Monitoring System (TCMS)?* [En ligne]. [Réf. du 10 février 2015]. Disponible sur https://www.railwaysignalling.eu/train-control-and-monitoring-systems-tcms

[193] ERTMS**,** *ERTMS Deployment Statistics – Overview. The figures indicate the lines and rolling stock in operation as well as contract signed by UNISIG companies*. [En ligne]. [Réf. de Oct. 2020]. Disponible sur https://www.ertms.net/facts-figures/deployment-statistics/?nowprocket=1

III.4. CONVERGENCE IT-OT

III.4.1. CONVERGENCE IT /OT, ATOUT MAJEUR DU FERROVIAIRE

Comme beaucoup de DSI, Gilles Lévêque, DSI du Groupe ADP, est convaincu que la convergence IT-OT est un facteur clé de succès de la transformation de nos entreprises et de leurs SI d'un point de vue d'architecture, d'organisation et de *gouvernance*[194]. Selon lui, le virage vers cette convergence a été pris il y a moins de cinq ans, poussé aussi par l'appel de plusieurs groupes industriels soumis à de plus en plus de contraintes et souhaitant utiliser les technologies numériques pour transformer leur chaîne logistique et construire de nouveaux sites industriels connectés, plus simples à administrer.



30 - Composantes IT versus OT

Le rapprochement entre le monde du système d'informations d'entreprise en charge principalement du traitement des données de l'entreprise et le monde des systèmes industriels regroupant les opérations couvrant les installations physiques de production « industrielle » de l'entreprise, est aujourd'hui considéré comme une évidence.

En effet, les leviers apportés par la digitalisation rendent la convergence des mondes IT et OT incontournable. La question posée est de savoir comment mettre en place une stratégie globale et une implication complète et engageante des parties prenantes au premier chef, la Direction Générale, mais bien évidemment les directions industrielles, les établissements, les directions des SI, les directions sûreté/sécurité ; les directions de ressources humaines, juridiques.

[194] Cigref - Clara Morlière, *Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels* [En ligne]. [Réf. du 18 février 2020]. Disponible sur https://www.cigref.fr/wp/wp-content/uploads/2019/12/Cigref-Convergence-IT-OT-Rapprochement-fructueux-Systemes-Information-et-Industriels-Decembre-2019-light.pdf

31 - Acteurs de l'entreprise concernés par la convergence IT-OT (Source : CIGREF)

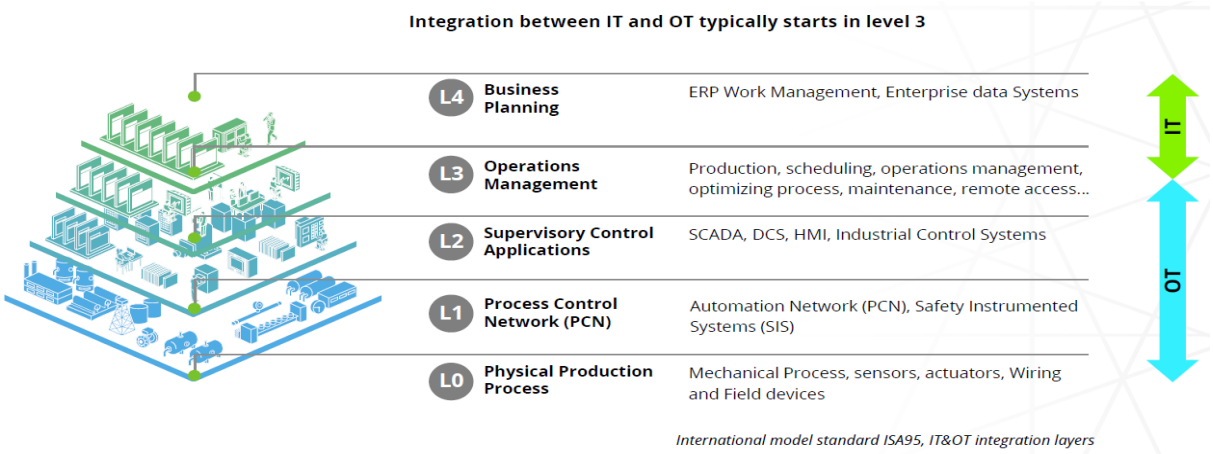
Mais il y a un passif qu'il faudrait solder. En effet, du fait de leurs profondes différences, tant dans leurs objectifs métiers, dans leurs solutions technologiques, de standards, dans leur temporalité, que dans leur organisation et leurs compétences, les SI industriel et d'entreprise sont longtemps restés cloisonnés l'un de l'autre. Cette logique s'inscrivait dans un concept de processus spécialisé, d'une sécurisation adaptée aux activités opérationnelles des sites industriels. Alors que les SI d'entreprise collectent les informations de pilotage de l'entreprise et contribuent à automatiser les processus support, les SI industriels contrôlent les équipements industriels et permettent d'exécuter les processus de production. Les technologies utilisées par chaque SI étaient fondamentalement différentes. En outre, si les SIE (Système d'Information d'Entreprise) nécessitent des compétences autour des Technologies de l'information, de la data, des réseaux et leur sécurité, les SII (Système d'Information Industrielle) font appel quant à eux à des compétences en automatisme industriel, en contrôle avancé ou en génie des procédés. Ces deux mondes avaient peu d'éléments communs du fait de leurs divergences en termes de besoins et finalités, leur cloisonnement systémique. Le peu de besoins d'interconnexion a par conséquent créé deux mondes dont l'interopérabilité n'avait pas de raison d'existence. Aussi quand on regarde les cursus de formation des experts de chaque domaine on comprend bien que la création de ponts entre ces deux mondes est un vaste chantier, mais à diligenter sans tarder.

À date, 80% des grands acteurs industriels ont déjà engagé une réflexion sur la convergence[195] IT-OT. Dans le but d'amorces les ruptures nécessaires et incontournables par rapport à l'époque des interconnexions RTC (réseau téléphonique commuté) où tous les équipements communiquaient entre eux. Du fait de leur étanchéité, ces réseaux étaient protégés par construction d'attaques informatiques externes. Avec la migration vers le réseau Ethernet ou vers les réseaux 4G et 5G, ces dispositifs sont devenus vulnérables à ces menaces cyber. Sous la poussée d'Internet, le protocole TCP/IP est vite devenu incontournable dans les réseaux IT et progressivement, s'installe aussi comme le principal protocole de communication des réseaux OT[196]. Du fait d'exigences de niveau de sécurité

[195] Sébastien Ropartz DELOITTE **-** *La convergence IT/OT : un enjeu stratégique majeur pour les groupes industriels*. [En ligne]. [Réf. du 22 juin 2017]. Disponible sur https://blog.deloitte.fr/convergence-itot-enjeu-strategique-majeur-groupes-industriels/
[196] NOVIPRO [En ligne] [Réf. Du 2 mars 2020] Disponible sur Comment intégrer un réseau TO industriel à un réseau TI? (novipro.com)

différentes, arriver à une intégration réussie des réseaux OT et IT est un véritable challenge. Dans l'environnement ferroviaire, un système d'OT dont le fonctionnement devient anormal peut causer des dommages matériels considérables, voire des dommages physiques aux usagers ou aux employés qui les côtoient, auxquels s'ajouteraient des conséquences économiques difficilement prévisibles dans leur globalité.

Le schéma qui suite nous donne un aperçu des couches des différentes SI et les zones d'interfaçage pour lesquels la vigilance doit être de mise.

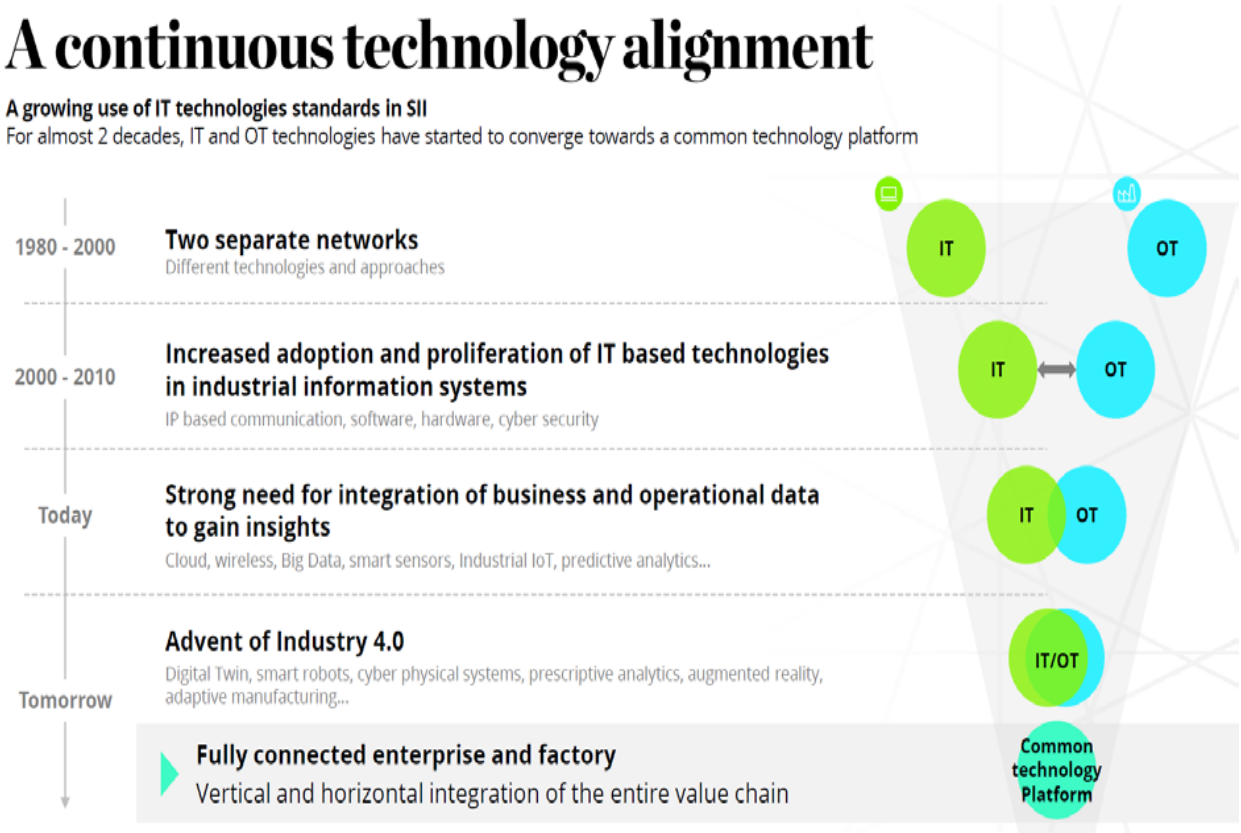


32 -Schéma théorique de l'intégration des systèmes IT et OT par la norme ISA95[197] Source : Deloitte 2019

L'avènement de nouveaux usages numériques et des possibilités des NTIC, ainsi que l'échange et l'exploitation de données de manière intensive et continue à travers des capacités exceptionnelles et croissantes de calcul du cloud, concourent dès maintenant à des gains de productivité et économiques sans précédent. Cela conduit de facto à une convergence inéluctable des systèmes IT et OT. Mais cette convergence IT et OT, comme le souligne Frédéric Lussignol, Directeur Cybersécurité chez SPIE ICS, s'est imposée sans avoir été réellement pensée ni planifiée[198].

[197] Cigref - Clara Morlière, *Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels* [En ligne]. [Réf. du 18 février 2020]. Disponible sur https://www.cigref.fr/wp/wp-content/uploads/2019/12/Cigref-Convergence-IT-OT-Rapprochement-fructueux-Systemes-Information-et-Industriels-Decembre-2019-light.pdf

[198] Forum FIC 2021 [En ligne] [Réf. Du 29 juin 2021] Disponible sur AvisdexpertSPIEICSSegmentationdesreseaux.pdf (forum-fic.com).



33 – Convergence progressive dans le temps de l'utilisation de technologies IT dans les systèmes industriels[199] *Source : Deloitte 2017*

Cette convergence n'est pas seulement technique ou technologique, mais constitue un enjeu stratégique majeur pour les groupes industriels[200]. Tel qu'on peut le découvrir dans le rapport 2019 du Cigref, les bénéfices attendus sont nombreux à savoir :

La Rentabilité : elle suit une logique de diminution des coûts de fonctionnement pour accroître la marge possible de l'entreprise. Elle passe par l'optimisation globale et la mutualisation des ressources. La maintenance de nouvelle génération permet en effet de réduire le taux d'immobilisation des infrastructures et d'avoir une meilleure réactivité en cas d'incidents.

Grâce à l'intégration de l'IT/OT, la captation des données par des équipements physiques et des dispositifs IIoT (côté OT) permet d'identifier les problématiques et renforcer la productivité[201]. Les données collectées, combinées puis utilisées de façon croissante dans des systèmes d'apprentissage de l'intelligence artificielle (Deep Learning[202]) au niveau des SI IT, facilitent les opérations de la maintenance dite prédictive. Le but poursuivi est de réduire l'inactivité induite par la maintenance inattendue. La durabilité, l'accroissement de la disponibilité et la fiabilité des matériels s'en trouvent renforcées, augmentant ainsi la

[199] Cigref - Clara Morlière, *Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels* [En ligne]. [Réf. du 18 février 2020]. Disponible sur https://www.cigref.fr/wp/wp-content/uploads/2019/12/Cigref-Convergence-IT-OT-Rapprochement-fructueux-Systemes-Information-et-Industriels-Decembre-2019-light.pdf
[200] Sébastien Ropartz DELOITTE **-** *La convergence IT/OT : un enjeu stratégique majeur pour les groupes industriels*. [En ligne]. [Réf. du 22 juin 2017]. Disponible sur https://blog.deloitte.fr/convergence-itot-enjeu-strategique-majeur-groupes-industriels/
[201] Fortinet, *Technologies industrielles (OT) ? Les technologies OT consistent à tirer parti de matériels et de logiciels pour contrôler les processus, dispositifs et infrastructures physiques*. [En ligne]. [Réf. de 2021]. Disponible sur https://www.fortinet.com/fr/solutions/industries/scada-industrial-control-systems/what-is-ot-security
[202] Jason Brownlee, *What is Deep Learning?*. [En ligne]. [Réf. Du 14 août 2020] Disponible sur https://machinelearningmastery.com/what-is-deep-learning/

capacité de répondre aux besoins de sûreté et sécurité. Il faut néanmoins garantir la cybersécurité des données qui sont échangées ainsi que des opérations de télémaintenance ou eMaintenance[203], surtout en termes d'intégrité et de traçabilité.

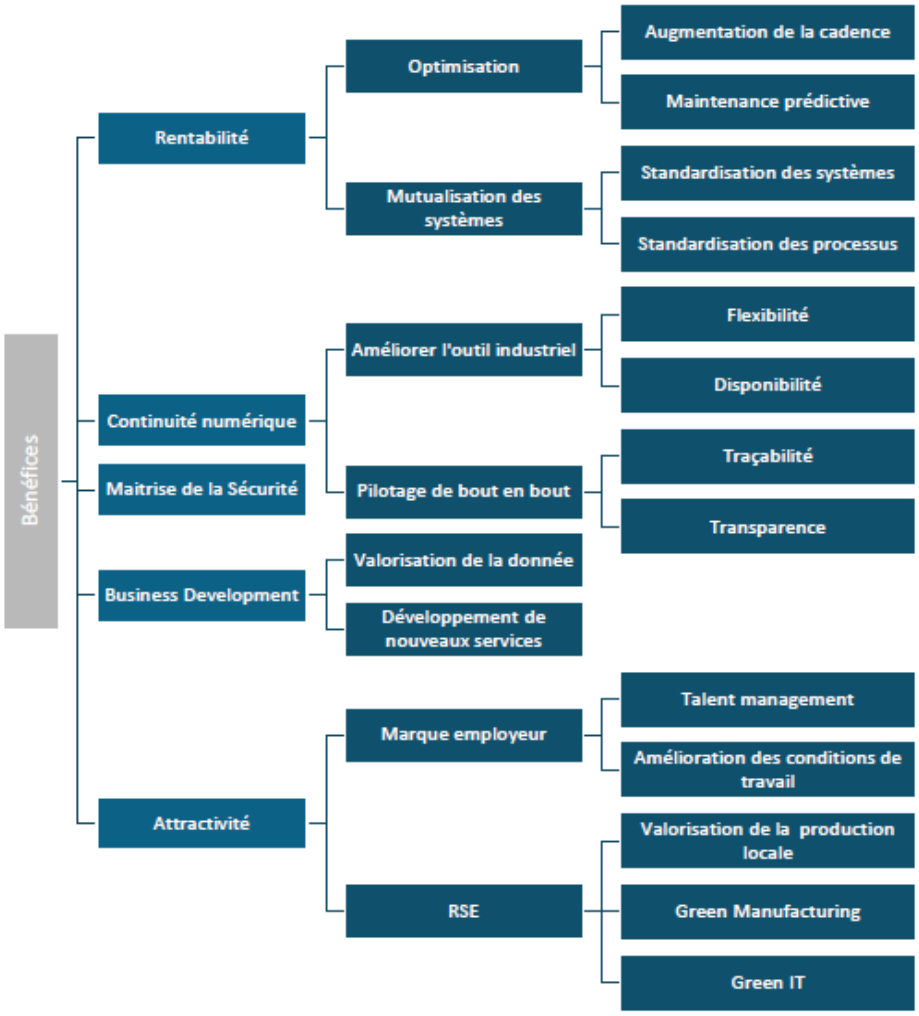
La continuité numérique : la disponibilité des machines et la flexibilité d'utilisation conditionnent toute l'activité. En neutralisant les effets de silos, la continuité numérique contribue à réduire les temps d'exécution et constitue un facteur clé pour assurer un time-to-market et un time-to-cash réduits[204]. De même, le pilotage de bout en bout permet d'assurer la traçabilité.

La sécurité : face aux menaces actuelles, la maîtrise de la sécurité, absolue nécessité, est un atout majeur. Le Maintien en Condition de Cybersécurité est un objectif visant à garantir une réactualisation des vulnérabilités et des menaces qui guettent les actifs/objets métiers notamment critiques. Une haute vigilance sur cette exigence est capitale avec l'intégration des systèmes IT dans les systèmes critiques.

Le développement de nouveaux services : la valorisation des données de l'entreprise via le développement de nouveaux services est un levier de croissance. L'utilisation croissante des PoV (« Proof of Value ») est un accélérateur de développement de nouveaux cas d'usages. C'est aussi le cas des jumeaux numériques, le jumeau étant le clone virtuel d'un système physique ou d'un processus, permettant de visualiser et mesurer en amont et sans dommages, l'impact de l'apport d'une nouvelle fonctionnalité ou la modification d'une fonctionnalité existante dans le monde physique. Ces concepts novateurs sont aussi utilisés pour challenger des nouveaux dispositifs et mesures de sécurité. De plus, le marché capitalisera sur les opportunités technologiques telles que les réseaux 5G/6G et les IoT, au travers d'offres claires une fois les standards maîtrisés.

[203] Ravdeep Kour**,** *Cybersecurity in railway. A Framework for Improvement of Digital Asset Security* [Thèse de doctorat en ligne]. [Réf. 2020]. Disponible sur https://www.diva-portal.org/smash/get/diva2:1423651/FULLTEXT01.pdf

[204] Christian Hohmann, *La continuité numérique, un facteur d'efficience,* [En ligne].[Réf. du 15 février 2015] Disponible sur https://nouvelleindustrie.wordpress.com/2020/02/15/la-continuite-numerique/



34 - Bénéfices attendus de la convergence IT-OT par les entreprises[205]

Pour réussir cette convergence et contribuer à un transport ferroviaire dit intelligent, une transformation des modes de pensées et d'organisation des deux mondes (IT / OT) est un passage incontournable ; mettre en œuvre une gouvernance pour notamment rendre plus lisibles les clés de succès d'une telle convergence. Quelques pistes sont déjà évoquées dans différents colloques et groupes de travail. À un plus haut niveau, la création d'une Direction Technologique Nationale pour gérer le patrimoine complexe des sites industriels en prenant en charge le socle IT/OT est un élément stratégique important.

Opérationnellement il faudrait prendre en compte les éléments structurants ci-dessous :

- La gestion des actifs, des flux, des menaces à leur portée et les risques associés ;
- La stratégie d'audit et d'homologation ;
- Les interfaces explicites (à sécuriser) entre les systèmes IT (systèmes d'entreprise, système IT opérationnel) et les systèmes OT (Systèmes de contrôle et composants physiques intégrant le protocole IP).

[205] Cigref - Clara Morlière, *Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels* [En ligne]. [Réf. du 18 février 2020]. Disponible sur https://www.cigref.fr/wp/wp-content/uploads/2019/12/Cigref-Convergence-IT-OT-Rapprochement-fructueux-Systemes-Information-et-Industriels-Decembre-2019-light.pdf

IV. TRANSPORT FERROVIAIRE INTELLIGENT

On entend constamment : « *Les datas sont aujourd'hui le nerf de la guerre !* ». Les données sont plus que jamais au centre de la transformation digitale pour atteindre les objectifs de performance économique et d'amélioration de l'expérience passagers. Cela passe par une massification conséquente de données, et d'une la capacité de les échanger et de les traiter. Ce qui demande des compétences et expertises pluridisciplinaires dans les différentes organisations qui interagissent.

Dans cette partie nous abordons les axes majeurs partagés dans la communauté ferroviaire considérés comme déterminants pour les transports ferroviaires intelligents de manière générale. Il s'agit de :

- L'amélioration de l'expérience client ;
- La sécurité des usagers et des collaborateurs ;
- La téléconduite et les trains autonomes ;
- La performance industrielle et économique ;
- Le transport durable, accélérateur des mobilités et moteur du développement économique et sociétal.
- Le Big data , la valorisation des données de bout en bout et l'Intelligence Artificielle

IV.1. AMELIORATION DE L'EXPERIENCE CLIENT ET SERVICES DIGITAUX POUR LES PASSAGERS

La filière ferroviaire est confrontée à la concurrence des différents modes de transport, au travers de changements sociétaux tels que le télétravail accéléré par la crise sanitaire COVID19, ou l'évolution des moyens alternatifs de transport tels que l'utilisation du vélo et de la trottinette électrique pour réaliser les trajets domicile – travail. Ces points sont autant d'incitation des opérateurs de mobilité à se renouveler en proposant des expériences voyageuses innovantes. Les performances économiques et le développement des entreprises du secteur dépendront indubitablement de leur capacité à conquérir et à fidéliser les clients, à proposer de nouveaux services et solutions d'agrément de transport, à se réinventer. À l'heure d'une digitalisation multimodale, cela passe bien évidemment par des solutions numériques avec des applications mobiles, des solutions de promotion et de communication multicanaux, et l'utilisation massive et maîtrisée des réseaux sociaux. Ces nouveaux services doivent par exemple permettre aux voyageurs la simplification de l'organisation de leurs voyages -qu'ils soient touristiques ou professionnels- la possibilité de faire des retours et partages d'expérience ou d'avoir une information actualisée sur les trajets, etc.

Nous avons ainsi vu émerger depuis quelques années des applications diverses pour faciliter les déplacements des usagers.

À titre d'exemple, nous pouvons citer quelques applications proposées aux voyageurs :

Les indispensables développés par la SNCF : SNCF-Connect ex (*Oui SNCF)*[206] *est l'application principale de la SNCF. Elle permet de réserver, de télécharger, d'échanger, d'annuler votre billet de train directement sur votre smartphone ou votre tablette.*

[206] [En ligne]. [Réf. 2022]. Disponible https://www.sncf-connect.com/

Trainline[207] : *application de billet électronique pour voyager en train et en bus dans toute l'Europe. En France, Trainline est partenaire de la SNCF (TGV, INOUI, INTERCITÉS, TER), de Ouibus, de OUIGO, d'Eurostar, de Thalys et de Flixbus.*

Kelbillet[208] : *le site ou l'application compare plus de 500 compagnies et propose tout type de billets (billets d'occasion compris) aussi bien de train, bus, de covoiturage ou encore d'avion.*

Tictactrip[209] : *c'est 650 millions de liaisons réparties dans 15 pays et dans 4800 villes. Le site promeut l'intermodalité afin de bien voyager tout en respectant l'environnement ; Tictactrip permet de combiner différents modes de transports, et ce à l'échelle européenne : train, bus et covoiturage.*

Citymapper[210] : *pour faciliter la planification d'un trajet en métro, bus, le train, ferry ou tout autre moyen de transport. Les itinéraires à vélo sont également inclus, si vous préférez un moyen de déplacement urbain plus actif !*

IV.2. SECURITE DES USAGERS ET DES COLLABORATEURS

La sécurité des personnes est la plus importante des priorités : sécurité physique dans les trains, dans les chantiers, les passages à niveaux, dans les gares ainsi que la sécurisation de leurs données au regard de la multiplicité des interconnexions et de l'exigence du respect des réglementations. Les transports intelligents de demain ont l'obligation de répondre à ces objectifs.

Selon BearingPoint[211], les technologies « *Big Data* » pourraient contribuer à l'amélioration de la sécurité des circulations et des réseaux, en limitant directement le nombre d'incidents techniques voire d'accidents. Le big data peut contribuer à améliorer la visualisation des modèles de risques par une approche prédictive voire prescriptive. Il pourra permettre d'optimiser la détection « d'événements déviants » et « de signaux faibles » afin de prévenir les risques complexes… et dans certains cas limiter les comportements à risque.

Entre 2015 et 2016, il a été constaté une augmentation[212] de 50 % de piétons percutés par les rames de tramway sur les réseaux en Île-de-France. Il est donc primordial de prendre en compte les nouveaux usages et leurs impacts lors des déplacements quotidiens. D'après une analyse effectuée par le responsable de la sécurité des tramways d'Île-de-France sur les accidents survenus sur le réseau de la RATP, la plupart des accidents se sont révélés être occasionnés du fait de la distraction des utilisateurs utilisant leurs smartphones. Des solutions comme la détection d'obstacle par l'utilisation des ultrasons[213] ont vu le jour pour réduire ce nombre d'accidents, un premier test a été réalisé avec la RATP en décembre 2018 sur un passage à niveau de test sur emprise SNCF.

---

[207] [En ligne]. [Réf. 2021]. Disponible sur thetrainline.com
[208] [[En ligne]. [Réf. 2021]. Disponible sur KelBillet.com
[209] [En ligne]. [Réf. 2021]. Disponible sur Tictactrip.eu
[210] [En ligne]. [Réf. 2021]. Disponible sur citymapper.com/paris
[211] François Lanquetot, Caroline Perrin, Laetitia Chatain, Eléonore Miédan-Gros, BearingPoint - *La Data au service de la Sécurité Ferroviaire* - [En ligne]. [Réf. 2021]. Disponible sur https://www.bearingpoint.com/fr-fr/notre-succes/blogs/secteur-public/la-data-au-service-de-la-sécurité-ferroviaire/
[212] Virginie Taillandier, Benjamin Charles, *Une réponse numérique à une problématique opérationnelle. Gouvernance, Sécurité et Aménagement, Technologie, Gestion de la circulation, Infrastructures de transport, Logistique, Mobilité durable, Viabilité hivernale* - [En ligne]. [Réf. du 31 décembre 2019]. Disponible sur https://aqtr.com/association/actualites/reponse-numerique-problematique-operationnelle
[213] INRS - *Prévenir les collisions engins-piétons. La place des dispositifs de détection et d'aide visuelle*. [En ligne]. [Réf. du 17 juin 2015]. Disponible sur https://www.inrs.fr/dms/inrs/CataloguePapier/ED/TI-ED-6083/ed6083.pdf

IV.3. TELECONDUITE ET TRAINS AUTONOMES

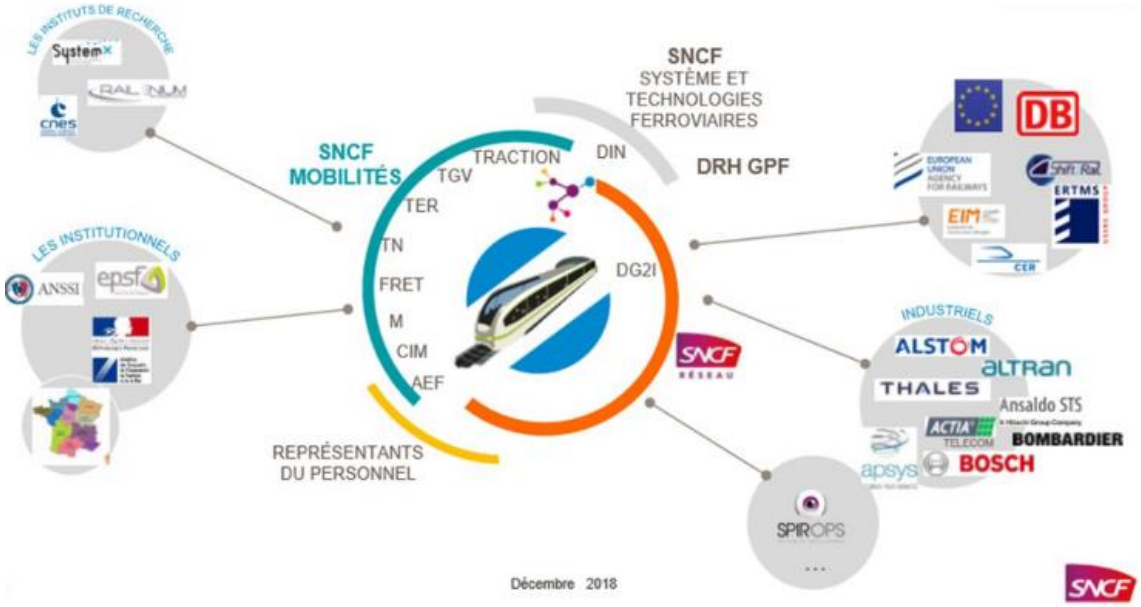
IV.3.1. LA TÉLÉCONDUITE

La Téléconduite d'un train est le maillon entre le train automatique (comme certaines rames de métro parisiennes), déjà en production, et le train autonome, perspective d'avenir. L'un des projets phares en la matière est le projet TC-Rail (Téléconduite sur rail) lancé le 18 octobre 2017 par un consortium, composé de la SNCF, de l'Institut de Recherche Technologique Railenium[214](IRT Railenium), du CNES, de Actia Telecom et de Thales. Ce projet s'inscrit dans le cadre d'un programme « train autonome » dont l'objectif affiché est l'amélioration de la compétitivité de la filière ferroviaire.

La télé conduite est une véritable avancée pour le ferroviaire du futur.

Les enjeux de ce projet ont été de résoudre les principales problématiques techniques pouvant porter atteinte à la sécurité en faisant la démonstration de la capacité à conduire un train à distance, avec un conducteur déporté tout en préservant un très haut niveau de sécurité. La mise en œuvre de ce type de système nécessite des compétences tant industrielles qu'académiques. La téléconduite ne peut se faire sans un réseau de communication avec une qualité optimale tout au long du trajet du train ; il a été nécessaire d'utiliser l'hybridation des technologies permettant la bascule automatique avec une utilisation alternée des transmissions satellitaires, de la 4G du réseau privé de la SNCF et de la 4G des opérateurs avec le système « Eiji by Thales ». Par ailleurs, de nouveaux systèmes de vision (IHM de téléconduite) ont été développés afin d'obtenir un niveau de performance suffisant pour garantir la remontée des informations. Au long du projet, les tests réalisés par la SNCF ont utilisé successivement trois types de voies : les voies de service, puis les voies principales et les voies uniquement électrifiées. Ce projet très inclusif a mobilisé plusieurs parties prenantes : opérateurs, constructeurs, autorités nationales de sécurité, instituts de recherche et des grands organismes européens du ferroviaire comme on peut le voir dans le schéma ci-dessous.

[214] *La téléconduite sur rail, SNCF, Thales, Actia Telecom, le CNES s'unissent avec Railenium* [En ligne]. [Réf. Octobre 2017].Disponible sur https://railenium.eu/la-teleconduite-sur-rail-sncf-thales-actia-telecom-le-cnes-sunissent-avec-railenium/



35 - Écosystème mobilisé pour la Téléconduite[215]

IV.4. LES TRAINS AUTONOMES

La SNCF et l'Institut de recherche technologique (IRT) Railenium ont annoncé en 2018 des trains autonomes à l'horizon 2023. Plusieurs parties prenantes (opérateurs comme constructeurs) s'accordent sur les avantages qu'apportent les trains autonomes. Le retour d'expérience des métros autonomes en est la preuve : en premier lieu l'augmentation de la capacité des lignes grâce à un trafic fluidifié (à l'instar des lignes automatisées de métro), capacité de transporter plus de voyageurs et plus de marchandises, une circulation harmonisée et une vitesse optimisée, permettant de mieux faire face aux imprévus. Parvenir à réaliser des économies d'énergie avec un transport plus écologique par une conduite plus optimale avec un niveau de sécurité garanti sont quelques-uns des bénéfices escomptés. Ces bénéfices favoriseront le report modal de la route vers le rail et contribueront ainsi à un mode de transport plus respectueux de l'environnement.

Deux consortiums rassemblant des entreprises technologiques et industrielles ont été créés en janvier 2018 pour piloter ses projets pour une durée de 5 ans :

- Un consortium dédié à la réalisation d'un prototype de train de Fret autonome, comprenant Alstom, HITACHI RAIL STS, Apsys (filiale d'Airbus) et Capgemini Engineering ;
- Un consortium dédié aux voyageurs pour la réalisation d'un prototype de train TER autonome. Il se compose de Alstom, Bosch, Spirops[216] et Thales.

Le budget global de cette phase de projet, destiné aux 2 consortiums, s'élève à 57 M€ : 30% financé par la SNCF, 30% par l'État et 40% par les partenaires.

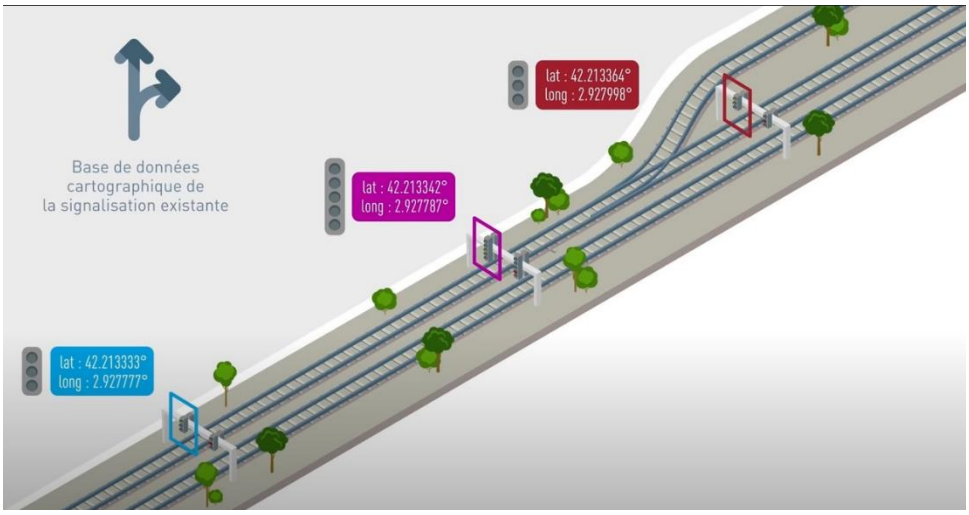
Plusieurs challenges étaient à relever, par exemple, la lecture de la signalisation latérale, par l'automatisation des fonctions d'observation du conducteur de train au travers d'un système de perception de l'environnement. Une des contraintes rencontrées par la SNCF est d'utiliser l'existant sans en modifier la conception.

---

[215] *Projet Train Autonome* [En ligne]. [Réf. du 14 février 2019]. Disponible sur https://www.sudrailpse.org/site/blog/2019/02/14/projet-train-autonome/

[216] François Gauthier, *Les trains sont lancés sur les rails d'une autonomie complète* [En ligne]. [Réf. du 14 février 2019]. Disponible sur https://www.sudrailpse.org/site/blog/2019/02/14/projet-train-autonome/

Le système imaginé par la SNCF repose principalement sur une géolocalisation de haute précision des trains en temps réel combinant des données d'outils cartographiques et les remontées en temps réel des données des capteurs installés le long des voies.



36 - Géolocalisation haute précision des trains en temps réel[217]

L'entreprise IRT SYSTEMX accompagne la SNCF sur le projet « Train autonome », et valide dans ses laboratoires installés dans des trains les différents algorithmes de reconnaissance grâce à une base de données où sont stockées près de 150 millions d'images de feu de signalisation, soit 40 To de données caractérisées ; on peut citer par exemple la couleur, le type, le lieu et l'heure de l'acquisition ou encore le modèle de caméra utilisée. Pour améliorer sa performance et son niveau de sécurité, et afin de garantir le meilleur résultat, ce système s'appuie sur plusieurs algorithmes parallélisés. Une fois le système finalisé, il est implanté dans le train d'essai pour être testé et permettre la validation des choix technologiques.

Il est aussi nécessaire de développer des solutions de détection des obstacles, tout aussi importants que la lecture de la signalisation latérale.

La Roadmap des essais du Train de Fret autonome fut présentée par Samuel Boucher, chef de projet Train Fret Autonome, en septembre 2019 sur le site de la SNCF. Il prévoyait dès cette date un rétroplanning sur trois ans permettant d'ajouter des fonctionnalités pour augmenter le niveau d'autonomie et progressivement atteindre l'objectif du projet, c'est-à-dire un train de fret intégralement autonome[218]. Il ne s'agissait déjà plus de projets futuristes et lointains, la digitalisation des locomotives ayant déjà plusieurs années.

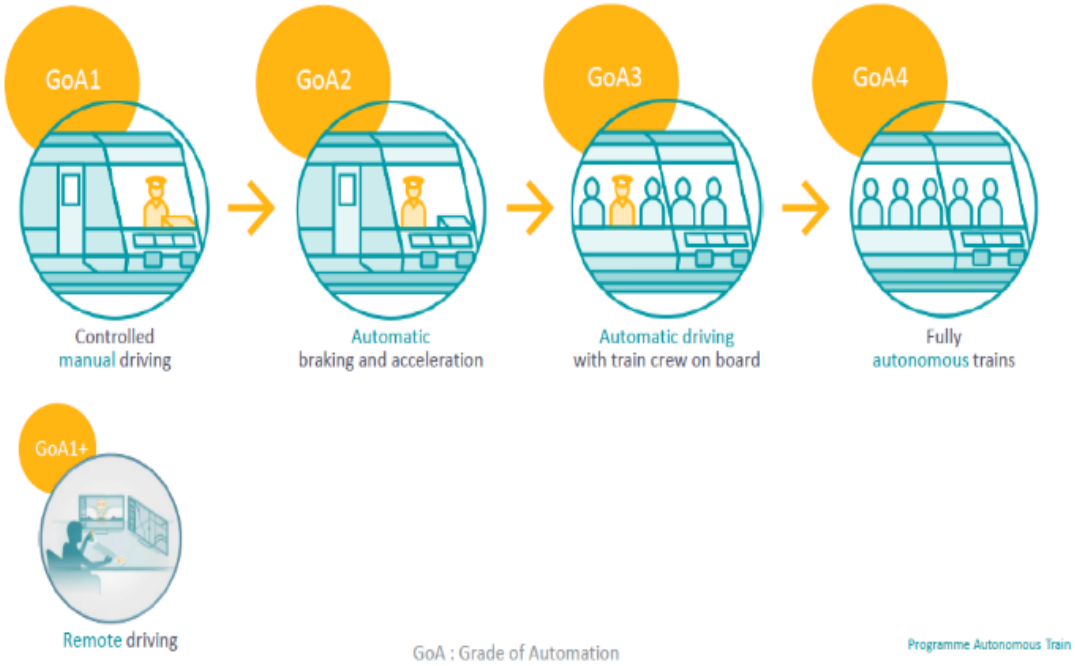
IV.4.1. LES 4 NIVEAUX D'AUTOMATISATION DES TRAINS (GOA)

Il y a quatre niveaux d'autonomies, appelés GoA (*Grades of Automation*) comme indiqué dans le schéma qui suit[219]" :

[217] Groupe SNCF, *Train autonome : automatisation de la lecture de la signalisation latérale* [Vidéo en ligne]. [Réf. du 02 avril 2019]. Disponible sur https://www.youtube.com/watch?v=WiYavvqh7Bk

[218] SNCF, *Train Fret Autonome : la locomotive entre en atelier*. [En ligne]. [Réf. Du 01 Oct. 2020]. Disponible sur https://www.sncf.com/fr/groupe/newsroom/essais-prototype-train-fret-autonome

[219] Léna Corot, *La SNCF présente son plan d'action pour le train autonome*. [En ligne]. [Réf. du 13 sept. 2018]. Disponible sur https://www.usine-digitale.fr/article/la-sncf-presente-son-plan-d-action-pour-le-train-autonome.N740699



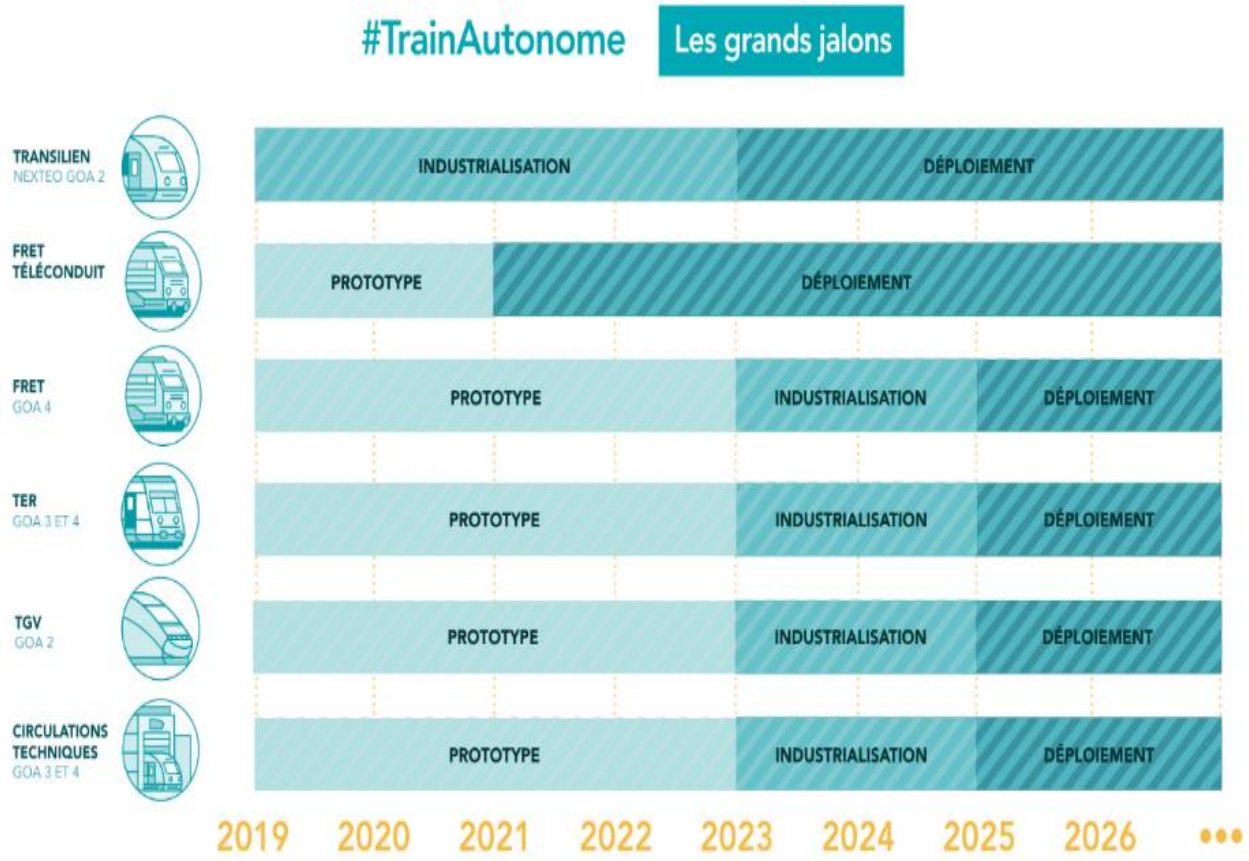
37 - Niveaux d'automatisation des trains (GoA) [220]

- Le GoA de niveau 1 équipe 99% des trains aujourd'hui et correspond à la mise en place d'un automatisme pour le contrôle de la vitesse ;
- Le GoA de niveau 2 permet la conduite sans les mains, une accélération et un freinage automatisés. Le conducteur s'occupe de l'ouverture et de la fermeture des portes ainsi que des fonctions de sécurité ;
- Le GoA de niveau 3 correspond à un train roulant en mode autonome, mais avec un chef de bord en capacité de reprendre le contrôle du train même sans être présent en cabine ;
- Le GoA de niveau 4 regroupe les trains totalement autonomes sans aucun personnel habilité à bord pour intervenir.

IV.4.2. TRAINS AUTONOMES POUR LES TER ET TGV

Les technologies GoA seront plus rapidement déployées sur les TER que les TGV. La SNCF prévoit de développer un prototype de TER répondant aux niveaux GoA 3 et 4 entre 2019 et 2023.

[220] UIC, *IRRB webinar autonomous technologies in rail -anticipating expectations*. [En ligne]. [Réf. De juin 2021]. Disponible sur https://uic.org/events/IMG/pdf/ato_webinar.pdf



38 - Roadmap Transport Ferroviaire Autonome[221]

Sur cette même période, l'autonomie du prototype de TGV relèvera uniquement du niveau 2. Toutefois, la SNCF espère parvenir à un niveau d'autonomie relevant des niveaux 3 et 4 pour tout ce qui relève des "circulations techniques" des trains dès 2023. Cela correspond par exemple aux trajets réalisés par le train entre le dépôt et le quai de gare.

SNCF a annoncé en début mars 2021 avoir fait circuler un train d'essai semi-autonome, dans la région des Hauts-de-France entre Aulnoyen et Busigny (59) et entre Busigny et Calais (62). Une rame TER a été spécialement modifiée et équipée par l'usine Alstom de Crespin (anciennement Bombardier) afin de réaliser ces essais. Le 22 juillet 2021, les équipes multipartenariales regroupant SNCF, Alstom, SPIROPS, Thales, Bosch, et Railenium ont réussi pour la 1ère fois à faire circuler un train au niveau GOA2 sur signalisation latérale. Ce niveau équivaut à un pilotage automatique du train avec la présence du conducteur en cabine qui intervient en cas de besoin[222].

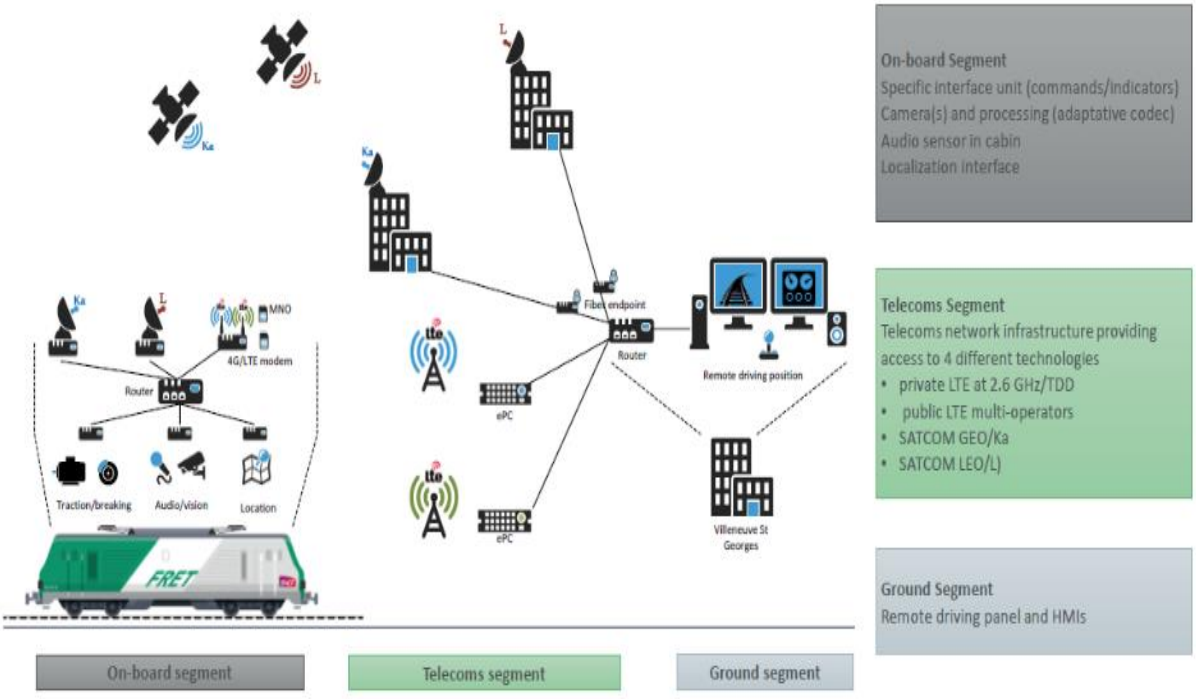
Les membres du consortium ont souligné qu'au cours de ces essais, les enjeux de cybersécurité ont été pris en compte très en amont, en partenariat avec l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Les trains ont été lancés sur les rails avec une autonomie complète.

« Les essais réalisés ces derniers mois ont marqué une avancée significative vers notre objectif d'inventer le transport du futur avec le train autonome » s'enthousiasme Eric Tregoat, Directeur Général de l'IRT de la filière ferroviaire Railenium. « Et ce en apportant

[221] [Image en ligne] Disponible sur https://medias.sncf.com/sncfcom/newsroom/pdf/SNCF_Pres_Conference_Presse_ATO_10SEPT.004.jpeg
[222] RailEnium, *Essais train autonome GOA2 sur signalisation latérale réussis*. [Vidéo en ligne]. [Réf. Du 29 juillet 2021]. Disponible sur https://www.youtube.com/watch?v=X6ON3xD5Ehw

nos compétences dans les domaines de l'intelligence artificielle, des maquettes numériques, de la modélisation numérique et de la sûreté de fonctionnement. »



39 - Architecture prototype[223]

Un autre essai encourageant est celui réalisé le 11 octobre 2021 en Allemagne avec le partenariat de Deutsche *Bahn et* Siemens. Pour Deutsche Bahn, l'automatisation doit permettre une « *meilleure offre sans devoir construire un kilomètre de nouveaux rails* »[224]

40 - Tracé du premier train autonome lancé le 11 octobre, à Hambourg, une "première mondiale"[225]*.*

[223]UIC, *IRRB webinar autonomous technologies in rail -anticipating expectations*. [En ligne]. [Réf. De juin 2021]. Disponible sur https://uic.org/events/IMG/pdf/ato_webinar.pdf

[224] Figaro par AFP, *Allemagne : un premier train autonome sur les rails à Hambourg* [En ligne]. [Réf. Du 11 octobre 2021]. Disponible sur https://www.lefigaro.fr/flash-eco/allemagne-un-premier-train-autonome-sur-les-rails-a-hambourg-20211011

[225] Kévin Comte**,** *Un train autonome est testé pour la première fois en Allemagne, la SNCF vise 2023*. [En ligne]. [Réf. de 11 Oct. 2021]. Disponible sur https://www.capital.fr/entreprises-marches/un-train-autonome-est-teste-pour-la-premiere-fois-en-allemagne-la-sncf-vise-2023-1416841

IV.5. TRANSPORT DURABLE

Le transport ferroviaire fait consensus sur les leviers dont il dispose au service de l'accélération des mobilités, de la croissance des entreprises et du développement économique des territoires et d'un pays. Il est aussi le transport de prédilection, comme le démontre plusieurs études, à même de réduire drastiquement l'empreinte carbone et la consommation énergétique. Mais cet objectif ne pourra être atteint sans une transformation profonde de son modèle de production et économique.

En effet, en France, le secteur des transports produit 36 % des émissions totales de CO2. La consommation énergétique du transport ferroviaire est estimée à 2,8 %, à comparer aux 10 % de passagers véhiculés. Le ratio consommation énergétique par passager est faible et se traduit mathématiquement par de faibles émissions de CO2 par passager au km. Pour ce qui est du train lui-même, plusieurs pistes de progrès applicables au transport ferroviaire en vue de la réduction des consommations énergétiques, et donc des émissions de CO2, sont envisagées ; par exemple, la récupération de l'énergie de freinage, chaîne de traction bimode (utilisation intelligente de l'énergie électrique en fonction des conditions du trafic et lissage de la consommation électrique, en particulier lorsque les lignes sont surchargées), la régulation du système de chauffage – climatisation[226].

Le potentiel du transport par fret est encore plus important, avec des gains économiques et énergétiques démontrables. La consommation énergétique par fret est deux à trois fois moindre que celle du transport routier.

Nous développerons amplement les trois volets de cette thématique environnemental, économique social et sociétal dans le chapitre « La Stratégie Responsabilité sociale et sociétale d'entreprise (RSE) »

IV.6. BIG DATA ET INTELLIGENCE ARTIFICIELLE AU CŒUR DE LA TRANSFORMATION

Le confort des passagers, l'information aux voyageurs, l'optimisation des flux voyageurs, la réduction des retards, l'amélioration de la sécurité, la maintenance prédictive, la géolocalisation par satellite[227] sont des pans d'activités ferroviaires pouvant bénéficier de l'exploitation efficiente des immenses gisements de données du réseau. La valorisation des données est un enjeu majeur pour la filière.

On est loin de la première révolution, celle du métier à tisser mécanique et de la machine à vapeur (1780), de la deuxième révolution industrielle avec la combustion interne et l'électricité (1870), mais encore proche de la troisième révolution industrielle avec Internet, la numérisation et l'échange d'une masse importante de données et des calculs complexes. La 4e révolution industrielle quant à elle ne fait que commencer avec des bouleversements sans précédent qui sont anticipés. On ne parle que d'elle dans les transformations de rupture. L'IA fascine, fait l'objet de fantasme et fait peur également (avec toutes ses questions aussi bien éthiques que juridiques). Une question prédominante est celle du « mythe » de la « Singularité technologique », « *L'intelligence artificielle va-t-elle bientôt dépasser celle des humains ?* », Jean-Gabriel Ganascia, dans son essai critique aborde la question de la menace transhumaniste de l'IA[228].

---

[226] Bernard Desmet**,** *Transport ferroviaire et développement durable* [En ligne]. Disponible sur https://www.cnam.fr/detours-verts-le-futur-des-transports/transport-ferroviaire-et-developpement-durable-777144.kjsp

[227] SNCF, *Big Data : les projets marquants de 2020* [En ligne] [Réf. Du 14 janvier 2021]. Disponible sur https://culture.cnam.fr/detours-verts-le-futur-des-transports/transport-ferroviaire-et-developpement-durable-777144.kjsp

[228] Jean-Gabriel Ganascia, *Le Mythe de la Singularité. Faut-il craindre l'intelligence artificielle ?* Editions Seuil. Juin 2019.

Cependant, plus concrètement, l'intégration de l'IA dans des applications existantes ou nouvelles fait émerger des possibilités et des performances sans précédent. « *C'est uniquement grâce à l'utilisation de l'IA que tout le potentiel des données, de l'analyse et du cloud peut être exploité pour améliorer l'expérience des passagers, les activités ferroviaires, la maintenance des actifs, la sécurité et la sûreté. In fine, cela se traduira par une augmentation de la satisfaction des clients et des revenus, ainsi que par une diminution des coûts*.[229] » selon Christian Marez, responsable principal du développement commercial pour les transports et la défense, chez ADLINK.

Un transport ferroviaire dit intelligent requiert des technologies de rupture qui permettent une efficience opérationnelle et une performance économique, mais surtout des nouveaux procédés pour des mobilités durables. L'intelligence Artificielle a toute sa place et les champs d'applications décrits ci-dessous sont loin d'être exhaustifs :

- **Maintenance prédictive** : détection des usures, des déformations, de la dégradation de l'état des caténaires, un objectif d'optimisation des processus logistiques et l'anticipation des approvisionnements de matériels. La maintenance prédictive se base soit sur des modèles purement statistiques (calculs basés sur l'historique de fonctionnement d'un grand nombre de systèmes identiques ou équivalents et pour extrapolation d'une base d'expérience avec l'identification des seuils critiques utilisés ensuite sur le système sous observation), soit par apprentissage via une technologie d'intelligence artificielle avec par exemple des réseaux neuronaux ;
- **Régulation du trafic, de la signalisation et trains autonomes** : les progrès de l'IA contribuent à permettre d'exploiter les trains de manière plus automatisée. Les systèmes de signalisation et de contrôle de la vitesse en cabine sont pris en charge par une technologie calculant la vitesse et les parcours optimisés en fonction de paramètres tels que la capacité des voies, les conditions météorologiques et la planification des horaires[230] ;
- **Localisation optimisée des trains** : l'analyse vidéo via l'IA permet de localiser la position exacte d'un train et de la communiquer au contrôle ferroviaire et aux autres trains du réseau. Ces systèmes de positionnement avancés pourront à terme permettre aux trains de se rapprocher les uns des autres et augmenter ainsi la capacité tout en réduisant les encombrements sur les voies.
- **Sécurisation des agents sur le terrain,** un exemple de contrôle de leurs équipements de protection à l'aide de caméras embarquées, etc. ;
- **Sécurité vidéo sur tout le réseau** : l'IA apporte une surveillance réelle et intelligente pour détecter les comportements suspects dans les trains ou dans les gares, les actes de vandalisme ou de fraude ;
- **Étude de la topographie et de la cartographie** : les drones dopés à l'IA permettent de numériser un site pour une exploitation de type BIM[231] (Building Information Modeling) ou de s'intégrer à une étude de projet. Le drone peut ainsi cartographier et faciliter la numérisation du réseau ferroviaire pour une mise à jour d'un SIG (Système d'Informations Géographiques) métier[232] ;
- **Inspection du matériel, des ouvrages d'art des installations électriques et des sites industriels ou des gares** à l'aide de drones et de caméras embarquées ;

[229] *En route pour la transformation digitale* [En ligne] [Réf. Du 27 juillet 2021]. Disponible sur https://lerail.com/news/44073-en-route-pour-la-transformation-digitale

[230] *En route pour la transformation digitale* [En ligne] [Réf. Du 27 juillet 2021]. Disponible sur https://lerail.com/news/44073-en-route-pour-la-transformation-digitale

[231] *Design and build with BIM. Building Information Modeling* [En ligne] [Réf. Du 27 juillet 2021]. Disponible sur https://www.autodesk.com/industry/aec/bim

[232] L'utilisation ferroviaire des drones avec Altametris. [En ligne]. [Réf. de Sept. 2021]. Disponible sur https://www.sncf-reseau.com/fr/entreprise/newsroom/sujet/innovation-utilisation-ferroviaire-drones-altametris

- **Transports durables** : on peut citer l'apport des techniques et d'outils de modélisation à base d'IA dans la meilleure gestion du ballast (« *un tas de caillou qui permet d'améliorer le confort des passagers tout en retardant l'usure des trains* ») et dont le comportement mécanique à une incidence sur la vitesse des trains ; l'énergie produite par ces derniers peut en retour avoir un impact sur la densité du ballast. Comprendre sur quelles portions de voies le ballast piège le plus d'énergie, ouvre notamment des perspectives pour l'augmentation de la durée de vie des voies de chemin de fer, et la diminution des coûts de maintenance[233]. On peut également citer la meilleure gestion de la végétation, de l'éclairage et de la consommation énergétique des trains. Plusieurs sociétés ouvrent la voie sur le sujet : Thalès propose déjà des systèmes complexes intégrant de l'I.A et basés sur l'apprentissage et la valorisation des connaissances[234] avec pour objectif de faire baisser de 30% la consommation énergétique des trains[235] grâce à des systèmes d'assistance à la conduite (GreenSpeedTM), d'optimisation de la conduite automatique des métros (GreenCBTC) et des trains autonomes (RailBotTM) et un calcul en temps réel des courbes d'accélération et de freinage optimisées ;
- Dans le domaine de la cybersécurité, la Cyber Threat Intelligence[236] moderne utilise des corrélations et des techniques d'apprentissage à partir d'une masse de données et d'informations collectées suite à des opérations de renseignements cyber des menaces et vulnérabilités. Des outils comme IBM Security QRadar[237] / SIEM combinés par exemple avec des tests d'intrusion en boîte noire ou grise sans limitation de périmètre ni de limites par des équipes RED TEAM contribuent grandement à cette « intelligence » dans la détection des cyberattaques.

La section Solutions ferroviaire en cybersécurité et Intelligence Artificielle, présente une sélection de sociétés dont les innovations disruptives pour des trains intelligents sont en totalité basées sur l'Intelligence Artificielle.

V. DÉMARCHE DE SÉCURISATION NUMÉRIQUE DE LA FILIÈRE FERROVIAIRE

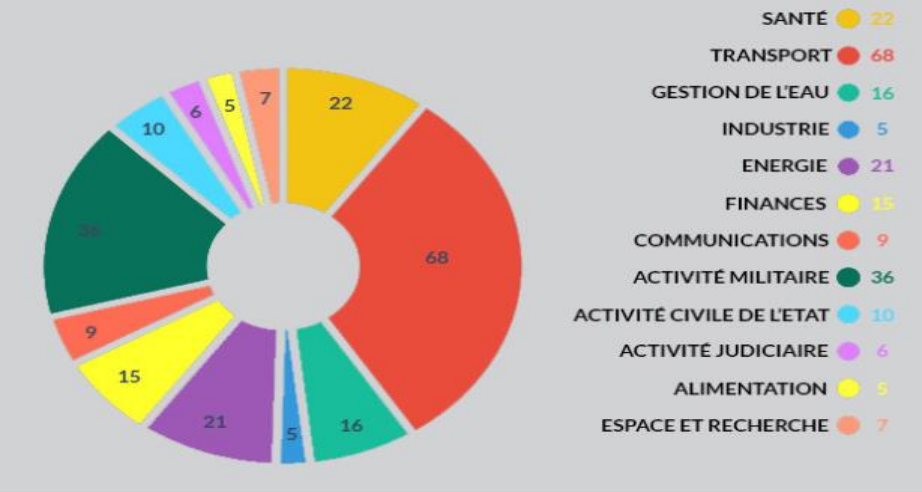
De par son ADN, la filière ferroviaire poursuit deux exigences à savoir :

- L'exigence de sécurité ferroviaire de manière générale : le but ici est de garantir la sécurité des personnes et biens transportés en veillant aux infrastructures, aux matériels roulants, aux systèmes de contrôle et commandes, à la signalisation, la distribution électrique, etc. ;
- L'exigence de sûreté de fonctionnement des équipements qui composent son écosystème technique et pour assurer le service, mais aussi la sécurité.

Au-delà de ces exigences « naturelles », la cybersécurité est entrée dans la liste des obligations des acteurs du ferroviaire. Ceux classés critiques et catégorisés en France comme Opérateurs d'Importance Vitale (OIV) selon la Directive 2008/114/CE et au sein de l'Europe comme Opérateurs de Services Essentiels (OSE) sont contraints de renforcer leur résilience. Dans la catégorie OIV/OSE, ceux du secteur des transports et ceux du

[233] CB, *Le ballast se comporte comme un milieu hétérogène* - [En ligne]. [Réf. du 3 Janv. 2018]. Disponible https://www.constructioncayola.com/rail/article/2018/01/03/116712/ballast-comporte-comme-milieu-heterogene
[234] Thales**,** *Thales augmente l'intelligence des trains pour optimiser le trafic ferroviaire et économiser 30% de leur consommation énergétique* [En ligne]. [Réf. du 25 Nov. 2020]. Disponible sur https://www.thalesgroup.com/fr/monde/transport/news/thales-augmente-lintelligence-des-trains-optimiser-le-trafic-ferroviaire
[235] Alice Pruvot, *Thales - comment les hautes technologies peuvent réduire à court terme les émissions de co2 mondiales.* [En ligne]. [Réf. du 07 oct. 2020]. Disponible https://www.thalesgroup.com/fr/group/journaliste/press-release/thales-comment-hautes-technologies-peuvent-reduire-court-terme
[236] Thales**,** *Renseignement d'intérêt Cyber (Cyber Threat Intelligence)* [Vidéo en ligne]. [Réf. du 11 octobre 2018]. Disponible sur https://www.youtube.com/watch?v=-Fi6M2w_uO8
[237] IBM**,** *IBM QRadar SIEM. Analyse de sécurité intelligente pour des connaissances exploitables sur les menaces les plus critiques* [En ligne]. Disponible sur https://www.ibm.com/fr-fr/qradar/security-qradar-siem/features

ferroviaire en particulier occupent la place prépondérante (68%) comme on peut l'apercevoir dans la répartition du graphique qui suit :



41 - La répartition des OIV par secteur (Source SGDSN)

Les entreprises ayant ce statut ont certes l'avantage de bénéficier de l'appui et l'accompagnement constant de l'ANSI, mais ont tout de même quelques contraintes à respecter. En effet d'après les obligations de la réglementation, et comme nous le confirme Sadio Bâ, coordinateur sectoriel Transport à l'ANSSI, toute entreprise ferroviaire ayant le statut d'OIV doit, outre la désignation d'un délégué pour la défense et la sécurité (interlocuteur privilégié de l'autorité administrative), fournir un Plan de Sécurité d'Opérateur (PSO) décrivant l'organisation et la politique de sécurité de l'opérateur, ainsi que faire approuver les Plans Particuliers de Protection (PPP) pour chacun des points d'importance vitale identifiés dans son entreprise. Ces obligations permettent de s'assurer de la couverture de l'exigence majeure de cybersécurité[238].

En raison des services qu'elles rendent à la nation, l'exigence de cybersécurité est un enjeu capital en termes de souveraineté. Le Livre Blanc sur la défense et la sécurité nationale identifiait dès 2008, les attaques contre les systèmes d'information comme l'une des principales menaces qui pèsent sur la défense et la sécurité en France[239]. Par ailleurs, la continuité numérique aujourd'hui permise par l'interconnexion des systèmes exige d'imposer de nombreuses règles, notamment concernant la cybersécurité qui devient à la fois une contrainte forte et un levier pour organiser la convergence IT-OT dans les entreprises[240]. En 2013, la mise à jour du Livre blanc sur la défense et la sécurité nationale, venait ajouter une pierre à l'édifice en imposant aux OIV via la LPM (Loi de Programmation Militaire) qui en a découlé, le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent, et plus précisément les systèmes d'information d'importance vitale (SIIV)[241].

À cet effet, les acteurs ferroviaires classés OIV doivent répondre aux exigences de conformité réglementaire, aux standards techniques et satisfaire par ailleurs les attentes des clients et métiers. En France, la LPM et les directives NIS (Network and Information

[238] Annexes I - Interviews -Sadio Bâ, Coordinateur Secteur Transport, ANSSI
[239] *La sécurité des activités d'importance vitale* [En ligne] [Réf. Octobre 2016]. Disponible sur plaquette-saiv.pdf (sgdsn.gouv.fr)
[240] Cigref - Clara Morlière, *Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels* [En ligne]. [Réf. du 18 février 2020]. Disponible sur https://www.cigref.fr/wp/wp-content/uploads/2019/12/Cigref-Convergence-IT-OT-Rapprochement-fructueux-Systemes-Information-et-Industriels-Decembre-2019-light.pdf
[241] Prise en compte des enjeux de cybersécurité au sein de la sécurité ferroviaire | EPSF (securite-ferroviaire.fr)

Security) imposent aux OIV et OSE des mesures contraignantes en matière de sécurité et de cybersécurité. Toutefois, la totalité des systèmes d'information nécessaires au fonctionnement du système ferroviaire n'est pas concernée par ces réglementations. Ces dernières ciblent uniquement les infrastructures critiques. Les contraintes des OIV et particulièrement des SI critiques que sont les SIIV (Système d'Information d'Importance Vitale) imposées par la LPM réglementant les OIV obligent les OIV de mettre tout en œuvre pour[242] :

- Identifier les SIIV à déclarer et à sécuriser ;
- Notifier sans délai H24 à l'ANSSI lors de la survenue d'un incident de sécurité sur ces SIIV ;
- Effectuer une opération d'urgence, typiquement couper leurs connexions Internet sous demande expresse du Premier ministre en cas de force majeure dans le pays ;
- Se mettre en conformité, et le cas échéant se faire contrôler par l'ANSSI ou des prestataires qualifiés par l'ANSSI pour vérifier le niveau de sécurité.

Pour bien s'aligner sur les exigences qu'oblige son statut, chaque OIV doit donc avoir une vision holistique de la cybersécurité. Les réponses uniquement technologiques ne permettent en effet pas d'atténuer les conséquences des attaques. Il ne suffit pas de se contenter de la diminution du nombre de vulnérabilités. Induisant un faux sentiment de confiance, les vulnérabilités résiduelles mineures peuvent être plus dévastatrices que celles majeures et critiques qui ont été remédié.

Outre les vulnérabilités liées aux architectures, aux infrastructures logicielles ou matérielles, d'autres facteurs viennent s'y greffer, augmentant la fragilité des écosystèmes d'entreprise. L'accélération du télétravail avec les augmentations des accès divers et variés, le BYOD, l'IoT, doivent d'après le représentant de l'ANSSI être saisies comme des opportunités pour intégrer l'analyse de risques en continu au cœur du programme cyber de toute entreprise. Il est alors important de trouver des leviers pour gagner du temps précieux sur ces analyses de risques devenues incontournables et surtout les rendre plus digestes pour ceux ou celles qui vont s'engager à accepter les impacts des risques résiduels. Le pilotage des projets par les délais et les coûts doit en ce sens s'adosser à la cybersécurité, gage de confiance pour leur bonne conduite.

La prise de conscience de la nécessité de considérer la cybersécurité comme un enjeu stratégique bien qu'étant encore poussive dans certaines entreprises devient par un juste de mélange de pédagogie et de persuasion un incontournable. Les grandes entreprises comme Saint-Gobain ayant subi les attaques de NotPetya en 2017[243] aux impacts au long cours l'ont bien intégré.

Les nouveaux usages sont aussi à considérer dans le processus de sécurisation qui devrait s'inscrire dans une démarche d'amélioration continue de type roue de Deming ou PDCA (Plan, Do, Check and Act).

D'ailleurs, lors des travaux du Cigref[244] regroupant les représentants de plusieurs grandes entreprises industrielles en France en 2019, trois sujets majeurs ont été mis en exergue à savoir la continuité numérique de bout en bout avec une valorisation massive des données, le besoin de nouvelles règles de cybersécurité et les enjeux de compétences et

[242] Annexes I - Interviews (S.Bâ, ANSSI)
[243] Cécile Desjardins, *Comment Saint-Gobain a tiré les leçons de « NotPetya »* [En ligne]. [Réf. du 26 février 2018. Disponible sur https://business.lesechos.fr/directions-financieres/comptabilite-et-gestion/gestion-des-risques/0301302070692-comment-saint-gobain-a-tire-les-lecons-de-notpetya-318947.php
[244] Cigref - Clara Morlière, *Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels* [En ligne]. [Réf. du 18 février 2020]. Disponible sur https://www.cigref.fr/wp/wp-content/uploads/2019/12/Cigref-Convergence-IT-OT-Rapprochement-fructueux-Systemes-Information-et-Industriels-Decembre-2019-light.pdf

d'organisation dans le cadre de la convergence de IT et de l'OT. Une phrase clé à retenir de ce rapport est : ***« Le grand défi, mais aussi le plus important levier est la contrainte d'assurer la sécurité des processus, des données, des personnes et des sites »***

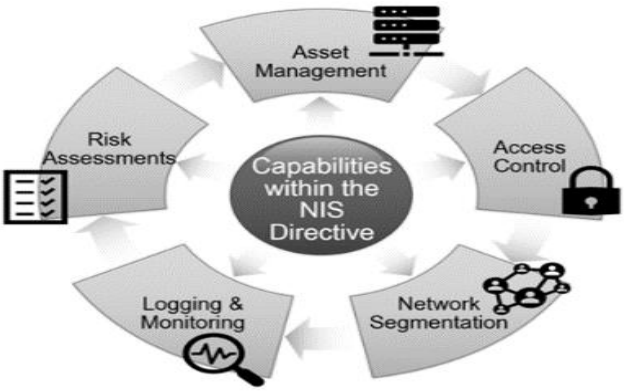
relever ce défi passe par une vision et une surveillance à 360° de la cybersécurité. Cela nécessite la maîtrise des quatre dimensions suivantes :

- Gouvernance, organisation et management ;
- Juridique et réglementaire ;
- Technique et Architecture ;
- Approche par les risques.

Plus concrètement, dans un contexte de convergence IT-OT, plusieurs challenges sont à relever :

- Sur le plan juridique et réglementaire :
  - ✓ Maîtriser les aspects juridiques et se conformer à la réglementation et aux directives nationales et européennes ;
  - ✓ Maîtriser les obligations des prestataires, fournisseurs et sous-traitants *et leurs applications.*
- Sur le plan organisationnel et managérial :
  - ✓ Mettre en œuvre un référentiel des valeurs métiers (actifs et fonctions critiques de l'entité) ;
  - ✓ Cartographier les menaces et les risques qui pèsent sur ces valeurs ou sur les grandes fonctions métier ;
  - ✓ Mettre en place une gouvernance transversale IT-OT notamment en matière d'homologation de la cybersécurité IT-OT ;
  - ✓ Mettre en place un dispositif transversal IT-OT de gestion d'incidents et de crise.
- Sur le plan technique et opérationnel :
  - ✓ Adopter une démarche de défense en profondeur :
    - Spécifier et implémenter une architecture sécurisée et hautement disponible ;
    - Mettre en œuvre et maintenir aussi bien des solutions de protection que les solutions métiers et technologiques ;
    - Garantir la résilience en prévoyant des plans de continuité ;
    - Disposer d'outils de détection des attaques et de veille pour la maîtrise des Cyber Kill Chain ; et un dispositif efficace de sécurité opérationnelle et de gestion de crise ;
- Sur le plan des ressources humaines :
  - ✓ Investir dans la mutualisation des compétences et surtout une complémentarité de compétences entre les experts IT et OT et vice-versa ; en effet, comme le souligne le rapport du groupe de travail du Cigref[245], au-delà des deux premiers enjeux que sont la donnée et la sécurité, le troisième enjeu identifié est celui des compétences ;
  - ✓ Le rapprochement des équipes et la gouvernance des projets sont l'une des clés du succès de la convergence IT-OT. Il s'agit donc de sensibiliser et former des experts OT aux risques cyber.

[245] Cigref - Clara Morlière, *Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels* [En ligne]. [Réf. du 18 février 2020]. Disponible sur https://www.cigref.fr/wp/wp-content/uploads/2019/12/Cigref-Convergence-IT-OT-Rapprochement-fructueux-Systemes-Information-et-Industriels-Decembre-2019-light.pdf



42 - Cinq piliers nécessaires à la mise en conformité des systèmes industriels critiques aux normes européennes (Source Fortinet[246] 2019)

V.1. DIMENSION REGLEMENTAIRE ET JURIDIQUE

Un certain nombre d'entreprises du secteur sont classées à Importance Vitale ou Services Essentiels et pour le cas de la France assujettie à la Loi de Programmation Militaire (LPM) A cela s'ajoute sur le plan réglementaire et la nécessité du respect du Règlement de Protection des Données (RGPD).

V.1.1. EXIGENCE DE CONFORMITÉ RÉGLEMENTAIRE D'OIV / OSE

La première directive NIS (Network and Information Security) votée en 2016 par l'Europe a été transposée en droit national français en 2018. Cette directive concerne les entreprises dont l'activité est d'une importance vitale pour la survie d'une Nation. Elles sont désignées comme des Opérateurs de Services Essentiels (OSE) [247] et Opérateurs d'Importance Vitale (OIV). La directive adresse essentiellement la sécurisation des systèmes d'information critiques appelés Systèmes d'Information d'Importance Vitale (SIIV).

« *La directive NIS vise à l'émergence d'une Europe forte et de confiance, qui s'appuie sur les capacités nationales des États membres en matière de cybersécurité, la mise en place d'une coopération efficace et la protection des activités économiques et sociétales critiques de la nation, pour faire face collectivement aux risques de cyberattaques*. » [248]

Le 16 décembre 2020, le Parlement européen, avec l'appui du Conseil européen, présente une abrogation de la directive UE2016/1148[249]. Cette nouvelle mouture dénommée NIS2 s'est substituée à la directive NIS sur la sécurité des réseaux de 2016, permettant ainsi d'étendre et de moderniser les obligations réglementaires afin de mieux se prémunir des cybermenaces. La nouvelle stratégie de cybersécurité de l'UE constitue, selon le Conseil européen, un élément clé pour « Façonner l'avenir numérique » et mettre en place un plan

[246] Fortinet**,** *Sécuriser l'OT : enjeux stratégiques et mise en conformité des systèmes industriels critiques* [En ligne]. [Réf. de 2021]. Disponible sur https://www.lemondeinformatique.fr/publi_info/lire-securiser-l-ot-enjeux-strategiques-et-mise-en-conformite-des-systemes-industriels-critiques-475.html

[247] Sénat français, *Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148* [En ligne]. [Réf. Du 16 décembre 2021]. Disponible sur https://www.senat.fr/ue/pac/EUR000006694.html#fnref2

[248] ANSSI **-** *Directive Network and Information System Security (NIS)* [En ligne]. Disponible sur https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/

[249]Sénat français, *Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148* [En ligne]. [Réf. Du 16 décembre 2021]. Disponible sur https://www.senat.fr/ue/pac/EUR000006694.html#fnref2

[249] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union [Réf. Du 19 juillet 2016] [En ligne]. Disponible sur https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033122937

de relance pour l'Europe. D'autres amendements à la directive (UE) 2016/1148 se sont rajoutés en date du 15 octobre 2021[250]

quelques points importants à retenir de cette directive[251] :

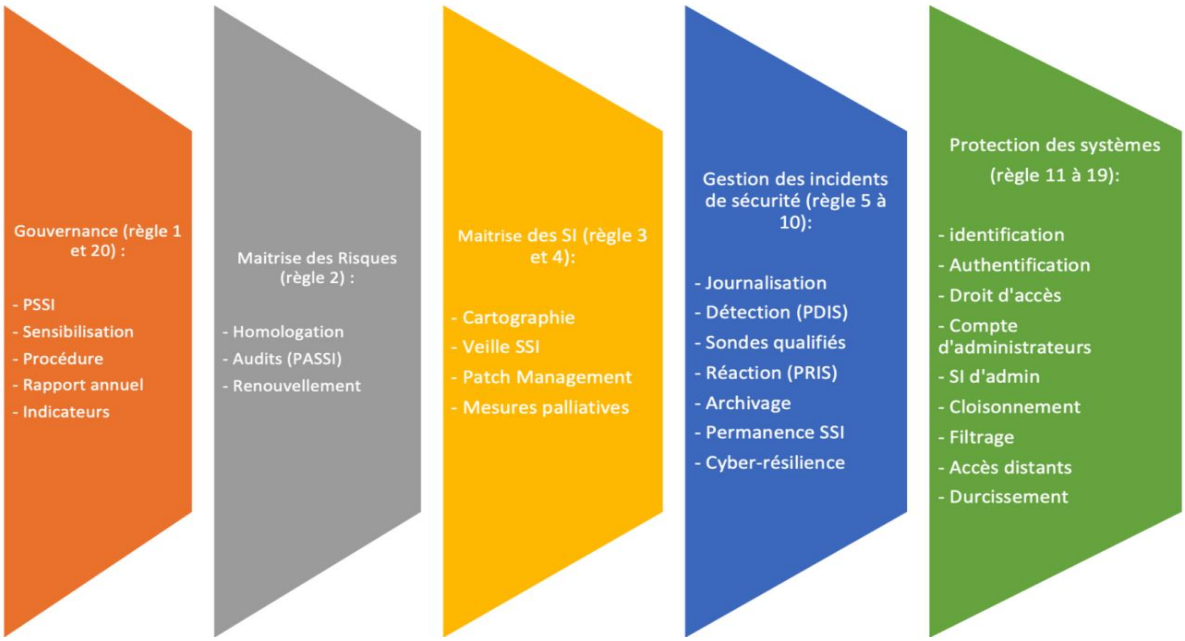
- Elle renforce les exigences de sécurité imposées aux entreprises, traite de la sécurité des chaînes d'approvisionnement et des relations avec les fournisseurs ;
- Elle rationalise les obligations de déclaration ;
- Elle introduit des mesures de surveillance plus strictes pour les autorités nationales ;
- Enfin elle renforce les exigences relatives à l'application de la législation et harmonise les régimes de sanctions dans tous les États membres.

V.1.2. LPM ET ARRÊTÉ SECTORIEL POUR LA CYBERSÉCURITÉ DANS LES TRANSPORTS

La LPM (Loi de Programmation Militaire) votée fin 2013 et entrée en vigueur au 1er juillet 2016 avec une déclinaison par des arrêtés sectoriels, stipule dans son article 22 le concept d'OIV (Opérateur d'Importance Vitale). La Revue Stratégique de Cyberdéfense rendue publique le 12 février 2018, (la nouvelle LPM pour les années 2019 à 2025), dans son chapitre II, propose, compte tenu de l'importante croissance en nombre, en ampleur, en intensité et en sophistication des cyberattaques, de renforcer le dispositif de prévention et de protection. L'ANSSI s'est vue dotée de prérogatives supplémentaires lui permettant, l'accompagne et le contrôle des OIV, le droit de diligence auprès des opérateurs de Télécommunications et d'installer ses propres moyens de détection sur leur réseau ou sur le système d'information. Les opérateurs de communications électroniques quant_à eux ont l'obligation de financer sur leurs fonds propres et non par les finances publiques, la mise en en œuvre de moyens de détection et de blocage des attaques, de prévention des incidents et d'alerte des victimes.

L'application de la LPM implique un investissement conséquent de la part des OIV. Ils doivent identifier ce qui relève d'un SIIV (Système d'information d'importance vitale) et le mettre en conformité vis-à-vis des règles édictées et aligner les processus et corpus documentaire sur les exigences imposées par la LPM[252]. Les arrêtés de la loi de programmation militaire prévoient un délai variant de 3 mois à 2 ans pour mettre en place les 20 règles de mise en conformité des SIIV regroupées par thématique (voir *schéma qui suit*).

[250] Clara Biasa Berti**,** *Commission des libertés civiles, de la justice et des affaires intérieures [Rapport* en ligne]. [Réf. Du 15 octobre 2021]. Disponible sur https://www.europarl.europa.eu/doceo/document/LIBE-AD-693822_FR.pdf
[251] Pierre Berthelet**,** *Directive "SRI 2" : l'Europe crée un CyCLONe pour gérer les crises cyber [E*n ligne]. [Réf. Du 03 mars 2021]. Disponible sur http://securiteinterieurefr.blogspot.com/2021/03/directive-sri-2-leurope-cree-un-cyclone.html
[252] Franck Miquel, *Réussir la mise en conformité de ses systèmes d'informations d'importance vitale (SIIV)* – [En ligne]. [Réf. du 6 juin 2019]. Disponible sur https://www.synetis.com/lpm-reussir-la-mise-en-conformite-de-ses-systemes-dinformations-dimportance-vitale-siiv/



43 -Piliers pour la mise en conformité des Systèmes d'Informations d'Importance Vitale (SIIV)[253]

V.1.3. RGPD, RÈGLEMENTATION GÉNÉRALE POUR LA PROTECTION DES DONNÉES

Tout acteur du ferroviaire comme toutes les autres entreprises doit se doter d'une organisation permettant de s'assurer du respect du RGPD (Réglementation Générale de la Protection des Données) imposant de mettre en place tous les moyens techniques et organisationnels afin d'assurer la protection des données à caractère personnel que les personnes concernées lui confient, sous peine en cas de manquement grave, d'une condamnation pénale et financière. Les sanctions liées à la violation au titre de la RGPD sont identiques à toutes les entreprises. Concernant les OIV et pour le cas des transports, le non-respect (après des injonctions et mise en demeure), des obligations de l'arrêté sectoriel en matière de cybersécurité sont passibles par la loi d'une amende de 150.000€ par écart identifié, s'élevant à 750.000€ pour les personnes morales. La loi française ne fait pas de distinction selon que le manquement est ou non intentionnel. La simple négligence est donc en principe condamnable[254].

V.1.4. DIMENSION JURIDIQUE

La cybercriminalité ordinaire tout comme l'espionnage industriel en particulier, le terrorisme, les manœuvres de déstabilisation soutenues par des États se sont déportés de l'espace géographique au cyberespace.

L'intelligence juridique va s'appliquer à toutes les réglementations, autour des données, des exigences imposées aux OSE et aux OIV, des chaînes de responsabilités avec les opérateurs, entreprises ferroviaires, fournisseurs, sous-traitant prestataires, et demain des

---

[253] Franck Miquel, *Réussir la mise en conformité de ses systèmes d'informations d'importance vitale (SIIV)* – [En ligne]. [Réf. du 6 juin 2019]. Disponible sur https://www.synetis.com/lpm-reussir-la-mise-en-conformite-de-ses-systemes-dinformations-dimportance-vitale-siiv/

[254] Betty Sfez, *Droit des TIC, informatique, propriété intellectuelle*
Quelles obligations pour les OIV en matière de cybersécurité : exigences européennes et françaises comparées. [En ligne]. [Réf. 18 avril 2014]. Disponible sur https://www.village-justice.com/articles/Quelles-obligations-pour-les-OIV,16739.html

problématiques liées aux impacts environnementaux, sociétaux, et celles liées aux usages de l'Intelligence Artificielle.

Il est en effet important de rappeler ici la place de l'intelligence juridique dans une démarche de sécurisation globale. La cybercriminalité ordinaire, le cyber espionnage industriel, le cyberterrorisme sont des batailles déjà émergentes. L'arsenal juridique est l'une des armes protectrices sur lesquelles s'appuyer. La cybersécurité est aujourd'hui considérée partout dans le monde, non seulement comme un enjeu majeur d'intelligence économique,[255] mais aussi un enjeu majeur de souveraineté d'un pays, la prise de contrôle à distance d'un train pour porter atteinte à la vie de ses passagers pouvant être qualifiée de déclaration de guerre.

Au niveau de la France, un certain nombre de dispositifs juridiques existent. La loi Godfrain[256] de 1988 condamne les fraudes informatiques sous toutes ses formes. La convention européenne de 2001 sur la cybercriminalité et les textes législatifs tels que la loi du 24 juillet 2015 ont durci quant à elles les peines contre les violations des systèmes d'information[257], les OIV peuvent bénéficier, dans le cadre de la LPM, de possibilités élargies d'interventions et d'appui d'organismes étatiques tels que l'ANSSI, par exemple lors de la vérification réglementaire de la mise en œuvre de mesures de sécurité auprès des opérateurs Télécoms ou encore la pose des sondes de protection et détection propres à l'ANSSI.

V.2. GOUVERNANCE, MANAGEMENT, ORGANISATION

V.2.1. DE LA SURETÉ A LA CULTURE DU RISQUE CYBER

Le monde ferroviaire, avec une maîtrise éprouvée sur de longues années d'expérience aux risques liés à la sécurité ferroviaire et à la sûreté de fonctionnement dont il avait déjà, doit maintenant intégrer de nouveaux types de risques qui sont liés à des menaces systémiques. Toutefois, intégrer des facteurs de risques aux impacts potentiels imprévisibles n'est pas dans la culture habituelle du secteur, jusqu'ici habitué à la prédictibilité des données sur lesquelles se basent les évaluations des risques Safety. La sécurité ferroviaire et la cybersécurité ont pourtant des chemins qui convergent et elles doivent dorénavant faire partie d'une stratégie globale de gestion du risque fondée sur les objectifs métiers et les valeurs intrinsèques au secteur.

Ce changement de paradigme demande un travail en profondeur de chaque acteur du ferroviaire et plus particulièrement des OIV et des OSE. Il faut en effet déterminer a minima le seuil de tolérance au risque, ou le « niveau de risque acceptable ». Ce seuil peut varier selon la catégorie d'actifs qui sont mis en jeu[258].

D'un autre côté les cybermenaces pèsent comme une chape de plomb ; ces derniers ne doivent pas être rédhibitoires et empêcher les décideurs d'oser les transformations indispensables dans le secteur. Les risques que pourrait faire émerger la convergence IT-OT et l'avènement des transports de nouvelle génération doivent aussi être vus comme des opportunités pour le transport ferroviaire. Les transformations appellent à de nouvelles gouvernances, voire des ruptures nécessaires dans les modes de management et

[255] *Romain GERARDIN-FRESSE* [En ligne] [Réf. Du 9 avril 2018]. Disponible sur La cybersécurité, un enjeu majeur de l'intelligence économique | Les Echo
[256] *LOI N°88-19 DU 5 JANVIER 1988 relative à la fraude informatique* [En ligne] [Réf. Du 5 Janvier 1988]. Disponible sur Loi du 5 janvier 1988 (ens.fr)
[257] *Code pénal, atteintes aux systèmes automatisés de traitement de données* [En ligne] [Réf. Du 25 juillet 2015]. Disponible sur Chapitre III : Des atteintes aux systèmes de traitement automatisé de données (Articles 323-1 à 323-8)
[258] *Gouvernance de la sécurité des TI Une approche globale* [En ligne] [Réf. 2016]. Disponible sur Gouvernance de la sécurité des TI - Une approche globale (cgi.com)

l'organisation de l'entreprise de manière générale. Embrasser ces nouvelles appétences aux risques demande une revisite des objectifs opérationnels moteurs de la convergence IT-OT, l'identification et la bonne compréhension des enjeux de la convergence des cultures IT et OT, et pour finir une activation d'une politique proactive et bien conçue de convergence IT-OT[259].

V.2.2. NOUVELLE GOUVERNANCE

Le rapprochement des mondes OT et IT appelle par construction à une organisation intégrée de bout en bout. Cela ne peut se faire sans un changement dans l'approche de la gestion des menaces et des risques qui pèsent sur les SI converger (SI Industriels et SI d'Entreprise). Il est nécessaire par ailleurs de dresser une cartographie des cyberrisques métiers intégrés.

Tout ceci implique une nouvelle gouvernance, des stratégies et des modes d'organisation au service des objectifs ci-dessous à savoir :

- La préservation des actifs de l'entreprise par la maîtrise des risques de sécurité de tous les systèmes de l'entreprise et par la réduction des surfaces d'exposition des systèmes ;
- La résilience de l'entreprise aux attaques et aux dysfonctionnements potentiels ;
- La conformité aux réglementations ;
- La capacité à réagir dans un délai adapté aux situations de crise.

Il est crucial de déterminer l'orientation à prendre et surtout de mettre en œuvre des mesures pour s'assurer que les modalités de cette gouvernance soient respectées.

Cette gouvernance doit donc veiller aux synergies entre les acteurs IT et OT ; la démarche de conformité « intégrée et de bout en bout » IT-OT peut en être un puissant levier. En effet, elle est à considérer comme un élément essentiel qui sert de boucle de rétroaction pour la gouvernance de la sécurité. C'est un moyen efficace pour s'assurer que toutes les parties prenantes travaillent ensemble pour réduire les risques et protéger l'ensemble des actifs de la chaîne. Le cas échéant, il s'agit alors de s'assurer que les écarts qui résultent de l'analyse de certaines expositions au risque sont partagés avec tous, ainsi que communiqués et compris par l'équipe dirigeante. Les membres qui la composant doivent disposer des éléments suffisants pour éclairer leur décision. Il s'agira de faire le choix entre l'acceptation des risques résiduels dans le cadre du respect des normes en vigueur, convenir des mesures et des ressources nécessaires pour y remédier ou les supprimer, trouver un organisme qui acceptera de les assurer (solution de déport du risque).

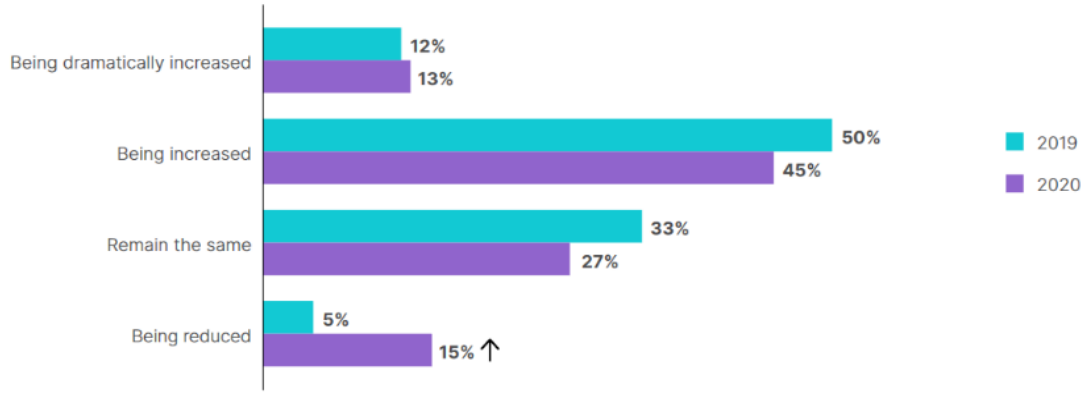
Autre point important, la gouvernance autour des données ne peut plus être considérée comme une activité subsidiaire ou optionnelle. C'est en effet un axe majeur de maîtrise du patrimoine immatériel que sont les données, elles-mêmes au cœur de la digitalisation. La valorisation, la maîtrise des circuits de données de bout en bout et leurs sécurisations sont donc des enjeux majeurs.

V.2.3. EFFORTS BUDGÉTAIRES

La cybersécurité longtemps utilisée comme variable d'ajustement lors des arbitrages budgétaires doit prendre sa place comme levier transverse soutenant toutes les activités de l'entreprise et notamment comme brique renforçant la sûreté et la sécurité ferroviaire. À ce titre, des efforts financiers doivent être concrétisés dans les budgets pour décliner en fait, en actions et en investissements, la volonté ou les intentions de renforcement de la posture en cybersécurité. Au regard du graphique de l'ENISA ci-dessous, un tassement des

[259] *3 moyens de simplifier la convergence IT / OT* [En ligne] [Réf. Du 3 mai 2021]. Disponible sur https://www.rockwellautomation.com/fr-fr/company/news/blogs/industrial-itot-convergence-improvement-tips.html

efforts budgétaires s'est fait ressentir en 2020 en Europe. Ces enveloppes budgétaires n'avaient pas prévu les vagues de cyberattaques exceptionnellement opportunistes engendrées par le contexte pandémique et l'augmentation des surfaces d'attaque correspondante engendrée par la massification nécessaire et réalisée en urgence du télétravail.



44 - Budget de la sécurité en 2020 (Source Fortinet[260])

V.2.4. RESSOURCES HUMAINES, SENSIBILISATION ET FORMATION
V.2.5. LA SENSIBILISATION, LA FORMATION

L'étude réalisée par IBM[261] en 2017 montre que 90 % des incidents de sécurité ont pour origine l'erreur humaine. Cette même étude pointe le fait que 44 à 48 % des entreprises ne se sentent pas protégées contre les menaces du fait du manque de prise de conscience de leurs salariés sur les risques de cybermenaces. La société de cybersécurité VMware Carbon Black révèle par ailleurs un triplement des cyberattaques en 2020 contre les institutions financières du fait du manque de sensibilisation des employés à la cybersécurité. Il en est de même du dernier rapport du Cesin (janvier 2021[262]), corroborant le fait que l'origine humaine est le principal vecteur d'attaque en 2020.

Sensibiliser les utilisateurs a minima à la sécurité web est indispensable afin de protéger votre entreprise des personnes malveillantes et prévenir une partie des attaques potentielles. En effet, les salariés sont les premiers visés par une attaque informatique de par leur manque de connaissance, et donc de vigilance, sur le sujet. En les formant, les entreprises érigent de premiers remparts forts utiles autour de leur parc informatique.

Un autre angle et pas des moindres est le Shadow IT (l'installation de logiciels non validés par les DSI ou les équipes cyber) souvent à l'origine des attaques réussies. Dans des contextes de besoin métiers volatils et d'offre logicielle évoluant en permanence, bien que les salariés soient de plus en plus sensibilisés, ils restent peu impliqués et ne suivent pas forcément les recommandations d'usage proposées, mettant leurs besoins opérationnels en opposition avec le besoin en protection de l'entreprise et de son patrimoine informationnel. Un important travail de pédagogie et de communication reste donc à faire, tant du côté des métiers pour qu'ils connaissent l'offre interne de logiciels validés par leurs entreprises, que du côté des DSI pour qu'elles mettent à disposition dans des délais

[260] *2020 State of Operational Technology and Cybersecurity Report – FORTINET* [En ligne] [Réf. Du 13 avril 2021]. Disponible sur State of Operational Technology and Cybersecurity Report (fortinet.com)
[261] *La sensibilisation des collaborateurs à la sécurité informatique.* [En ligne] [Réf. 2019]. Disponible sur Livre-blanc-sensibilisation-a-la-securite-informatique.pdf (kaspersky.com)
[262] *Baromètre cybersécurité des entreprises françaises CESIN* [En ligne] [Réf. Du 6 janvier 2021]. Disponible sur https://www.cesin.fr/document/view/4e0928de075538c593fbdabb0c5ef2c3

acceptables par les métiers, les logiciels dont ils ont besoin au quotidien dans leur environnement numérique.

Une sensibilisation et le cas échéant des formations de base doivent être au cœur des politiques vis-à-vis des personnes, des entreprises comme de l'État et même au niveau européen et en l'occurrence dans le secteur ferroviaire.

Le 16 décembre 2020, la Commission européenne a publié sa boîte à outils sur la cybersécurité des transports, un répertoire de conseils et de pratiques recommandées pour renforcer la cybersécurité et la cyber résilience dans le secteur des transports[263]. La Commission européenne l'a mise en place partant du constat que malgré le fait que la cybersécurité soit une préoccupation croissante pour l'industrie des transports, de nombreux employés restent insuffisamment conscients des risques, et leurs actions peuvent parfois ouvrir par inadvertance la porte à des attaquants. C'est dans ce contexte que la boîte à outils sur la cybersécurité des transports a été créée et proposée, pour contribuer à élever le niveau de cyber-sensibilisation et de cyber-hygiène dans le secteur des transports, en retard sur des secteurs comme le bancaire. Le kit s'adresse ainsi aux organisations de transport et de logistique, quels que soient leur taille et leur domaine d'activité, ainsi qu'à tout le personnel de transport, les décideurs, les fournisseurs et les prestataires de services.

La plateforme et le programme couvrent de façon contextualisée, les thématiques relatives aux menaces spécifiques, susceptibles d'affecter les organisations de transport telles que la diffusion de logiciels malveillants, le déni de service, l'accès non autorisé et le vol de données, et la manipulation de logiciels. Ces éléments incluent aussi bien des informations détaillées sur ces menaces que les bonnes pratiques d'atténuation correspondantes. Il existe également dans sa formule avancée des conseils sur l'identification, la protection, la détection et la réponse aux cybermenaces.

Comme le rappelle si bien Catherine Jarrige Responsable de la Recherche et Développement International à la Direction de la Défense et de l'International de la SNCF, « *l'approche managériale à long terme de la sécurité pour l'ensemble de l'entreprise repose sur quatre piliers : le respect des procédures ; la sensibilisation ; sécurité des TI; et obligations en matière de discrétion et de confidentialité* » [264]

V.2.6. LE RECRUTEMENT ET LA GESTION DE COMPÉTENCES

Une stratégie sans ressources compétentes à même de pouvoir la décliner opérationnellement est une coquille vide. Le secteur de la cybersécurité souffre globalement d'une pénurie importante en ressources formées. Attirer de nouveaux talents à hautes compétences techniques et relationnelles dans le secteur de la cybersécurité est un challenge mondial. La lutte entre les employeurs pour s'attacher les candidats trop peu nombreux sur le marché induisant une progression toujours plus forte des salaires dans ce secteur[265]. Cela est d'autant plus vrai dans les secteurs industriels comme le ferroviaire ; bien qu'offrant des services essentiels le ferroviaire souffre d'une image peu moderne, et de budgets pour les salaires encore très désalignés sur le marché.

L'état du marché de l'emploi cyber et la convergence entre les mondes IT et OT appellent donc à investir de manière conséquente dans la mutualisation des compétences et surtout une complémentarité entre les experts IT et OT et vice-versa. De fait, la gestion des

---

[263] *Transport Cybersecurity Toolkit training* [En ligne] [Réf. 2021]. Disponible sur Transport Cybersecurity Toolkit Training (transport-cybersecurity-toolkit.com)

[264] *UIC Security Week 2018 – eyes and ears!* [En ligne] [Réf. Du 23 juin 2018]. Disponible sur UIC Security Week 2018 – eyes and ears! – Passion4Transport

[265] *Salaires, Stress… et Souveraineté | SSI – CESIN | Alain Bouillé* [En ligne] [Réf. 28 octobre 2021]. Disponible sur https://www.cesin.fr/article-ssi-salaires-stress-et-souverainete-alain-bouille-cesin.html

ressources humaines représente l'un des principaux défis de la convergence des réseaux IT et OT. La convergence implique une montée en compétences des équipes informatiques et opérationnelles, qui parlent un langage commun, clé d'une sécurité optimale de l'infrastructure globale.

Les grands acteurs comme SNCF pourraient par exemple étoffer les modules de formation en cybersécurité ferroviaire pour les acteurs IT et OT dans le cadre de l'Université de l'Ingénierie dont dispose la SNCF.

V.3. APPROCHE PAR LES RISQUES

Pour relever les défis modernes en matière de sécurité, les organisations doivent constamment appliquer des méthodes efficaces de gestion du risque à tous les niveaux. En l'absence d'un processus de suivi de la conformité, il est impossible de garantir que les risques soient gérés comme souhaité, détecter et corriger les problèmes éventuels lorsque ce n'est pas le cas[266].

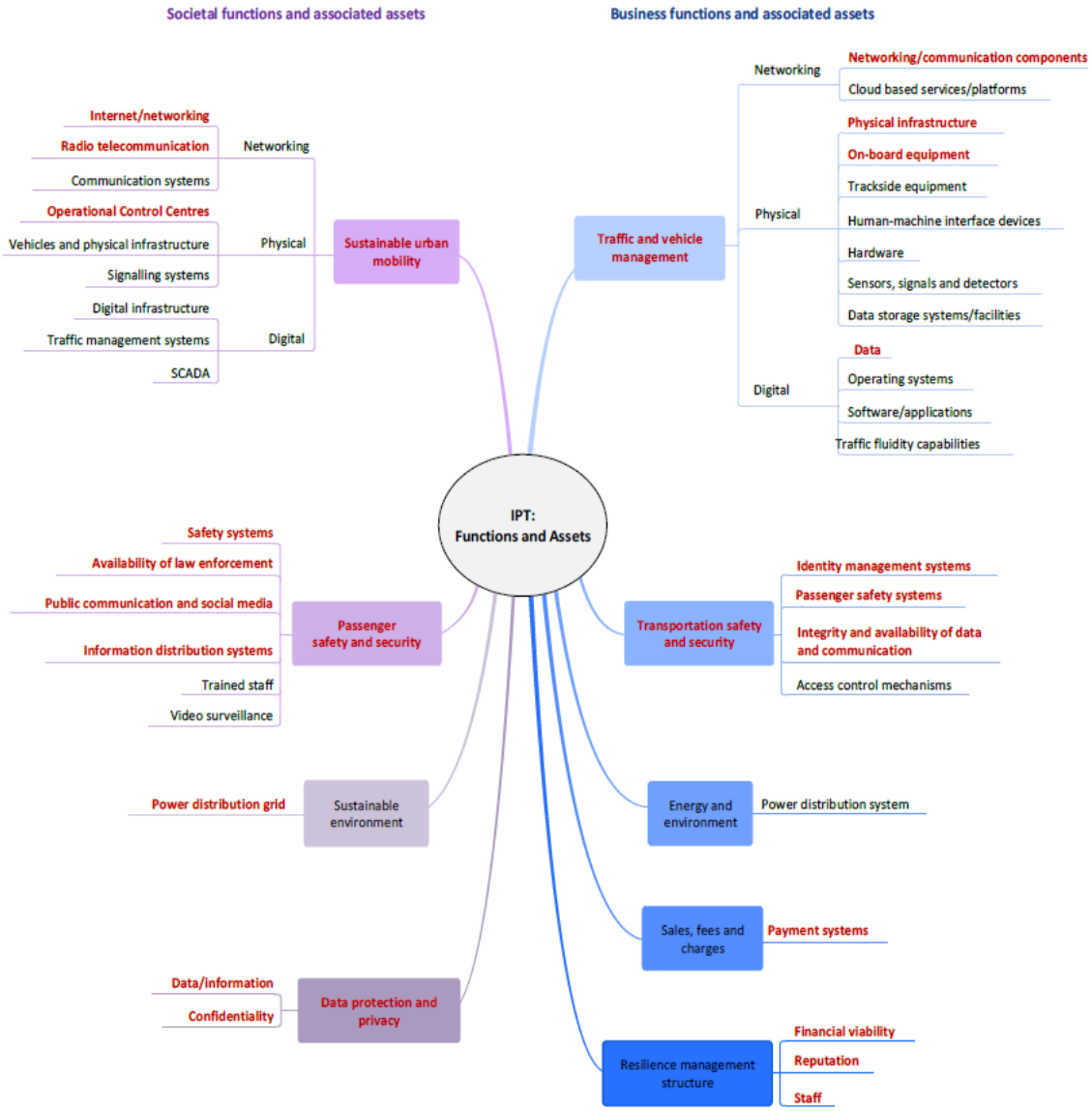
Quand on évoque une gouvernance de la cybersécurité, que ce soit avec les systèmes d'information (IT) ou les systèmes industriels (OT), deux points clés reviennent en premier :

1) La cartographie exhaustive des fonctions et l'inventaire des biens essentiels de son système d'information,
2) La mise en œuvre d'une analyse de risques ou en fonction de ses objectifs une analyse de criticité. Dans le cas des analyses de risques, deux approches coexistent, celle par conformité, fondée sur un socle de sécurité qui sert de référence, et celle par les risques en eux-mêmes. La première se réfère aux normes et règlements encadrant le domaine couvert de l'analyse, la seconde s'appuie sur une identification des menaces et de leurs scénarios d'attaque stratégiques et opérationnels auquel le domaine est potentiellement soumis. L'approche par conformité n'est pas toujours adaptée aux enjeux ou applicable à certaines contraintes opérationnelles, c'est le cas du monde industriel. En effet, la gestion de la sécurité dans le monde ferroviaire nécessite une approche structurée permettant le contrôle continu des risques, mais aussi l'identification des dangers inhérents aux activités métiers. Bien que l'ensemble des acteurs du système ferroviaire met en œuvre des actions qualifiables d'approches par les risques, le choix d'une analyse de criticité proportionnée est à privilégier.

V.4. REFERENTIEL, FONCTIONS, BIENS METIERS - ESSENTIELS

Les entreprises ferroviaires et en particulier les Gestionnaires d'Infrastructure (GI) sont confrontées à une difficulté majeure en raison du volume et la dissémination de valeurs patrimoniales à répertorier. À cela s'ajoute pour certains gestionnaires d'infrastructure la complexité des organisations. Réaliser un inventaire et une ne cartographie d'un système industriel sont des projets d'envergure eu égard la nature hétéroclite du réseau à laquelle se rajoute la dimension géographique assez conséquente.

[266] *Gouvernance de la sécurité des TI Une approche globale* [En ligne] [Réf. 2016]. Disponible sur Gouvernance de la sécurité des TI - Une approche globale (cgi.com)



45 - Principaux assets critiques dans les transports publics intelligents (Source ENISA) [267]

Au regard de cette difficulté d'inventaire du périmètre se pose la question dans le cadre d'une convergence IT-OT, du comment déterminer les vulnérabilités éventuelles sans disposer d'une véritable visibilité du patrimoine. Celles-ci peuvent être liées par exemple à l'obsolescence de certains actifs clés, leur exposition aux usures précoces ou aux cyberattaques potentielles et protéiformes. Pouvoir identifier a minima les groupements d'assets critiques devant faire l'objet d'une intervention rapide en cas d'attaque du fait de leur importance opérationnelle est une tâche à diligenter en première intention, car il y va de la pérennité des activités de l'entreprise, voire dans le cas de structures OIV ou OSE, de vies humaines. Dans tous les cas, rappelons que l'inventaire revêt un intérêt de premier plan en cybersécurité, et ce à plusieurs titres [268] :

1. La prévention : la cartographie permet en effet de :
   - ✓ Répertorier les vulnérabilités, traiter rapidement et de façon exhaustive les alertes d'un CERT ;

[267] *Cyber Security and Resilience of Intelligent Public Transport* [En ligne] [Réf. De décembre 2015]. Disponible sur Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations — ENISA (europa.eu)
[268] *Guide cybersécurité des systèmes industriels - CLUSIF* [En ligne] [Réf. De février 2021]. Disponible sur Guide cybersécurité des systèmes industriels.pdf)

- ✓ Gérer l'obsolescence et les vulnérabilités des logiciels, des applicatifs et des matériels ;

2. La détection : il s'agit d'ici de pouvoir identifier à temps les disparitions d'équipements ainsi que les modifications, malveillantes ou par erreur, de configuration, de logiciel et de matériel ;
3. La réaction : en cas de suspicion, la connaissance des assets mis en cause permet en effet de les déconnecter en fonction de la criticité, de l'impact, le temps de réaliser les levées de doute.

V.5. CLASSE DE RISQUE DANS LE MONDE INDUSTRIEL

Du point de vue industriel, il existe des référentiels proposant de classer les systèmes industriels en 4 ou 5 niveaux. Les premiers niveaux dépendent le plus souvent de la sûreté de fonctionnement. Seuls les niveaux en relation avec les besoins de sécurité seront considérés dans ce document.

Ces niveaux de cybersécurité sont définis en fonction des conséquences pour la nation et non en fonction des conséquences propres aux entités responsables[269].

Chaque classe intègre nécessairement les mesures de la classe inférieure. On distingue trois classes de cybersécurité des systèmes industriels :

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 doit pouvoir être appliqué en complète autonomie. Ce niveau correspond principalement aux règles d'hygiène informatique basiques listées dans le guide de l'ANSS[270]I.

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 est vérifiée par l'autorité étatique ou un organisme accrédité à intervalles réguliers.

VI. GESTION DES RISQUES - RISK MANAGEMENT

VI.1. DEFINITIONS

La survie d'une entreprise impose entre autres de préserver son image de marque, de garder secret son savoir-faire, d'assurer sa compétitivité, de protéger ses données sensibles, y compris celles de ses clients le cas échéant, et d'assurer la continuité de son activité métier.

[269] *La cybersécurité des systèmes industriels – Méthode de classification et mesures principales – ANSSI* [En ligne] [Réf. De janvier 2014]. Disponible sur securite_industrielle_GT_methode_classification-principales_mesures.pdf
[270] *Guide d'hygiène informatique. Renforcer la sécurité de son système d'information en 42 mesures* [En ligne] [Réf. xxx]. Disponible sur https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

La sécurité de ses informations passe par des exigences liées à leur *confidentialité*, leur *intégrité* et leur *disponibilité*. En outre, d'autres propriétés telles que leur *authenticité*, leur *imputabilité*, leur *non-répudiation* et leur *fiabilité*, peuvent également être considérées[271].

Une sécurité efficace de l'information réduit les risques en protégeant l'organisation contre les *menaces* et les *vulnérabilités*, ce qui réduit les *conséquences* sur les actifs. La sécurité de l'information est assurée par la mise en œuvre de mesures adaptées[272].

Le risque lié à la sécurité de l'information est associé à la possibilité que des *menaces* exploitent les *vulnérabilités* d'un *actif* ou d'un *groupe d'actifs* informationnels et nuisent donc à une organisation. Un risque lié à la sécurité de l'information est souvent exprimé en termes *de combinaison de la probabilité d'occurrence d'un événement lié à la sécurité de l'information et de ses conséquences*.

La gestion du risque doit englober :

- L'identification et l'estimation du risque, on parle d'*appréciation* du risque ;
- La maîtrise de ce risque par des mesures adéquates (techniques et/ou organisationnelles) : c'est le *traitement* du risque ;
- L'*acceptation* du risque résiduel par les porteurs de risques légitimes (IT et métiers) ne doit pas être omise.

Avant d'aborder à proprement parler des menaces et les risques qui pèsent sur le secteur ferroviaire, nous allons commencer par décrire les normes et autres spécifications assimilées qui fixent le cadre d'étude de la gestion de la sûreté, de la sécurité et des risques.

VI.2. LES NORMES EN GESTION DE RISQUES

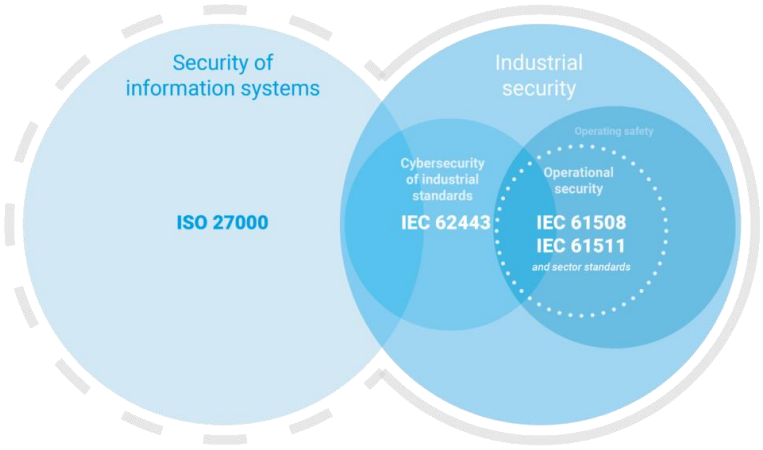
Une norme est un document approuvé par un organisme indépendant reconnu, qui a été mis au point par voie de consensus entre des experts du domaine, et qui fournit des recommandations sur la conception, l'utilisation ou la performance des produits, processus, services, systèmes ou personnes[273].

Dans le domaine de la sécurité de l'information, il s'agit en particulier de la famille des normes ISO/IEC 27 000 publiées en 2005 par l'Organisation internationale de Normalisation (ISO) et la Commission Electronique internationale (CEI). Le système de management de la sécurité d'information ISO 27001 comme l'ISO 27 006 sont les seuls de la famille ISO 27 000 à être des normes d'exigences c'est-à-dire qu'elles permettent de

46 - Les normes ISO/IEC 27 000 (Source Protectam)

[271] *Information technology — Security techniques — Information security management systems — Overview and vocabulary* [En ligne] [Réf. De février 2018]. Disponible sur ISO 27000 :2018
[272] *Information technology — Security techniques — Code of practice for information security controls* [En ligne] [Réf. D'octobre 2013]. Disponible sur ISO 27002:2013
[273] *Les normes dans le monde d'aujourd'hui* [En ligne] [Réf. 2021]. Disponible sur COPOLCO (iso.org)

définir *ce qu'il faut faire,* mais ne précisent pas *comment il faut le faire*. [274]

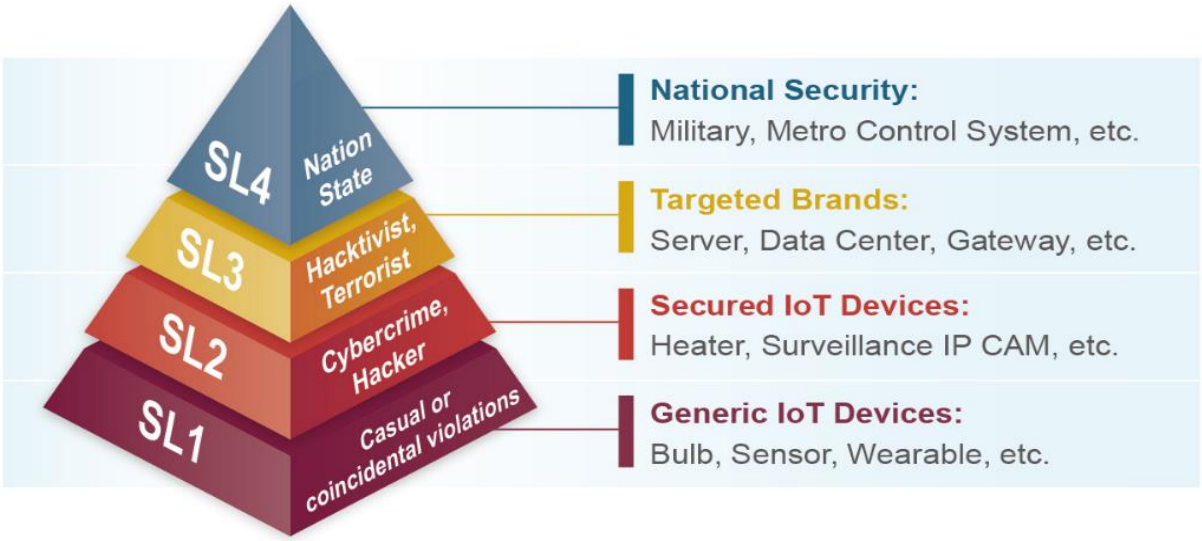


47 - Gestion des risques dans la convergence IT / OT (source Stormshield 2019)

Dès 2007 les premiers référentiels spécifiques à la cybersécurité industrielle ont été publiés. Ils émanent principalement du comité 99 de l'International Society of Automation (ISA) et sont communément appelés normes ISA 99. Sous l'égide de la CEI (ou IEC – International Electrotechnical Commission), sont progressivement publiées des normes comme la sûreté de fonctionnement et la sécurité fonctionnelle avec l'IEC 61 508.

La norme IEC 61 508 définit aujourd'hui les règles de l'art pour les techniques de sécurité fonctionnelle. Elle détermine quatre niveaux de sécurité appelés SIL (Safety Integrity Level, en français ou niveau d'intégrité de la sécurité) classé de SIL 1 à SIL 4. SIL 4 correspondant au risque le plus élevé. Plus la criticité est élevée, plus les tâches et vérifications à effectuer seront nombreuses. L'intégrité correspond à la probabilité que le système exécute la fonction requise relative à la sécurité dans toutes les conditions définies sur une période de temps donnée. L'analyse des dangers et des risques détermine tous les risques liés à un système, elle sert à décider si des systèmes instrumentés de sécurité sont nécessaires. La norme IEC/DIN EN 61 511 découle de la norme CEI/DIN EN 61 508 en tant que norme de base pour l'industrie des process.

[274] *Compréhension des besoins et attentes des parties intéressées* [En ligne] [Réf. Du 27 juillet 2021]. Disponible sur Clause 4.2 : Attentes Des Parties Intéressées - ISO 27001 - Protectam



48 - IEC 62 443- Modèles d'évaluation des niveaux de cyber risques[275]

C'est en 2013 qu'est publiée sur le site de l'ISA France, la norme ISA/IEC 62 443. Cette norme est le liant entre les deux environnements IT et OT qui deviennent de plus en plus convergents. Elle constitue un cercle vertueux au service d'une gestion du risque de cybersécurité des installations industrielles dans son ensemble[276]. La norme IEC 62443 apporte un ensemble de recommandations, mais comme toutes les normes ISO, elle ne s'impose pas aux industriels. Elle est néanmoins adaptée aux contextes et aux spécificités des configurations et installations critiques.

VI.2.1. IEC 62443, NORME DE GESTION DE RISQUE DE CYBERSÉCURITÉ DES INSTALLATIONS INDUSTRIELLES

La rédaction de la norme IEC 62443 débutée en 2013 est toujours en cours. L'objectif de cette norme est de définir les exigences de cybersécurité applicables aux systèmes suivants :

- IACS (Industriel Automation and Control Systems);
- SCADA (Supervisory Control And Data Acquisition);

Ces derniers sont communément utilisés pour la supervision des industries ci-dessous :

- Réseaux de transport et de distribution d'électricité ;
- Réseaux de distribution d'eau et de gaz ;
- Production de gaz et de pétrole ;
- Pipelines et gazoducs.

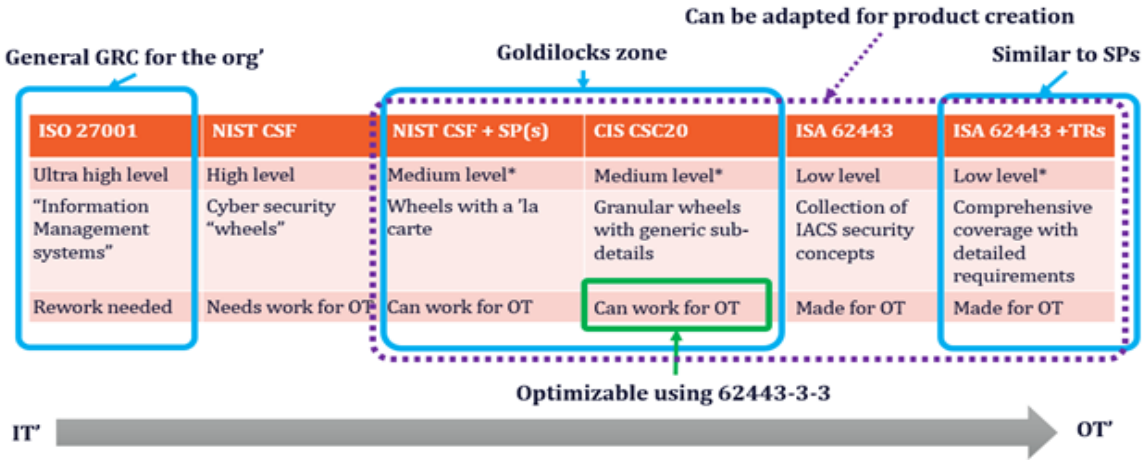
Cette norme inspirée de la sécurité fonctionnelle tient compte des spécificités propres à la cybersécurité et couvre un ensemble très large de circonstances possibles et une diversité d'équipements matériels ou logiciels susceptibles d'être porteurs de vulnérabilités. Il existe, en outre, des difficultés inhérentes au secteur pour identifier et « probabiliser » de façon objective les risques dans un contexte d'évolutivité permanente des situations et de diversité des conséquences possibles de la réalisation d'une menace. La norme IEC 62443

[275] *Who Needs our Cybersecurity Test Solution?* [En ligne] [Réf. 2021]. Disponible sur https://www.allion.com/test-lab/security-lab/
[276] *IEC 62443, le standard incontournable de la cybersécurité industrielle par Vincent NICAISE* [En ligne] [Réf. 15 avril 2021]. Disponible sur IEC 62443, un standard en cybersécurité industrielle | Stormshield

est composée d'un ensemble de 14 documents structurés en 4 niveaux, elle couvre et distingue les aspects organisationnels et les aspects techniques.

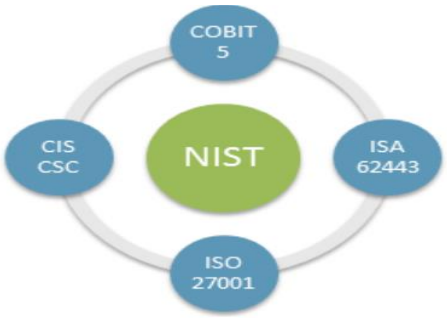
VI.2.2. SYNTHESE COMPARATIVE DES NORMES

Comme le montre le schéma ci-dessous, les règles de la norme IEC 62443 correspondent peu ou prou à d'autres directives bien connues telles que celles du NIST CSF, et recouvrent sur les thématiques IT celles de l'ISO27001. On dénote quand même quelques différences substantielles qui nécessitent parfois une adaptation pour gérer les spécificités dans un environnement OT/IT convergé. La norme commune IS027001 est très prescriptive et très orientée processus et l'informatique. La directive NIST CSF et son supplément OT (NIST-SP800-82) non prescriptifs s'adaptent au monde OT. L'IEC 62443 facilite l'identification des lacunes, des besoins et des améliorations potentielles à apporter dans les programmes existants. Elle permet de tenir compte de l'impact de la numérisation sur la sécurité des processus et protocoles mécaniques traditionnels, notamment des domaines tels que la reprise après sinistre[277].



49 - Comparaison des normes et des lignes directrices avec la norme CEI 62443 (Source Verve Industrial)

Sa version 2.0 publiée en juillet 2021 compatible NIST CSF (NIST Cybersecurity Framework) est parfaitement adaptée au ferroviaire. Elle intègre nativement les spécificités de IT/OT, SCADA, ICS, IoT, IIoT etc[278]. Rappelons que NIST CSF est un cadre volontaire initialement conçu pour les infrastructures critiques[279] et est essentiellement une auto-évaluation réalisée par l'organisation concernée. En l'absence d'une autorité de contrôle, aucune garantie de la



50 - Le Framework NIST CSF

[277] *This comprehensive collection of standards is laser-focused on industrial controls. Here's how to make the most of them*. [En ligne] [Réf. Du 23 juin 2021]. Disponible sur The Ultimate Guide to Protecting OT Systems with IEC 62443 - Verve Industrial
[278] *A Timeline of Frameworks for Cybersecurity and Compliance* [En ligne] [Réf.Du 29 avril 2021]. Disponible sur A Timeline of Frameworks for Cybersecurity and Compliance - Security Boulevard
[279] *Framework for Improving Critical Infrastructure Cybersecurity – NIST* [En ligne] [Réf. Du 16 avril 2018]. Disponible sur Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)

bonne application du framework au sein de l'entreprise ne peut être apportée[280].

VI.3. TYPOLOGIE DES MENACES DANS LE SECTEUR FERROVIAIRE

Les cyberattaques contre les chemins de fer et autres infrastructures de transport ne sont plus des scénarios hypothétiques. Les principaux chemins de fer aux États-Unis, en Europe et en Asie ont déjà été touchés par au moins une cyberattaque. La combinaison de vulnérabilités et d'impacts potentiels désastreux, d'impacts économiques, voire de pertes de vies humaines, fait des chemins de fer du monde entier les cibles idéales à la fois pour les groupes criminels motivés par l'appât du gain (cybercriminalité, apparentée au Droit Commun), mais aussi des acteurs malveillants poussés par des motivations à visée de déstabilisation (terrorisme, hacktivisme, étatique).

Au cours des dernières années, plusieurs entreprises du secteur ferroviaire ont été la cible de cyberattaques. Des entreprises européennes comme Stadler, le fabricant de matériel roulant suisse, ainsi que Adif, le gestionnaire d'infrastructure ferroviaire espagnol, ont subi des compromissions, notamment des compromissions de données avec demandes de rançon[281]. Le gestionnaire de l'infrastructure ferroviaire espagnole Adif a fait l'objet aussi d'un chantage d'un cyberattaquant qui aurait menacé de divulguer 800 Go de données. Selon le Dr Jesus Molina de Waterfall Security Solutions, si les cybercriminels se rendent compte que la perte de données n'est pas suffisamment dissuasive pour que les entreprises paient des rançons, les attaques s'intensifieront, touchant probablement les systèmes de technologie opérationnelle (OT) par exemple par l'entremise du spear phishing utilisé pour accéder aux réseaux informatiques des entreprises afin de prendre éventuellement le contrôle de leur système OT, tandis que les ransomwares de base sont utilisés pour chiffrer les données[282].

On peut regrouper les attaques qui ciblent le secteur ferroviaire en quatre catégories :

- Attaques involontaires ou accidentelles souvent liées à des bugs ou des erreurs opératoires ;
- Attaques intentionnelles avec des moyens simples, peu de ressources, des compétences de base et une faible motivation ;
- Attaques intentionnelles avec des moyens avancés, des ressources moyennes, des compétences génériques ou peu spécifiques au système et une motivation limitée, ces attaques touchent généralement les systèmes et/ou l'infrastructure, au moyen d'actes malveillants dans le but de voler, de modifier ou de détruire une cible spécifiée ; cas de la cyberattaque ayant paralysé le système ferroviaire iranien en juillet 2021[283]
- Attaques intentionnelles avec des moyens avancés, des ressources supérieures à la moyenne, des compétences spécifiques au système et une forte motivation ; Il s'agit ici d'actions offensives intentionnelles potentiellement à grande échelle et qui visent à obtenir un maximum d'impact, de perturbation, de destruction, d'altération, de vol ou d'accès non autorisé à des actifs tel que l'infrastructure, le matériel ou les connexions TIC avec une forte exposition médiatique. Ce fut le cas de la cyberattaque perpétrée par des hacktivistes non étatiques biélorusses en janvier 2021, pour mettre la pression sur le gouvernement Biélorusse. Avec pour revendications, la libération de 50

[280] *Cybersécurité, Framework, Les Assises, NIST, NIST CSF, NIST Cybersecurity Framework, risques* [En ligne] [Réf. Du 4 octobre 2018]. Disponible sur Qu'est-ce que le NIST Cybersecurity Framework 1.1 et comment l'aborder ? (beijaflore.com)
[281] Is cybersecurity in rail more important now than ever? [En ligne] [Réf. 29 avril 2021]. Disponible sur Is cybersecurity in rail more important now than ever? (railway-technology.com)
[282] *Cybersecurity in rail: three lessons we learnt from the IRS webinar* [En ligne] [Réf. Du 24 aout 2020]. Disponible sur https://www.railway-technology.com/features/cybersecurity-rail-three-lessons-irs-webinar/
[283] *Cyberattaque en Iran : les attaquants ont utilisé un logiciel malveillant destructeur de données* [En ligne] [Réf. Du 30 juillet 2021]. Disponible sur https://www.zdnet.fr/actualites/cyberattaque-en-iran-les-attaquants-ont-utilise-un-logiciel-malveillant-destructeur-de-donnees-39926907.htm

prisonniers politiques détenus suite aux manifestations du pays contre le dictateur Alexandre Loukachenko, ainsi qu'un engagement des chemins de fer biélorusses à ne pas transporter de troupes russes alors que le Kremlin se prépare à une éventuelle invasion de l'Ukraine sur plusieurs fronts.[284]

VI.4. PROFILS DES ATTAQUANTS

Les menaces sont protéiformes et d'origines diverses. Internes, externes, étatiques, de groupes criminels, etc. Selon une enquête[285] de Verizon parue en février 2020, 30% des attaques dans le secteur industriel sont d'origine interne. Les motivations restent majoritairement financières à 68% contre 27% qui sont rattachés à l'espionnage industriel. Dans le secteur des transports ferroviaires, la grande majorité des attaques sont généralement opérées avec l'appui d'un État. Les profils sont généralement ceux listés ci-dessous :

- **Employés insatisfaits ou autres attaquants internes** (potentiellement recrutés à cet effet) : cela représente la majorité des cyberattaques de l'intérieur jusqu'en 2001 malgré l'augmentation de l'activité des attaquants externes. La menace peut être beaucoup plus importante, car les attaquants internes n'ont aucune barrière pour passer et peuvent rester invisibles plus longtemps, puisque leurs accès aux systèmes sont légitimes. Dans ce contexte, le principe de protection périmétrique n'est pas valable et la mesure la plus utile reste l'application stricte de la politique de moindre privilège. Et comme on le verra plus loin, l'adoption du principe de Zéro Trust Network (ZTN).
- **Organisations gouvernementales ou affiliées à un État** : se trouvant hors du périmètre de l'entreprise, ces attaquants avec généralement une composante politique doivent surmonter les barrières de sécurité, ce qui nécessite une expertise appropriée, suffisamment de temps et des ressources financières et humaines en adéquation. Il faut souligner que les scénarios de conflits futurs incluent des scénarios de cyber-guerre, puisque les cyber-attaques permettent aux perpétrant de passer inaperçus et partant, d'exploiter les ambiguïtés ou lacunes du droit international ;
- **Cybercriminels** : généralement guidés par l'intention d'enrichissement, ils se focalisent la plupart du temps sur le vol d'identité et/ou de données et leur vente, ainsi que l'extorsion – par exemple par chiffrement des données ; le développement des places de marchés sur le darkweb favorise la disponibilité d'outils pour les moins criminels les moins qualifiés techniquement.
- **Cyber-terroristes** : l'échange accru entre les cybercriminels et les cyber-terroristes, appelé Crime-Terror-Nexus, favorise le développement et l'acquisition de compétences, et sécurise le financement des groupes terroristes. L'Office européen de police met en garde contre la menace croissante du cyberterrorisme, éventuellement accompagné par des attaques terroristes conventionnelles.
- **Hacktivistes et hackers amateurs** : ces derniers n'ont généralement pas de motivation financière, mais ont par contre une bonne expertise technique pour l'acquisition ou le développement d'exploits. Ils ont souvent recours à des logiciels disponibles gratuitement pour effectuer sans compétences spécifiques des attaques largement automatisées contre des systèmes présentant des vulnérabilités communes, et peuvent causer des dommages considérables si des mesures de détection appropriées ne sont pas en place.

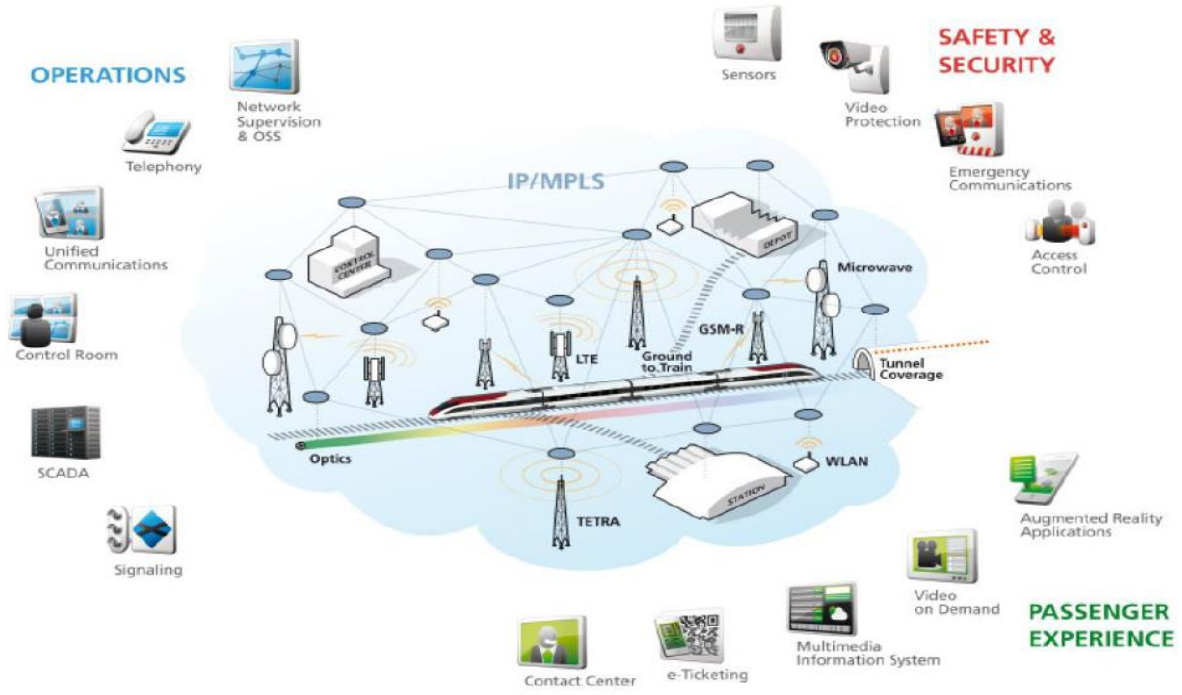
---

[284] *The politically motivated attack represents a new frontier for hacktivists—and won't be the last of its kind.* [En ligne] [Réf. Du 25 janvier 2022]. Disponible sur https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/

[285] *2019 Data Breach Investigations Report – VERIZON* [En ligne] [Réf. 2019]. Disponible sur https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

VI.5. CARTOGRAPHIE DES MENACES DE SECURITE ET CYBERSECURITE

Le transport ferroviaire se distingue par la spécificité de son éclatement géographique et comme le montre le schéma ci-dessous, par l'hétérogénéité des architectures, des composants matériels et logiciels qui concourent à la réalisation de ses missions essentielles, mais qui en augmentent par construction, l'exposition aux menaces potentielles.



51 - Schéma de l'écosystème du Transport Ferroviaire (source CYRail) [286]

Les grands challenges concernant la sécurité découlent de l'introduction des échanges TCP/IP dans les écosystèmes de signalisation, d'aiguillage et de la distribution de l'électricité, utilisés dans le réseau ferroviaire. Ces extensions du réseau IP sont poussées par les demandes croissantes des clients, engendrant la nécessité de remplacer les systèmes existants par des infrastructures plus modernes et standardisées, afin d'améliorer la fiabilité, l'efficacité, la capacité et l'expérience client.

Tant que l'industrie ferroviaire demeurait avec ses systèmes électriques et une signalisation par relais, le problème des menaces cyber ne se posait pas. L'introduction des formes numériques de transmission de données et des commandes à distance à partir de l'ordinateur d'un technicien via un modem annonçait fin des années 90 l'arrivée de nouvelles menaces. Historiquement, une cybersécurité spécifique à l'OT n'était pas considérée comme nécessaire, puisque les systèmes OT n'étaient pas connectés à Internet. Ils n'étaient donc pas exposés aux menaces externes. De plus, la généralisation des accès aux réseaux OT par des fournisseurs tiers distants a étendu la surface d'attaque, et a créé de nouvelles vulnérabilités[287] et a fait naitre de nouvelles menaces. Ces dernières ne sont

[286] *CYbersecurity in the RAILway sector – CYRAIL.EU* [En ligne] [Réf. Du 30 septembre 2018]. Disponible sur D6.1-Introduction.docx

[287] Fortinet, *Technologies industrielles (OT) ? Les technologies OT consistent à tirer parti de matériels et de logiciels pour contrôler les processus, dispositifs et infrastructures physiques*. [En ligne]. [Réf. 2021]. Disponible sur https://www.fortinet.com/fr/solutions/industries/scada-industrial-control-systems/what-is-ot-security

plus considérées comme conceptuelles. D'après le rapport de Fortinet[288], 9 organisations sur 10 du secteur industriel (parmi lesquels des leaders) ont été confrontées à des intrusions des systèmes OT. 65% d'entre elles ont été classées avec un niveau minimum de 3. Même si la plupart les impacts n'ont pas été considérés comme graves, l'extrême vigilance est de mise.

Concernant la sécurité des assets du transport ferroviaire, trois points essentiels sont à noter :

- Les actifs des transports ferroviaires dits intelligents sont soumis à un large éventail de menaces pouvant affecter leur sécurité : lorsque les actifs deviennent des hybrides cyber-physiques, ils deviennent vulnérables à la fois aux cyberattaques et aux attaques physiques.
- La cybersécurité et la sûreté physique ne peuvent plus être traitées comme des préoccupations distinctes et décorrélées : lorsque les attaquants peuvent affecter le fonctionnement physique de trains compatibles avec les TIC ou d'autres actifs physiques, la cybersécurité et la sûreté physique des réseaux deviennent interdépendantes, voire intriquées.
- Déterminer où s'arrêtent les responsabilités d'un opérateur de transport est de plus en plus complexe : le partage des actifs, des réseaux TIC et des données avec différentes parties prenantes dans les sous-traitances et les mandatures temporaires, floute les frontières des responsabilités en cas d'accident et partant, en rend difficile les attributions.

L'ANSSI, dans son Annexe A du Guide de la cybersécurité des systèmes industriels[289], énumère les vulnérabilités les plus fréquemment rencontrées dans le monde industriel en général. Ces vulnérabilités souvent liées concernent principalement :

- Les défauts de l'architecture, un manque de plan de résilience et de cartographie du SI ;
- Le déficit de mesures techniques préventives relativement aux politiques de mots de passe, aux droits et aux privilèges, au partage de fichiers, à la prise en main à distance, aux protocoles non sécurisés ;
- Le défaut de Maintien de la Condition de Sécurité (dans la durée) : manque de plans de sauvegarde de données, d'une gestion de configuration efficace, de mises à jour, et de signature des firmwares.

Les grandes menaces pouvant occasionner des impacts majeurs concernent principalement deux grands niveaux, la couche de contrôle et commande du réseau, c'est-à-dire la tour de contrôle qui vérifie tout le trafic ferroviaire, l'emplacement des trains, les itinéraires ; et la couche opérationnelle avec les systèmes de signalisation et d'aiguillage. Ces menaces peuvent avoir comme impacts : une perturbation du trafic, la mise en danger de vies humaines, l'atteinte à la réputation ou des pertes d'informations financières ou de données personnelles, sachant que ces impacts peuvent être cumulatifs.

VI.5.1. MENACES SUR LE SYSTÈME DE DISTRIBUTION ÉLECTRIQUE

Le contrôle de la distribution électrique s'opère de plus en plus à partir de serveurs distants dont certains utilisent des accès via TCP/IP. Des boîtiers électroniques embarqués dans les engins, qui permettent d'enregistrer la consommation électrique des entreprises

[288] *2020 State of Operational Technology and Cybersecurity Report – FORTINET* [En ligne]. [Réf. Du 13 avril 2021]. Disponible sur https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf
[289] *Maîtriser la SSI pour les systèmes industriels* [En ligne] [Réf. De juin 2012]. Disponible sur Guide_securite_industrielle_Version_finale-2.pdf (ssi.gouv.fr)

ferroviaires utilisant les réseaux ferrés en vue de leur facturation, possèdent par exemple des interfaces IP.

Dans un avenir proche, les barres de *shuntage*, qui permettent de détecter la présence d'un train sur les voies grâce au passage d'un léger courant et donc permettant de simuler la présence d'un train pour bloquer la circulation si nécessaire, pourraient être automatisées.

La simple utilisation des protocoles ouverts de type TCP/IP en fait aussi de potentielles cibles de menaces. La paralysie même sur une courte durée du réseau de distribution électrique peut générer une désorganisation et des pertes financières considérables.

VI.5.2. MENACES SUR LES SYSTÈMES DE CONTRÔLE INDUSTRIEL (SCI/ICS)

Les attaques malveillantes contre les ICS, les systèmes de contrôle de supervision et d'acquisition de données (SCADA) ont considérablement augmenté ces dernières années. IBM a estimé que les attaques sur ICS ont augmenté de 600 % entre 2012 et 2014. Selon Dell, dans son rapport annuel de 2015, les attaques sur les systèmes de type SCADA ont été multipliées par plus de 7 sur la même période [290].

Selon le rapport de Kaspersky ICS CERT, sur presque tous les appareils des ICS, des objets malveillants ont été détectés. L'étude 2019 de Kaspersky ICS CERT sur les menaces affectant les systèmes de contrôle industriels (SCI) met en évidence 103 nouvelles vulnérabilités trouvées en 2019 qui pourraient être exploitées par des cyberattaques[291]. Le nombre de vulnérabilités identifiées a quasiment doublé par rapport aux 61 signalées en 2018.

Les défaillances sur les fonctionnalités critiques peuvent avoir des impacts significatifs. Elles font partie des grands risques ferroviaires (déraillements par survitesse, collisions, etc.)[292]. Pour les systèmes de Contrôle et Commande de la Signalisation et/ou de l'aiguillage, quelques cyberattaques se sont révélées être liées aux vulnérabilités des systèmes SCADA[293]. Ces vulnérabilités représentent de potentielles cibles de cyberattaques. Les statistiques de Kapersky ICS CERT de 2020 puis 2021 confirment les tendances soutenues des attaques vers les systèmes industriels. Avec en 2020 une augmentation de 62% d'attaques d'ordinateurs reliés à des systèmes industriels et 32% de plus de malwares bloqués par rapport à 2019[294]. Généralement avec comme source Internet, les périphériques amovibles (type clé usb, disque externe, etc.), emails clients (phishing, ransomware,etc.) , logiciels espions (chevaux de Troie, portes dérobées et enregistreurs de frappe), Crypto Mineurs fichiers exécutables pour Windows[295].

---

[290] Cybersecurity: guarding rail against evolving threats [En ligne]. [Réf. Du 15 avril 2018]. Disponible sur Cybersécurité : se prémunir contre l'évolution des menaces | International Railway Journal (railjournal.com)

[291] Kapersky ICS CERT - *Panorama des menaces pour les systèmes d'automatisation industrielle. Vulnérabilités identifiées en 2019* [En ligne]. [Réf. D'avril 2020]. Disponible sur https://ics-cert.kaspersky.com/publications/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-vulnerabilities-identified-in-2019/ ou https://ics-cert.kaspersky.com/media/KASPERSKY_H22019_ICS_REPORT_FINAL_EN.pdf

[292] *La signalisation Ferroviaire par Roger RETIVEAU* – Ecole Nationale des Ponts et Chaussée [En ligne]. [Réf. 1987]. Disponible sur La Signalisation Ferroviaire (lafibre.info)

[293] *Fiches Incidents Cyber SI Industriels – CLUSIF* [En ligne]. [Réf. D'avril 2017]. Disponible sur clusif-2017-fiches-incidents-scada_vf.pdf

[294] Kapersky ICS CERT - *Threat landscape for industrial automation systems. Statistics for H2 2020* [En ligne]. [Réf. de mars 2021]. Disponible sur https://ics-cert.kaspersky.com/publications/reports/2021/03/25/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/

[295]Kapersky ICS CERT - *Threat landscape for industrial automation systems. Statistics for H2 2021* [En ligne]. [Réf. de mars 2022]. Disponible sur https://ics-cert.kaspersky.com/publications/reports/2022/03/03/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2021/ ou https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Threat-landscape-for-industrial-automation-systems-statistics-for-H2-2021-En.pdf

Les dix principales menaces de cybersécurité pesant sur les systèmes de contrôle industriels (ICS)[296] suite à la convergence avec les systèmes IT sont :

- L'infiltration de logiciels malveillants via des supports amovibles et du matériel externe ;
- L'infection par des logiciels malveillants via Internet et intranet ;
- L'erreur humaine et le sabotage ;
- La compromission des composants extranet et cloud ;
- L'ingénierie sociale et l'hameçonnage ;
- Les attaques DDoS (Deni de Service Distribué) ;
- La prise de contrôle des composants connectés à Internet ;
- L'intrusion via des accès distants ;
- Le dysfonctionnement technique de force majeure ;
- La compromission des smartphones dans l'environnement de production.

VI.5.3. MENACES LIÉES À L'ERTMS

Les menaces autour de l'ERTMS reposent essentiellement sur les deux composantes principales à savoir le système de signalisation ETCS et le système de communication GSM-R.

Les risques vont s'accroître sur le système ERTMS (ETCS 1, ETCS 2 et ETCS 3 en expérimentation au fur et à mesure de son déploiement au sein des systèmes nationaux existants. L'arrivée prévue du système FRMCS (Future Railway Mobile Communication System), successeur du système de communication GSM-R, requiert des normes et des procédures de cybersécurité hautement intégrées et complètes. Il en est de même du besoin croissant de télémaintenance, cette dernière pouvant être opérée par des prestataires tiers.

VI.5.4. MENACES PESANT SUR LE SYSTÈME DE SIGNALISATION ETCS

Les menaces pesant sur le système de signalisation ETCS (même à partir du niveau 1) restent à des niveaux faibles en raison du très haut niveau de technicité, une motivation et des efforts assez conséquents pour pouvoir exploiter une faille. Les normes européennes, notamment EN50128, EN50129 ainsi que les exigences de niveau d'intégrité de sécurité 4 (SIL4) sur lesquelles ont été développés les systèmes ETCS lui confèrent un niveau de sécurité élevé. Une analyse récente du groupe de travail WG CYSIS (sous-groupe : ETCS et sécurité) indique qu'au regard des fonctions de sécurité mises en œuvre dans le système ETCS, la réussite d'une attaque sur les balises est très peu probable, à condition que ces mesures de protection soient implémentées bien entendu.

VI.5.5. MENACES SUR LES ÉCHANGES ENTRE BALISES ET LE GSM-R

Les communications via GSM-R respectent l'état de l'art conformément au Subset 037[297]. D'après des experts en cybersécurité industrielle (voir Annexes I - Interviews (JBR, Alstom, YGR & QRE de SNCF)), compromettre les échanges effectués entre les balises KVB par exemple, et l'antenne engin moteur est évalué comme ardu, compte tenu de la courte durée de l'activation de la balise. En effet les balises analogiques ou numériques, inertes par nature, sont activées lors du passage du train par l'énergie électromagnétique émise par l'antenne de l'engin moteur. La balise émet par rayonnement (radius) des messages codés, qui seront captés par l'antenne de l'engin moteur. Des interrogations

[296] *IT/ OT-Security for Internet of Railway Things (IoRT)* [En ligne]. [Réf. Du 18 janvier 2021]. Disponible sur Cyber Security for Railways - ETCS Aspekte (haselnuss-projekt.de)
[297] *Moving Europe towards a sustainable and safe railway system without frontiers.- ERA* [En ligne]. [Réf. 2021]. Disponible sur Set of specifications 3 (ETCS B3 R2 GSM-R B1) | ERA (europa.eu)

sur les menaces sur les systèmes de communications sont tout à fait légitimes. Le risque est faible. Les communications sont chiffrées avec des clés asymétriques ; les attaques de l'homme du milieu (Man In The Middle / MtoM) sont possibles à condition que des clés symétriques soient utilisées, exfiltrées simultanément, et disposer des capacités de déchiffrement de la communication. Cela nécessite des moyens très conséquents, restreints à des attaquants de type étatiques ou péris étatiques. Bien qu'infime, la probabilité d'une compromission est donc à considérer dans les analyses de risques.

VI.5.6. MENACES LIÉES AUX OBJETS CONNECTES IOT/IIOT ET AU PROTOCOLE MODBUS

L'Internet des Objets (IoT) est un accélérateur de la convergence IT-OT en raison du besoin de collecte massive de données qui sont rendues possibles par l'IoT. Un rapport de 2018 d'IBM rappelle que la sécurité des objets connectés (IoT) restait limitée, voire inexistante, et que les industries attirées par l'IIoT (Industrial Internet Of Things) devaient développer de nouvelles stratégies pour gérer et atténuer les cyber-risques induits. Le danger est induit de la rapidité avec laquelle les industriels déploient les IIoT, avec un rythme largement plus soutenu que leur sécurisation. Ceci favorise la prolifération incontrôlée de systèmes non sécurisables et donc, de failles de sécurité, et transforme l'OT en une cible facile à atteindre et à compromettre. Cette catégorie représenterait aujourd'hui 30 % des cibles des cyberattaques.

Comme les systèmes SCADA, la plupart des capteurs déjà existants dans l'industrie utilisent le protocole, série ModBus. D'autres capteurs utilisent SNMP ou bien collectent des données via des API's. ModBus est basé sur le protocole série RS485[298]. Une vigilance est apportée sur ce protocole en raison de quelques vulnérabilités connues,[299] dont la possibilité d'atteinte à l'intégrité des données traitées. Il n'existerait à ce jour aucun mécanisme de sécurité pour ce protocole[300].

VI.5.7. MENACES LIÉES AUX NOUVEAUX USAGES DE TÉLÉDIAGNOSTICS ET TÉLÉMAINTENANCE

De nouvelles fonctionnalités ont apporté des ruptures dans la manière d'opérer la maintenance, la collecte des défauts et les pannes sur les équipements électroniques ; la télémaintenance peut désormais se faire à distance sans besoin d'intervention du personnel sur le terrain. Cela facilite l'anticipation des réparations et évite ou réduit le temps d'immobilisation du train pour des motifs de maintenance, avec l'avantage non négligeable d'augmenter très sensiblement la disponibilité de ce dernier. Initialement « descendante » pour assurer des fonctions essentiellement liées à la maintenance, la communication train/sol est devenue progressivement « montante » pour charger des contenus à bord comme des bases de données sonores et visuelles pour l'information voyageur, ou même pour activer des services destinés à des fonctions de pilotage comme la téléconduite ou les trains autonomes[301]. Cette communication montante peu s'avérer être un vecteur de compromission potentielle.

---

[298] *Les enjeux de la supervision IOT (Internet of Things)* [En ligne]. [Réf. Du 5 février 2019]. Disponible sur Les enjeux de la supervision IOT (Internet of Things) - Syloe

[299] CERT.FR [En ligne]. [Réf. Du 11 avril 2019]. Disponible sur SCADA Vulnérabilité dans Schneider Electric Modbus Serial Driver – CERT-FR (ssi.gouv.fr)

[300] *Le protocole Modbus* [En ligne]. [Réf. 17 oct. 2017]. Disponible sur Fun with Modbus 0x5A (riskinsight-wavestone.com)

[301] *Architecte général Contrôle/Commande et Systèmes d'Information Alstom* [En ligne]. [Réf. Du 10 octobre 2020]. Disponible sur Le contrôle/commande ferroviaire : Dossier complet | Techniques de l'Ingénieur (techniques-ingenieur.fr)

VI.5.8. MENACES LIÉES AU CLOUD

La technologie Cloud est omniprésente et affiche de nombreux avantages. Son usage de plus en plus important par les entreprises met les DSI au-devant de challenges et de problématiques en matière de risques de sécurité. Le cloud est la cible par excellence des attaquants, qui y trouvent aujourd'hui toutes les solutions et les ressources nécessaires leur permettant sans grande compétence de déployer des cyberattaques et cela, quelle que soit la cible. Les principaux services de Cloud computing, d'infrastructure en tant que service (IAAS), de plate-forme en tant que service (PAAS) et le software en tant que service (SAAS), offrent aux attaquants des surfaces d'attaque sans précédent.

Bien que de plus en plus sécurisées, toutes les solutions restent quand même vulnérables surtout quand on sait le penchant de certaines DSI à vouloir bénéficier rapidement des avantages du cloud sans une réflexion préalable et minutieuse des risques. Une évaluation mesurée de l'attrait des grandes capacités et flexibilité qu'offrent le cloud et le besoin du time-to-market en regard des risques sécuritaires potentiels encourus et qui peuvent être désastreux.

Selon un sondage mené auprès de 241 experts industriels, 11 nouvelles menaces et vulnérabilités pour les environnements Cloud[302] ont été révélées à savoir : les fuites de données, le contrôle insuffisant des identifiants d'accès, l'absence de stratégie de sécurité, les menaces internes, le piratage de compte, les APIs et UI mal sécurisées, la mauvaise configuration, une visibilité insuffisante de l'usage des services Cloud rendant le contrôle opaque et la sécurisation difficile, l'utilisation des ressources Cloud par des personnes malveillantes à des fins de cyberattaque.

VI.5.9. MENACES LIÉES A L'INTELLIGENCE ARTIFICIELLE

Les besoins actuels et ceux du futur, pour être satisfaits, ont recours à l'IA en raison de ses multiples possibilités et avantages : c'est un accélérateur de la prise de décision, de la conception et la mise en œuvre de solutions innovantes).

Le carburant de l'Intelligence Artificielle (IA) est principalement constitué de données (et même d'un volume colossal de données), d'algorithmes capables d'apprendre de ces données pour aider à la prise de décision, et d'une puissance de calcul afin d'effectuer les traitements. Ces éléments sont des vecteurs d'attaques.

Il est possible de porter atteinte à l'intégrité des données d'entraînement pour modifier in fine le comportement de l'IA ou l'identification de failles dans les algorithmes. L'interférence sur le périmètre et les objectifs fixés d'une IA permettent des exploitations malveillantes (on peut citer, par exemple, le détournement des chatbots, potentielle prise de contrôle des véhicules autonomes).[303]

Dans le monde ferroviaire, la préoccupation première est de garantir à tout moment, quelles que soient les conditions, une sûreté de fonctionnement et une sécurité. Les techniques d'apprentissage de l'IA sont par construction, sensibles aux variations de données. Le risque d'une prise de décisions ou d'actions erronées, car biaisées par un jeu de données d'entraînement non intègres peut conduire au chaos (une perte de contrôle d'un véhicule autonome avec atteinte aux vies humaines par exemple est tout à fait plausible). En raison de l'indéterminisme qui la caractérise, comment l'IA peut garantir que des successions de variations de données malveillantes potentiellement indétectables n'induisent pas des résultats aberrants (par analogie, on peut penser aux effets

[302] *Cloud : quelles sont les principales menaces et comment s'en protéger* [En ligne]. [Réf. Du 23 aout 2019]. Disponible sur Cloud : quelles sont les principales menaces et comment s'en protéger (lebigdata.fr)
[303] SIDO 2019 : À la croisée de l'IoT, de la robotique et de l'intelligence artificielle [En ligne]. [Réf. Du 10 avril 2019]. Disponible sur SIDO 2019 : A la croisée de l'IoT, de la robotique et de l'intelligence artificielle - DigitalCorner (digitalcorner-wavestone.com)

« négligeables » d'un ajout de pixel dans des images, etc.). En effet, on sait déjà que même sans attaque cyber, c'est-à-dire sans intrusion dans les systèmes informatiques, on pourra tromper le système en fournissant aux capteurs de fausses données extérieures (lidar jamming/ brouilleur de radar par exemple). Le composant continuera à fonctionner comme prévu, mais avec des données d'entrée erronées et des réponses en conséquence[304] correctes par rapport aux données entrées, mais non fiables.

VI.5.10. MENACES LIÉES AU WIFI

De plus en plus de dispositifs électroniques nécessitent une connexion sans fil telle que le Wi-Fi. Les principales catégories de menaces sont les points d'accès Evil Twin (hotspot sans fil malveillant qui se fait passer pour un hotspot légitime)[305] et les point d'accès mal configurés, etc.

VI.5.11. MENACES SPÉCIFIQUES LIÉES A LA 5G

L'arrivée de la 5G permet de nouveaux usages ainsi que de nouveaux services numériques. Grâce à la 5G, on assiste au développement de nouvelles technologies et innovations avec l'accélération des IIoT (Industrial Internet Of Things), le déploiement de villes intelligente et d'industrie connectées dites industries 4.0. Ces possibilités permettent la gestion en temps réel des infrastructures, des procédures de travail ou encore des plannings des équipes.

Les cybercriminels y voient surtout de nouvelles opportunités de cyberattaques. En effet, la 5G est identifiée comme une future menace à prendre en compte par la plupart des institutions et des entreprises, les experts en cybersécurité convergent sur ce point. Par exemple, la 5G ne propose aucun chiffrement dans sa phase de connexion. Cette fenêtre non chiffrée peut être exploitée par un cybercriminel. Des scénarios d'attaques par l'homme du milieu (Man in the Middle / MitM) et par déni de service se sont révélés concluants et ont montré qu'il est vital d'assurer une protection complète des réseaux 5G[306].

VI.5.12. MENACES DE LA CHAINE D'APPROVISIONNEMENT

La gestion de la chaîne d'approvisionnement ou logistique (Supply Chain en Anglais) est une des formes organisationnelles et opérationnelles contemporaines les plus courantes dans l'entreprise. La gestion des risques associés, désignée par l'acronyme SCRM pour Supply Chain Risk Management est de nos jours un de ses principaux enjeux. La détection et l'atténuation des menaces pesant sur la chaîne logistique contribuent à sa continuité et à sa rentabilité. 80% des responsables de la chaîne logistique considèrent ces menaces, souvent imprévisibles, comme potentiellement destructrices et demandant une vigilance permanente. Dans son livre blanc « Gestion des risques opérationnels de la Supply Chain », l'éditeur d'applications collaboratives Generix Group[307] précise : « *tous ces événements entraînent des coûts directs, indirects, une altération de l'image de l'entreprise, des pertes de clients, voire la faillite de l'entreprise, si celle-ci n'est pas capable de conserver, de bout en bout, la maîtrise opérationnelle de sa Supply Chain* »

---

[304] *ATELIER SÉCURITÉ FERROVIAIRE DU FUTUR - FONCSI* [En ligne]. [Réf. Du 23 mars 2021]. Disponible sur synthese-atelier-ferroviaire-futur (foncsi.org)

[305] *Comment détecter et se protéger des attaques Evil Twin – TITAN HQ* [En ligne]. [Réf. Du 4 mars 2019]. Disponible sur Comment détecter et se protéger des attaques Evil Twin (jumeau maléfique) (titanhq.fr)

[306] Les nouvelles vulnérabilités 5G permettent des attaques par déni de service et par l'homme du milieu – Milena DIMITROVA[En ligne]. [Réf. Du 17 décembre 2020]. Disponible sur De nouvelles vulnérabilités 5G permettent une attaque par déni de service et par l'homme du milieu- (sensorstechforum.com)

[307] Avec « GENERIX SUPPLY CHAIN HUB », Generix Group remet la Supply Chain au coeur de la stratégie d'entreprise [En ligne]. [Réf. Du 16 fevrier 2018]. Disponible sur Generix Group est un expert de la Supply Chain Collaborative

Dans le monde ferroviaire, le nombre de parties prenantes est conséquent (sociétés de fret, entreprises ferroviaires, transitaires, fournisseurs de matériels, de solutions, sous-traitants, prestataires de services, clients, douanes, services de police, organismes administratifs, divers mainteneurs …). Cette multiplicité d'acteurs de plus en plus interconnectés est un facteur de risques, notamment celui lié à la cascade de fournisseurs.

Pour Eddy Thésée[308], la Supply Chain en Cascade ne doit pas être vue comme un problème, mais un sujet de vigilance régulière et a abordé par le développement des capacités certaines sur plusieurs angles :

Angle 1 (vis-à-vis des fournisseurs) :

- Capacité des fournisseurs à pouvoir gérer leurs secrets et leur cybersécurité,
- Capacité à aligner les produits qu'ils livrent avec les exigences de cybersécurité. Ces exigences peuvent être spécifiques à un projet donné ou un produit particulier ou alors très génériques. Dans ce dernier cas, ces derniers doivent s'assurer du Maintien en Condition de Cybersécurité (MCS), et a minima fournir un bulletin de sécurité de façon régulière.

Angle 2 (vis-à-vis de l'entreprise Cliente elle-même) :

- Capacité à réagir face aux attaques cyber et à se protéger en sécurisant également les accès qu'ont certaines entreprises aux SI d'Entreprises tierces dans le cadre de la relation d'affaires entretenue avec elles.

L'anticipation des risques et la diminution des impacts par des réactions rapides ne sont possibles qu'en ayant une vision de bout en bout de la chaîne. Toute la difficulté est d'identifier de quelle manière parvenir à cette vision. Les raisons sont principalement dues à la complexité des processus, à la vitesse d'exécution attendue et à la couverture géographique des échanges.

VI.5.13. LES MENACES DANS LE DOMAINE IT

Le dernier rapport de Sophos sur les principales menaces en 2021 est formel, l'Intelligence Artificielle sera largement utilisée par les hackers pour aider les renseignements à s'attaquer aux grandes entreprises. Comme dans la plupart des entreprises, le vol des données via l'usurpation de *credentials* ou l'utilisation de l'ingénierie sociale est aussi applicable dans les systèmes IT ferroviaires. Pour les attaquants des entreprises ferroviaires, les informations clients seront très lucratives. Elles présentent intrinsèquement un fort pouvoir de chantage du fait de la législation contraignante les protégeant. Le cyber-espionnage est un autre sujet à craindre dans l'industrie ferroviaire : des contrats peuvent être perdus en raison des connaissances par le concurrent, des forces et faiblesses de l'offre d'un soumissionnaire.

Les attaques de type DDoS (Distributed Denial Of Service) ciblent généralement plusieurs vulnérabilités en parallèle sur les systèmes IT sensibles avec des origines de plus en plus difficiles à identifier[309]. Ces attaques seront tout autant préjudiciables pour les entreprises ferroviaires. C'est le cas des attaques ciblant les informations et services de conforts aux voyageurs qui peuvent rendant inopérants le bon fonctionnement des services.

Selon explique Alexander Szoenyi, « Lls attaques DDoS sur l'infrastructure réseau sont possibles, car les fournisseurs de services ferroviaires utilisent les mêmes systèmes que

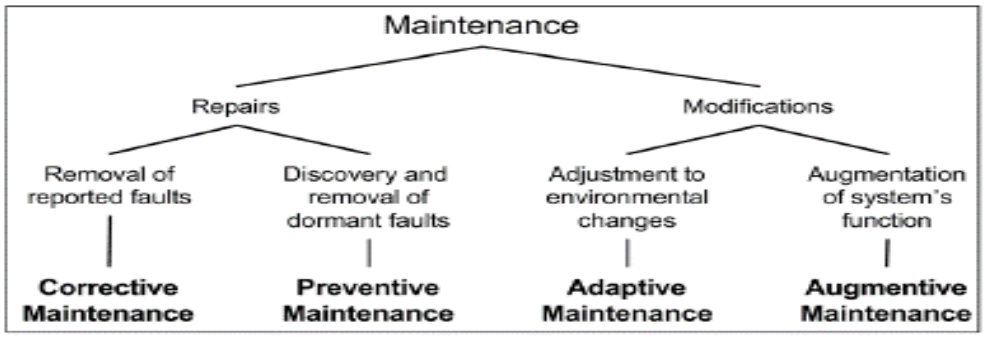
[308] Annexes I – Interview Eddy Thésée VP Cybersécurité Alstom
[309] *NETSCOUT Smart Data is hands-down the best solution for analyzing hybrid cloud environments* [En ligne]. [Réf. 2021]. Disponible sur Performance du réseau, applications et sécurité | NETSCOUT

les opérateurs de télécommunications et nous savons que certains fournisseurs ont été piratés par le passé »[310].

Pour Orange Cyber Défense, de nouvelles menaces sur l'IT doivent être anticipées dès aujourd'hui : l'informatique quantique, à plus ou moins long terme, remettra en cause le système de cryptographie[311], ce qui pourrait mettre à bas la sécurité de chiffrement implantée par exemple dans les flux de communication des interfaces IT-OT.

VI.5.14. MENACES LIÉES A LA MAINTENANCE

On distingue quatre types de maintenance : corrective, préventive, adaptative et augmentée, comme schématisé ci-dessous. Quel que soit le mode de maintenance, on a la possibilité de la réaliser sur site ou à distance. La menace exploitant ce vecteur est à prendre sérieusement en compte. On retrouve du fait de la convergence IT-OT tous les problèmes de cybersécurité précédemment évoqués.



52 - Les différentes formes de maintenance

VI.6. SCENARII DE MENACES

L'interconnexion des réseaux industriels dits OT avec les réseaux IT augmente l'exposition aux attaques cyber. Le réseau industriel aura beau avoir toutes les sécurisations nécessaires qu'exigent les normes ferroviaires, ce dernier n'est pas à l'abri d'attaque en raison des faiblesses sur le réseau traditionnel IT. Cela peut se produire par e exemple via un malware suite à une campagne de phishing ou de spear phishing[312]. Pour Alan Paller, directeur de recherche à l'Institut SANS, « *95% de toutes les attaques sur les réseaux d'entreprise sont le résultat d'un spear phishing réussi* ».[313]

L'industrie 4.0, de par sa convergence IT-OT est aujourd'hui entièrement connectée. Pour qu'elle soit efficiente et globale, l'approche de sa sécurité se doit donc d'être holistique. Cela nécessite d'être en mesure de définir la liste plus ou moins exhaustive de scénarios de menaces, ce qui devient une gageure pour un sujet aussi volatil.

En 2019, avant les challenges supplémentaires apportés par la pandémie de COVID-19, 65% des groupes d'attaque utilisaient déjà le spear-phishing comme premier vecteur d'infection[314]. La crise sanitaire et le bouleversement dans les habitudes de travail ont fait augmenter ce pourcentage. La généralisation du télétravail a fait entrer la tendance du

---

[310] Thales, Cybersecurity Authority,

[311] *Cybersécurité : quelles sont les principales menaces en 2021 ?* [En ligne]. [Réf. Du 12 décembre 2021]. Disponible sur Cybersécurité : quelles sont les principales menaces en 2021 ? (orange.fr)

[312] Le spear phishing est une méthode d'hameçonnage qui cible des individus ou des groupes spécifiques au sein d'une organisation par des techniques d'ingénierie sociale.

[313] *Améliorer vos campagnes de sensibilisation à la sécurité* [En ligne]. [Réf. Du 14 juin 2015]. Disponible sur Improving Your Security Awareness Campaigns With Behavioral Science (securityintelligence.com)

[314] *Spear Phishing vs. Phishing : tout ce que vous devez savoir* [En ligne]. [Réf. Du 7 janvier 2021]. Disponible sur Spear Phishing vs Phishing | Terranova Security

BYOD (Bring Your Own Device)[315] et la pratique du Shadow IT (installation et utilisation de logiciels non validés par les DSI). Afin de faciliter l'usage du matériel personnel, les services informatiques ont parfois opté pour l'élévation des privilèges des comptes utilisateurs afin de leur faciliter l'accès aux ressources de l'entreprise, permettant alors aux collaborateurs dans certains contextes d'avoir les droits nécessaires pour installer par eux-mêmes des logiciels non autorisés sur les assets de l'entreprise.

D'autres vecteurs de menaces recouvrent les systèmes de contrôle d'automatisation de certaines opérations ferroviaires intégrant des composantes IT comme le couplage automatique des rames en gare, l'arrivée et le départ automatique des trains en station, l'acheminement des trains du dépôt en station, la gestion des triages.

Le dernier rapport de l'ENISA en date du 25 novembre 2021, présente plusieurs scénarios[316] de cyber-risque dans le domaine ferroviaire, facilitant les analyses des risques dans la filière ferroviaire. Ces scénarios sont issus des ateliers avec différents acteurs du secteur ferroviaire. Ce sont 24 experts (principalement des Entreprises Ferroviaires et des Gestionnaires d'Infrastructure) d'Allemagne, de Belgique, d'Espagne, de France, d'Italie, du Luxembourg, de Norvège, des Pays-Bas, du Portugal et de Suède, de l'ER-ISAC et du groupe de travail sur la cybersécurité de l'UNIFE. Les sept scénarios ci-dessous ont été identifiés (:

- ***Scénario 1*** : compromission d'un système de signalisation ou un système de contrôle automatique des trains, entraînant un accident de train ;
- ***Scénario 2 :*** *s*abotage des systèmes de supervision du trafic, entraînant l'arrêt de la circulation des trains ;
- ***Scénario 3*** : attaque par ransomware, entraînant une perturbation de l'activité ;
- ***Scénario 4*** **:** vol des données personnelles des clients dans le système de gestion des réservations ;
- ***Scénario 5*** : fuite de données sensibles due à une base de données non sécurisée et exposée ;
- ***Scénario 6*** : attaque par déni de service distribué (DDoS), empêchant l'achat de billets ;
- ***Scénario 7*** : un événement désastreux détruit le centre de données, entraînant l'interruption des services informatiques.

Vous trouverez les détails des scénarios en Annexes II – Scénarios d'attaque identifiés par l'ENISA)

VI.6.1. EXEMPLE DE SCÉNARII STRATÉGIQUES AFFECTANT LA SÉCURITÉ FERROVIAIRE

Les scénarios décrits ci-dessous sont essentiellement tirés du document *Maîtrise des risques lies aux aspects de cybersécurité et sécurité ferroviaire*[317]

Le chemin d'attaque présenté ci-dessous utilise comme point d'entrée les analyses de sécurité ferroviaire généralement considérées comme exhaustives et les prolonge en identifiant tous les différents états du système à même de provoquer une situation

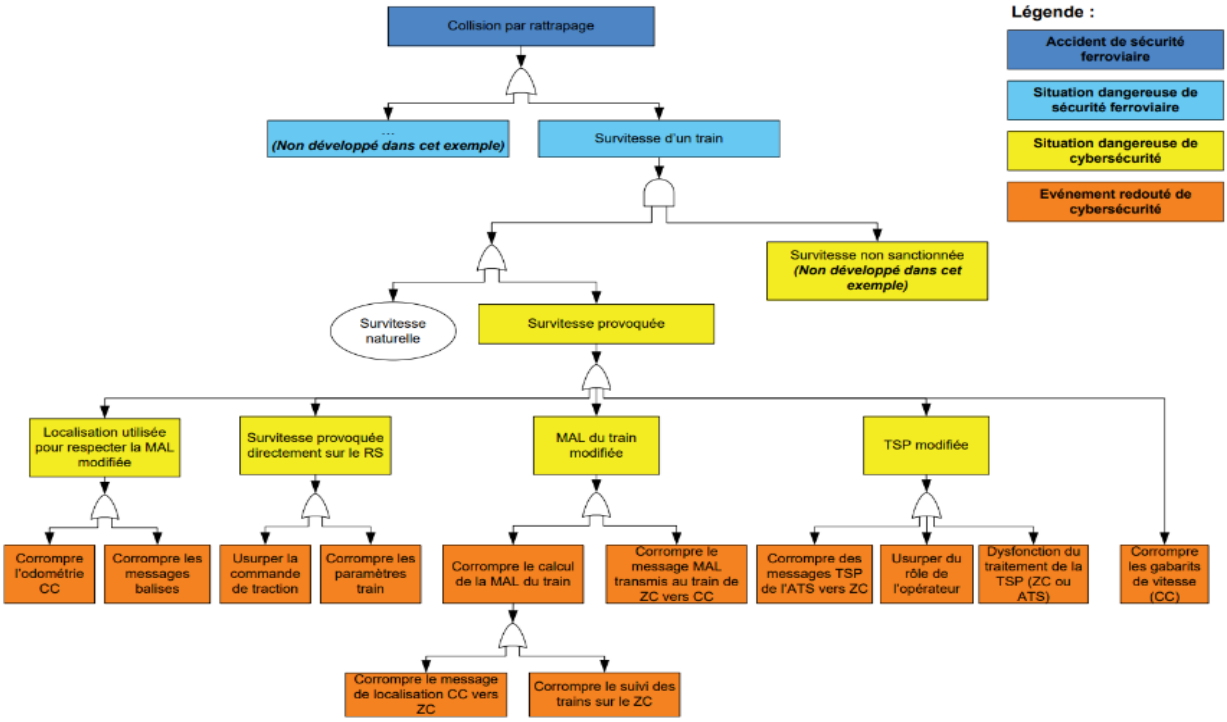
[315] Bring Your Own Device, « apportez votre équipement personnel de communication », est une pratique qui consiste à utiliser ses équipements personnels dans un contexte professionnel

[316] Good Practices in Cyber Risk Management [En ligne]. [Réf. Du 25 novembre 2021]. Disponible sur Risk Management: Helping the EU Railways Catch the Cybersecurity Train — ENISA

[317] - Joanna Peres, Jean Caire, Véronique Delebarre. *Maîtrise des risques lies aux aspects de cybersécurité et sécurité ferroviaire* [En ligne]. [Réf. Du 20 mars 2019]. Disponible sur MAITRISE DES RISQUES LIES AUX ASPECTS DE CYBERSECURITE ET SECURITE FERROVIAIRE (archives-ouvertes.fr)

dangereuse de sécurité ferroviaire. On part du postulat qu'il existe toujours un principe systématique de dysfonction de la sécurité causée par une quelconque compromission d'un composant IT de la chaîne industrielle. Le pirate provoque cette situation et court-circuite la protection qui permet du point de vue de la sécurité ferroviaire de garantir l'atteinte d'un état sûr. Le cybercriminel engendre donc ladite situation en trompant les mécanismes de détection et/ou en bloquant les mécanismes de protection.

Un arbre d'attaque (ou de défaillance) est développé afin de modéliser les différentes options possibles, en partant de la situation dangereuse étudiée de sécurité ferroviaire jusqu'aux événements redoutés. Ils sont formalisés par des modes d'action appliqués à des composants particuliers. La figure affichée plus bas illustre un cas de collision par rattrapage, provoquée par une situation de survitesse qui ne sera pas bloquée.



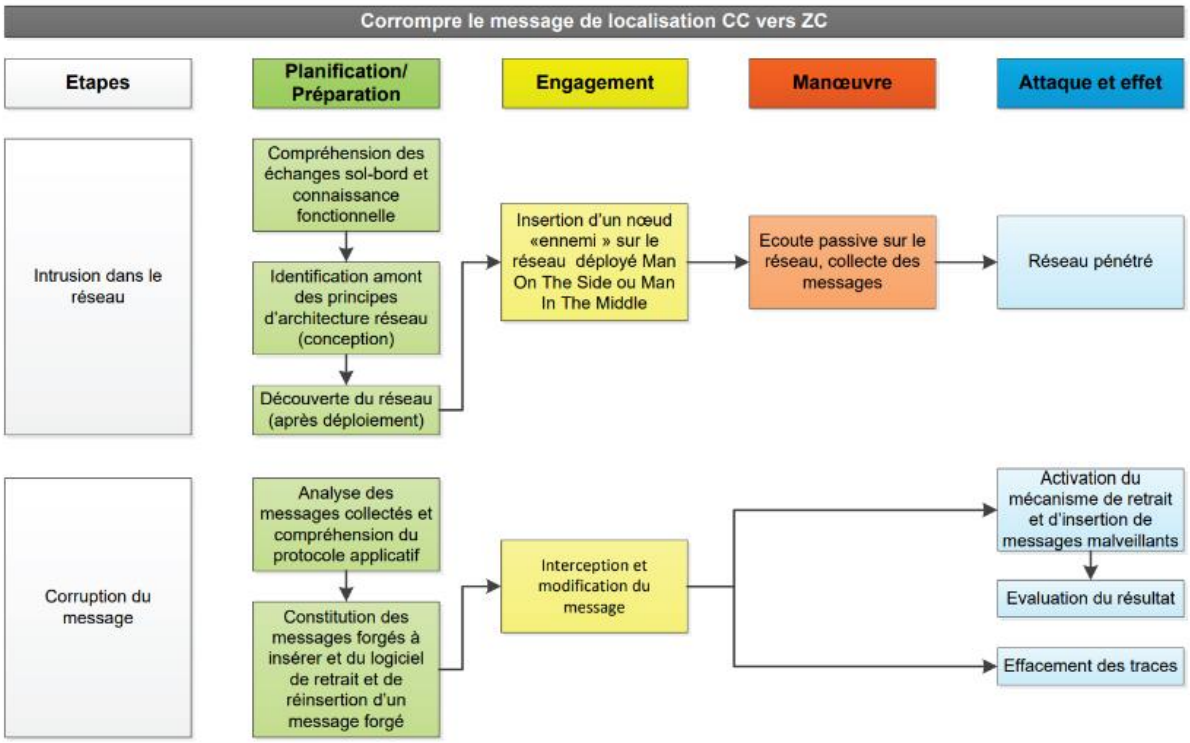
53 - Chemin d'attaque, Collision par rattrapage provoquée par une survitesse[318]

VI.6.2. SCÉNARII OPÉRATIONNELS

Dans cette approche complémentaire, on identifie les scénarios d'attaque opérationnels qui permettent à l'attaquant de provoquer les événements redoutés cyber nécessaires à leurs survenues. Pour cela, il faut projeter les scénarios stratégiques, obtenus au module précédent, sur l'architecture de conception générale. Dans le cas de cette étude pratique, 915 scénarios stratégiques complets ont été analysés, mais étant donné que l'on ne considère ici que les ER (événements redoutés) cyber (on en dénombre 70), seuls 70 cas sont à traiter par les équipes cyber et IT.

On utilise l'exemple de la corruption d'un message MAL (Message Authority Limit) transmis du ZC (zone controller) vers le CC (carbon controler) (cf. fig 27) pour illustrer la démarche. La progression spatio-temporelle du scénario détermine les différentes actions que doit réaliser le cybercriminel sur certains composants du système pour réaliser l'événement redouté cyber et en exploiter les impacts. Ce mode opératoire identifie in fine une liste des

composants d'architecture générale critiques pour la cybersécurité, qu'il convienne donc de protéger et monitorer de façon appropriée.



54 - Scénarios opérationnels pour la corruption du message de localisation ZC vers CC[319]

VI.7. ANALYSES DES RISQUES

VI.7.1. DE L'UTILITE DE L'INVENTAIRE ET LA CARTOGRAPHIE DES ACTIFS INDUSTRIELS

Dans la gouvernance de la Cybersécurité, deux étapes sont indispensables et préliminaires : la réalisation d'un inventaire et d'une cartographie sur un périmètre considéré.

L'inventaire, dans le contexte d'un système industriel, identifie les différents équipements communicants, les automates, les postes de travail, les stations opérateurs et les différents routeurs. L'inventaire apporte pour chacun de ces éléments, les données et métadonnées nécessaires pour les identifier et les caractériser, comme, le modèle, la référence, la version logicielle installée et si possible leur géolocalisation. Dans le contexte des systèmes d'information, nous retrouvons sensiblement les mêmes éléments, hors ceux spécifiques aux systèmes industriels.

La réalisation d'une cartographie permet la représentation graphique des systèmes d'information de l'organisme considéré et de ses différentes connexions internes et celles avec l'extérieur. La cartographie est essentielle aux analyses, elle rend possibles les modifications en limitant les risques et elle facilite la détection d'anomalies et les prises de décisions sur les actions correctives prioritaires. Elle permet un gain de temps dans la maintenance, dans l'intégration de nouveaux projets, dans l'évolution des systèmes existants, dans les maintiens en condition opérationnelle grâce au référencement centralisé

[319] *MAITRISE DES RISQUES LIES AUX ASPECTS DE CYBERSÉCURITÉ ET SÉCURITÉ FERROVIAIRE*- Joanna Peres, Jean Caire, Véronique Delebarre [En ligne]. [Réf. Du 20 mars 2019]. Disponible sur https://hal.archives-ouvertes.fr/hal-02074253/document

de la localisation des différents systèmes, et dans la facilitation des échanges entre les différentes parties prenantes de l'organisation qui auront de facto un périmètre fini commun.

L'intérêt des inventaires pour la cybersécurité peut se résumer dans les apports en termes de prévention, de détection, et de réaction. Dans la prévention, on peut citer l'identification des vulnérabilités, le traitement des alertes des CSIRT, la gestion de l'obsolescence et des vulnérabilités grâce à l'identification des versions tant au niveau des firmwares que des matériels. Au niveau de la détection, un inventaire a pour intérêt de détecter des équipements non identifiés, la disparition de matériel, les modifications non conformes voire malveillantes, de configuration de logiciel voire de matériel. Enfin les inventaires permettent en termes de réaction de pouvoir identifier les propriétaires (*owners* responsables), les utilisateurs et les administrateurs des équipements, de connaître ceux accrédités ou leurs fonctions, et d'en tirer des bénéfices décisionnels, par exemple est-il possible de les déconnecter, de quelle façon et avec quels impacts ?

Pour la cybersécurité, la cartographie permet l'identification des informations indispensables pour l'analyse de risques et contient les éléments nécessaires à l'établissement des plans de continuité et de reprise d'activité. La cartographie est nécessaire dans la détection d'intrusion et d'anomalies. Elle permet de contextualiser un événement de sécurité, par ses impacts, son degré de criticité dans le contexte, sa localisation physique et une réaction rapide et pertinente. Aussi, au titre de la remédiation, elle apporte un support notamment pour connaître ce qu'il est possible de déconnecter. Enfin, dans la phase d'investigation numérique (inforensic), elle permet par la vue d'ensemble fournie de retenir l'ensemble des éléments nécessaires pour comprendre et remonter le chemin d'attaque.

VI.7.2. ANALYSE DES RISQUES CYBER

La suite de ces différentes étapes est la mise en œuvre de l'appréciation des risques cyber. Elle est une composante fondamentale dans le processus de gestion des risques d'un système d'information. L'analyse de risque, clé de voûte du processus itératif de gestion des risques, est avant tout un processus permettant l'évaluation de la sécurité des systèmes d'information qu'il soit issu du monde de l'IT, celui de l'OT et aujourd'hui de leur convergence.

L'analyse de risque n'est qu'une partie de la gouvernance de la sécurité des systèmes d'information avec sa gestion des risques. Ce système de management de la sécurité se compose de différents standards, de normes et de méthodes pour les piloter et les mettre en œuvre, certaines sont communes et d'autres spécifiques. À l'origine de la sécurité des systèmes informatiques, l'*Orange book*[320] ou les Trusted Computer System Évaluation Criteria, (TCSEC), sont des ensembles de critères définis par le département de la Défense (DOD) des États-Unis, permettant l'évaluation de la fiabilité des systèmes informatiques centralisés. (15 aout 1983).

Différentes méthodes d'analyse de risque existent et peuvent répondre à différents aux besoins.

[320] *DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA – DOD* [En ligne]. [Réf. De décembre 1985]. Disponible sur Trusted Computer System Evaluation Criteria ["Orange Book"] (nist.gov)

VI.7.3. LES MÉTHODES D'ANALYSE DE RISQUE

- **ISO 27005, L'ANALYSE DE RISQUE SUIVANT LES STANDARDS INTERNATIONAUX**

La norme ISO/IEC 27005[321] s'intègre dans la suite des normes ISO 27000 qui concerne la Sécurité de l'information et publiée conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI). Elle fournit des recommandations pour la mise en œuvre d'un processus de gestion des risques en sécurité de l'information. Elle donne des lignes directrices qu'il convient de suivre, d'adapter et parfois d'ignorer (en documentant cette exclusion) dans la conception, le développement et l'exploitation de son système de gestion de risques.

- **EBIOS RM, MÉTHODE MISE AU POINT PAR L'ANSSI**

La méthode de référence française EBIOS RM[322] pour Expression des Besoins pour Identifier les Objectifs de Sécurité Risk Manager accompagne les organisations pour identifier et comprendre les risques numériques qui leur sont propres. Elle est un outil complet de gestion des risques SSI conforme au RGS[323] (Référentiel général de sécurité) et aux dernières versions des normes ISO/IEC 27001, ISO/IEC 27005 et ISO/IEC 31000. Elle permet de déterminer les mesures de sécurité adaptées à la menace et au contexte du périmètre audité, et de mettre en place le cadre de suivi et d'amélioration continue à l'issue d'une analyse de risques partagée au plus haut niveau.

EBIOS RM permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maîtriser. Elle permet aussi de valider le niveau de risque acceptable et de s'inscrire à plus long terme dans une démarche d'amélioration continue. Enfin, cette méthode permet de faire émerger les ressources et arguments utiles à la communication et à la prise de décisions au sein de l'organisation et vis-à-vis de ses partenaires.

- **NIST 800-30**

L'objectif de la publication 800-30[324] est de fournir des conseils pour la réalisation d'évaluations des risques des systèmes d'information et des organisations, en complétant les directives de la publication spéciale 800-39. Les évaluations des risques, effectuées aux trois niveaux de la hiérarchie de la gestion des risques, font partie d'un processus global de gestion des risques qui fournit aux dirigeants et aux cadres supérieurs les informations nécessaires pour déterminer les mesures à prendre en cas d'urgence en réponse aux risques identifiés.

- **AMDEC - ANALYSE DES MODES DE DÉFAILLANCE, DE LEURS EFFETS ET DE LEUR CRITICITÉ**

L'AMDEC[325] est un outil de sûreté, de fonctionnement et de gestion de la qualité. AMDEC est la traduction de l'anglais FMECA, et désigne cette méthode élaborée par l'armée américaine dans les années 1940. L'AMDEC est une méthode d'analyse prévisionnelle de

---

[321] *Information technology — Security techniques — Information security risk management* [En ligne]. [Réf. 2021]. Disponible sur ISO - ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management

[322] *La méthode EBIOS Risk Manager – Le Guide* [En ligne]. [Réf. De décembre 2018]. Disponible sur La méthode EBIOS Risk Manager – Le guide | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

[323] *Le référentiel général de sécurité – ANSSI* [En ligne]. [Réf. 2021]. Disponible sur https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

[324] Special Publication 800-37 Rev. 2 Risk Management Framework for Information Systems et Organizations: A System Life Cycle Approach for Security and Privacy

[325] *Qu'est-ce que l'AMDEC – Alain FERNANDEZ* [En ligne]. [Réf. Du 3 février 2020]. Disponible sur AMDEC Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (piloter.org)

la fiabilité. Elle permet de recenser les défaillances potentielles dont les conséquences affectent le bon fonctionnement des moyens de production ou de l'équipement étudié. Elle permet ensuite d'estimer les risques liés à l'apparition de ces défaillances, afin d'engager les actions correctives à apporter lors de la conception, de la réalisation ou de l'exploitation (production, maintenance).

- **ANALYSE QUANTITATIVE DES RISQUES**

L'évaluation quantitative des risques (Bedford 2001) traduit de l'anglais Quantitative Risk Assessment (QRA), est une méthode qui évalue la probabilité de dommages causés par un accident potentiel. Développée initialement dans le nucléaire et dans le domaine des transports, cette méthode a graduellement été adaptée à l'industrie des procédés et notamment dans les pays du nord de l'Europe. C'est la façon de représenter et d'exprimer les résultats de l'analyse de risques qui fait la particularité des méthodes de QRA. Le résultat du calcul réalisé en partant de la probabilité qu'un individu meure des effets de l'accident sera qualifié de risque individuel. La partie de la population risquant de mourir des effets de l'accident sera qualifiée de risque sociétal. Il est à préciser que l'EQR (QRA) ne s'intéresse souvent qu'aux effets létaux sur les personnes. Pour leur représentation il est habituel de s'appuyer sur des courbes fréquence/gravité (ou courbe F/N) pour le risque sociétal ou des courbes iso-risque (courbes des risques équivalents[326]) pour le risque individuel.

- **FAIR - FACTOR ANALYSIS OF INFORMATION RISK**

FAIR (Factor Analysis of Information Risk) s'est imposé comme le premier modèle de Value at Risk (VaR) pour la cybersécurité et le risque opérationnel. Le FAIR Institute et sa communauté se concentrent sur l'innovation, l'éducation et le partage des meilleures pratiques pour faire progresser le modèle FAIR™ et les professions de la gestion du risque cybernétique et opérationnel.

Il fournit aux responsables du risque informationnel, de la cybersécurité et des affaires les normes et les meilleures pratiques pour les aider à mesurer, gérer et rendre compte du risque informationnel du point de vue des affaires.

VI.8. TRAITEMENT DES RISQUES

Il existe quatre options pour le traitement des risques, leur réduction, leur maintien, leur refus et leur partage ou déport. Une fois mises en œuvre les recommandations et les décisions sur le traitement des différents risques, il restera des risques résiduels qui seront décrits aux porteurs des risques appropriés. S'ils ne sont toujours pas acceptables, un nouveau cycle est lancé pour les traiter jusqu'à l'atteinte du niveau souhaité ; dans le cas contraire, le processus alternera entre en phase de surveillance (potentiellement continue) et réexamen ponctuel des risques.

VI.8.1. PLAN DE TRAITEMENT DE RISQUES

Pour les risques qualifiés « d'inacceptables », ou pour lesquels il a été décidé qu'il fallait en réduire les impacts ou la vraisemblance, des mesures doivent être décidées puis mises en œuvre.

[326] *Fondamentaux de l'analyse de risqué- Regard fiabiliste sur la sécurité industrielle – Yves MORTUREUX - FONCSI* [En ligne]. [Réf. De février 2016]. Disponible sur https://www.foncsi.org/fr/publications/regards/fondamentaux-analyse-risque-regard-fiabiliste/rgd_2016-02_fiabiliste page 9

Pour choisir les mesures de réduction, il peut être utile de s'appuyer sur des standards adéquats (normes internationales type ISA/IEC 62443, NIST Cybersecurity framework aux États-Unis, CPNI au Royaume-Uni, guides ANSSI en France, ISO, etc.).

La mise en œuvre d'un échange avec les interlocuteurs qualifiés (délégué à la protection des données, responsable PCA, ingénierie et sûreté de fonctionnement, responsable sécurité/sûreté physique,) sera nécessaire pour s'assurer de l'adhérence du plan de traitement du risque avec les domaines connexes tels que :

- La sûreté de fonctionnement ;
- La continuité d'activité ;
- La sûreté des bâtiments (contrôle d'accès, système anti-intrusion, vidéosurveillance, réseaux mobiles privés de type PMR…) ;
- La sécurité physique et environnementale (sécurité électrique, sécurité, incendie, dégâts des eaux, chantiers, etc.) ;
- La protection des données à caractère personnel (données usagers, vidéoprotection dans les espaces publics…).

Il est nécessaire que les mesures sélectionnées ne soient ni redondantes ni contradictoires.

VII. ASPECTS TECHNIQUES ET OPÉRATIONNELS

Dans cette partie nous aborderons les thématiques indispensables pour renforcer une posture de cybersécurité au sein des SI des gestionnaires d'infrastructure et des entreprises ferroviaires.

La démarche doit être alignée de bout en bout dans une perspective de cybersécurité globale et en profondeur, garantissant in fine le rendu des services proposés par l'entreprise et la sauvegarde des vies humaines. La défense en profondeur tel qu'illustrée dans le schéma ci-dessous, promue par la norme CEI-62443 et la TS 50701[327] publiée en juillet 2021, en est un puissant marqueur !

[327] *Railway applications CyberSecurity* [En ligne]. [Réf. 16 mars 2021]. Disponible sur 4-status-update-on-cenelec-wg-26-benoliel-schlehuber.pdf

55 - Démarche de défense en profondeur spécifique aux ICS[328]

VII.1. EXIGENCES DE SECURITE, SURETE DE FONCTIONNEMENT, ET CYBERSECURITE

Commençons par rappeler quelques terminologies : dans les systèmes industriels et selon la norme CEI 60050, la **sûreté de fonctionnement** est l'aptitude du système de remplir les fonctions pour lesquelles il a été conçu et est relié aux dysfonctionnements intrinsèques au système[329]. La sûreté de fonctionnement comprend la disponibilité, la fiabilité, la récupérabilité, la maintenabilité, l'efficacité de la logistique de maintenance et, dans certains cas, d'autres caractéristiques telles que la durabilité, la sûreté et la sécurité.

La sécurité industrielle, selon les normes CEI 60050 et ISO/ IEC GUIDE 51, est potentiellement intriquée avec à la cybersécurité. Elle désigne les moyens humains, techniques et organisationnels de prévention et d'intervention contre les risques à caractère accidentel. Elle est donc liée aux attaques externes.

Sûreté, sécurité et cybersécurité poursuivent la même finalité, préserver les personnes et les biens contre des actions involontaires ou intentionnelles de malveillance. Avec la quête d'une défense en profondeur dans un contexte de convergence IT-OT, ces deux exigences vont être amenées à être pensées conjointement.

Les exigences de **sécurité IT** (cybersécurité) se regroupent autour de quatre critères sous l'acronyme DICT-P (Disponibilité, Intégrité, Confidentialité, Traçabilité ou Preuve).

Dans l'OT, la première des exigences à respecter (loin même devant la confidentialité) est l'intégrité des données transmises. Une falsification de ces données peut en effet entraîner des conséquences significatives sur le bon fonctionnement des sous-systèmes (signalisation, aiguillage, distribution électrique) et sur leur disponibilité. Au-delà des critères DICT, l'architecture des systèmes et des réseaux doit également prendre en

[328] *IEC 62443, le standard incontournable de la cybersécurité industrielle* [En ligne]. [Réf. Du 15 avril 2021]. Disponible sur IEC 62443, un standard en cybersécurité industrielle | Stormshield

[329] Cigref - Clara Morlière, *Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels* [En ligne]. [Réf. du 18 février 2020]. Disponible sur https://www.cigref.fr/wp/wp-content/uploads/2019/12/Cigref-Convergence-IT-OT-Rapprochement-fructueux-Systemes-Information-et-Industriels-Decembre-2019-light.pdf

compte les notions de fiabilité et de maintenabilité, pour rendre plus visibles les menaces pesant sur les opérations de maintien en condition opérationnelle[330].

Pour atteindre les objectifs de performances de fiabilité, les solutions de signalisation mettent en œuvre des techniques et des technologies très spécifiques, souvent coûteuses dans le domaine ferroviaire. Comme dans l'aéronautique, les calculateurs sont par exemple très souvent basés sur des architectures électroniques multiplexées où plusieurs chaînes de traitement fonctionnel diversifiées ou homogènes, synchronisées ou asynchrones, collaborent pour élaborer une information intègre (votée par exemple à la majorité des chaînes). Les langages informatiques de programmation sont quelquefois très spécialisés et formels, pour démontrer mathématiquement la conformité du code exécuté en regard de la spécification de développement interdisant les erreurs de programmations. Les méthodes et processus appliqués sont enfin très robustes et normalisés, avec une traçabilité de bout en bout très rigoureuse.

Les différences entre IT et OT se reflètent souvent dans l'architecture réseau et dans les approches de mise en œuvre de la technologie : la segmentation réseau, la cybersécurité et les protocoles d'accès peuvent par exemple fortement varier entre IT et OT.

La convergence IT-OT et la continuité numérique qui en découlent induisent une nouvelle approche d'architecture IT- OT. Établir un socle commun de terminologie à minima compréhensible par l'IT et l'OT, est un préalable. Les concepts des deux mondes sont à rapprocher afin de partager une vision d'ensemble de l'architecture IT-OT. Rockwell Automation et Cisco ont ainsi spécifié un modèle de référence d'architecture « convergée » désigné par Converged Plantwide Ethernet (CPwE). Cette CPwE est un point de départ pour faciliter aux professionnels de l'IT et de l'OT, la conception et le déploiement d'infrastructures réseaux industrielles fiables et sûres.

La défense en profondeur et le zéro trust / zéro trust network sont aujourd'hui au cœur des préoccupations de la démarche d'architecture sécurisée. Le but est de garantir in fine les niveaux d'exigence DICT de chacun des projets mis en œuvre. Le respect des normes actuelles IEC 62443 ou TS 50701 passent par la mise en application de 4 piliers fondamentaux à savoir : Security-by-design, gestion sécurisée des accès, architecture en "zones et conduits" (segmentation, cloisonnement), gestion sécurisée des flux.

VII.2. ARCHITECTURES SECURISEES

On entend par « architecture sécurisée[331] » une architecture fonctionnelle et technique intégrant l'ensemble des principes et dispositifs de sécurité permettant la protection du système industriel des attaques par leur détection, ainsi que le ralentissement de leur propagation. Une architecture sécurisée doit couvrir fonctionnellement l'ensemble des cas d'usage métier rencontrés (consultation de l'état d'une production, paramétrage, maintenance à distance, etc.) et les potentielles déviances associées. Elle est basée sur le principe de la défense en profondeur[332], semblable à un château fort avec plusieurs barrières indépendantes.

Lors de la conception d'une architecture sécurisée d'environnements converger soumis à une transformation digitale croissante, quelques points sont à considérer. Il s'agit en particulier de garder en fils conducteurs, d'un côté la préservation des exigences de

[330] *Basic Concepts and Taxonomy of Dependable and Secure Computing* [En ligne]. [Réf. 2004]. Disponible sur TECHNICAL RESEARCH REPORT

[331] *Guide cybersécurité des systèmes industriels - CLUSIF* [En ligne] [Réf. De février 2021]. Disponible sur Guide cybersécurité des systèmes industriels.pdf)

[332] *La défense en profondeur appliquée aux systèmes d'information* [En ligne]. [Réf. Du 19 juillet 2004]. Disponible sur mementodep-v1-1.pdf (ssi.gouv.fr)

sécurité DICT dans le cyberspace (ISO/IEC 27032 : 2012) des systèmes IT qui pilotent l'OT, et de l'autre côté l'exigence impérative de non-compromission de la sûreté de fonctionnement des systèmes OT. En outre, il faut avoir sous contrôle de manière globale toutes les opérations de maintien en condition opérationnelle, comme celles de maintien en condition de cybersécurité, et conserver une attention permanente sur le risque de compromission de systèmes obsolètes. Quelques recommandations faisant maintenant consensus et conformes aux normes CEI 62443 sont à suivre à savoir :

- L'identification, la classification et la hiérarchisation des valeurs des ressources ;
- La segmentation du réseau, en tenant compte en particulier des valeurs des assets;
- L'implémentation des filtrages réseau et des ruptures protocolaires ;
- La sécurisation des accès filaires et sans fil ;
- La mise en place d'outils et de processus d'analyse de trafic réseau et de recherche de vulnérabilités.

De manière similaire, le guide cybersécurité des systèmes industriels du Clusif[333] sorti en février 2021, aborde aussi ce sujet et propose une méthodologie pour construire une architecture cyber sécurisée, basée sur les points ci-dessous et selon le périmètre étudié :

- Identification des machines et équipements (ressources) ;
- Rassemblement des ressources au sein de regroupements ;
- Identification des mesures de sécurité encadrant les échanges entre les groupements ;
- Identification des mesures de sécurité à définir au sein d'un groupement.

Le travail de regroupement, assez fastidieux, est un travail (itératif) à mener en tenant compte de la fonctionnalité et de la criticité de la ressource ainsi que du niveau de confiance. Dans le monde industriel, le modèle *Purdue Enterprise Reference Architecture* (PERA[334]) permet la catégorisation facilitée des fonctionnalités des composants des différentes couches d'un système IT-OT, du composant physique aux systèmes IT d'entreprise (ERP, CRM, etc.), en passant par les équipements de contrôle PLC (Programmable logical controller), HMI (Humain Machine Interface), et les systèmes de Surveillance, de Supervision et contrôle. Une cartographie, établie selon ce modèle PERA, est une étape majeure qui permet de partager une vision commune de l'installation et l'esquisse des premières pistes de segmentation.

Pour les mesures de sécurité, le minimum pour une défense en profondeur est :

- Le durcissement des équipements (mise en place d'une configuration sécurisée standardisée) ;
- La mise en place d'un contrôle d'accès physique ;
- La surveillance de l'activité au sein d'une zone ;
- La mise à jour des équipements (en spécifiant la démarche et la fréquence) ;
- La spécification et l'implémentation de règles d'authentification sur les équipements ;
- La mise en place d'un pare-feu ou de passerelle afin d'assurer un filtrage des flux.

La méthodologie d'évaluation du niveau de sécurité proposée par le consortium CYRail basée sur les standards IEC 62443 permet d'instruire en profondeur les différentes couches architecturales IT-OT (du capteur au sol aux serveurs applicatifs accessibles depuis l'environnement IT).

---

[333] *Guide cybersécurité des systèmes industriels - CLUSIF* [En ligne] [Réf. De février 2021]. Disponible sur Guide cybersécurité des systèmes industriels.pdf)
[334] *PERA Enterprise Integration Web Site* [En ligne]. [Réf. 2021]. Disponible sur http://www.pera.net/

Pour relever ce challenge, il est indispensable de vérifier :

1. Les niveaux de sécurité cible et l'estimation des écarts avec ceux déjà mis en œuvre
2. La capacité intrinsèque de l'entreprise à déployer la cybersécurité.

VII.3. SECURITY BY DESIGN

Le concept de « Security-by-design » est considéré aujourd'hui comme la démarche à adopter en regard du concept de zéro-trust ou zéro-trust network. Cela veut dire, en termes simples, « penser sécurité » dès les phases d'émergence et de conception. La sécurité ne sera dans ce cas plus considérée comme une variable d'ajustement tant économique que fonctionnelle, mais fera partie intégrante des briques garantissant la fourniture des services et les bénéfices attendus par les métiers. Le CYRail [335] (projet du programme européen Shift2Rail) indique clairement qu'il s'agit d'une approche qui tient compte des risques et qui nécessite un travail d'équipe multidisciplinaire et une stratégie de sécurité claire [336]. Les grands principes du « Security-by-design » sont la réduction de la surface d'attaque, le moindre privilège et la « défense en profondeur »[337]. CYRAIL les décline au travers des points suivants :

- **Le moindre privilège** : un sujet ne devrait recevoir que les privilèges dont il a besoin pour accomplir sa tâche et opérer clairement une séparation (ségrégation) des privilèges et des rôles. Aussi, un système ne devrait pas accorder d'autorisation sur la base d'une seule condition ;
- **Médiation complète** : tous les accès aux objets doivent être vérifiés pour s'assurer qu'ils sont autorisés ; c'est-à-dire qu'il ne doit pas y avoir possibilité d'obtenir de valeurs ni d'accès par défaut : à moins qu'un sujet ne reçoive un accès explicite à un objet, il devrait se voir refuser l'accès à cet objet ;
- **Économie de mécanisme** : les mécanismes de sécurité doivent être aussi simples que possible ;
- **Conception ouverte** : la sécurité d'un mécanisme ne devrait pas dépendre du secret de sa conception ou de sa mise en œuvre : « pas de sécurité par l'obscurité » ;
- **Mécanisme le moins commun** : les mécanismes utilisés pour accéder aux ressources ne doivent pas être partagés ;
- **Acceptabilité psychologique** : les mécanismes de sécurité ne doivent pas rendre la ressource plus difficile d'accès que si les mécanismes de sécurité n'étaient pas présents.

La notion de *conception ouverte* est le point pivot pouvant enclencher l'accélération d'une réflexion en profondeur de la cybersécurité, car elle sous-tend une nécessité de gestion fine des accès, un contrôle des flux et un dispositif efficient de détection et de réaction face aux incidents. C'est un challenge immense quand on touche, dans le cas d'une convergence IT-OT, à des systèmes critiques.

Les équipementiers et autres fournisseurs de produits et solution doivent donc être des partenaires et moteurs au sujet de la cybersécurité. L'intégration systématique dans les contrats d'exigences de cybersécurité oblige ainsi les partenaires d'affaires à démontrer leur capacité à être à la hauteur de ces exigences, en veillant par ailleurs à ce que cela soit respecté dans toute leur chaîne d'approvisionnement. Comme explique un responsable de la sécurité des produits chez Apsys-Airbus « *L'objectif était de faire entrer la cybersécurité*

---

[335] *CYbersecurity in the RAILway sector.* [En ligne]. [Réf. Du 22avril 2018]. Disponible sur CYRail project
[336] *CYRail Recommendations on cybersecurityt of rail* signalling and communication systems [En ligne]. [Réf. De septembre 2018]. Disponible sur CYRail Recommendations on cybersecurity of rail signalling and communication systems
[337] *Sécurité by-design : analyse des 3 grands principes - Jacques de LA RIVIERE* [En ligne]. [Réf. 23 janvier 2019]. Disponible sur Sécurité by-design : analyse des 3 grands principes - Silicon

dans l'ADN de [338]*l'entreprise. Nous avons travaillé en étroite collaboration avec Alstom sur l'analyse des risques, l'élaboration d'objectifs de sécurité clé et conception du système. Ceux-ci sont transmis aux fournisseurs et quand les produits sont livrés, nous travaillons ensemble sur l'audit et les tests d'intrusion* ».

VII.4. SEGMENTATION ET CLOISONNEMENT DES ENVIRONNEMENTS

Selon Amir Levintal, CEO de la société israélienne Cylus, la paralysie du réseau ferré iranien en juillet 2021 vient confirmer selon lui qu'en général, les réseaux ferroviaires sont pour la plupart non segmentés et conçus avec des composants qui n'ont pas été prévus pour faire face aux menaces externes ni pour générer des logs pour des besoins inforensic[339].

Dans la logique de cyberdéfense en profondeur, la norme IEC 62443 dans son volet 3 **(IEC 62443-3),** décrit la méthode et les moyens pour structurer une architecture en zones et conduits qui sont une des techniques architecturales pour se prémunir des cyberattaques. Elle propose la segmentation des IACS (Industrial Automation and Control Systems) par zones en fonction des niveaux de criticité des équipements (62443-3-2), avec une communication possible entre zones (par clé USB, câble, réseau ou encore liaison VPN)[340].

VII.4.1. SEGMENTATION DES ZONES

Les zones de sécurité telles que présentées dans le graphique ci-dessous sont les préconisations minimales de la norme IEC 62443. On peut y voir les regroupements d'actifs logiques ou physiques ayant des exigences de sécurité communes.

Toutefois, le découpage doit être au service de la production et être aligné sur les exigences prioritaires que sont la sécurité, la fiabilité et l'efficacité.

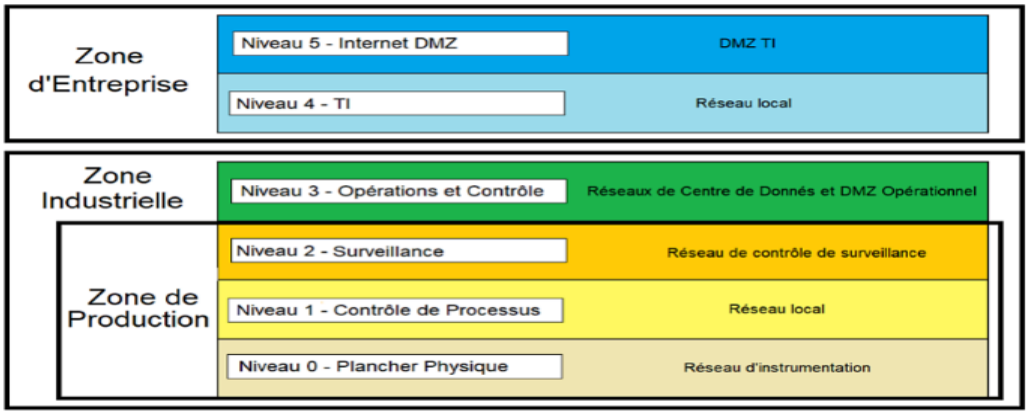
La norme IEC 62443, préconise une segmentation et isolation physique des SI industriels et des SI de gestion, ainsi que le cloisonnement des systèmes critiques (systèmes de sûreté) et des systèmes de conduite des procédés.

La sécurité en couches en opérant des segmentations logiques et physiques établit des remparts entre les différentes zones de sécurité d'un système[341] et vient ainsi renforcer la sécurité périmétrique. Les architectures multicouches permettent de garantir une séparation des réseaux cœurs. Les zones de sécurité ainsi que les communications à

---

[338] *Cybersecurity, For Safe and Secure Mobility - ALSTOM* [En ligne]. [Réf. De 2020]. Disponible sur Whitepaper Cybersecurity.pdf (alstom.com)
[339] *Cyberattaque contre le réseau ferroviaire iranien* [En ligne]. [Réf. 18 juillet 2021]. Disponible sur In cyberattack against Iran's rail network, the capabilities of the attackers weren't compromised: Cylus CEO | Israel Defense
[340] *IEC 62443, le standard incontournable de la cybersécurité industrielle par Vincent NICAISE* [En ligne] [Réf. 15 avril 2021]. Disponible sur IEC 62443, un standard en cybersécurité industrielle | Stormshield
[341] *Philippe Gaufreteau, Lilian Planche, Cybersécurité des systèmes de, transport application à la ligne 18 du Grand Paris Express,* [en ligne]. [Réf. du 20 mars 2019]. Disponible sur CYBERSECURITE DES SYSTEMES DE TRANSPORT

l'intérieur et entre ces zones sont définies en fonction de la criticité et de l'impact d'une potentielle compromission. Le schéma ci-dessus est une déclinaison du schéma précédent en fonction des usages et/ou réseaux IT OT.



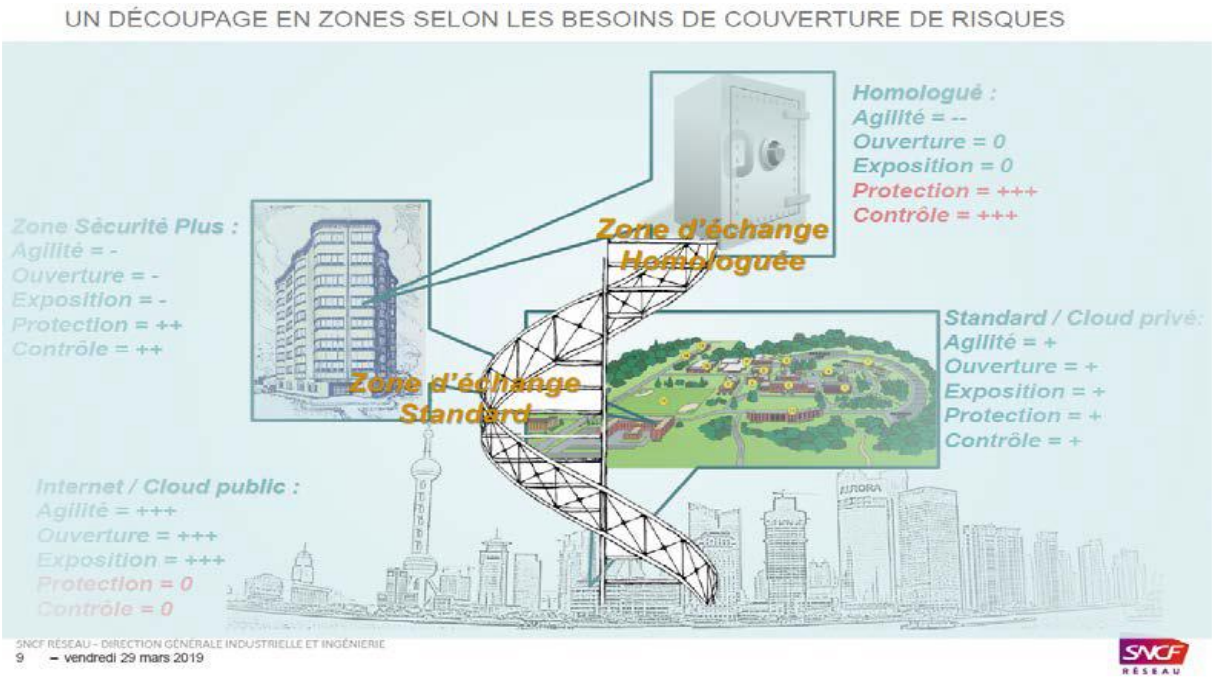
56 - Type de segmentation pour la protection des réseaux[342]

L'entreprise peut découper son réseau en zones autonomes en fonction des besoins de couverture des risques. Chaque zone est déterminée sur la base des critères tels que : l'agilité affectée à cette couche, son ouverture, son exposition, les niveaux de protection et de contrôle à apporter. Une évaluation pour chacun des critères a conduit à une déclinaison des zones suivantes :

- ✓ Zone internet / cloud public (logique de réseau externe, très agile et ouvert aux systèmes)
- ✓ Zone standard / cloud privée (logique de réseau interne)
- ✓ Zone sécurité plus (logique de réseau fermé qui contrôle sans empêcher toute flexibilité)
- ✓ Zone homologuée (logique de coffre-fort, avec un maximum de protection et de contrôle)

L'entreprise peut découper son réseau en zones autonomes en fonction des besoins de couverture des risques. C'est aussi ce qui a été mis en œuvre chez SNCF RÉSEAU dans une logique de sécurisation adaptée aux différentes zones. Ce qui donne le découpage illustré dans le schéma ci-dessous[343].

[342] *Comment segmenter le reseau pour bien protéger les téchnologies opérationnelles* [En ligne]. [Réf. Du 5 mars 2020]. Disponible sur Comment segmenter le réseau pour bien protéger les TO? (novipro.com)
[343] Cigref - Clara Morlière, *Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels* [En ligne]. [Réf. du 18 février 2020]. Disponible sur https://www.cigref.fr/wp/wp-content/uploads/2019/12/Cigref-Convergence-IT-OT-Rapprochement-fructueux-Systemes-Information-et-Industriels-Decembre-2019-light.pdf



57 - Zones à isoler en cas d'incident (source SNCF RÉSEAU /CIGREF)

Ces critères de découpage se rapprochent de ceux caractérisant les trois classes de SI industriels définis par l'ANSSI et dont le niveau de criticité dépend des critères de connectivité, des fonctionnalités, du niveau d'exposition, de l'attractivité pour un attaquant, de la vraisemblance et des impacts en cas d'attaque. Pour chacune des classes, des règles plus ou moins strictes font émerger entre autres des principes forts d'architectures sécurisées. À noter que l'ANSSI émet des préconisations en regard des impacts pour la population, l'environnement et l'économie nationale, sans se soucier de l'impact direct pour l'entreprise concernée[344].

VII.5. CONDUITS ET COMMUNICATION ENTRE ZONES

La notion de « conduit » représente l'interconnexion entre deux zones et le type de communication entre ces zones. Bien comprendre et maîtriser chaque conduit rend possible une meilleure surveillance et protection du trafic passant par ces conduits et pouvant avoir des incidences négatives sur les zones destinatrices. Cela nécessite la mise en place de dispositif et de règles claires en fonction de la criticité et des impacts des flux échangés.

Par exemple, dans le cas concret des écosystèmes conçus pour le projet de ligne 18 de métro[345] parisien, les échanges entre réseaux de niveau de sécurité différents ont été réduits au strict nécessaire ; les systèmes des réseaux les plus sécurisés étant les seuls à pouvoir initier des échanges avec les systèmes des réseaux moins sécurisés. De manière similaire, dans le cas spécifique de l'architecture mise en œuvre chez SNCF RÉSEAU, n'ont été autorisées entre la zone de sécurité plus (ZSP) et la zone homologuée, que des

[344] *Cloisonnement et segmentation : standards et réglementations se mettent d'accord* [En ligne]. [Réf. 2015]. Disponible sur Architecture de sécurité des SI Industriels : de la théorie à la pratique - RiskInsight (riskinsight-wavestone.com)
[345] Philippe Gaufreteau, Lilian Planche, *Cybersécurité des systèmes de, transport application à la ligne 18 du Grand Paris Express*, [en ligne]. [Réf. du 20 mars 2019]. Disponible sur https://hal.archives-ouvertes.fr/hal-02074202/document

communications machine à machine avec un filtrage et une rupture protocolaire permettant d'augmenter le niveau de protection[346].

VII.6. FILTRAGE DE FLUX

Les standards ou référentiels de sécurité tels que l'IEC 62443 ou les guides de l'ANSSI recommandent sur ce sujet les mesures de sécurité suivantes[347] :

- Mise en place d'un pare-feu ou de passerelle afin d'assurer un filtrage des flux ;
- Mise en place d'un proxy ou reverse proxy afin de s'assurer de la destination ou source des flux ;
- Mise en place de sondes d'analyse des flux afin de détecter des attaques ;
- Mise en place de serveurs ou postes de rebonds durcis pour assurer un niveau de confiance élevé lors de l'accès à une zone de criticité élevée ;
- Mise en place de postes d'administration dédiés ;
- Mise en place d'un serveur d'échange de fichiers permettant de réaliser une analyse antivirale des fichiers échangés entre des zones de confiance ou de criticité différentes ;
- Mise en place de mécanismes de chiffrement des flux (VPN) ; rappelons toutefois que si cela est une sécurité et réduit drastiquement les attaques de type Homme du Milieu, cela n'empêche pas une compromission des SI d'entreprise en cas de compromission d'un PC légitimement connecté via ce VPN ;
- Mise en place d'une solution de sécurisation des accès distants.

VII.7. GESTION DES ACCES

Depuis 2018, le nombre moyen d'incidents dus à la négligence d'un collaborateur ou d'un sous-traitant est passé de 13,2% à 14,5% par entreprise. Le nombre moyen d'incidents liés au vol d'identifiants de connexion a quant à lui pratiquement triplé ces deux dernières années, passant de 1% à 2,7% par entreprise[348]. La gestion des accès en continu doit être parmi les plus hautes priorités, par exemple au-dessus de la nécessité de remédier aux vulnérabilités qui réapparaissent le plus souvent à une fréquence non maîtrisable. La plupart des attaques majeures ou critiques sont facilitées par des possibilités d'usurpation de droits et de permissions et leurs élévations par les acteurs malveillants.

L'un des points clés dans l'instruction d'architecture est de clarifier les cas d'usage du besoin exprimé. Ces cas d'usage permettent de dégager les différents acteurs et parties prenantes. Il est donc crucial lors de cette phase de bien identifier les profils et leurs besoins d'accès à telle ou telle ressource ou fonctionnalité. En regard du principe du moindre privilège, l'adoption du postulat de base « par défaut l'accès à une ressource est interdit, sauf à en démontrer le besoin » pousse à challenger les différents accès et habilitations. Ces accès peuvent être regroupés dans des rôles par facilité de gestion ; ces rôles doivent alors être challengés deux à deux afin que la somme des différents accès en cas d'octroi de plusieurs rôles à un sujet, ne permette pas l'obtention de droits incompatibles entre eux (matrice de ségrégation des rôles).

Une solution de gouvernance des identités et des habilitations permet de mettre en évidence la politique de sécurité informatique mise en place dans l'entreprise : c'est un

[346] *Profils de protection pour les systèmes industriels – ANSII* [En ligne]. [Réf. 2021]. Disponible sur Profils de protection pour les systèmes industriels | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
[347] *Guide cybersécurité des systèmes industriels - CLUSIF* [En ligne] [Réf. De février 2021]. Disponible sur Guide cybersécurité des systèmes industriels.pdf)
[348] *Rapport 2020 sur le coût des menaces internes à l'échelle mondiale – Observe IT – Proofprint* [En ligne]. [Réf. 2020]. Disponible sur Rapport 2020 sur le coût des menaces internes à l'échelle mondiale (bitpipe.com)

outil d'analyse et d'évaluation. La gestion des accès et des identités, comprenant la revue et la recertification des droits, consiste à vérifier que les identités numériques des utilisateurs et des entités sont toujours nécessaires et disposent par ailleurs du niveau d'accès approprié aux ressources de l'entreprise comme les réseaux et les bases de données.

VII.8. SECURISATION DE L'INTEGRATION AVEC LE CLOUD

Pour offrir des solutions plus intelligentes répondant aux besoins des clients et optimiser sa production ferroviaire, sa maintenance et sa chaîne d'approvisionnement, l'industrie ferroviaire active, par le biais de l'intelligence artificielle (IA), du big data, du cloud computing combiné au Edge computing[349] et de la blockchain, des puissants leviers pour opérer le changement en profondeur de son réseau. La puissance de calcul, les capacités de stockage, la rapidité de déploiement dans le cloud, l'élasticité de ses architectures sont des accélérateurs mis à profit par les entreprises pour étendre leurs SI d'entreprise (SIE) et parfois industriels (SII). Aujourd'hui, l'usage de l'IA dans les entreprises ne peut déployer tout son potentiel qu'au travers de l'usage du cloud qui permet la mutualisation des expertises et des investissements. Cela engendre cependant d'autres portes d'accès aux SIE et SII. L'intégration vers le cloud doit donc être alignée à la stratégie de défense en profondeur et faire l'objet d'une stricte vigilance sur les données qui y sont stockées, même si leur criticité unitaire semble a priori faible. Toutes les données ont de la valeur et peuvent être exploitées à des fins d'espionnage industriel ou de concurrence, sur des appels d'offres par exemple. Les contrats, les types et les niveaux de services fournis par les fournisseurs de solutions cloud sont à regarder méticuleusement par des équipes expertes dans chacun des domaines (technique, commerciale, juridique, etc.). Cette vigilance est nécessaire aussi bien lors de l'étude d'évaluation de l'éligibilité au cloud (*cloud assessment un véritable outil d'aide à la décision pour vous aider à concevoir votre stratégie de modernisation*[350]) que tout au long de l'utilisation du cloud.

Autres points, les services de sécurité mis à disposition par le fournisseur cloud sont à prendre en compte lors de l'audit d'éligibilité et tout ou long de la vie du projet. Les éléments structurants, tels que le dimensionnement, les problématiques d'intégration des dispositifs de journalisations, de détection et de corrélation entre les écosystèmes cloud et ceux déployés sur les datacenters on-premise[351], les plans d'adressage, les localisations exactes de l'emplacement géographique des logs applicatifs et systèmes, ainsi que la capacité de réaction en cas d'incident, sont à minima à considérer dans la démarche de sécurisation avec le cloud.

Le Visa de sécurité dédié de l'ANSSI (SecNumCloud), lancé en 2016[352] et revisité au premier semestre 2021, repose sur l'expertise de centres d'évaluation privés agréés et permet de faire des choix de solutions de sécurité disponibles sur le cloud et ainsi de contribuer au renforcement des capacités de cyberdéfense de la France et de l'Europe.

L'Agence Européenne pour la Cybersécurité (ENISA) prévoit d'ailleurs d'emboîter le pas à l'ANSSI et son SecNumCloud en proposant *différents schémas de certification de la*

[349] *Edge computing : définition et cas d'usage de la technologie* [En ligne]. [Réf. Du 11 janvier 2021]. Disponible sur 1440664-edge-computing-definition-et-cas-d-usage-de-la-technologie/

[350] *Cloud Assessment, auditez votre éligibilité à migrer dans le Cloud* [En ligne]. [Réf. Du 8 mars 2021]. Disponible sur Cloud Assessment, auditez votre éligibilité à migrer dans le Cloud (linkbynet.com)

[351] *On-premise, cloud, hybride : DSI où en êtes-vous ?* [En ligne]. [Réf. 2021]. Disponible sur https://www.napsis.fr/actualite/cloud-on-premise/

[352] *SecNumCloud évolue. Le référentiel inclut notamment de nouvelles exigences en matière de protection des données à caractère personnel – ANSSI* [En ligne]. [Réf. 2021]. Disponible sur SecNumCloud évolue et passe à l'heure du RGPD | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

cybersécurité : Critères Communs, cloud et 5G harmonisés au niveau européen, tel que décrit dans le Cybersecurity Act[353] .

Le SecNumCloud précise un certain nombre de règles pour une utilisation sécurisée de l'infrastructure et des services cloud. Quelques-unes d'entre elles doivent faire l'objet d'une vigilance accrue lors d'une contractualisation avec un fournisseur de services cloud[354] :

- S'assurer d'une implémentation réelle de la continuité de l'application « des zones et conduits » dans le Cloud sachant que « *la virtualisation généralement utilisée dans les services d'informatique en nuage ne doit pas être considérée comme un mécanisme de cloisonnement équivalent à une séparation physique* » ;
- S'assurer que le prestataire a veillé à sécuriser la *confidentialité des données par des tiers impliqués dans la fourniture du service (fournisseurs, sous-traitants, etc.)* » ;
- Garantir que les données techniques (identités des bénéficiaires et des administrateurs de l'infrastructure technique, journaux de l'infrastructure technique, annuaire, certificats, configuration des accès, etc.) sont stockées et traitées au sein de l'Union européenne ;
- Vérifier le respect du modus operandi relatif à la gestion et la manipulation des données nécessaires et utilisées dans le cadre d'une intervention par le support technique, lors d'un diagnostic et à la résolution d'un problème rencontré sur les services contractés ou plus généralement sur l'environnement du fournisseur de solution cloud. Ce point vaut aussi pour le télédiagnostic ou la télémaintenance de composants de l'infrastructure ;
- Vérifier la bonne mise en œuvre des directives suivantes relatives au stockage de données : le prestataire doit « *documenter et mettre en œuvre une procédure de sauvegarde hors-ligne* » de la solution. Il doit également « *documenter et mettre à disposition du commanditaire un service de sauvegarde de ses données* ». En fin de contrat, le prestataire doit procéder à un « *effacement sécurisé de l'intégralité des données du commanditaire* ». Désormais, il est précisé qu'il « *doit faire l'objet d'un préavis formel au commanditaire de la part du prestataire respectant un délai de vingt et un jours calendaires* » ;
- Enfin, concernant les risques d'extra-territorialité, le SecNumCloud *précise les règles pour s'assurer l'immunité au droit extracommunautaire ;*

Dernier point, la sécurisation des authentifications et les API utilisées (tant consommateur que fournisseurs) sont des sujets connexes nécessitant une vigilance accrue dans le cadre de l'intégration avec le cloud.

VII.9. STRATEGIE D'HOMOLOGATION

Pour limiter les risques, les opérateurs de services essentiels, comme le ferroviaire, sont soumis à des directives strictes. Dans le cas de la France par exemple, les gestionnaires d'infrastructure sont régis par l'arrêté sectoriel de transport ferroviaire relevant du Code de la Défense. L'homologation de cybersécurité des Systèmes d'Information qui y sont soumis est obligatoire, avec des conditions renforcées à remplir. Pour être homologué, un tel SI doit :

- Respecter les règles de cybersécurité définies dans l'arrêté sectoriel ;

---

[353] *la cybersécurité est « en pleine expansion » en France et en Europe* [En ligne]. [Réf. Du 1er juillet 2021]. Disponible sur ANSSI : la cybersécurité est « en pleine expansion » en France et en Europe (nextinpact.com)

[354] *SecNumCloud : l'ANSSI adapte son référentiel au Cloud de confiance, qu'est-ce qui change ?* [En ligne]. [Réf. Du 18 octobre 2021]. Disponible sur SecNumCloud : l'ANSSI adapte son référentiel au Cloud de confiance, qu'est-ce qui change ?

- Avoir une cartographie complète et documentée ; ceci reste encore un challenge pour les raisons évoquées plus haut relatives à la difficulté de l'exercice ; elle doit néanmoins exister à minima pour les assets critiques des SIIV et PIIV.
- Avoir fait l'objet d'une analyse de risques et d'un audit complet effectué par les équipes dédiées de l'ANSSI ou par les prestataires qualifiés PASSI (Prestataires d'audit de la sécurité des systèmes d'information).

La démarche est encadrée et interpelle quant aux possibilités d'agilité. En effet, le délai moyen peut, pour un changement simple, aller jusqu'à 18 mois. Selon SNCF RÉSEAU, gestionnaire historique de l'infrastructure ferroviaire en France, toutes les opérations ci-dessous (liste non exhaustive) sont soumises à un (ré) examen du dossier d'homologation pouvant conduire à un retrait d'une décision favorable ; il s'agit de :

- Raccordement d'un nouveau site sur le SI soumis à homologation cybersécurité ;
- Ajout d'une fonctionnalité majeure ;
- Succession de modifications mineures ;
- Réduction de l'effectif affecté à une tâche impactant la sécurité ;
- Changement d'au moins un prestataire ;
- Non-respect d'au moins une des conditions de l'homologation de cybersécurité ;
- Changement du niveau de sensibilité des informations traitées et/ou du niveau du risque SSI ;
- Évolution du statut de l'homologation de cybersécurité des systèmes interconnectés ;
- Publication d'incidents de nature à remettre en cause les garanties recueillies dans le dossier de cybersécurité

Contrairement à la LPM qui impose aux OIV de recourir à des produits et prestataires qualifiés par l'autorité nationale de cybersécurité et de cyberdéfense (l'ANSSI), notamment pour la détection des incidents de sécurité[355] et pour l'audit réalisé dans le cadre de l'homologation[356], la transposition de la directive européenne NIS (qui s'impose à tous les OSE – les OIV étant un cas spécifique d'OSE en France) demande "simplement" de s'appuyer sur les exigences des référentiels de qualification des prestataires de confiance pour ces domaines[357].

VII.10. PROTECTION ET DETECTION DES ATTAQUES

Les opérateurs de transport terrestre doivent mettre en œuvre des mesures de sécurité permettant de protéger leurs réseaux et leurs systèmes d'information des cyber-attaques et cela, quel que soit leur domaine IT ou OT.

Le corpus documentaire incluant les politiques de sécurité et les procédures (par exemple, politiques de mot de passe, procédures de stockage…) doit également couvrir à minima la gestion des vulnérabilités de systèmes matériels et logiciels (y compris les correctifs pour les domaines IT et OT), la gestion des incidents et la protection du système et du réseau.

VII.10.1. SYSTÈME DE PROTECTION DES INTRUSIONS

- **MESURES GÉNÉRALES**

Les mesures générales de protection contre les intrusions comprennent, tant pour l'IT que l'OT, les antivirus éprouvés, les outils de sécurisation de la messagerie (contre les menaces

[355] *Détection d'intrusion (IDS)* [En ligne]. [Réf. De septembre 2018]. Disponible sur Mémo CERTITUDE - Détection d'intrusion - IDS (certitudenumerique.net)
[356] *Homologation de sécurité* [En ligne]. [Réf. De janvier 2020]. Disponible sur Mémo CERTITUDE - Homologation des systèmes numériques (certitudenumerique.net)
[357] *LPM vs NIS* [En ligne]. [Réf. De janvier 2020]. Disponible sur Mémo CERTITUDE - LPM-NIS (certitudenumerique.net)

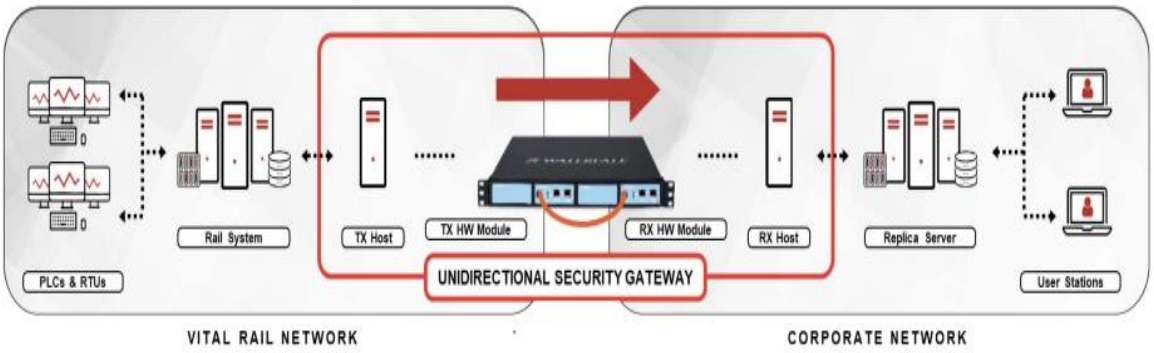
telles que fraude à la messagerie, ransomware, phishing, etc.), les EDR et les générations suivantes (XDR, SOAR etc.). Il faut cependant souligner que disposant de privilèges élevés, ces outils peuvent aussi servir de vecteur d'attaques en cas de compromission (par exemple lors d'une attaque de type Supply Chain.).

- **MESURES TECHNIQUES DE SÉCURISATION D'ARCHITECTURE**

Les normes de sécurité industrielle telles que la CEI 62443 et la TS-50701 (mise à jour en septembre 2021) présentent les pare-feux et en particulier les passerelles unidirectionnelles comme des moyens de protection des liaisons entre des zones de criticité différente. Les dispositifs de cybersécurité physiques et notamment les passerelles unidirectionnelles (« diodes ») sont parfois désignés comme plus efficaces et mieux adaptés pour les échanges entre zones de niveaux de criticité différents, en raison de la porosité des pare-feux à certains types de cyberattaques, même lorsque les communications sont chiffrées, eu égard à leur nature intrinsèquement bidirectionnelle.

- Tous les pare-feux logiciels présentent à un moment donné des vulnérabilités de sécurité (CVE) fréquentes. Il en est de même des VPN ;
- Tous les pare-feux physiques transfèrent le trafic réseau « autorisé » entre réseaux. En compromettant un pare-feu, il est possible pour un cybercriminel de masquer son propre flux dans des flux qui lui semblent correspondre à du trafic « autorisé » une fois les règles du pare-feu compromis identifiées (encapsulation du flux malveillant).

L'introduction de diodes[358] ou passerelles unidirectionnelles permet de restreindre l'échange de données au juste nécessaire entre les systèmes critiques et d'autres réseaux ayant des niveaux de sensibilité plus bas. Certains industriels proposent du matériel de cybersécurité de couche 2 « BITW - Bump in the Wire » combinés avec une puce implémentant une protection utilisant le protocole IPSec[359] et pouvant être intégrée dans des systèmes existants pour améliorer l'intégrité, la confidentialité ou la fiabilité des communications sans rajouter de latence. Il est alors rendu possible avec ce type de matériel de pouvoir effectuer des inspections poussées des paquets des conduits les plus cruciaux[360].



58 - Waterfall Gateway Sécurisé Unidirectionnel (Source Waterfall)

[358] *NEXOR DATA DIODE, EAL7+, guaranteed one-way data flow* [En ligne]. [Réf. 2021]. Disponible sur Data Diodes - Unidirectional Data Flow Control | Nexor Diode
[359] *Recommandations de sécurité relatives à IPsec1 pour la protection des flux réseau* [En ligne]. [Réf. Du 3aout 2015]. Disponible sur NT_IPsec.pdf (ssi.gouv.fr)
[360] *Décomposition des normes de cybersécurité industrielle, ISA99/ISA/CEI62443 et NERC-CIP* [En ligne]. [Réf. 2021]. Disponible sur Décomposition des normes de cybersécurité industrielle | Anixter

C'est le cas de la solution de passerelle physique Waterfall, qui selon le fournisseur ne remplace pas les pare-feux, mais constitue une couche sur la pile de firewalls permettant d'éviter des compromissions provenant d'un réseau externe ou d'entreprise[361].

C'est aussi le cas de la solution « Seclab Secure XChange Network », qui selon le site de la société permet de prévenir des scans, des attaques de 0-day (vulnérabilité non identifiée ou identifiée, mais non corrigée par l'éditeur), des attaques sur les couches de transport jusqu'à toutes les couches OSI. Cette solution empêche les routages réseau autres que ceux strictement prédéfinis (technique d'ACL basée sur le matériel). Elle est censée rendre la découverte du réseau impossible[362].

- **MESURES DE SÉCURISATION DES ACCÈS**

Le rapport de mars 2021 de Forrester (société de recherche et de conseil) révèle un chiffre interpelant pour les professionnels de la sécurité et les décideurs, en leur rappelant que leurs propres utilisateurs constituent une menace : un quart des attaques étudiées sont d'origine interne[363].

Une solution efficace de gestion des identités et des habilitations dans une entreprise implique de créer un guichet unique au sein du système d'information afin de gérer l'ensemble des mouvements des collaborateurs, des habilitations et des accès aux ressources informatiques. Plusieurs outils de gestion d'identités et d'habilitations existent sur ce marché. Le challenge est de trouver des solutions permettant une gestion des accès aux ressources aussi bien IT qu'OT dans le temps et dans l'espace, car la dimension d'espace géographique physique est à prendre en compte dans le ferroviaire.

VII.10.2. SYNOPSIS D'UNE RAILWAYS CYBER KILL CHAIN

Au regard de la convergence IT/OT, comme nous l'avons expliqué plus haut, il devient impératif de maîtriser les chemins d'attaques de bout en bout depuis l'IT (point entrant majoritaire de l'attaquant) jusqu'aux systèmes opérationnels (cibles de l'attaquant).

Les sources de dysfonctionnement peuvent être de l'IT vers l'OT ou inversement (même si cela arrive plus rarement). Une campagne de phishing peut être une porte d'entrée pour une compromission de systèmes embarqués. De même, des actions frauduleuses sur un capteur ou une carte à puce d'un composant OT peuvent permettre de remonter jusqu'à des serveurs IT et générer des perturbations bureautiques avec des impacts financiers, légaux ou d'images non maîtrisables.

Une cyberattaque sur une infrastructure est susceptible de provoquer un effet en cascade avec une succession de dommages sur des infrastructures ou sur l'organisation elle-même. Par exemple, tout type de cyberattaque sur l'alimentation électrique ou le réseau TIC peut entraîner des coupures de courant, compromettre la sécurité, affecter les opérations et la maintenance, endommager les infrastructures et l'image de marque.

Pour parer aux cyberattaques et atténuer ou réduire leurs impacts, les procédures détaillées et mesures de protection ne sont pas toujours suffisantes ; d'une part des erreurs et des omissions peuvent survenir, d'autre part le système considéré peut évoluer (en particulier, la menace en elle-même). Pour réagir efficacement lorsqu'un incident se produit, qu'il soit sur l'OT ou l'IT, qu'il soit causé par des raisons internes ou externes,

---

[361] *CYBERSECURITY IMPERATIVES FOR VITAL RAIL NETWORKS AT OPERATIONS CONTROL CENTERS - WATERFALL*[En ligne]. [Réf. 2021]. Disponible sur https://waterfall-security.com/wp-content/uploads/Rails_OCC_CyberSecurity_eBook.pdf

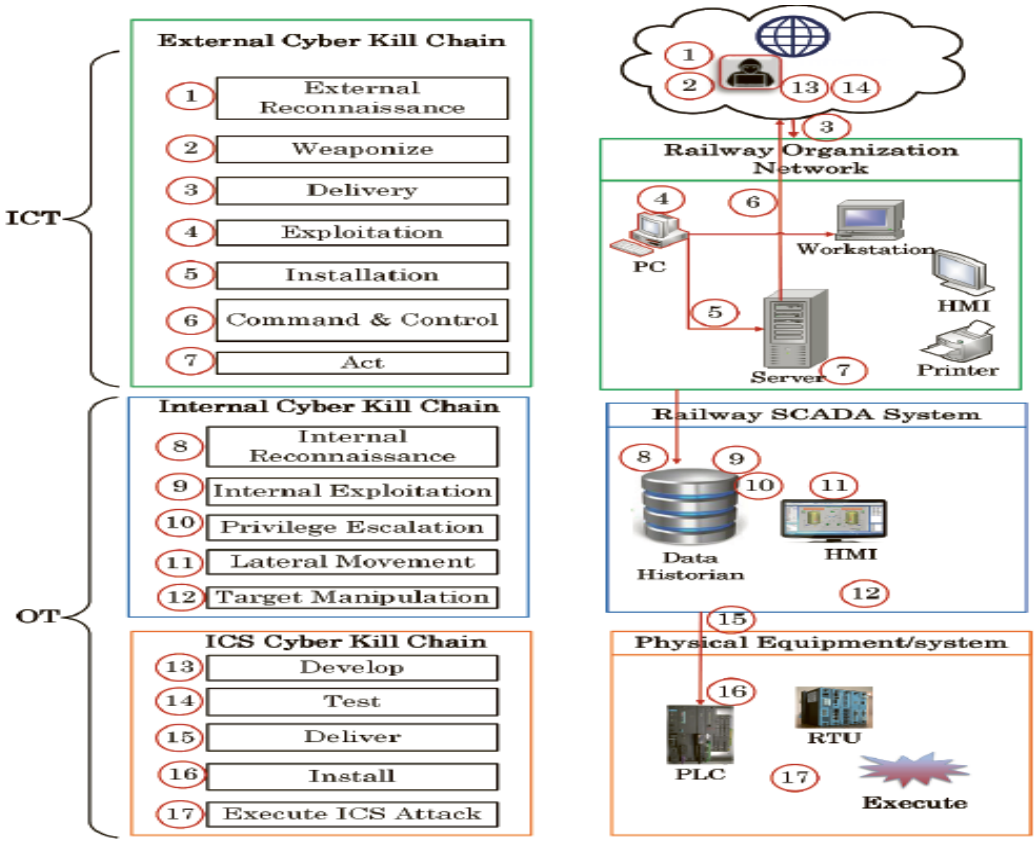
[362] *Provide your critical networks with the highest end to end security* [En ligne]. [Réf. 2021]. Disponible sur Seclab Secure Xchange Network - Seclab ICS CyberSecurity (seclab-security.com)

[363] *Thoughts on New Forrester Report: "Best Practices: Mitigating Insider Threats"* [En ligne]. [Réf. Du 28 avril 2021]. Disponible sur Best Practices: Mitigating Insider Threat

savoir se protéger ou se défendre requiert une très bonne connaissance des chemins d'attaque possibles.

Dans cette Cyber Kill Chain interne, l'attaquant suit une série d'étapes pour accéder au système de contrôle industriel (ICS), en passant des postes de travail aux serveurs par une escalade de privilèges, des déplacements latéraux, etc. (Zhou et al., 2018)

Le schéma ci-dessous[364], décrit étape par étape le cheminement d'une attaque.



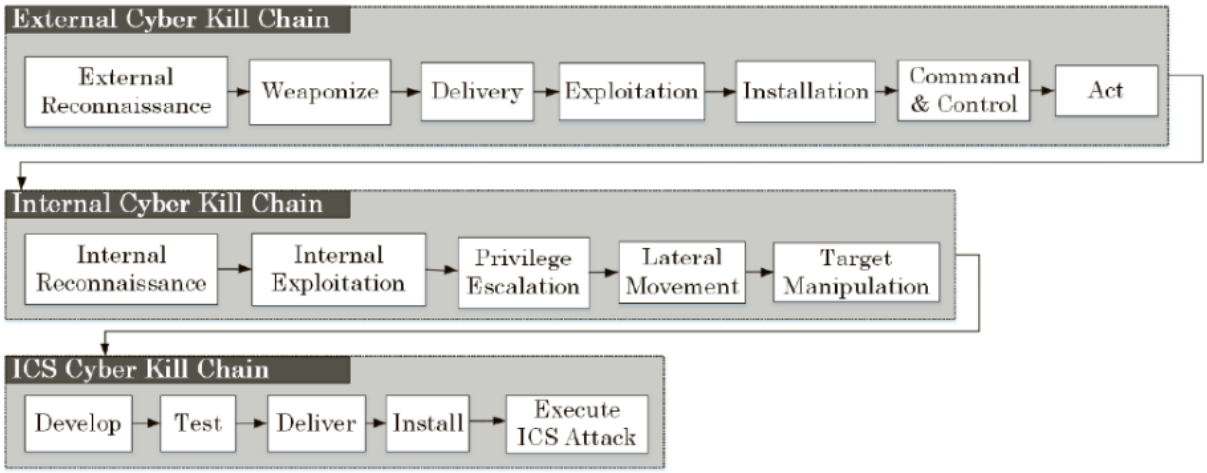
59 - Cyberattaque en plusieurs étapes dans un système SCADA ferroviaire[365]

Si l'objectif de l'adversaire est d'atteindre uniquement la zone IT, ses actions peuvent compromettre la disponibilité, l'intégrité et/ou la confidentialité (DIC) d'un ou plusieurs actifs. Dans des cas heureusement encore rares, son objectif est d'atteindre la zone OT et compromettre la sécurité, la fiabilité et/ou la disponibilité (SFD) d'un ou plusieurs actifs au sein du système ferroviaire opérationnel. Cela peut entraîner un ralentissement ou une suspension des opérations, voire un ou des accidents de train. Une fois que l'acteur malveillant se latéralise à l'intérieur du système de commande et contrôle (SCC ou OCC en anglais) du réseau ferroviaire, il peut amorcer une reconnaissance interne, avec potentiellement des accès via le LDAP (Lightweight Directory Access Protocol) aux annuaires d'entreprise, établissant une cartographie du réseau interne et une recherche de vulnérabilités (en scannant par exemple les OT pour trouver des IHM – Interface Homme Machine). Ensuite, il pourra exploiter les vulnérabilités potentielles découvertes dans les systèmes internes, immédiatement ou ultérieurement.

[365] Ravdeep Kour, *Cybersecurity in railway. A Framework for Improvement of Digital Asset Security* [Thèse de doctorat en ligne]. [Réf. de 2020]. Disponible sur https://www.diva-portal.org/smash/get/diva2:1423651/FULLTEXT01.pdf

In fine, l'attaquant pourra lancer un script malveillant, par exemple un changement de configuration dans le contrôleur logique programmable (PLC) ou du Terminal Distant (RTU), et endommager l'équipement physique. Comme il a déjà été mentionné plus haut, la compromission de la sécurité du système SCC peut entraîner des impacts importants tels que des blocages d'exploitation et d'entretien de l'infrastructure des réseaux ferroviaires, voire des accidents de train.

Le schéma ci-dessous décrit une Cyber Kill Chain unifiant l'IT et l'OT et illustre le cheminement d'une attaque de l'IT à l'OT :



60 - Chaîne de cyber-destruction étendue unifiée et de cyber-destruction ICS

VII.11. SYSTEME DE DETECTION DES INTRUSIONS

Le transport ferroviaire est un écosystème où, en l'absence de mesures appropriées et suffisantes, le fort degré de perturbation et de déstabilisation générale et l'atteinte à l'intégrité physique des personnes ont une probabilité élevée. Cet enjeu impose donc d'adopter une démarche de sécurisation en profondeur avec, en particulier, la mise en œuvre d'un système de détection d'intrusion[366] (IDS) basé sur le principe de « zéro-trust-network[367] ».

Les systèmes de détection d'intrusion regroupent 2 familles :

- Système de détection d'intrusion hôte (HIDS, Host-based Intrusion Detection System) : il analyse des données telles que les fichiers journaux, les appels système, les accès aux fichiers, le comportement des applications et des utilisateurs, etc., et génère des alertes si une intrusion a été détectée. De plus ce type d'IDS a la capacité de rechercher des modèles et signatures de cybermenaces ;
- Système de détection d'intrusion réseau (NIDS, Network-based intrusion Detection System), il s'agit généralement d'un ensemble d'appliances autonomes placées à différents points d'un réseau pour analyser tout le trafic entrant et sortant afin d'y déceler des comportements d'attaquant (patterns).

La plupart des technologies IDS modernes utilisent plusieurs méthodologies, séparées ou intégrées, pour fournir une détection plus large et plus précise.

Les principales méthodologies sont les suivantes :

---

[366] *CYRail Recommendations on cybersecuritytof rail* signalling and communication systems [En ligne]. [Réf. De septembre 2018]. Disponible sur CYRail Recommendations on cybersecurity of rail signalling and communication systems

[367] *Market Guide for Zero Trust Network Access* [En ligne]. [Réf. Du 29 avril 2019]. Disponible sur Market Guide for Zero Trust Network Access | Gartner

- Détection basée sur les signatures (SIDS, Signature-based Intrusion Detection System) : reconnaissance de programmes malveillants basés sur des modèles et des règles, eux-mêmes basés sur des bibliothèques de description d'attaques passées ;
- Détection basée sur les anomalies (AIDS, Anomaly-based Intrusion Detection System) : ce mode détecte les écarts par rapport à un modèle représentant les bons comportements ; il est souvent associé à de l'apprentissage automatique dans une phase initiale ;
- Système de Détection d'intrusion hybride (NIDPS ou HIDPS, Network-based ou Host-Based Intrusion Detection And Prevention System) : solution mixte SIDS et AIDS ; par exemple : OSSIM[368] et PRÉLUDE[369] ;

Aucune des solutions IDS actuellement disponibles sur le marché, qu'elles soient commerciales ou open-source, n'a à ce jour été spécifiquement adaptée aux chemins de fer.

VII.11.1. PRINCIPALES EXIGENCES D'UN IDS/IPS (INCIDENT DETECTION SYSTEM, INCIDENT PREVENTION SYSTEM)

Les directives européennes NIS dont la dernière version amendée en 2020 a augmenté les prérogatives des autorités nationales de cybersécurité en matière d'intervention auprès des fournisseurs Télécom. Comme l'indique Sadio Bâ coordinateur sectoriel Transport à l'ANSSI, cette possibilité d'installation des sondes de détection directement chez les FAI et la possibilité de contraindre ces FAI à l'installation à leurs frais des outils de protection en amont est une très bonne manière d'avoir une première défense périmétrique[370] ;

Les exigences attendues d'un IDS/IPS sont généralement les suivantes :

- **La précision** : capacité à détecter et distinguer les activités malveillantes des activités légitimes (réduire la masse de faux positifs). Cela contribue à ne pas se faire leurrer par les attaquants et surtout à rendre pertinentes les actions à cibler, et à les prioriser en fonction de la fréquence, du volume des types d'activités suspectes et des impacts potentiels relevés dans l'analyse de risques ;
- **La performance** : capacité d'effectuer une détection d'intrusion en temps réel ;
- **L'exhaustivité** : il ne doit pas manquer de détecter une intrusion. Cette exigence est extrêmement difficile à remplir, car il est presque impossible de détecter une attaque ayant une méthode totalement inconnue ;
- **La tolérance aux pannes** : résistance et robustesse contre les attaques malveillantes ou les erreurs ;
- **L'évolutivité** : capacité de surveiller le plus grand nombre d'événements dans une topologie de réseau hétérogène et de grande taille.

Dans le cas du système ferroviaire intégrant de l'IT et l'OT, les capteurs IDS doivent prendre en charge les protocoles de l'IT ou de l'OT ou des deux types en fonction de leur emplacement. Les informations récoltées par un IDS doivent être utilisables pour des actions de renforcement de la posture de sécurité - sinon la pertinence de cette solution et/ou de sa configuration est à revoir.

Cumuler à la fois les signatures et les anomalies est l'option la plus efficace, même si cela rend l'IDS plus complexe à gérer. L'utilisation d'un processus d'apprentissage entièrement automatisé pour créer la ligne de base du comportement peut être

[368] *AlienVault OSSIM is Trusted by Thousands of Security Professionals in 140 Countries… and Counting* [En ligne]. [Réf. 2021]. Disponible sur OSSIM: The Open Source SIEM | AlienVault (att.com)
[369] *Prelude OSS project* [En ligne]. [Réf. 2021]. Disponible sur Aperçu - PRELUDE SIEM - UNITY 360 (prelude-siem.org)
[370] Annexes I – Interview Sadio Bâ – Coordinateur Sectoriel « Transport » à l'ANSSI

risquée, si tout ou partie des systèmes était déjà compromis au moment où la ligne de base servant de référentiel a été générée. Pour atténuer ce risque, les fournisseurs d'IDS fournissent souvent des connaissances d'experts ou opérationnelles pour ajuster les règles de détection des anomalies ou préparamétrer l'IA correspondante.

Les systèmes de contrôle de l'exploitation, fonctionnant avec une infrastructure très spécifique, sont des dispositifs implantés dans les systèmes ferroviaires innovants comme les systèmes d'enclenchement électroniques, les systèmes de signalisation ECTS et les systèmes de radio mobile GSM-R. Ils permettent de stopper les tentatives de connexion par des cybercriminels. Ce type de technologie ne fonctionne cependant que sur des réseaux connectés à Internet et n'est exécutable qu'à partir de serveurs classiques (IT), comme d'autres applications classiques. Cela augmente considérablement la surface d'attaque et peut exposer à des tentatives d'intrusion par des tiers non autorisés.

Selon *Nextgov*[371], la newsletter du gouvernement fédéral américain consacrée aux technologies de l'information, des pirates informatiques ont lancé en décembre 2011 une attaque contre les ordinateurs d'une compagnie ferroviaire du nord-ouest des États-Unis qui a perturbé les signaux ferroviaires pendant deux jours. Si l'incident n'a eu aucune conséquence dramatique, il a néanmoins révélé les failles technologiques.

Les systèmes de détection des intrusions ne sont toutefois pas conçus pour bloquer les attaques. Ils se contentent de surveiller le réseau et d'envoyer des alertes aux administrateurs si une menace potentielle est détectée. A contrario, les IPS (Intrusion Prevention Système) sont conçus pour surveiller les données d'intrusion et prendre les mesures nécessaires pour éviter qu'une attaque ne se déclenche[372].

Pour répondre au besoin de proactivité et réagir de manière appropriée aux attaques avant qu'elles ne se concrétisent, Thales a développé CyberRail[373], une solution de supervision de la sécurité des réseaux. Fonctionnellement, CyberRail est en mesure de détecter, modéliser, analyser et stopper les menaces et attaques dirigées vers les systèmes ferroviaires. À l'aide de sondes, la solution analyse en continu et sans intervention humaine les flux de données du système interne et collecte les événements inhabituels. En cas d'alerte, l'opérateur identifie la nature et la localisation de l'incident et déclenche les mesures de protection prévues.

Sur la base d'analyses conjointes des risques, Thales propose aussi des solutions de sécurité complètes pour stopper les cyberattaques potentielles.

À la question "*Pensez-vous que la signalisation ferroviaire devrait être cyber-protégée avec une solution ferroviaire dédiée, ou est-ce que n'importe quelle cyber-IDS (Intrusion Detection System) le fera ?*", Israël Baron Directeur du développement des affaires chez Cervellosec[374], une des rares sociétés de cybersécurité ferroviaire (basée en Israël) fournissant des solutions qualifiées de « révolutionnaires et éprouvées » pour sécuriser les chemins de fer contre les cyberattaques, répond :

"*Pour cyber-protéger les systèmes de signalisation ferroviaire, il faudrait utiliser des technologies spécifiques au rail développées par des cyber-experts ayant une expérience ferroviaire et les meilleures pratiques* »

---

[371] *Hackers manipulated railway computers, TSA memo says* [En ligne]. [Réf. Du 23 janvier 2021]. Disponible sur Hackers manipulated railway computers, TSA memo says - Nextgov

[372] *Qu'est-ce qu'un Système de prévention des intrusions (IPS) ?* [En ligne]. [Réf. 2021]. Disponible sur Qu'est-ce qu'un Système de prévention des intrusions (IPS) ? | Forcepoint

[373] *CYBER RAIL - STOPPER NET LES CYBERATTAQUES* [En ligne]. [Réf. Du 28 juin 20116]. Disponible sur Cyber Rail - Stopper net les cyberattaques | Thales Group

[374] *Relever les défis de sécurité de l'industrie ferroviaire* [En ligne]. [Réf. 2021]. Disponible sur Cervello | Railway Cyber Security (cervellosec.com)

Selon lui : « *Les IDS proposés sur le marché aujourd'hui sont dédiés aux systèmes informatiques ou aux systèmes OT génériques. Le système de signalisation ferroviaire a une architecture compliquée et combine à la fois des environnements IT et OT. De plus, le système de signalisation est un système de systèmes et comprend une communication P2P, nécessitant une compréhension approfondie des réseaux opérationnels ferroviaires.* »

VII.12. GESTION D'INCIDENTS

Les organisations doivent définir, mettre en œuvre et tester des procédures de gestion des incidents. C'est la condition pour assurer la continuité des activités des services et des systèmes en cas d'incidents de cybersécurité. Les mesures d'atténuation visent à contenir ou à limiter l'impact des incidents de cybersécurité.

La planification de l'intervention et du rétablissement doit tenir compte des mesures de sécurité, en atténuant l'impact des attaques de cybersécurité. Pour ce faire, il faut :

- Assurer la coordination et la collaboration avec les CSIRT (Computer Security Incident Response Team) / CERT (Computer Emergency Response Team) national, public et/ou commercial et les ISACs (Cooperative Models for Information Sharing and Analysis Centers) au cours des incidents de cybersécurité, ainsi que la coordination des incidents et des crises au niveau paneuropéen ;
- Réaliser périodiquement des exercices de cyberattaque (avec une coordination de haut niveau, mais aussi technique) pour évaluer les mesures et les procédures de sécurité ainsi que la résilience de l'organisation face aux cybers incidents ;
- S'assurer de l'accès aux emplacements de stockage archivés ou aux sauvegardes en cas de compromission de l'intégrité et de la disponibilité des stockages de données en ligne ;
- Disposer de playbooks de sécurité avec des procédures détaillées pour gérer les incidents de cybersécurité et ramener les services et les systèmes à des conditions opérationnelles nominales ;
- Être en mesure de rediriger le trafic réseau vers des services redondants lors d'attaques par déni de service. ;
- Définir des procédures manuelles pour l'exploitation avec des services et des systèmes en modes de fonctionnement dégradés ;
- Définir des procédures pour traiter les atteintes à la protection des données conformément au Règlement Général sur la Protection des Données (RGPD) et à toute autre réglementation ou directive sectorielle pertinente ;
- Acquérir une cyber assurance afin de déporter partiellement le risque associé aux cyber incidents graves ;
- Contractualiser un mandat de réponse aux incidents avec une ou plusieurs entreprises spécialisées pour prévoir une capacité de débord et une expertise supplémentaire si nécessaire ;
- Veiller au partage des informations pertinentes sur la gestion de crise avec d'autres organisations, y compris les fournisseurs de la chaîne d'approvisionnement des services ferroviaires ;
- Définir des procédures pour le partage d'informations sur les incidents de cybersécurité avec les parties prenantes concernées, y compris des procédures de notification des incidents conformément à la directive N/5 (directive 2016/1148 de l'UE concernant des mesures visant à atteindre un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'ensemble de l'Union européenne).

VII.13. GESTION DE CRISE

« *Nous avons l'habitude de gérer les pannes dans le domaine ferroviaire, mais gérer des crises cyber nécessite de nouveaux schémas de pensées* », observe Gilles Berthelot[375](Directeur de la Sûreté Numérique du Groupe SNCF).

La résilience du système est directement liée au plan de continuité des activités d'un opérateur de transport. Il est essentiel pour un tel acteur, dont la vie de milliers de clients dépend, de fournir un service ininterrompu et fiable. Sa résilience sera mesurée sur sa capacité à mitiger la perturbation des services et à revenir rapidement à son état initial d'origine après un incident.

La gestion de crise procède d'une démarche de résilience globale quand un incident ne peut être résolu dans les délais acceptables prévus dans le plan de gestion d'incidents, ou lors de la survenue d'un événement aux impacts graves et multiformes.

La cellule de crise aura pour vocation de répondre à une situation exceptionnelle par un dispositif exceptionnel de gestion de l'information et de l'activité – au sens notamment de « temporaire » – et permettre ainsi une gestion optimale (organisée, efficace et rapide) des situations de crise, selon les deux principes clés de la gestion d'une crise : **coordination et réactivité**[376].

VII.13.1. DISPOSITIF DE CRISE

L'enjeu d'un dispositif de gestion de crise SSI est de traiter rapidement et efficacement des événements afin de limiter leur atteinte au fonctionnement, aux ressources, aux clients et à l'image de l'entreprise ferroviaire. Ce dispositif doit comprendre un schéma d'alerte permanent, court et redondé sur des médias autres que ceux de l'entreprise. Les exigences de subsidiarité, de complémentarité et de transparence doivent en être des socles solides :

- La subsidiarité : la gestion de la crise doit pouvoir être opérée à l'échelon le plus proche ou le plus bas couvrant l'ensemble du périmètre impacté ;
- La complémentarité : elle est d'autant plus importante dans le contexte de convergence IT-OT où la mobilisation et la coordination des cellules de crise de l'ensemble des périmètres impactés sont importantes ;
- La transparence : un partage d'information clair et non biaisé entre les intervenants de la gestion de la crise est l'une des clés du succès et de l'efficience d'une gestion de crise.

VII.13.2. LES MOYENS NECESSAIRES

Il s'agit de valider la logistique en s'assurant que la crise peut être efficacement gérée avec les outils à disposition, sinon il convient de revoir et aligner les équipements au besoin. Dès que la crise est confirmée, il faut s'assurer que les moyens pour la gérer sont opérationnels :

- Canaux de communication : vérifier les options possibles et fonctionnelles, celles pouvant être compromises ;
- Logistique opérationnelle : pour avoir les informations, les outils pour faire ou faire faire, sur place ou à distance ;
- Logistique basique : salle(s) de crise et tous les moyens élémentaires prenant en compte la possibilité de ne plus avoir accès au SI voire ne plus avoir de SI du tout ;

---

[375] *Profil Linkedin* [En ligne]. [Réf. 2022]. Disponible sur gilles BERTHELOT - Directeur Sécurité Numérique Groupe SNCF (GROUP CISO* : Chief information and security officer) - SNCF | LinkedIn

[376] *Qu'est-ce qu'une cellule de crise ?* [En ligne]. [Réf. 2021]. Disponibled sur Cellule de crise : organisation et management | LaFrenchCom

- Logistique pour s'inscrire dans le temps *(repas, repos, remplacement).* La crise va perdurer...

VII.13.3. LES ETAPES NECESSAIRES

L'un des enjeux majeurs dans une gestion de crise impliquant les domaines IT et OT est l'ordonnancement des priorités, car dans ce type de crise tout le monde se veut prioritaire. Le besoin de coordination se trouve en particulier entre les acteurs IT et OT, qui peuvent être confrontés à des enjeux antagonistes, l'un estimant la nécessité de stopper une propagation d'attaque et l'autre ayant l'exigence d'assurer la sécurité. Évaluer le bénéfice-risque[377] est un exercice qui se prépare en amont de toute crise et qui nécessite d'avoir défini en amont qui seront responsables des prises de décision de différents niveaux.

La cellule de gestion de crise doit, de fait, disposer des éléments d'information durant les différentes étapes de sa gestion. Par exemple, être en mesure d'avoir les contacts ayant le pouvoir décisionnaire de l'arrêt d'un SI critique dans les plus brefs délais.

Les phases à mettre en place sont les suivantes :

- Prise en compte de tous les éléments du contexte, facilitant la prise de décisions rapides et pertinentes : ceci est déterminant dans la capacité de traiter l'attaque dans les meilleurs délais ;
- Réalisation d'une première analyse ayant pour objectif de donner une vision claire sur une première stratégie de préservation de l'activité de l'entreprise voire de l'entreprise ; il s'agit de détourer et qualifier les problèmes, confirmer la cyberattaque et en identifier l'origine, définir les mesures conservatoires, recueillir les premiers éléments d'analyse et d'enquête ;
- Lancement d'une communication de début de crise, alerte de la direction, prise de contact avec les autorités dont celles de contrôle (ANSSI en France), alertes de différentes équipes préalablement identifiées qui seront décisionnaires, régulatrices, exécutantes ou informées ;
- Mise en œuvre des plans pour contenir et remédier à l'attaque :
  - ✓ Une cellule opérationnelle de monitoring comprenant des ressources des équipes du Security Operation Center (SOC) qui sont à l'origine de la détection de l'attaque et devant actualiser le suivi de manière continue ; le SOC et le Network Operation Center (NOC) monitorent respectivement la sécurité des systèmes d'information et les activités du système d'information ;
  - ✓ Une cellule opérationnelle d'intervention ou de réponse à incident, afin de mettre en place les contre-mesures. Dans le cas d'une structure importante ou appartenant à un groupe, la cellule pourra prendre la forme d'un Computer Security Incident Response Team (CSIRT) ;
- Mise en place d'une communication transversale en relation avec la direction Marketing, juridique et communication ;
- Journalisation au travers d'un registre de crise de tous les événements survenus, des décisions et des actions mises en œuvre avec leurs porteurs et leur timeline.

VII.13.4. L'APRES-CRISE

Le retour d'expérience à froid (Retex), permet la création ou la mise à jour de fiches réflexes sur les actions à mener lors d'une crise cyber.

---

[377] *rapport bénéfices/risques article extrait de l'ouvrage « Larousse Médical »* [En ligne]. [Réf. 2021]. Disponible sur https://www.larousse.fr/encyclopedie/medical/rapport_b%C3%A9n%C3%A9ficesrisques/185222

VII.14. DEFENSE, CENTRE UNIFIE DE SECURITE OPERATIONNELLE

Il est, dans une entreprise, un lieu où la sécurité des réseaux d'entreprise (IT) et celle des réseaux opérationnels (OT) convergent plus vite qu'ailleurs. On parle du centre des opérations de sécurité, plus communément appelé SOC (Security Operations Center) et plus précisément SOC unifié du fait de sa capacité à traiter la sécurité réseau d'entreprise et opérationnel.

Pour Eddy Thésée, Vice-Président Cybersécurité chez Alstom, *un SOC ferroviaire doit se démarquer de la valeur ajoutée ferroviaire qu'il embarque. Le choix doit être drivé par deux choses : premièrement, comment interpréter un incident de cybersécurité dans le contexte ferroviaire, qui n'a rien à voir avec un incident de sécurité dans une voiture, un bâtiment, ou dans un autre écosystème et deuxièmement quelle est la démarche adaptée pour résoudre cet incident dans un tel contexte*. À la question de savoir quelle est la bonne tactique de mise en place d'un tel SOC, il nous répond « *C'est une bonne préconisation de séparer le SOC corporate du SOC industriel. Par contre pour le SOC industriel il est important de réunir au même endroit des personnes IT et OT pour mutualiser les connaissances et compétences et surtout avoir une force d'analyse et de réaction rapide et la plus globale possible en cas d'incident* »[378]

Un SOC unifié doit pouvoir développer les capacités suivantes :

- Notification et réponse aux incidents ;
- Rétroaction sur les résultats de la réponse aux incidents ;
- Analyse des erreurs. Il s'agit de s'assurer que les erreurs sont éliminées et que des mesures correctives sont prises ; de s'assurer que ces mesures n'ont pas été elles-mêmes compromises et que toutes les mesures prises ont été dûment autorisées ;
- La gestion des incidents doit comprendre la prévention, la détection, l'analyse, la résolution des problèmes et la continuité des fonctions automatiques ferroviaires. Tous les incidents liés à la sécurité de l'information doivent être surveillés et documentés en permanence.

61- Le centre d'opérations de sécurité axé sur l'intelligence[379]

En raison de clivages culturels et organisationnels entre le monde des SI dits d'entreprise et le SI industriel, il peut être difficile d'obtenir un accord sur les formats de rapport d'incident et d'alerte des différents opérateurs de SOC impliqués dans différents segments des écosystèmes de l'entreprise[380].

Dans le cadre d'un système industriel OIV ou pas, la mise en place d'un SOC unifié est donc un levier stratégique de recherche d'excellence opérationnelle. Ce type d'organisation est justifiée pour deux bonnes raisons :

---

[378] Annexes – Interview Eddy Thésée, VP Cybersécurité Alstom

[379] *Need Of Security Operations Over SIEM* [En ligne]. [Réf. Du 10 avril 2019]. Disponible sur https://www.slideshare.net/Siemplify/need-of-security-operations-over-siem

[380] *CYbersecurity in the RAILway sector* [En ligne]. [Réf. De décembre 2016]. Disponible sur D1.1 – Project Quality Assurance Plan

- **Stratégique et tactique** : un SOC unifié rend possible la synergie entre les experts de sécurité OT et de cybersécurité (IT). Il permet une analyse systémique et holistique des risques des deux mondes ;
- **Excellence opérationnelle** : l'efficacité face aux menaces passe par la mutualisation des intelligences et l'utilisation d'un référentiel commun des assets, des vulnérabilités, des menaces et des attaques.

Dans le cas des OIV, les exigences contraignantes auxquelles ils sont soumis posent la question des séparations et spécialisations des SOC, étant donné que tous les SI ne sont pas forcément régis par les LPM ou les arrêtés sectoriels. Pour Orange Cyber Défense, un OIV dispose de deux choix[381] :

- N'avoir qu'un seul SOC, qui surveille l'ensemble du SI (SIIV compris) ;
- Mettre en place deux SOC : l'un pour son SIIV, l'autre pour le reste du SI. C'est le choix privilégié chez la plupart des OIV., pour éviter que les règles à respecter pour le/les SIIV ne le deviennent pour l'ensemble du SI, alourdissant les processus et restreignant l'accès à certaines informations, avec les impacts financiers qu'une telle extension induit.

VII.15. CYBER-RESILIENCE, MAINTIEN EN CONDITION DE SECURITE

VII.15.1. CYBER-RÉSILIENCE

Les définitions foisonnent pour définir ce terme. Nous en présentons deux qui nous paraissent appropriées :

« La cyber résilience, est la capacité d'une entreprise à savoir adopter une approche globale d'anticipation et d'acceptation qu'elle peut être la cible d'une cyberattaque à tout moment. [382] »

« La *Cyber-résilience est la capacité d'une entreprise à maintenir son objectif principal et son intégrité face aux cyberattaques. Une entreprise cyber-résiliente est une entreprise qui peut prévenir, détecter, contenir et se récupérer d'une pléthore de menaces graves contre les données, les applications et l'infrastructure informatique. Une entreprise cyber-résiliente garantit la continuité, la gestion et la reprise après sinistre avec des opérations de sécurité de manière holistique.* [383]»

Il est illusoire, au mieux une gageure qui coûte cher, de chercher à atteindre le risque zéro par un arsenal de mesures techniques et organisationnelles de protection. Les écosystèmes vivent et de nouvelles vulnérabilités peuvent y apparaître, soit en raison de leur obsolescence, soit en raison des développements de techniques des adversaires, le plus courant étant une combinaison dans le temps de ces deux facteurs.

Un processus de cyber-résilience est donc stratégique et doit s'inscrire dans l'ADN de toute entreprise pour la préservation de son patrimoine vital et la continuité de ses services en limitant les impacts potentiels d'une attaque. Ce concept recouvre tous les périmètres : organisation des équipes, processus opérationnels, machines, données, etc.

Une gouvernance globale de la cybersécurité par les risques impliquant l'IT et l'OT doit pouvoir déclencher sans délai des travaux de protection, de détection, mais aussi de

---

[381] *OIV et PDIS : tout ce qu'il faut savoir – Orange Cyberdéfense*[En ligne]. [Réf. 2019]. Disponible sur OIV et PDIS : tout ce qu'il faut savoir | Le Blog d'Orange Cyberdefense

[382] *COMMENT PASSER DE LA CYBERSÉCURITÉ À LA CYBER RÉSILIENCE ?* [En ligne]. [Réf. Du 30 juillet 2020]. Disponible sur Comment passer de la Cybersécurité à la Cyber Résilience ? - TEHTRIS

[383] *Apprendre à prospérer face aux menaces- Bob SULLIVAN* [En ligne]. [Réf. Du 17 septembre 2015]. Disponible sur Learning to thrive against threats | Ponemon-Sullivan Privacy Report (ponemonsullivanreport.com)

capacité à pouvoir se relever d'un incident. L'effort et la rapidité de rétablissement sont fonction des impacts de la non-disponibilité des valeurs métiers et des services identifiés lors des phases conjointes d'analyse de risques.

C'est bien l'approche proactive de la cybersécurité qui est mise à l'épreuve dans la cyber-résilience sur tous les systèmes en cas de cyber événement indésirable. Pour ce faire, quatre principaux objectifs (repris du rapport Cyrail) sont à diligenter sans délai : anticiper, résister, récupérer et évoluer.

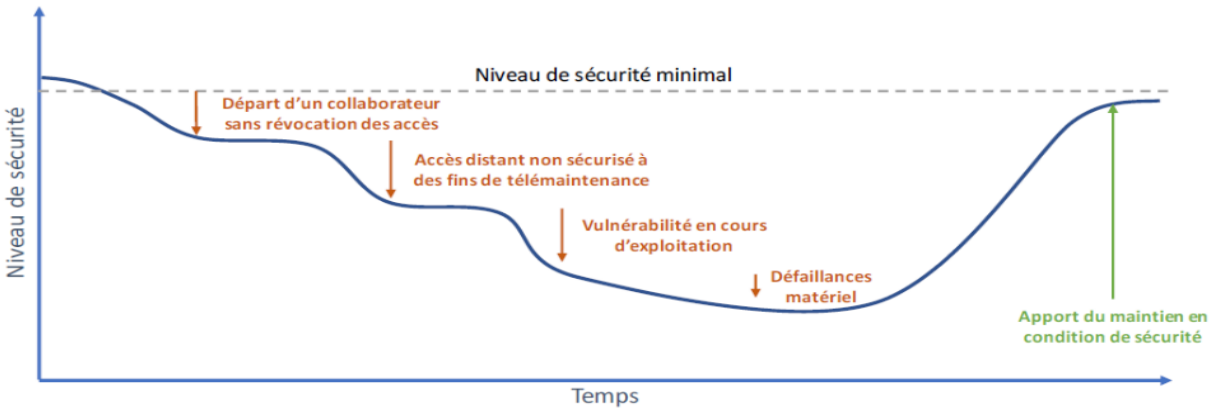
- **Anticiper** : Afin d'anticiper et de surmonter avec succès une attaque, il faut une compréhension complète de l'environnement de sécurité de l'entreprise ou du système, c'est-à-dire ses informations, ses actifs (humains ou non), ses composants, ses risques et ses vulnérabilités ;
- **Résister** : Pour la cyber-résilience, résister, c'est maintenir les fonctions métiers essentielles malgré l'exécution réussie d'une attaque par un adversaire ;
- **Remédier / récupérer :** Il s'agit de la détermination des dommages et de la restauration des capacités. Le système doit pouvoir contrer l'attaque en attendant qu'elle soit traitée, pour entrer ensuite dans la phase de **récupération** ;
- **Évoluer :** au fil du temps, il peut être essentiel de transformer les processus existants ou même de réorganiser le système pour s'adapter à l'évolution de la menace.

L'expérience d'Ian Maxwell, responsable des systèmes de contrôle des trains à l'Office of Rail and Road (ORR) du Royaume-Uni pour la gestion d'une crise majeure, est intéressante : selon lui le plan d'urgence doit être activé et doit se faire en deux phases ; confinement et récupération. « *Sur le chemin de fer, nous avons beaucoup d'expérience en matière de confinement et de récupération. La récupération exige généralement que le personnel assiste, évalue et répare les dommages. Pendant ce temps, l'exploitation du chemin de fer est modifiée jusqu'à ce que l'équipement défaillant soit pleinement fonctionnel. Les techniciens et les opérateurs ont des règles et des procédures à suivre qui ont été développées au fil des ans. Ceux-ci aident à assurer la sécurité du chemin de fer pendant les opérations dégradées et pendant les enquêtes et les réparations. Lorsque le système informatique devient défectueux, la même logique devrait s'appliquer. Le confinement et la récupération sont toujours les principes à suivre. La tactique de gestion d'incident dans le chemin de fer est la même, que l'événement soit causé par des sources internes ou externes* »[384]

VII.15.2. MCS – MAINTIEN EN CONDITION DE SÉCURITÉ

Le maintien en conditions de sécurité vise à s'assurer que les systèmes respectent les règles et mesures de sécurité préalablement définies (au travers de la PSSI qui elle-même découle des analyses de risques). Les systèmes étant amenés à évoluer, le maintien en conditions de sécurité (MCS) évolue avec ces systèmes. En effet, au cours du cycle de vie du système, le niveau de sécurité décline au cours du temps pour des raisons diverses telles que l'évolution des usages, l'évolution des menaces, la découverte de nouvelles vulnérabilités, etc.

[384] *Is the railway sufficiently prepared for a cyber-attack?* [En ligne]. [Réf. Du 24 février 2020]. Disponible sur Is the railway sufficiently prepared for a cyber-attack? (globalrailwayreview.com)



62 - Évolution du niveau de sécurité d'un système au cours du temps[385]

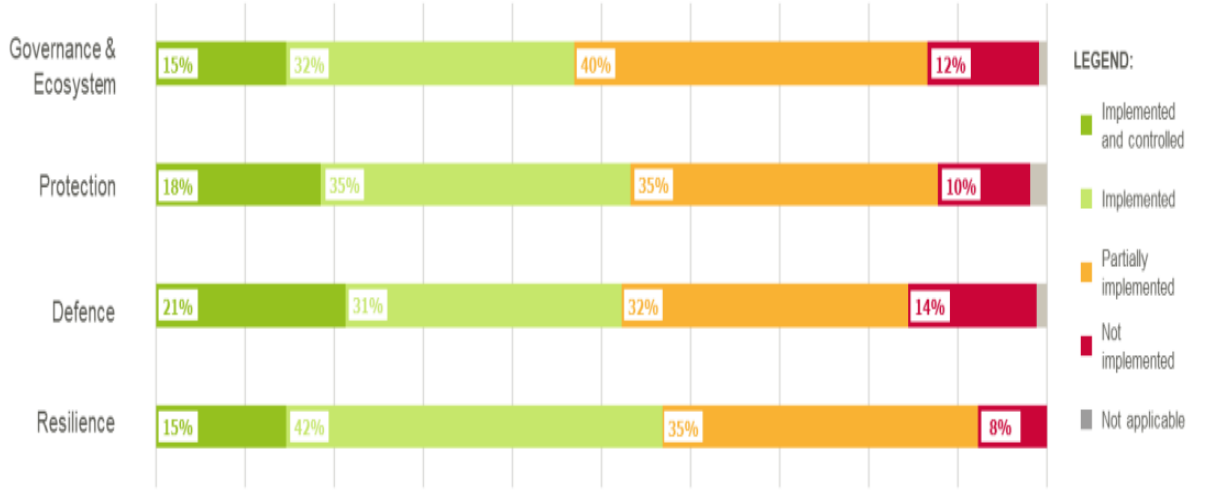
Le niveau de sécurité peut aussi évoluer au cours du temps en raison de l'évolution de la réglementation entraînant l'apparition de nouvelles exigences de sécurité : le système désormais non conforme reçoit alors un nouveau niveau de sécurité arbitrairement plus bas dans la nouvelle échelle d'évaluation.

Pour garantir un maintien en condition opérationnelle en toute circonstance, chaque écosystème ferroviaire doit être doté d'un système de Maintien en Condition de Sécurité (MCS). Le MCS vise à gérer les mesures, dispositifs et processus de sécurité des systèmes tout au long de leur cycle de vie afin qu'ils restent au même niveau de risque accepté. Le maintien en conditions de sécurité d'un système permet ainsi d'assurer la continuité du service fourni par le système en réduisant la probabilité d'occurrence d'une panne, comme un arrêt de production dû à un incident de sécurité. Le maintien en conditions de sécurité est interdépendant et fortement couplé au MCO dont il constitue généralement un sous-ensemble. Un certain nombre d'actions (qui peuvent parfois relever d'un MCO) sont à entreprendre en permanence pour maintenir le niveau de sécurité des systèmes à un niveau acceptable.

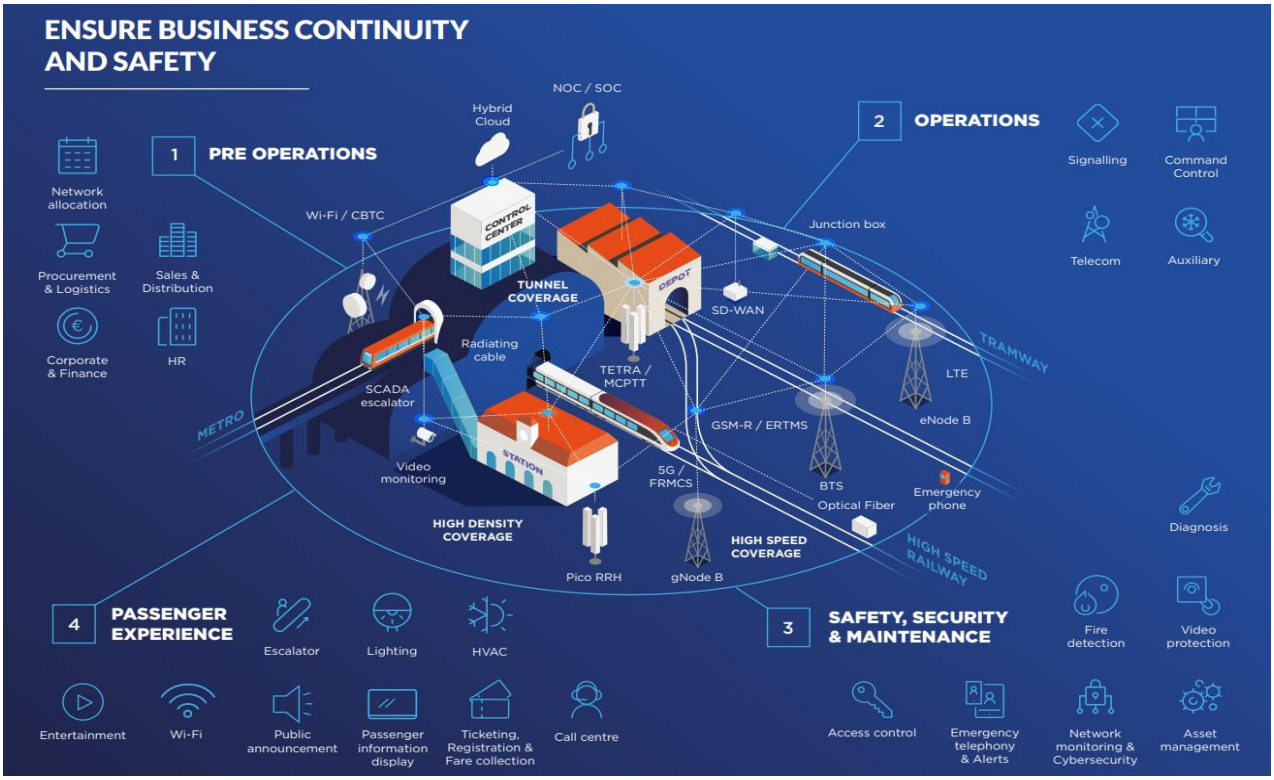
Vu la complexité des interconnexions des SI du réseau ferroviaire (comme on peut le voir dans le schéma ci-dessous[386]), assurer une cyber-résilience globale est un sujet stratégique et un programme d'ampleur à adresser au plus haut niveau du management.

Dans le graphique ci-dessous, tiré du rapport de l'ENISA[387], force est de constater que des axes de progrès existent. Le niveau de mise en œuvre de la résilience dans le secteur ferroviaire est à hauteur de 57% avec 42% d'acteurs qui n'ont pas été éprouvés ou ne contrôlent pas leur dispositif de résilience, et 43% qui l'ont partiellement ou pas du tout mis en œuvre, ce qui interpelle À l'heure où les menaces se multiplient et se diversifient.

[385] *Guide cybersécurité des systèmes industriels - CLUSIF* [En ligne] [Réf. De février 2021]. Disponible sur Guide cybersécurité des systèmes industriels.pdf)
[386] *Resilient transport infrastructure No trust without cybersecurity* [En ligne]. [Réf. De janvier 2021]. Disponible sur systra-cybersecurity-brochure-2021-01.pdf
[387] *Security measures in the Railway Transport Sector* [En ligne]. [Réf. De novembre 2020]. Disponible sur https://www.enisa.europa.eu/publications/railway-cybersecurity/at_download/fullReport



63 - Vue de haut niveau du niveau de mise en œuvre des mesures de sécurité pour les OSE dans le secteur ferroviaire[388]



64 - Continuité des services et la sûreté au vu de la complexité du ferroviaire[389]

Avec les techniques d'ingénierie du chaos, il est possible de tester la robustesse d'un écosystème en rendant inopérants de manière aléatoire les systèmes en production.

---

[388] *Security measures in the Railway Transport Sector* [En ligne]. [Réf. De novembre 2020]. Disponible sur https://www.enisa.europa.eu/publications/railway-cybersecurity/at_download/fullReport

[389] *CYBERSÉCURITÉ : POUR DES INFRASTRUCTURES DE TRANSPORT PLUS SÛRES ET PLUS RÉSILIENTES* [En ligne]. [Réf. Du 01février 2021]. Disponible sur Cybersécurité : pour des infrastructures de transport plus sûres et plus résilientes - Groupe (systra.com)

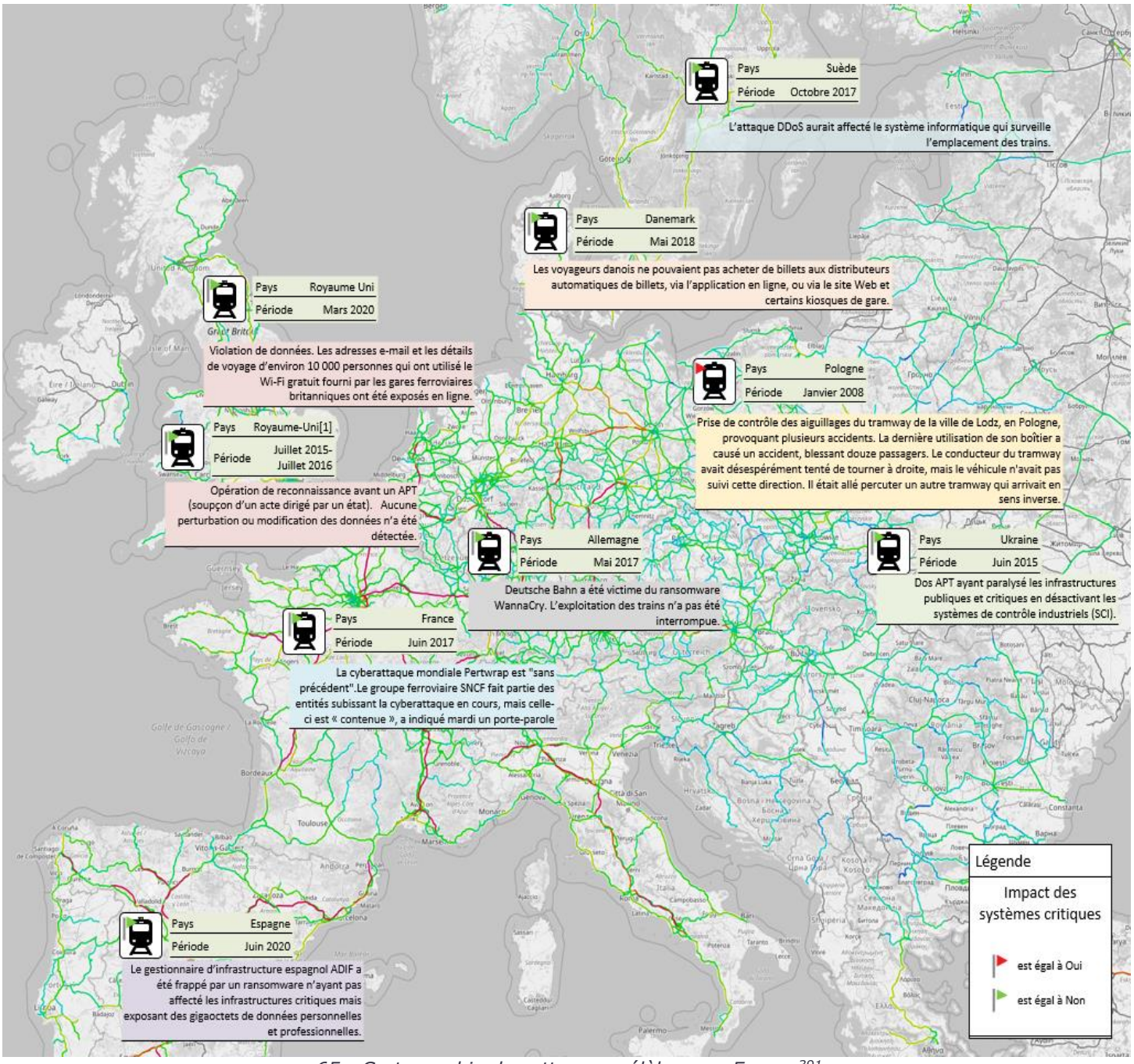
L'utilisation du Chaos Monkey[390] pourrait aider certaines entreprises à mieux se préparer et renforcer leur résilience.

VII.16. CYBERATTAQUES FERROVIAIRES ET IMPACTS DANS LE TEMPS

Aujourd'hui les chefs d'entreprises sensibilisés à la Cybersécurité ne se demandent pas s'ils vont être la cible d'une cyberattaque, mais quand ? Le nombre d'entreprises touchées par la cybercriminalité est toujours plus important de mois en mois et d'année en année avec conséquences parfois désastreuses, et cela quel que soit leur taille.

[390] *L'ingénierie du chaos expliquée – Scott CAREY* [En ligne]. [Réf. Du 13 mai 2020]. Disponible sur Qu'est-ce que Chaos Monkey ? L'ingénierie du chaos expliquée | InfoMonde (infoworld.com)

Les cyberattaques du système ferroviaire touchent selon les informations publiques beaucoup plus que les systèmes d'information IT qu'OT. La carte ci-dessous montre quelques célèbres cyberattaques réussies perpétrées au sein de l'Union européenne.



65 - Cartographie des attaques célèbres en Europe[391]

Selon Antony Couzian-Marchand, ancien commandant de gendarmerie, Magistrat de la cour des comptes et Directeur Général de GALLICE International, société de sûreté et sécurité, interrogé par le CNFCE (centre de formation pour entreprise), les enjeux et les conséquences des cyberattaques sont de divers ordres[392] :

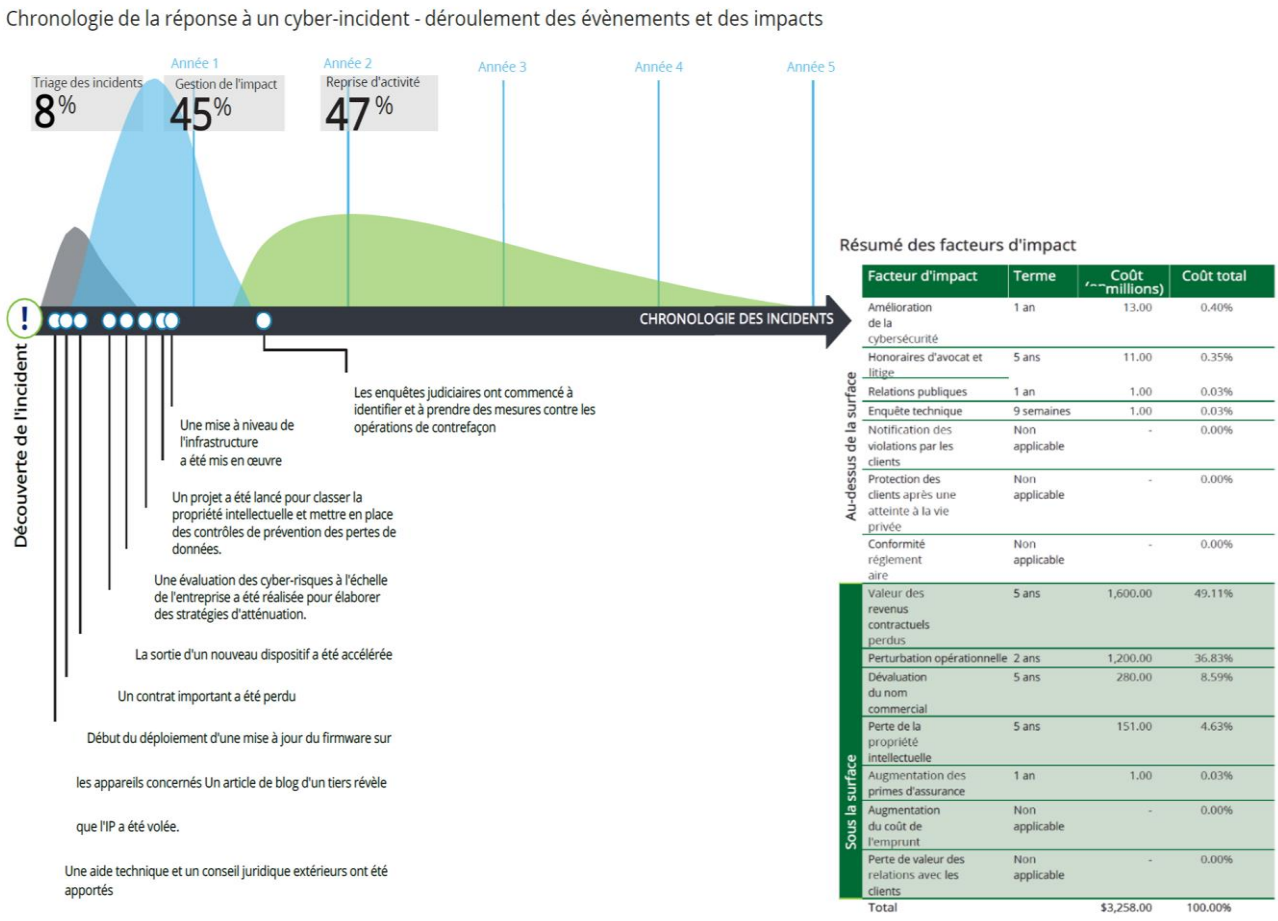
- Une paralysie des systèmes (donc une perte d'exploitation à court terme et d'image à moyen terme) ;

[391] source interne
[392] *Les conséquences d'une cyberattaque sur une entreprise – CNFCE* [En ligne]. [Réf. 2021]. Disponible sur Les conséquences d'une cyberattaque sur une entreprise - CNFCE

- Le vol ou la perte de données sensibles ;
- La création de brèches dans un système de sécurité ;
- L'exposition à un chantage (ransomware…) ;
- L'atteinte à la réputation (en particulier quand la sécurité est un élément essentiel de la politique de communication de l'entreprise) ;
- Un préjudice commercial (dans le cas précis de vol de données sensibles en matière concurrentielle).

Toujours selon lui, les cyberattaques les plus dévastatrices pour une entreprise (TPE/PME ou grande entreprise), quel que soit le moyen de pénétration dans le système (faille, attaque, virus) sont généralement liées au piratage, au vol, à la destruction de données très sensibles. Une prise de contrôle à distance de systèmes industriels automatisés de type ICS/IACS/SCADA peut avoir également de graves conséquences. Ces systèmes sont utilisés dans différents secteurs comme l'énergie, la distribution d'eau, chaîne de fabrication, raffinerie…
Dans une étude393 de 2020, Deloitte a simulé plusieurs scénarios avec une estimation des risques et de l'impact financier associés aux cyberattaques.
Dans l'un des scénarios, pour lequel un fabricant américain de technologies a été victime d'une exfiltration de données stratégiques par ce qui semble être une cyberattaque perpétrée par un État, il a fallu 5 ans à cette entreprise pour se rétablir avec par ailleurs de graves conséquences. Catégorisés comme cyberattaque de vol de propriété intellectuelle, les dommages globaux, tous facteurs d'impact confondus, ont dépassé 3,2 milliards de dollars sur une période de cinq ans. À première vue les coûts directs sur le vol à proprement parler (impacts « au-dessus de la surface ») ne représentaient que 1% du coût total de l'attaque à 5 ans. Le bilan au bout de 5 ans a révélé tous les coûts dits "sous la surface" représentant 99% et appartenant aux domaines suivants : dévaluation du nom commercial, perte de la valeur des revenus contractuels, perturbation opérationnelle et perte de propriété intellectuelle.

[393] *Sous la surface d'une cyberattaque : Éviter les collisions L'application commerciale de la quantification des cyberrisques* [En ligne]. [Réf. 2020]. Disponible sur us-beneath-the-surface.pdf (deloitte.com)



66 - Chronologie de réponse aux cyberincidents - déroulé des événements et impacts[394]

VIII. BILAN ET RECOMMANDATIONS

VIII.1. BILAN

La sécurité des transports autant pour les biens et marchandises que des personnes est une des préoccupations essentielles et historiques des acteurs ferroviaires.

Se prémunir des menaces intentionnelles et non intentionnelles (accidentelles) liées directement à l'utilisation du système et à son fonctionnement intrinsèque est un enjeu capital. Pour cela, le secteur est soumis au respect des référentiels internationaux IEC 61508[395] pour les systèmes électriques, électroniques et électroniques programmables déclinés pour la sécurité ferroviaire sous les normes EN 50126, EN 50128 et EN 50129[396]. L'application de ces normes approuvées par l'instance de régulation européenne CENELEC[397], contribue à minimiser ou à contenir les pannes et les défaillances pouvant

[394] *Sous la surface d'une cyberattaque : Éviter les collisions L'application commerciale de la quantification des cyberrisques* [En ligne]. [Réf. 2020]. Disponible sur us-beneath-the-surface.pdf (deloitte.com)
[395] *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité* [En ligne]. [Réf. D'avril 2010]. Disponible sur IEC 61508
[396] *Sécurité Ferroviaire : les EN 50126, 50128 et 50129 et leurs évolutions* [En ligne]. [Réf. 2021]. Disponible sur https://www.isit.fr/fr/article/en-50128-repondre-aux-exigences-de-la-norme-de-surete-de-fonctionnement-logiciel-ferroviaire.php
[397] *Le Comité européen de normalisation électrotechnique est l'un des trois organismes européens de normalisation.* [En ligne]. [Réf. 2021]. Disponible sur https://www.cencenelec.eu/about-cenelec/

conduire à l'émergence d'un risque jugé inacceptable lors de la phase d'analyse préliminaire.

Un enjeu majeur réside dans la maîtrise des cycles de vie des produits, solutions et applications dans un contexte de convergence IT OT pour concilier les exigences de cybersécurité IT des exigences de sûreté OT.

Une autorité de régulation a en charge l'homologation de toute nouvelle application en tenant compte du contexte dans le lequel le système devra évoluer. Ce qui rend les processus de développement et donc plus largement les cycles de vie des solutions longs et coûteux proportionnellement au niveau d'intégrité à atteindre. En France, les accréditations de fonctionnement sont délivrées par l'EPSF (Établissement public de sécurité ferroviaire) pour les chemins de fer « grandes lignes » ou par l'autorité STRMTG (Service technique des remontées mécaniques et des transports guidés) pour les applications urbaines, métro et tramway. L'évolution, la correction, ou le rajout de nouvelles fonctionnalités du système existant passe obligatoirement par une réévaluation du niveau de risque, de l'impact et de la non-innocuité de l'évolution sur le niveau de sécurité actuel. C'est à ce prix que la validité du certificat d'accréditation peut être prolongée.

Utilisant historiquement des solutions propriétaires des constructeurs, les systèmes et solutions utilisés dans le secteur ferroviaire embarquent de plus en plus des NTIC (nouvelles technologies de l'information et de la communication). Cette unification technologique entre le domaine ouvert du grand public et le domaine industriel, le domaine ferroviaire embarqué en l'occurrence, a fortement augmenté au cours du temps l'exposition des applications aux risques de malveillance. Comment arriver à concilier le besoin de saisir les opportunités économiques qu'apportent les NTIC avec l'agilité qui les accompagne tout en garantissant les niveaux de sûreté et de sécurité ferroviaire chers à l'industrie ferroviaire ? Tel est le double enjeu majeur.

La France définit des opérateurs d'importance vitale (OIV) pour le transport ferroviaire et pour d'autres secteurs économiques au travers d'une loi de programmation militaire (LPM) ce qui démontre la portée et l'importance de ce domaine d'activité.

La progression exponentielle des cyberattaques, la convergence IT/OT, les changements de paradigme des groupes mafieux sont certainement les enjeux les plus critiques dans le domaine des cybermenaces et pour lesquels la filière doit investir le plus dès maintenant et dans les années à venir.[398]

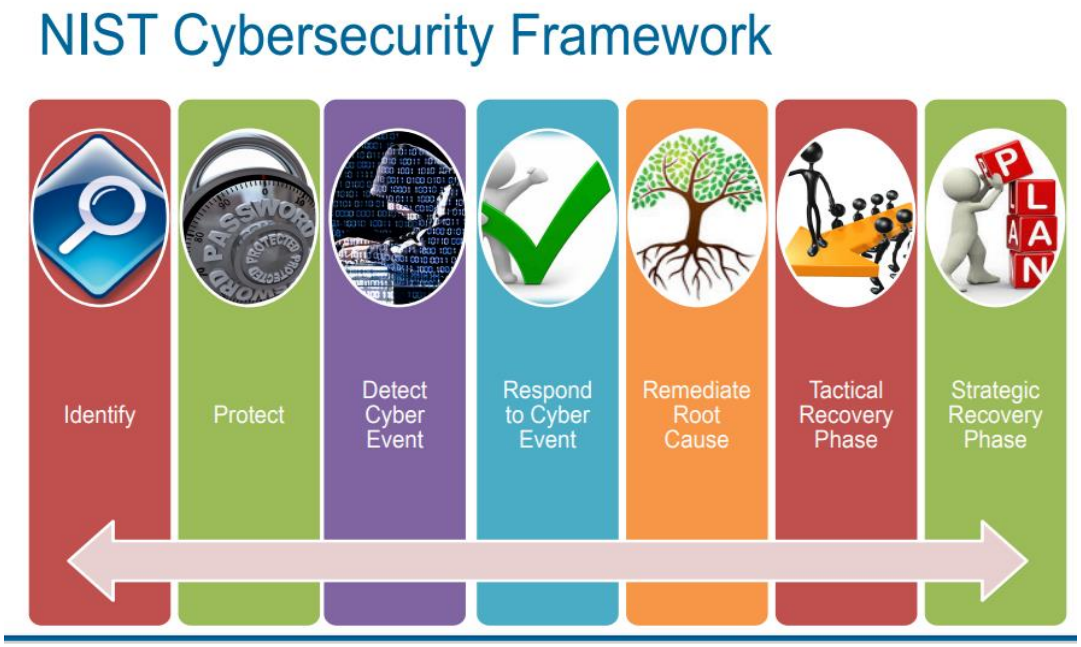
[398] *FUTURS ENJEUX ET CHALLENGES* [En ligne]. [Réf. Du 10 octobre 2020]. Disponible sur Le contrôle/commande ferroviaire : Futurs enjeux et challenges | Techniques de l'Ingénieur (techniques-ingenieur.fr)

VIII.2. RECOMMANDATIONS PRATIQUES

- ✓ **Piloter par les risques**
  - Cartographier les actifs IT et OT liés et vérifier leurs mises à jour ; identifier les cibles critiques en fonction de l'analyse d'impact ;
  - Cartographier les flux ;
  - Étudier les menaces et les vulnérabilités, en prévoyant le scénario du pire ;
  - Faire une revue de risques à fréquence régulière
- ✓ **Sensibiliser et former les employés à la cybersécurité**
  - Hygiène de base, responsabilités, processus et prévention sur les menaces internes
  - Formation des collaborateurs OT à la cybersécurité
- ✓ **Adopter la démarche de Security-by-design**
- ✓ **Implémenter les principes de zero-trust-network et d'architecture en « zones et conduits »**
  - Segmenter les zones et implémenter une protection périmétrique avec pare-feux, passerelles et/ou diodes de données. En particulier, sécuriser les systèmes obsolètes : cloisonnement, durcissement, surveillance spécifique,
  - procéder à la spécification, l'implémentation et une revue régulière des règles de filtrage.
  - Adopter le principe du moindre privilège et renforcer l'unification des contrôles pour les accès physiques et logiques selon une approche basée sur les rôles (RBAC),
  - établir des processus rigides d'accès physique aux équipements OT,
  - sécuriser les accès filaires et sans fil,
- ✓ **Appliquer les mécanismes de résilience de l'IT à l'OT ou définir des contre-mesures organisationnelles et les faire éprouver**
  - Assurer la redondance matérielle,
  - Avoir des plans de sauvegardes et de restauration éprouvés : sauvegardes, sur des supports non connectés sur le réseau et stockés hors ligne, des systèmes d'exploitation, des programmes automates et des firmwares,
  - disposer de processus de reprise sur incident,
  - Mettre en place un dispositif de gestion de crise et faire des exercices réguliers.
- ✓ **Mettre en œuvre des moyens de détection** tels que les systèmes de prévention de la détection d'intrusion et centralisation de la collecte des journaux (logs applicatifs et systèmes de type Syslog)
- ✓ **Déployer des outils de corrélation des événements** pour des besoins d'investigation et de veille CTI (Cyber Threat Intelligence)
  - Analyser le trafic à la recherche de menaces et de vulnérabilités.
- ✓ **Définir un plan de Maintien en Condition de Cybersécurité**
  - Définir les fenêtres de maintenance pour anticiper et planifier les actions de MCS,
  - Mettre en place des équipements dédiés à la maintenance : équipements sécurisés, durcis d'un point de vue sécurité, antivirus installés et à jour,
  - Renforcer et corriger la configuration des systèmes (Modifier la configuration par défaut des équipements et applicatifs constituant le système industriel.
- ✓ **Faire des audits de sécurité OT/IT réguliers**

Nous avons repris ici les recommandations réputées (d'après les bonnes pratiques) renforcer la cybersécurité industrielle. Elles sont alignées sur des normes de sécurité ISO 27001, IEC 62443 et conformes également aux directrices NIS (Network and Information Security) de l'ENISA, de l'Agence Nationale Française de Sécurité des Systèmes d'Information (ANSSI) en France et du National Institute of Standards and Technology de NIST (USA) et pour la plupart partagées par Clusif. Le leitmotiv : la défense en profondeur !

Comme le précise SYSTRA groupe mondial d'ingénierie et de conseil, spécialisé dans les transports publics et les solutions de mobilité notamment ferroviaires, les implémentations de ces recommandations doivent prendre en compte les spécificités OT et les normes de sécurité telles que IEC 61508 et méthodes de sécurité communes (CSM) par ERA[399]. Les exigences OT par ordre de priorité décroissante sont les suivantes : Intégrité et Disponibilité puis Confidentialité



67 - Framework de cybersécurité NIST[400]

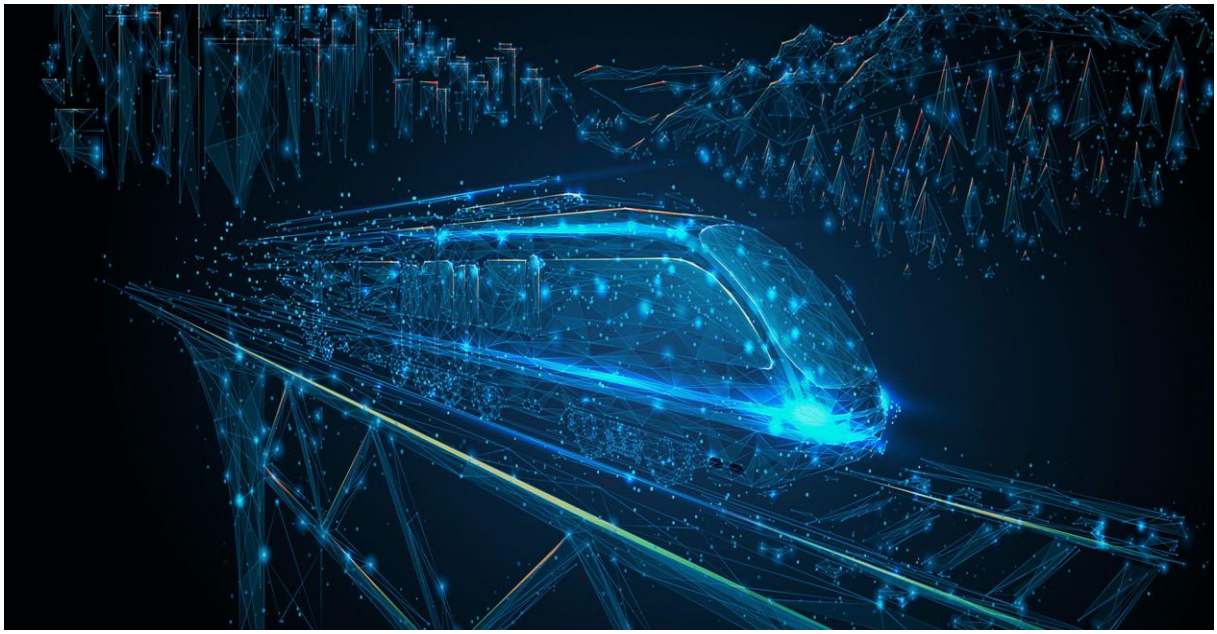
À termes

- ✓ Vers une analyse convergente de risques : actuellement les deux mondes IT et OT font leur analyse de risques chacun de leur côté. S
- ✓ À la suite d'échanges avec la Responsable cybersécurité industrielle, la recommandation qui en ressort est de repenser l'analyse de risques pour qu'elle tienne compte des risques spécifiques aux deux écosystèmes, ceux liés à la convergence, les chemins d'attaque descendants, mais aussi montants… Quid de la IEC/CEI 62443

[399] *CYBERSÉCURITÉ : POUR DES INFRASTRUCTURES DE TRANSPORT PLUS SÛRES ET PLUS RÉSILIENTES* [En ligne]. [Réf. Du 1er février 2021]. Disponible sur Cybersécurité : pour des infrastructures de transport plus sûres et plus résilientes - Groupe (systra.com)

[400] *Se remettre d'un incident de cybersécurité - Que faire avant et après ? - NIST* [En ligne]. [Réf. Du 1er décembre 2017]. Disponible sur Recovery Webinar (nist.gov)

REFERENCES BIBLIOGRAPHIQUES, INTERVIEWS, ANNEXES



i401

401 https://www.teleste.com/news-and-insights/articles-and-blogs/vsi/blog/beware-future-railway-mobile-communication-system-is-almost-here/

I. REFERENCES BIBLIOGRAPHIQUES

La liste ci-dessous est une partie des références bibliographiques significatives des notes de bas page du document.

Type	N°	Références
Article	**[1]**	CB, **Le ballast se comporte comme un milieu hétérogène - [en ligne]. [Réf. du 3 Janv. 2018]. Disponible sur « Le ballast se comporte comme un milieu hétérogène » - Construction Cayola**
Rapport	**[2]**	ERRAC**, Vision Rail 2050. Le Rail - l'Epine Dorsale de la Mobilité en Europe – [en ligne]. [Réf. de Févr. 2021]. Disponible sur 122017_errac_rail_2050_vision.pdf (uic.org)**
Guide	**[3]**	CLUSIF **- Guide de cybersécurité des systèmes industriels [en ligne]. Disponible sur 20210303-Guide-cybersécurité-des-systemes-industriels.pdf (clusif.fr)**
Article	**[4]**	**L'AMDEC (Analyse des modes de défaillance, de leurs effets et de leur criticité** *– En Anglais FMECA) est une méthode d'analyse prévisionnelle de la fiabilité qui permet de recenser les défaillances potentielles dont les conséquences affectent le bon fonctionnement du moyen de production ou du bien d'équipement étudié***. – [En ligne]. [Réf. de Févr. 2020]. Disponible sur** AMDEC Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (piloter.org)
Article	[5]	Jacques de La Rivière**, Sécurité by-design : analyse des 3 grands principes [en ligne]. [Réf.]. Disponible sur** Sécurité by-design : analyse des 3 grands principes - Silicon
Site	**[6]**	**L'initiative S2R / Shift2Rail [en ligne]. Disponible sur** À propos - Shift2Rail
Site	**[7]**	**Agence de l'Union européenne pour la cybersécurité (ENISA) [en ligne]. [. Disponible sur** Agence de l'Union européenne pour la cybersécurité (ENISA) | Union européenne (europa.eu)
Article	**[8]**	**Prelude est un SIEM français (Security Information & Event Management). C'est une solution complète de gouvernance de la sécurité des systèmes d'information. [en ligne]. Disponible sur** Prelude SIEM | Logiciel de supervision de sécurité | Le SIEM européen (prelude-siem.com)
Article	[9]	Anthony Di Prima**, Architecture de sécurité des SI Industriels : de la théorie à la pratique. Cloisonnement et segmentation : standards et réglementations se mettent d'accord. [en ligne]. [Réf. de 2014]. Disponible sur** Architecture de sécurité des SI Industriels : de la théorie à la pratique - RiskInsight (riskinsight-wavestone.com)
Support conférence	**[10]**	UIC**, IRRB webinar autonomous technologies in rail -anticipating expectations. [en ligne]. [Réf. De Juin 2021]. Disponible sur** ato_webinar.pdf (uic.org)
Article	**[11]**	**Cybersécurité des environnements industriels. La segmentation du système d'information est-elle un rempart incontournable pour éviter les attaques ? [Réf. du 29 Juin 2021]. Disponible sur** Forum International de la Cybersécurité 2021 : Comment aborder la cybersécurité d'un système industriel ? | SPIE ICS (spie-ics.com) AvisdexpertSPIEICSSegmentationdesreseaux.pdf (forum-fic.com).
Rapport	[12]	Joseph Blankenship, Claire O'Malley with Stephanie Balaouras, Heidi Shey, Alexis Bouffard, Peggy Dostie, **Best Practices - Mitigating Insider Threat. Processes: The Zero Trust Security Playbook. [en ligne]. [Réf. de mars 2021]. Disponible sur** Best Practices: Mitigating Insider Threat (forrester.com)
Article	[13]	Rédaction Digital SNCF**, SNCF - Big Data : les projets marquants de 2020** *Avec 10 millions de données récoltées quotidiennement, le Big Data est au cœur des priorités de SNCF. De nombreux outils permettant de les faire fructifier ont ainsi été mis en place en 2020, afin d'améliorer toujours plus les services offerts aux voyageurs***. [en ligne]. Disponible sur** Big Data : les projets marquants de 2020 | #DIGITALSNCF
Site	**[14]**	CER **- La voix des chemins de fer européens – [en ligne]. [Réf. du 17 Nov. 2021]. Disponible sur** CER:Home | The Voice of European Railways
Site	**[15]**	**Sécurisation des chemins de fer. Protection des personnes.** *La cybersécurité ferroviaire permet de garantir un transport sûr et fiable des passagers et des marchandises***. [en ligne].. Disponible sur** Cervello | Railway Cyber Security (cervellosec.com)
Texte législatif	**[16]**	**Chapitre III : Des atteintes aux systèmes de traitement automatisé de données (Articles 323-1 à 323-8) – Version en vigueur en Novembre 2021 [en ligne]. [Réf. de Novembre 2020]. Disponible sur** Chapitre III : Des atteintes aux systèmes de traitement automatisé de données (Articles 323-1 à 323-8) - Légifrance (legifrance.gouv.fr)
Article	**[17]**	Bastien L. **Cloud : quelles sont les principales menaces et comment s'en protéger. [en ligne]. [Réf. du 23 Août 2019]. Disponible sur** Citymapper - L'appli de transport réinventée Cloud : quelles sont les principales menaces et comment s'en protéger (lebigdata.fr)
Article	**[18]**	Linkbynet**, Voyage vers le cloud en 6 grandes étapes -. [en ligne]. [Réf. du 8 mars 2021]. Disponible sur** Cloud Assessment, auditez votre éligibilité à migrer dans le Cloud (linkbynet.com)
Article	**[19]**	**Comment détecter et se protéger des attaques Evil Twin (jumeau maléfique) – [en ligne]. [Réf. de mars 2019]. Disponible sur** Comment détecter et se protéger des attaques Evil Twin (jumeau maléfique) (titanhq.fr)

Type	N°	Références
Article	**[20]**	Wavestone**, Comment évaluer efficacement sa maturité en cybersécurité ? [en ligne]. [Réf. de 2020]. Disponible sur** Comment évaluer efficacement sa maturité en cybersécurité ? - RiskInsight (riskinsight-wavestone.com)
Article	**[21]**	NOVIPRO**, Comment intégrer un réseau OT industriel à un réseau IT ? [en ligne]. [Réf. du 2 Marsr 2020]. Disponible sur** Comment intégrer un réseau TO industriel à un réseau TI? (novipro.com)
Article	**[22]**	Tehtris**, Comment passer de la Cybersécurité à la Cyber Résilience ? – TEHTRIS [en ligne]. [Réf. du 10 octobre 2021]. Disponible sur** Comment passer de la Cybersécurité à la Cyber Résilience ? - TEHTRIS
Guide	**[23]**	Clara Morlière, CIGREF**, Convergence IT – OT. Un rapprochement fructueux des systèmes d'information et ses systèmes industriels. en ligne]. [Réf. de décembre 2019]. Disponible sur** Convergence IT – OT : Un rapprochement fructueux des systèmes d'information et des systèmes industriels (cigref.fr)
Article	[24]	Khobeib Ben Boubaker**, Réseaux IT-OT : les raisons d'une convergence délicate [en ligne]. [Réf. du 18 nov. 2019]. Disponible sur** Convergence OT-IT : les défis cyber des systèmes industriels | Stormshield
Article	**[25]**	**Waterfall. Cybersecurity imperatives for vital rail networks at operations control centers [en ligne]. [Réf. du 30 Juin 2020]. Disponible sur** Rails OCC CyberSecurity eBook (waterfall-security.com)
Site	**[26]**	ENISA **- CSIRTs in Europe.** *Depuis plus de dix ans, l'ENISA soutient les États membres et les communautés CSIRT pour construire et faire progresser leurs capacités CSIRT***. [en ligne]. [Réf. de 2021]Disponible sur** CSIRTs in Europe — ENISA (europa.eu)
Site	**[27]**	ENISA **- Cyber Exercises***. L'ENISA mène un large éventail d'activités dans le domaine des cyber exercices. Ce sujet est lié aux activités de l'ENISA sur la gestion des cyber crises***. [en ligne]. [Réf. de 2021]. Disponible sur** Cyber Exercises — ENISA (europa.eu)
Article	**[28]**	KPMG **– Cyber Maturity Assesment. Évaluer la maturité de votre entreprise face aux menaces. – [en ligne]. [Réf. du 28 Janv. 2020]. Disponible sur** Cyber Maturity Assessment (assets.kpmg)
Article	**[29]**	Thales **- Cyber Rail - stopper net les cyberattaques – [en ligne]. [Réf. du 28 Juin 2016]. Disponible sur** Cyber Rail - Stopper net les cyberattaques | Thales Group
Rapport	**[30]**	ENISA **- Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations [en ligne]. [Réf. de Janv. 2016]. Disponible sur** Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations — ENISA (europa.eu)
Guide	**[31]**	**Working Group CYSIS IT/ OT-Security for Internet of Railway Things (IoRT)– [en ligne]. [Réf. du 18 Janv. 2021. Disponible sur** Cyber Security for Railways - ETCS Aspekte (haselnuss-projekt.de)
Support conférence	**[32]**	ENISA **- Cyber security solution platform project. [en ligne]. [Réf. de mars 2021]. Disponible sur** Cyber Security Solution Platform (europa.eu)
Article	**[33]**	SYSTRA**, Cybersécurité : pour des infrastructures de transport plus sûres et plus résilientes. [en ligne]. [Réf. de février 2021]. Disponible sur** Cybersécurité : pour des infrastructures de transport plus sûres et plus résilientes - Groupe (systra.com)
Article	[34]	Orange**, Cybersécurité : quelles sont les principales menaces en 2021 ? [en ligne]. [Réf. du 18 oct.2021]. Disponible sur** Cybersécurité : quelles sont les principales menaces en 2021 ? (orange.fr)
Article	[35]	Keith Barrow, **Cybersécurité : protéger les chemins de fer contre l'évolution des menaces. [en ligne]. [Réf. du 15 avril 2018]. Disponible sur** Cybersécurité : se prémunir contre l'évolution des menaces | International Railway Journal (railjournal.com)
Site	**[36]**	CYRAIL **CYbersecurity in the RAILway sector***. Les infrastructures ferroviaires évoluent vers des systèmes plus intelligents, connectés, centrés sur l'utilisateur et collaboratifs. Si cette évolution présente de nombreux avantages pour le secteur et les utilisateurs, elle offre également de nouvelles possibilités aux cybercriminels et aux terroristes***. [en ligne]. Disponible sur** CYRail project
Guide	**[37]**	**CYRail recommendations on cybersecurity of railway signaling and communication systems. [en ligne]. [Réf. de Sept. 2018]. Disponible sur** CYRail Recommendations on cybersecurity of rail signalling and communication systems
Article	[38]	Milena Dimitrova, **De nouvelles vulnérabilités 5G permettent des attaques par déni de service et par l'homme du milieu. [en ligne]. [Réf. du 17 Déc. 2020]. Disponible sur** De nouvelles vulnérabilités 5G permettent une attaque par déni de service et par l'homme du milieu- (sensorstechforum.com)
Article	[39]	Dan French, **Décomposition des normes de cybersécurité industrielle. ISA99/ISA/CEI62443 et NERC-CIP. [en ligne]. [Réf. de 2020]. Disponible sur** Décomposition des normes de cybersécurité industrielle | Anixter
Texte législatif	**[40]**	**Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. [en ligne]. [Réf. du 19 Juil. 2016]. Disponible sur** Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union
Article	**[41]**	**Edge computing : définition et cas d'usage de la technologie***. L'edge computing se traduit en français par "traitement des données à la périphérie du réseau". Le terme, principalement utilisé dans l'IoT, désigne ainsi l'analyse des données au plus près de l'objet.* **[en ligne]. [Réf. du 11 Janv.2021]. Disponible sur** Edge Computing

Type	N°	Références
Article	**[42]**	**EU Policy Cycle - EMPACT. EMPACT 2022+ Fighting crime together.** *EMPACT signifie Plate-forme multidisciplinaire européenne contre les menaces criminelles. Il introduit une approche intégrée de la sécurité intérieure de l'UE, impliquant des mesures allant des contrôles aux frontières extérieures, de la coopération policière, douanière et judiciaire à la gestion de l'information, l'innovation, la formation, la prévention et la dimension extérieure de la sécurité intérieure, ainsi que des partenariats public-privé où approprié***. [en ligne]. [Réf. du 14 Déc. 2021]. Disponible sur** Empact
Article	**[43]**	**En route pour la transformation digitale | Le Rail – [en ligne]. [Réf. du 27 Juil. 2021]. Disponible sur** En route pour la transformation digitale | Le Rail
Site	**[44]**	ENISA **–Sécuriser la société de l'information en Europe - [en ligne]. [Réf. de 2021]. Disponible sur** ENISA - En français — ENISA (europa.eu)
Site	**[45]**	*ERFA représente les compagnies ferroviaires privées et indépendantes de toute l'Europe.* *L'association a été créée à Bruxelles en 2002 par une poignée de nouveaux opérateurs de fret ferroviaire. Elle a été établie comme la voix des nouveaux entrants pour soutenir la vision européenne d'un marché ferroviaire libéralisé***. [en ligne]. Disponible sur** ERFA - European Rail Freight Association - (erfarail.eu)
Site	**[46]**	*European Rail Research Advisory Council (ERRAC) a été créé en 2001 avec l'objectif ambitieux de créer un organisme européen unique ayant à la fois la compétence et la capacité d'aider à faire évoluer le secteur ferroviaire européen et à le rendre plus compétitif, en favorisant une innovation accrue et en orientant les efforts de recherche au niveau européen***. [en ligne]. Disponible sur** ERRAC
Rapport	**[47]**	ERRAC**, Rail 2030 – Research and innovation priorities. Brief version. [en ligne]. [Réf. du 24 Nov. 2021]. Disponible sur** ERRAC_2030.pdf
Rapport	**[48]**	**– Rail 2050 vision. rail - The backbone of Europe's mobility [en ligne]. [Réf. du 21 mai 2019]. Disponible sur** 122017_errac_rail_2050_vision.pdf (uic.org)
Article	[49]	Arnaud Soullié**, Fun with Modbus 0x5A.** *Le protocole Modbus est un standard de communication utilisé dans les SI industriels. Développé dans les années 70 sur liaison série RS-485, il est désormais très répandu dans sa version TCP utilisable sur une liaison Ethernet classique***. [en ligne]. [Réf. de 2017]. Disponible sur** Fun with Modbus 0x5A (riskinsight-wavestone.com)
Site	**[50]**	**La Société Industrielle Lesaffre choisit le TMS (Transport Management System) de Generix Group pour piloter son écosystème transport [en ligne]. Disponible sur** Generix Group est un expert de la Supply Chain Collaborative
Site	**[51]**	**Profil LinkedIn de Gilles BERTHELOT Directeur Sécurité numérique du groupe SNCF – 2021 [en ligne]. Disponible sur** gilles BERTHELOT - Directeur Sécurité Numérique Groupe SNCF (GROUP CISO* : Chief information and security officer) - SNCF | LinkedIn
Article	**[52]**	CGI **- Gouvernance de la sécurité des TI. Une approche globale [en ligne]. [Réf. de 2016]. Disponible sur** Gouvernance de la sécurité des TI - Une approche globale (cgi.com)
Guide	**[53]**	**Maîtriser la SSI pour les systèmes industriels en ligne]. [Réf. de Juin 2012 []. Disponible sur** Guide_securite_industrielle_Version_finale-2.pdf (ssi.gouv.fr)
Article	[54]	Aliya Sternstein**, Hackers manipulated railway computers, TSA memo says. [en ligne]. [Réf. du 23 Janv. 2012]. Disponible sur** Hackers manipulated railway computers, TSA memo says - Nextgov
Site	**[55]**	Judit Sandor**, International Train Operation. Shift2Rail Joint Undertaking Project Officer for T4R, opened the event by highlighting that rail plays an important role, … [en ligne]. Disponible sur** Home - Railnet Europe, Rail Net Europe (rne.eu)
Site	**[56]**	**UIC - International union of railways [en ligne]. Disponible sur** Home | UIC - International union of railways
Site	**[57]**	UNIFE**, Horizon2020 project de UNIFE [en ligne]. Disponible sur** HORIZON2020 Projects - UNIFE
Article	**[58]**	Olivier Castellani, Jean-Marc Pourchier, Sandrine Chrun et Jean-Marie Cloarec**, Une Matrice de risque, pourquoi faire ? [en ligne]. [Réf. du 23 oct. 2014]. Disponible sur** Une matrice de risque : Pour faire quoi ? (inist.fr)
Site	**[59]**	Shift2Rail**, About S2R = Shift2Rail.** *Shift2Rail est la première initiative ferroviaire européenne à rechercher des solutions axées sur la recherche et l'innovation (R&I).* **[en ligne] Disponible sur** About S2R - Shift2Rail
Site	**[60]**	Ecologie.gouv.fr, **Référentiel RSE en Logistique [en ligne]. [Réf. du 25 Sept. 2018]. Disponible sur** R├®f├®rentiel RSE en logistique version compl├¿te.pdf (ecologie.gouv.fr)
Rapport	**[61]**	Commission Européenne**, Décennie numérique de l'Europe : objectifs numériques pour 2030 [en ligne]. [Réf. du 2030]. Disponible sur** Décennie numérique de l'Europe: objectifs numériques pour 2030 | Commission européenne (europa.eu)
Rapport	**[62]**	Verizon **- 2019 Data Breach Investigations Report. [en ligne]. [Réf. du mai 2019]. Disponible sur** 2019-data-breach-investigations-report.pdf (verizon.com)
Site	**[63]**	ERA**, Agence de l'Union européenne pour les chemins de fer (ERA) [en ligne]. Disponible sur** ERA (europa.eu)
Article	**[64]**	EU Parliament**, Communication from the commission to the European parliament, the council, the european economic and social committee and the committee of the regions. 2030 Digital Compass:**

Type	N°	Références
		the European way for the Digital Decade [en ligne].[Réf. du 09 mars 2021] Disponible sur communication-digital-compass-2030_en.pdf (europa.eu)
Article	**[65]**	**RSE : Une dimension Sociale ou Sociétale. Le concept de RSE est apparu dans les années 50 aux États-Unis dans la littérature consacrée aux entreprises sous le nom de Corporate Social Responsibility. [en ligne]. [Réf. de 2012]. Disponible sur** RSE : Une dimension Sociale ou Sociétale - Le Blog RH
Article	**[66]**	Dominique Grusso**, Transition numérique - industrie du futur La cybersécurité s'enseigne à l'Institut d'Informatique Appliquée. [en ligne]. [Réf. du 21 Janv. 2021]. Disponible sur** Cybersécurité ou les enjeux d'une souveraineté numérique | CCI Maine et Loire
Rapport	**[67]**	**CYbersecurity in the RAILway sector. D1.1 – Project Quality Assurance Plan– [en ligne]. [Réf. de décembre 2016]. Disponible sur** https://projects.shift2rail.org/download.aspx?id=84660a15-e3e2-4f7c-a11b-bfbad84ed734
Article	**[68]**	Alexandre**, Clause 4.2 : Attentes Des Parties Intéressées – ISO 27001 – [en ligne]. [Réf. du 27 Juil. 2021]. Disponible sur C**lause 4.2 : Attentes Des Parties Intéressées - ISO 27001 - Protectam
Document pédagogique	**[69]**	EPSF **- Les signaux. Les régimes d'exploitation des lignes. Les systèmes d'espacement des trains[en ligne]. [Réf. du 05 Juil. 2017]. Disponible sur** https://securite-ferroviaire.fr/sites/default/files/users/reglementations/pdf/document-pedagogique-signaux-regimes-exploitation-v1.pdf
Article	**[70]**	Nancy Mead**, The Common Criteria.** *Les niveaux d'évaluation 1 à 7 de la norme Critères communs* **[en ligne]. [Réf. du 10 août 2006, revu le 05 Juil. 2013] Disponible sur** The Common Criteria | CISA
Norme internationale	**[71]**	**Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements IEC 61508-1. [en ligne]. [Réf. de Avril 2010]. Disponible sur** info_iec61508-1{ed2.0}b.pdf
Article	**[72]**	**Le cabotage ferroviaire. [en ligne]. Disponible** sur Le cabotage ferroviaire - Autorité de régulation des transports (anciennement Arafer) (autorite-transports.fr)
Article	**[73]**	Pierre Berthelet**, La directive SRI 2 (NIS 2). [en ligne]. [Réf. du 3 mars 2021]. Disponible sur** secu-interieure: Directive "SRI 2" : l'Europe crée un CyCLONe pour gérer les crises cyber (securiteinterieurefr.blogspot.com)
Site	**[74]**	*More than 200.000 technical experts from industry, associations, public administrations, academia and societal organizations are involved in the CEN and CENELEC network*. **[en ligne]. Disponible sur** CEN-CENELEC - CEN-CENELEC (cencenelec.eu)
Article	**[75]**	**Mémo CERTitude - Les systèmes industriels.** *Système informatisé/numérique réalisant de manière automatique des traitements, à partir d'informations collectées par des capteurs, ayant pour effets des actions sur des organes physiques*. **[en ligne]. [Réf. de Sept. 2019] Disponible sur** Mémo CERTITUDE - Les systèmes industriels (certitudenumerique.net)
Rapport	**[76]**	Alain BOUILLE, **Rapport CESIN - Baromètre de la cyber-sécurité des entreprises. Vague 6 [en ligne]. [Réf. de Janvier 2021]. Disponible sur** https://www.cesin.fr/document/view/4e0928de075538c593fbdabb0c5ef2c3
Site	**[77]**	**Organisme de formation CNFCE.** *Depuis sa création en 2005, le Centre National de la Formation Conseil en Entreprise a conforté son savoir-faire dans le domaine de la formation professionnelle et continue*. **[en ligne].. Disponible sur** Présentation de notre organisme de formation - CNFCE
Rapport	**[78]**	Rapport ENISA **- RAILWAY CYBERSECURITY. Security measures in the Railway Transport Sector [en ligne]. [Réf. de Nov. 2020]. Disponible sur** https://www.enisa.europa.eu/publications/railway-cybersecurity/at_download/fullReport
Article	**[79]**	Frédéric Gouardères et Christina Ratcliff**, Une stratégie numérique pour l'Europe. [en ligne]. [Réf. de Oct. 2021]. Disponible sur** Une stratégie numérique pour l'Europe | Fiches thématiques sur l'Union européenne | Parlement européen (europa.eu)
Rapport	**[80]**	Arren Yan**, 2020 State of Operational Technology and aCybersecurity Report. [en ligne]. [Réf. du 08 Août 2021]. Disponible sur** State of Operational Technology and Cybersecurity Report (fortinet.com)
Article	**[81]**	Emma Boyle**, UK rail network attacked by hackers four times in a year. [en ligne]. [Réf. du 13 Juillet 2016]. Disponible sur** UK rail network attacked by hackers four times in a year | The Independent | The Independent
Article	**[82]**	INRS **- Prévenir les collisions engins-piétons. La place des dispositifs de détection et d'aide visuelle. [en ligne]. [Réf. du 17 Juin 2015]. Disponible sur** https://www.inrs.fr/dms/inrs/CataloguePapier/ED/TI-ED-6083/ed6083.pdf
Article	**[83]**	**Les normes dans le monde d'aujourd'hui [en ligne]. Disponible sur** COPOLCO (iso.org)
Article	**[84]**	Fortinet**, Sécuriser l'OT : enjeux stratégiques et mise en conformité des systèmes industriels critiques [en ligne]. [Réf. de 2021]. Disponible sur** Sécuriser l'OT : enjeux stratégiques et mise en conformité des systèmes industriels critiques - Le Monde Informatique
Article	**[85]**	Jean-François Lecole. *Étude prospective sur la filière matériel roulant ferroviaire horizon 2015 –2025.* Rapport Novembre 2015 [En ligne]. Disponible sur https://www.observatoire-metallurgie.fr/secteurs/ferroviaire**.**

Type	N°	Références
Article	**[86]**	Ilaria Grasso Macola, **Is cybersecurity in rail more important now than ever? [Réf. du 22 mai 2021]. Disponible sur** Is cybersecurity in rail more important now than ever? (railway-technology.com)
Article	**[87]**	Dan Roessler**, Simplifier la convergence IT / OT [en ligne]. [Réf. du 3 mai 2021]. Disponible sur** 3 moyens de simplifier la convergence IT / OT | Rockwell Automation France
Site	**[88]**	ANSSI **- Certification critères communs [en ligne]. Disponible sur** Certification Critères Communs | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
Site	**[89]**	ANSSI **– Glossaire -** Point d'Importance Vitale (PIV), Opérateur d'Importance Vitale (OIV) **[en ligne]. Disponible sur** Glossaire | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
Site	**[90]**	ANSSI **- Directive Network and Information System Security (NIS) [en ligne]. Disponible sur** Directive Network and Information Security (NIS) | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
Site	**[91]**	ANSSI **- Opérateurs de services Essentiels (OSE) [en ligne]. Disponible sur** FAQ – Opérateurs de services essentiels (OSE) | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
Article	**[92]**	Vincent Nicaise**, STORMSHIELD - IEC-62443. Le standard incontournable de la cybersécurité industrielle. [en ligne]. [Réf. du 15 avr. 2021]. Disponible sur** IEC 62443, un standard en cybersécurité industrielle | Stormshield
Article	**[93]**	Thales **- cyberthreat handbook: Thales et Verint présentent leur « who's who » des hackers. [en ligne]. [Réf. du 07.10.2019]. Disponible sur** CyberThreat Handbook : Thales et Verint présentent leur « Who's Who » des hackers | Thales Group
Article	**[94]**	SNCF**, SNCF Réseau et ses métiers de la maintenance, des travaux et de la circulation ferroviaire. [en ligne]. [Réf. du 28 mai 2020]. Disponible sur** SNCF Réseau et ses métiers de la maintenance, des travaux et de la circulation ferroviaire. - YouTube
Vidéo	**[95]**	Gilles Berthelot**, Défi 2 min : comprendre la cybersécurité. [en ligne]. [Réf. du 24 Nov. 2020]. Disponible sur** Défi 2 min : comprendre la cybersécurité - YouTube
Site	**[96]**	IBM**, IBM QRadar SIEM. Analyse de sécurité intelligente pour des connaissances exploitables sur les menaces les plus critiques [en ligne]. Disponible sur** IBM QRadar SIEM - Détails - France | IBM
Article	**[97]**	Christophe Veltsos**, Improving Your Security Awareness Campaigns: Examples From Behavioral Science. [en ligne]. [Réf. du 24 Juin 2015]. Disponible sur** Improving Your Security Awareness Campaigns With Behavioral Science (securityintelligence.com)
Article	**[98]**	Ami Rojkes Dombe**, In cyberattack against Iran's rail network, the capabilities of the attackers weren't compromised: Cylus CEO [en ligne]. [Réf. du 18 Juil. 2021]. Disponible sur** In cyberattack against Iran's rail network, the capabilities of the attackers weren't compromised: Cylus CEO | Israel Defense
Site	**[99]**	**ENISA - Information Sharing and Analysis Centers (ISACs).** *Les centres d'analyse et de partage de l'information (ISAC) sont des organisations à but non lucratif qui fournissent une ressource centrale pour la collecte d'informations sur les cybermenaces (dans de nombreux cas pour les infrastructures critiques).* **[en ligne].Disponible sur** Information Sharing and Analysis Centers (ISACs) — ENISA (europa.eu)
Article	**[100]**	Ian Maxwell**, Is the railway sufficiently prepared for a cyber-attack? [en ligne]. [Réf. du 24 février 2020]. Disponible sur** Is the railway sufficiently prepared for a cyber-attack? (globalrailwayreview.com)
Normes	**[101]**	**ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management [en ligne]. Disponible sur** ISO - ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management
Article	**[102]**	SNCF **- L'aiguillage sous toutes ses coutures. [en ligne]. [Réf. du 23 Janv. 2019]. Disponible sur** L'aiguillage sous toutes ses coutures | SNCF
Article	**[103]**	Sébastien Ropartz DELOITTE **- La convergence IT/OT : un enjeu stratégique majeur pour les groupes industriels. [en ligne]. [Réf. du 22 Juin 2017]. Disponible sur** La convergence IT/OT : un enjeu stratégique majeur pour les groupes industriels - Le blog business (deloitte.fr)
Rapport	[104]	Sébastien MEURANT et Rémi CARDON**, SÉNAT - La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ? [en ligne]. [Réf. du 10 Juin 2021]. Disponible sur** Prévenir et guérir : quels remèdes contre les cyber virus ?
Article	**[105]**	Romain GERARDIN-FRESSE, La cybersécurité, un enjeu majeur de l'intelligence économique | Les Echo [en **ligne]. [Réf. du . 9 avril 2018]. Disponible sur** La cybersécurité, un enjeu majeur de l'intelligence économique | Les Echo
Article	**[106]**	François Lanquetot, Caroline Perrin, Laetitia Chatain, Eléonore Miédan-Gros**, BearingPoint - La Data au service de la Sécurité Ferroviaire - [en ligne]. [Réf. du 2021]. Disponible sur** La Data au service de la Sécurité Ferroviaire | BearingPoint France
Article	**[107]**	ANSSI **- Méthode d'analyse de Risques : EBIOS RM [en ligne]. Disponible sur** La méthode EBIOS Risk Manager – Le guide | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
Article	**[108]**	Parlement européen, **La politique commune des transports en Europe - [en ligne]. [Réf. de mai 2021]. Disponible sur** La politique commune des transports: généralités | Fiches thématiques sur l'Union européenne | Parlement européen

Type	N°	Références
Rapport	**[109]**	Roger Rétiveau, **La signalisation ferroviaire – [en ligne]. [Réf. de 1987]. Disponible sur** La Signalisation Ferroviaire (lafibre.info)
Article	**[110]**	Léna Corot, **La SNCF présente son plan d'action pour le train autonome. [en ligne]. [Réf. du 13 sept. 2018]. Disponible sur** La SNCF présente son plan d'action pour le train autonome (usine-digitale.fr)
Site	**[111]**	**La téléconduite sur rail, SNCF, Thales, Actia Telecom, le CNES s'unissent avec Railenium [en ligne]. Disponible sur** La Téléconduite sur Rail, SNCF, THALES, ACTIA TÉLÉCOM, le CNES s'unissent avec RAILENIUM | RAILENIUM
Article	**[112]**	Christian Chaumette**, Le contrôle/commande ferroviaire : Dossier complet | Techniques de l'Ingénieur. [en ligne]. [Réf. du 10 décembre 2020]. Disponible sur** Le contrôle/commande ferroviaire : Dossier complet | Techniques de l'Ingénieur (techniques-ingenieur.fr)
Livre	**[113]**	Jean-Gabriel Ganascia, **Le Mythe de la Singularité. Faut-il craindre l'intelligence artificielle ?. Editions Seuil. Juin 2019 [en ligne] Disponible sur** Le Mythe de la Singularité, Jean-Gabr... | Editions Seuil.
Article	**[114]**	Thierry**, Le secteur ferroviaire en France et dans le monde : un exceptionnel potentiel de croissance. [en ligne]. [Réf. du 14 Sept. 2020]. Disponible sur** Le secteur ferroviaire en France et dans le monde : un exceptionnel potentiel de croissance | Ametra Group
Article	**[115]**	Larry Ponemon**, Learning to thrive against threats Apprendre à survivre face aux menaces. [en ligne]. [Réf. de Sept. 2015]. Disponible sur** Learning to thrive against threats | Ponemon-Sullivan Privacy Report (ponemonsullivanreport.com)
Article	**[116]**	FJALADE **Les enjeux de la supervision IOT (Internet of Things). [en ligne]. [Réf. de Févr. 2019]. Disponible sur** Les enjeux de la supervision IOT (Internet of Things) - Syloe
Livre blanc	**[117]**	Commission Européenne**, Feuille de route pour un espace européen unique des transports – Vers un système de transport compétitif et économe en ressources. [en ligne]. [Réf. du 28 mars 2011]. Disponible sur** LIVRE BLANC Feuille de route pour un espace européen unique des transports – Vers un système de transport compétitif et économe en ressources - Publications Office of the EU (europa.eu)
Livre blanc	**[118]**	Kapersky**, La sensibilisation des collaborateurs à la sécurité informatique. Il est temps d'ouvrir les yeux ! [en ligne]. [Réf. de Juin 2019]. Disponible sur** Livre-blanc-sensibilisation-a-la-securite-informatique.pdf (kaspersky.com)
Texte législatif	**[119]**	**LOI N°88-19 DU 5 JANVIER 1988 relative à la fraude informatique [en ligne]. [Réf. du 5 Janvier 1988]. Disponible sur** Loi du 5 janvier 1988 (ens.fr)
Article	**[120]**	Joanna PERES, Jean CAIRE et Véronique DELEBARRE -RATP et SafeRiver**., Maîtrise des risques lies aux aspects de cybersécurité et sécurité ferroviaire. [en ligne]. [Réf. du 20 mars 2019]. Disponible sur** MAÎTRISE DES RISQUES LIES AUX ASPECTS DE CYBERSÉCURITÉ ET SÉCURITÉ FERROVIAIRE (archives-ouvertes.fr)
Guide	**[121]**	Steve Riley, Neil MacDonald, Lawrence Orans**, Market Guide for Zero Trust Network Access - [en ligne]. [Réf. du 29 avril 2019]. Disponible sur** Market Guide for Zero Trust Network Access | Gartner
Guide	**[122]**	**Défense en profondeur appliquée aux systèmes d'information. [en ligne]. [Réf. du 19 Juil. 2004]. Disponible sur** mementodep-v1-1.pdf (ssi.gouv.fr)
Site	**[123]**	Mémo CERTitude **- Détection d'intrusion (IDS).** *La détection d'intrusion (IDS) participe au dispositif global de la sécurité numérique et à son volet réaction.* **[en ligne]. [Réf. de Sept. 2018]. Disponible sur** Mémo CERTITUDE - Détection d'intrusion - IDS (certitudenumerique.net)
Site	**[124]**	Mémo CERTitude **- Homologation de sécurité.** *L'homologation de sécurité vise à donner et à garantir un certain niveau de confiance dans les services rendus par un système numérique au travers d'une démarche structurée, réglementaire pour certains acteurs et engageant la responsabilité des personnes concernés***. [en ligne]. Disponible sur** Mémo CERTITUDE - Homologation des systèmes numériques (certitudenumerique.net)
Site	**[125]**	Mémo CERTitude **- LPM vs NIS.** *La Loi de Programmation Militaire votée fin 2013, adresse, au travers de son article 22, les Opérateurs d'Importance Vitale (OIV) s'inscrivant dans le dispositif national de Sécurité des Activités d'Importance Vitale en place depuis 2006 (cf. Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale).* **[en ligne]. Disponible sur** Mémo CERTITUDE - LPM-NIS (certitudenumerique.net)
Site	**[126]**	ENISA **- National Cybersecurity Strategies.** *Dans un environnement de cybermenaces en constante évolution, les États membres de l'UE doivent disposer de stratégies de cybersécurité flexibles et dynamiques pour faire face aux nouvelles menaces mondiales***. [en ligne]. Disponible sur** National Cybersecurity Strategies — ENISA (europa.eu)
Article	**[127]**	Sébastien Roncin**, OIV et PDIS : tout ce qu'il faut savoir** *La qualification PDIS permet aux OIV d'identifier des prestataires capables de leur fournir un service de détection des incidents de sécurité en conformité avec les exigences de l'ANSSI, pour répondre à la LPM.* **[en ligne]. [Réf. de février 2019]. Disponible sur** OIV et PDIS : tout ce qu'il faut savoir | Le Blog d'Orange Cyberdéfense
Rapport	**[128]**	Oliver Wyman **: Mondialisation des services : dix années qui vont tout changer.** *Estimations fondées sur données Insee.* **[en ligne]. [Réf. du 27 Juil. 2015 Disponible sur** PAR-CIVSTF01-001 Service Globalization (FR_long) (oliverwyman.com)

Type	N°	Références
Site	**[129]**	**AlienVault® OSSIM™, Open Source Security Information and Event Management (SIEM),** *Un SIEM open source riche en fonctionnalités, avec collecte, normalisation et corrélation des événements. Lancé par des ingénieurs en sécurité en raison du manque de produits open source disponibles***. [en ligne]. Disponible sur** OSSIM: The Open Source SIEM | AlienVault (att.com)
Article	**[130]**	Napsis**, On-premise, cloud, hybride : DSI où en êtes-vous ? [en ligne]. Disponible sur** On premise
Article	**[131]**	Arafer**, Ouverture à la concurrence du transport ferroviaire - les paquets ferroviaires et la création de l'ARAFER (Autorité de régulation des activités ferroviaires et routières). [en ligne]. [Réf. du 22 mars 2017]. Disponible sur** Ouverture à la concurrence du transport ferroviaire - les paquets ferroviaires et la création de l'ARAFER | Ministère de la Transition écologique (ecologie.gouv.fr)
Site	**[132]**	EPSF **- Positionnement de l'EPSF parmi les acteurs du système ferroviaire français [en ligne]. Disponible sur** Positionnement de l'EPSF parmi les acteurs du système ferroviaire | EPSF (securite-ferroviaire.fr)
Fiches	**[133]**	**CLUSIF - Fiches Incidents Cyber, SI Industriels. CLUSIF – Groupe de Travail SCADA – [en ligne]. [Réf. d'avril 2017]. Disponible sur** Présentation PowerPoint (clusif.fr)
Article	**[134]**	EPSF **- ENR135 - Prise en compte des enjeux de cybersécurité au sein de la sécurité ferroviaire. [en ligne]. [Réf. du 26 mars 2021]. Disponible sur** Prise en compte des enjeux de cybersécurité au sein de la sécurité ferroviaire | EPSF (securite-ferroviaire.fr)
Site	**[135]**	ANSSI **- Profils de protection pour les systèmes industriels [en ligne]. Disponible sur** Profils de protection pour les systèmes industriels | Agence nationale de la sécurité des systèmes d'information
Article	**[136]**	ANSSI **- Profil de protection d'un progiciel serveur applicatif SCADA. [en ligne]. [Réf. du 1er Juil. 2015]. Disponible sur** 20151005_NP_ANSSI_SDE_4067_PJ4_serveur_scada_moyen_terme_PJ4.vfp_.pdf
Article	**[137]**	Morand Fachot**, Protecting railway networks from cyber threats.** *Rail networks, as integral parts of critical infrastructure, continue to come under cyber attack***. [en ligne]. [Réf. du 15 mars 2018]. Disponible sur** Protéger les réseaux ferroviaires contre les cybermenaces | E-tech IEC
Article	**[138]**	Forcepoint, CYBER EDU **- Qu'est-ce qu'un Système de prévention des intrusions (IPS) ? Système de prévention des intrusions (IPS) – Définition – 2021 [en ligne]. [Réf. du 14 Janvier 2020]. Disponible sur** Qu'est-ce qu'un Système de prévention des intrusions (IPS) ? | Forcepoint
Article	**[139]**	Scott Carey**, What is Chaos Monkey? Chaos engineering explained***? L'ingénierie du chaos expliquée. En provoquant des ravages aléatoires sur vos systèmes en production, Chaos Monkey vous apprend à renforcer ces systèmes***. [en ligne]. [Réf. du 13 mai 2020]. Disponible sur** Qu'est-ce que Chaos Monkey ? L'ingénierie du chaos expliquée | InfoMonde (infoworld.com)
Article	**[140]**	Betty Sfez, **Droit des TIC, informatique, propriété intellectuelle** **Quelles obligations pour les OIV en matière de cybersécurité : exigences européennes et françaises comparées. [en ligne]. [Réf. 18 avril 2014]. Disponible sur** Quelles obligations pour les OIV en matière de cybersécurité : exigences européennes et françaises comparées. Par Betty Sfez, Avocat. (village-justice.com)
Rapport	**[141]**	**Rapport 2020 de Observer-IT et Proofpoint - Coût des menaces internes à l'échelle mondiale. Mars 2020 [en ligne]. [Réf. du 14 Janvier 2020]. Disponible sur** Rapport 2020 sur le coût des menaces internes à l'échelle mondiale (bitpipe.com)
Article	**[142]**	Franck Miquel, **Réussir la mise en conformité de ses systèmes d'informations d'importance vitale (SIIV) –. [en ligne]. [Réf. du 6 juin 2019].** Réussir sa mise en conformité (SIIV) | SYNETIS
Article	**[143]**	ANSSI **- AVIS DU CERT-FR- SCADA Vulnérabilité dans Schneider Electric Modbus Serial Driver – [en ligne]. [Réf. du 11 avril 2019]. Disponible sur** SCADA Vulnérabilité dans Schneider Electric Modbus Serial Driver – CERT-FR (ssi.gouv.fr)
Site	**[144]**	**Seclab Secure Xchange Network (SXN) [en ligne]. [Réf. de 2021]. Disponible sur** Seclab Secure Xchange Network - Seclab ICS CyberSecurity (seclab-security.com)
Article	**[145]**	Jacques de La Rivière**, SNCF - l'aiguillage sous toutes ses coutures – [en ligne]. [Réf. du 23 janv. 2019]. Disponible sur** Sécurité by-design : analyse des 3 grands principes - Silicon
Guide	**[146]**	**Sécurité industrielle GT méthode de classification et mesures principales (ANSSI - page 10) – [en ligne]. [Réf. de Janv. 2014]. Disponible sur** securite_industrielle_GT_methode_classification-principales_mesures.pdf
Site	**[147]**	**Set of specifications 3 (ETCS B3 R2 GSM-R B1) [en ligne]. Disponible sur** Set of specifications 3 (ETCS B3 R2 GSM-R B1) | ERA (europa.eu)
Site	**[148]**	Shift2Rail**, Shift2Rail: the joint undertaking to build the railway system of tomorrow [en ligne]. Disponible sur** Shift2Rail - UNIFE
Article	**[149]**	Enéa bell, Ornella Dante et Yassine M'Hamdi, **SIDO 2019 : À la croisée de l'IoT, de la robotique et de l'intelligence artificielle. [en ligne]. [Réf. d' avril 2019]. Disponible sur** SIDO 2019 : À la croisée de l'IoT, de la robotique et de l'intelligence artificielle - DigitalCorner (digitalcorner-wavestone.com)
Article	**[150]**	Terranova Security**, Spear Phishing vs. Phishing: Everything You Need to Know- [en ligne]. [Réf. du 07 Janv. 2021]. Disponible sur** Spear Phishing vs Phishing | Terranova Security

Type	N°	Références
Spécifications	**[151]**	NIST**, SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. [en ligne]. [Réf. de Déc. 2018]. Disponible sur** SP 800-37 Rev. 2, RMF: A System Life Cycle Approach for Security and Privacy | CSRC (nist.gov)
Article	**[152]**	Systra **- Resilient transport infrastructure. No trust without cybersecurity. [en ligne]. [Réf. du 22 Janvier 2021]. Disponible sur** systra-cybersecurity-brochure-2021-01.pdf
Article	**[153]**	railwaysignalling.eu**, What is a Train Control and Monitoring System (TCMS)? ? [en ligne]. [Réf. du 10 février 2015]. Disponible sur** TCMS (Train Control Monitoring System) - raiwaysignalling.eu (railwaysignalling.eu)
Article	**[154]**	Fortinet**, Technologies industrielles (OT) ? Les technologies OT consistent à tirer parti de matériels et de logiciels pour contrôler les processus, dispositifs et infrastructures physiques. [en ligne]. [Réf. de 2021]. Disponible sur** Technologies OT : Perspectives sur la sécurité des technologies industrielles | Fortinet
Article	**[155]**	Alice Pruvot, Thales **- comment les hautes technologies peuvent réduire à court terme les émissions de co2 mondiales. [en ligne]. [Réf. du 07 oct. 2020]. Disponible sur** Thales : comment les hautes technologies peuvent réduire à court terme les émissions de CO2 mondiales | Thales Group
Article	**[156]**	Thales**, Thales augmente l'intelligence des trains pour optimiser le trafic ferroviaire et économiser 30% de leur consommation énergétique [en ligne]. [Réf. du 25 Nov. 2020]. Disponible sur** Thales augmente l'intelligence des trains pour optimiser le trafic ferroviaire | Thales Group
Site	**[157]**	UNIFE**, The European rail supply industry [en ligne]. Disponible sur** The European Rail Supply Industry - UNIFE
Site	**[158]**	Ron Brash, **The ultimate guide to protecting OT systems with IEC 62443. [en ligne]. [Réf. du 23 Juin 2021] Disponible sur** The Ultimate Guide to Protecting OT Systems with IEC 62443 - Verve Industrial
Article	**[159]**	**Transport Cybersecurity Toolkit training [en ligne]. [Réf. de 2020]. Disponible sur** Transport Cybersecurity Toolkit Training (transport-cybersecurity-toolkit.com)
Article	**[160]**	Union européenne**, Transport Ferroviaire***, La politique européenne des transports ferroviaires vise la création d'un espace ferroviaire unique. L'ouverture du secteur des transports ferroviaires à la concurrence, commencée en 2001, a fait l'objet, en l'espace de dix ans, de trois paquets et d'une refonte***. [en ligne]. [Réf. de Juil. 2021]. Disponible sur** Transport ferroviaire (europa.eu)
Article	**[161]**	Bernard Desmet**, Transport ferroviaire et développement durable [en ligne]. Disponible sur** Transport ferroviaire et développement durable | Culture | Cnam
Livre Orange	**[162]**	Donald C. Latham**, "Department of Defense Trusted Computer System Evaluation Criteria",** DoD Directive 5200.28 **– [en ligne]. [Réf. du 2-décembre 1985]. Disponible sur** Trusted Computer System Evaluation Criteria ["Orange Book"] (nist.gov)
Guide	**[163]**	UIC**, Solutions techniques pour le rail opérationnel. [en ligne]. [Réf. du 10 mai 2021]. Disponible sur** uic-solutions-techniques-pour-le-rail-operationnel.pdf
Article	**[164]**	Kévin Comte**, Un train autonome est testé pour la première fois en Allemagne, la SNCF vise 2023. [en ligne]. [Réf. de 11 Oct. 2021]. Disponible sur** Un train autonome est testé pour la première fois en Allemagne, la SNCF vise 2023 - Capital.fr
Article	**[165]**	Deborah Golden, Jeffrey Kennedy, **Beneath the surface of a cyberattack: Collision avoidance. The business application of cyber risk quantification. [en ligne]. [Réf. de 4 Août 2020]. Disponible sur** us-beneath-the-surface.pdf (deloitte.com)
Article	**[166]**	Waterfall**, Waterfall pour les IDS. Waterfall Security Solutions. [en ligne]. [Réf. du 05 oct. 2020]. Disponible sur** Waterfall for Intrusion Detection Systems eBook french V3 (waterfall-security.com)
Article	**[167]**	Railengineer**, What is TCMS.** *Train Control & Management System (TCMS) is a train-borne distributed control system.* **[en ligne]. [Réf. du 11 Août 2015]. Disponible sur** What is TCMS? | Rail Engineer
Article	**[168]**	Maurizio Palumbo, **La signalisation ferroviaire depuis la naissance jusqu'à ERTMS. [en ligne]. [Réf. de Nov. 2015]. Disponible sur** White_Paper_Signalisation_Ferroviaire_II (railwaysignalling.eu)
Livre blanc	**[169]**	Alstom **- Cybersécurité - Pour une mobilité sûre et sécurisée. [en ligne]. [Réf. du 09 sept.2020]. Disponible sur** Whitepaper Cybersecurity.pdf (alstom.com)
Guide	**[170]**	UTP**, Les métiers du ferroviaire ONISEP. [en ligne]. [Réf. du 22 mars 2017]. Disponible sur** ZOOM-FERROVIAIRE.pdf (utp.fr)
Site	**[171]**	**Chiffre d'affaires des principales sociétés de transport ferroviaire à l'échelle mondiale en 2019 – 2021 [en ligne]. Disponible sur** • Chiffre d'affaires des plus grandes sociétés ferroviaires du monde 2019 | Statista
Site	**[172]**	SNCF**, Le réseau du futur [en ligne]. Disponible sur** Le réseau du futur | Sujet | SNCF RÉSEAU (sncf-reseau.com)
Article	**[173]**	Jonathan Greig, **Cyberattaque ferroviaire en Iran, [en ligne]. [Réf. du 30 Juillet 2021.]. Disponible sur** Cyberattaque en Iran : les attaquants ont utilisé un logiciel malveillant destructeur de données - ZDNet
Article	**[174]**	Reynald Fléchaux, **Cyberattaque pour faire dérailler un train. [en ligne]. [Réf. du 06 Janv. 2016]. Disponible sur** Scada : une cyberattaque peut-elle faire dérailler un train ? | Silicon

Type	N°	Références
Site	**[175]**	ANFR**, Le futur système de radiocommunication ferroviaire,** *L'après GSM-R***, [en ligne]. [Réf. du 31 mars 2020]. Disponible sur** ANFR-Le futur système de radiocommunication ferroviaire
Article	**[176]**	Commission Européenne**, Cybersécurité de l'UE: la Commission propose la création d'une unité conjointe de cybersécurité afin d'intensifier la réaction aux incidents majeurs de sécurité, 1 [en ligne]. [Réf. du 23 Juin 2021]. Disponible sur** Cybersécurité de l'UE: la Commission propose la création d'une unité conjointe de cybersécurité (europa.eu)
Article	**[177]**	Futura sciences**, Cyberattaques : l'Union européenne va se doter d'une unité de défense commune, [en ligne]. [Réf. du 02 Juillet 2021]. Disponible sur** Cyberattaques : l'Union européenne va se doter d'une unité de défense commune (futura-sciences.com)
Article	**[178]**	IHEMI**, Gestion de crise et chaînes cyber : organisation européenne et française, [en ligne]. [Réf. du 03 Juin 2020]. Disponible sur** Gestion de crise et chaînes cyber : organisation européenne et française | IHEMI
Dossier Thématique	**[179]**	Collectifs d'auteurs, Le **système ferroviaire au cœur des transports [en ligne]. [Réf. du 23 Sept. 2019]. Disponible sur** Le système ferroviaire au cœur des transports (ifsttar.fr)
Livre Blanc	**[180]**	Reilly, Kaitlyn**, Cyber Resilience White Paper. An Information Technology Sector Perspective. [en ligne]. [Réf. du 11 mai 2017]. Disponible sur** Cyber Resilience White Paper (it-scc.org)
Article	**[181]**	Philippe Gaufreteau, Lilian Planche, **Cybersécurité des systèmes de, transport application à la ligne 18 du Grand Paris Express, [en ligne]. [Réf. du 20 mars 2019]. Disponible sur** CYBERSÉCURITÉ DES SYSTÈMES DE TRANSPORT APPLICATION A LA LIGNE 18 DU GRAND PARIS EXPRESS
Rapport	**[182]**	Cyrille Schott et Pascal Buffard, **Risques et sécurité, de la connexion, des systèmes, industriels sur internet, Rapport INHESJ [en ligne]. [Réf. de décembre 2014]. Disponible sur** Securite industrielle.indd (cigref.fr)
Thèse	**[183]**	Ravdeep Kour**, Cybersecurity in railway. A Framework for Improvement of Digital Asset Security [en ligne]. [Réf. de 2020]. Disponible sur** 147934_omslag_DOCTORAL_THESIS_170x240mm.indd (diva-portal.org)
Textes Législatifs	**[184]**	Parlement européen**, Textes de lois européennes sur la sécurité ferroviaire [en ligne]. [Réf. du 07 Juil. 2021]. Disponible sur** Textes adoptés - Mercredi 7 juillet 2021 (europa.eu)
Site	**[185]**	**ERTMS in brief, The European Railway Traffic Management System (ERTMS) is a major industrial project developed by eight UNIFE members – Alstom Transport, AZD Praha, Bombardier Transportation, CAF, Hitachi Rail STS, Mermec, Siemens Mobility and Thales – in close cooperation with the European Union, railway stakeholders and the GSM-R industry. [en ligne].. Disponible sur** ERTMS in brief - ERTMS
Textes Législatifs	**[186]**	Journal Officiel**, Arrêté du 11 août 2016 règles de sécurité et 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 » [en ligne]. [2020]. Disponible sur** JORF n° 0197 du 25 août 2016 - Légifrance (legifrance.gouv.fr)
Site	**[187]**	COLPOFER**, Mission***, Organisme européen pour la protection des personnes, des locaux, des trains et de l'information au sein du système ferroviaire* **[en ligne]. Disponible sur** Mission (colpofer.org)
Site	**[188]**	**L'utilisation ferroviaire des drones avec Altametris***. Utilisé our inspection du matériel, des voies, des ouvrages d'art et des installations électriques***. [en ligne]. [Réf. de Sept. 2021]. Disponible sur** L'utilisation ferroviaire des drones avec Altametris | Sujet | SNCF RÉSEAU (sncf-reseau.com)
Guide Prospectif	**[189]**	Clotilde Gagey, **2 juillet 2033… Le train autonome 0277 pour Amiens s'apprête à quitter la gare de Paris-Gare du Nord…. Atelier sécurité ferroviaire du futur [en ligne]. [Réf. du 23 mars 2021]. Disponible sur** synthese-atelier-ferroviaire-futur
Guide	**[190]**	Patricia Toth**, Recovering from a Cybersecurity Incident What to do Before and After. [en ligne]. [Réf. de Déc. 2017 Disponible sur** Recovery Webinar (nist.gov)
Guide	**[191]**	Eleni Darra **, Information Sharing and Analysis Centres (ISACs) Cooperative models . [en ligne]. [Réf. de Févr. 2018]. Disponible sur** https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/
Site	**[192]**	EPSF**, Opérateurs ferroviaires autorisés [en ligne]. [Réf. du 14 Janvier 2020]. Disponible sur** OPÉRATEURS FERROVIAIRES AUTORISÉS | EPSF (securite-ferroviaire.fr)
Site	**[193]**	EUROPOL**, European Cybercrime Centre - EC3. Combating crime in a digital age [en ligne]. [Réf. du 19 Nov. 2021]. Disponible sur** European Cybercrime Centre - EC3 | About Europol | Europol (europa.eu)
Journal Officiel européen	**[194]**	ENISA**, Regulation (eu) 2019/881 of the european parliament and of the council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)). [en ligne]. [Réf. du 17 avril 2019]. Disponible sur** EUR-Lex - 32019R0881 - EN - EUR-Lex (europa.eu)
Article	**[195]**	Conseil européen**. Cybersécurité : comment l'UE lutte contre les cybermenaces [en ligne]. Disponible sur** Cybersécurité: comment l'UE lutte contre les cybermenaces - Consilium (europa.eu)
Article	**[196]**	**Secure 5G networks: Questions and Answers on the EU toolbox. [en ligne]. [Réf. du 29 Janv. 2020]. Disponible sur** Secure 5G networks: the EU toolbox

Type	N°	Références
Site	**[197]**	ANSSI**, Directive network and information system security (NIS) [en ligne]. . Disponible sur** Directive Network and Information Security (NIS) | Agence nationale de la sécurité des systèmes d'information
Article	**[198]**	Site KAN**, Processus d'élaboration d'une norme européenne. [en ligne]. [Réf. de mai 2020]. Disponible sur** L'élaboration d'une norme européenne - KAN
Site	**[199]**	**EU Cybersecurity Certification Framework [en ligne]. Disponible sur** [1] Certification — ENISA (europa.eu)
Site	**[200]**	CEN-CENELEC, **, About CEN and CENELEC. The European Committee for Standardization is one of three European Standardization Organizations (together with CENELEC and ETSI) that have been officially recognized by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European levelen ligne]. Disponible sur** About CEN - CEN-CENELEC (cencenelec.eu)
Site	**[201]**	Commission Européenne**, Formal methods and csirt for the railway sector [en ligne]. Disponible sur** MÉTHODES FORMELLES ET CSIRT POUR LE SECTEUR FERROVIAIRE | 4SECURAIL Projet | Fiche d'information | | H2020 | CORDIS
Support conference	**[202]**	Antonio López, Marcos Sacristán**, EU-CSIRT collaborative environment dedicated to rail. Cybersecurity in Railways, ENISA-ERA Conference [en ligne] [Réf. de mars 2021]. Disponible sur** PowerPoint Presentation (europa.eu)
Article	**[203]**	Morand Fachot**, Protecting railway networks from cyber threats. Rail networks, as integral parts of critical infrastructure, continue to come under cyber attack. [en ligne]. [Réf. du 15 mars 2028]. Disponible sur** Protecting railway networks from cyber threats | IEC e-tech
Site	**[204]**	Conseil de l'UE**, Le Centre de compétences en matière de cybersécurité, basé à Bucarest, obtient le feu vert du Conseil,** *Centre de compétences en matière de cybersécurité, réunira également les principales parties prenantes européennes, notamment des entreprises, des organisations universitaires et de recherche et d'autres associations de la société civile concernées, afin de constituer une communauté de compétences en matière de cybersécurité destinée à renforcer et diffuser l'expertise en matière de cybersécurité dans toute l'Union***. [en ligne]. [Réf. du 20 avril 2021]. Disponible sur** Le Centre de compétences en matière de cybersécurité, basé à Bucarest, obtient le feu vert du Conseil - Consilium (europa.eu)
Dossier interinstitutionnel	**[205]**	**RÈGLEMENT (UE) 2021/…DU PARLEMENT EUROPÉEN ET DU CONSEIL établissant le Centre de compétences européen pour l'industrie, les technologies et la recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination. [en ligne]. [Réf. du 6 avril 2021]. Disponible sur** pdf (europa.eu)
Site	**[206]**	Commission Européenne**, Transport cybersecurity toolkit,** *Boîte à outils pour améliorer la sensibilisation et la préparation des parties prenantes du secteur des transports aux menaces cyber au sein de l'UE* **[en ligne]. [Réf]. Disponible sur** DG-MOVE-Transport-Cybersecurity-Toolkit-FINAL.pdf (fecc.org)
Site	**[207]**	Worldbank**, Railways. Partenariat de la filière ferroviaire avec la Banque Mondiale [en ligne]. Disponible sur** Railways (worldbank.org)
Guide	**[208]**	PPIAF, WorldBank, **Réforme des Chemins de fer. Manuel pour l'amélioration de la performance du secteur ferroviaire [en ligne]. [Réf. de 2017]. Disponible sur** La Réforme des Chemins de fer: Manuel pour l'Amélioration de la Performance du Secteur Ferroviaire (ppiaf.org)
Article	**[209]**	**Worldwide rail market is expected to grow by 2025, UNIFE says. [en ligne]. [Réf. du 02 Oct. 2020]. Disponible sur** Global railway market is expected to grow until 2025 (railwaypro.com)
Article	**[210]**	Frédéric Schaeffer**, CRRC, le géant chinois qui fait peur à Alstom et Siemens. Le constructeur ferroviaire remporte de beaux succès dans des appels d'offres à l'étranger. Alstom et Siemens invoquent cette menace pour justifier leur projet de fusion, mais n'ont pas réussi à convaincre Bruxelles. [en ligne]. [Réf. du 06 Févr. 2019]. Disponible sur** CRRC, le géant chinois qui fait peur à Alstom et Siemens | Les Echos
Site	**[211]**	**Independent innovation, open innovation and collaborative innovation, improve the technology innovation system, and constantly upgrade technology innovation capabilities. Selon le site de CRRC [en ligne]. Disponible sur** CRRC > About Us > Company Profile (crrcgc.cc)
Site	**[212]**	**Valeur du marché ferroviaire mondial accessible de 2017 à 2025, selon le produit (en milliards d'euros). [en ligne]. [Réf. de 2021]. Disponible sur** • Marché ferroviaire mondial par produit 2025 | Statista
Article	**[213]**	Andreas Schwilling**, Global rail market continues to grow despite drop in transport volumes due to COVID-19. [en ligne]. [Réf. du 02 Oct. 2020]. Disponible sur** UNIFE World Rail Market 2020 | Roland Berger
Article	**[214]**	Christopher Mims **, Les trains autonomes sont sur la bonne voie pour accroître le fret aux États-Unis. [en ligne]. [Réf. du 14 Oct. 2020]. Disponible sur** Les trains autonomes sont sur la bonne voie pour accroître le fret aux États-Unis - l'Opinion (lopinion.fr)
Site	**[215]**	**Prévision de la croissance du marché ferroviaire mondial pour 2021-2023 par rapport à 2015-2017, selon la zone géographique [en ligne]. [Réf. de 2021]. Disponible sur** • Variation du marché ferroviaire mondial par régions 2023 | Statista
Article	**[216]**	Jean-Michel Gradt**, L'Europe, terre de conquête pour les acteurs du ferroviaire** *Alors que Bruxelles vient de rejeter la fusion Alstom-Siemens, l'Europe reste le principal marché mondial*

Type	N°	Références
		accessible à toutes les entreprises, contrairement à la Chine et au Japon. **[en ligne]. [Réf. du 06 Févr. 2019]. Disponible sur** L'Europe, terre de conquête pour les acteurs du ferroviaire | Les Echos
Site	**[217]**	**Introduction à l'itinéraire china railway express [en ligne]. [Réf. de 2021]. Disponible sur** China Railway Express-Suzhou Sohologistics CO., LTD.
Article	**[218]**	Henri de Grossouvre**, CHINE-EUROPE, le boom passé inaperçu du fret ferroviaire et ses conséquences économiques et géopolitiques. [en ligne]. [Réf. du 12 mai 2021]. Disponible sur** CHINE-EUROPE, le boom passé inaperçu du fret ferroviaire et ses conséquences économiques et géopolitiques - AgoraVox le média citoyen
Article	**[219]**	Jean-Michel Bezat**, Thales vend sa signalisation ferroviaire au japonais Hitachi** **Le groupe entend se focaliser sur des métiers de l'aéronautique civile et militaire, de l'aérospatiale et de la sécurité numérique. [en ligne]. [Réf. du . 4 Aout 2021]. Disponible sur** Thales vend sa signalisation ferroviaire au japonais Hitachi (lemonde.fr)
Rapport	**[220]**	**Railway Cybersecurity Market by Type (Infrastructural & On-board), Offering, Security Type (Network, Application, Endpoint, System Administration and Data Protection), Application (Passenger & Freight), Rail Type and Region - Global Forecast to 2027. [en ligne]. [Réf. de Juil. 2021]. Disponible sur** Railway Cybersecurity Market by Type Offering, Security Type
Article	**[221]**	**La Thailande renforce la sécurité ferroviaire dans 48 gares grâce à Thales. [en ligne]. [Réf. du 18 Sept. 2019]. Disponible sur** La Thailande renforce la sécurité ferroviaire dans 48 gares grâce à Thales | Thales Group
Article	**[222]**	Global Railway Review**, Airbus CyberSecurity and Alstom sign cyber-security partnership. Airbus CyberSecurity and Alstom have agreed to a new partnership that will provide leading solutions and security of industrial information systems for cyber-security across rail transport. [en ligne]. [Réf. du 13 sept. 2021]. Disponible sur** Airbus CyberSecurity and Alstom sign cyber-security partnership (globalrailwayreview.com)
Article	**[223]**	Axio**, A Timeline of Frameworks for Cybersecurity and Compliance [en ligne]. [Réf. du 19 avril 2021]. Disponible sur** A Timeline of Frameworks for Cybersecurity and Compliance - Security Boulevard
Article	**[224]**	**Cybersecurity Capability Maturity Model (C2M2) [en ligne]. [Réf. du 21 Juil. 2021]. Disponible sur** Cybersecurity Capability Maturity Model (C2M2) | Department of Energy
Guide	**[225]**	NIST**, Framework for Improving Critical Infrastructure Cybersecurity [en ligne]. [Réf. du 16 avril 2018]. Disponible sur** Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)
Article	**[226]**	Quentin Recoursé**, Qu'est-ce que le NIST Cybersecurity Framework 1.1 et comment l'aborder ? [en ligne]. [Réf. du 04 Oct. 2018]. Disponible sur** Qu'est-ce que le NIST Cybersecurity Framework 1.1 et comment l'aborder ? (beijaflore.com)
Article	**[227]**	EPSF**, Accord de coopération EPSF/ANSFISA ITALIE - [en ligne]. [Réf. de septembre 2021]. Disponible sur** Accord de coopération EPSF/ANSFISA - mai 2021 | EPSF (securite-ferroviaire.fr)
Autres	**[228]**	PGIC **- Cartographie Capacité. Informations confidentielles et services utilisateurs au sein de SNCF Réseau. [en ligne]. [Réf. de Oct. 2016]. Disponible sur** autorite-transports.fr/wp-content/uploads/2016/10/Annexe2bis.pdf
Article	**[229]**	Emmanuelle Ducros**, Ce que l'intelligence artificielle va changer pour les transports ferroviaire et aérien. [en ligne]. [Réf. du 28 Janv. 2019]. Disponible sur** Ce que l'intelligence artificielle va changer pour les transports ferroviaire et aérien - l'Opinion (lopinion.fr)
Vidéo	**[230]**	**Séminaire IA et infrastructure ferroviaire. [en ligne]. [Réf. de décembre 2019]. Disponible sur** Terry Wykle - séminaire IA et infrastructure ferroviaire - YouTube
Livre blanc	**[231]**	Franck Mamalet, Eric Jenn, Gregory Flandin, Hervé Delseny, Christophe, Gabreau, Adrien Gauffriau, Bernard Beaudouin, Ludovic Ponsolle, Lucian, Alecu, Hugues Bonnin, et al. **White Paper Machine Learning in Certified Systems. [en ligne]. [Réf. du 22 mars 2021]. Disponible sur** White Paper Machine Learning in Certified Systems (archives-ouvertes.fr)
Autres	**[232]**	ISO**, Information technology — Artificial intelligence (AI) — Use cases. Technologies de l'information — Intelligence artificielle (IA) — Cas pratiques [Réf. du 14 Janvier 2020]. Disponible sur** ISO/IEC TR 24030:2021(en), Information technology — Artificial intelligence (AI) — Use cases
Normes	**[233]**	ISO**, Cas pratiques détaillés d'IA [en ligne]. [Réf. de Févr. 2021]. Disponible sur** Use+cases-v05_electronic_attachment_022021.pdf (iso.org)
Normes	**[234]**	ISO**, ISO/TR 22100-5 :2021** **Sécurité des machines — En relation avec l'ISO 12100 — Partie 5 : Implications de l'intelligence artificielle pour l'apprentissage automatique [en ligne]. [Réf. de Janv. 2021]. Disponible sur** ISO - ISO/TR 22100-5:2021 - Sécurité des machines — En relation avec l'ISO 12100 — Partie 5: Implications de l'intelligence artificielle pour l'apprentissage automatique
Site	**[235]**	**Plateforme de partage d'info CERT [en ligne et accès réservé]. Disponible sur** https://www.enisa.europa.eu/activities/cert/support/data-sharing
Article	**[236]**	ENISA**, Actionable information for security incident response. [en ligne]. [Réf. du 19 Janv. 2015]. Disponible sur** Actionable information for security incident response — ENISA (europa.eu)

Type	N°	Références
Article	**[237]**	Benoît Georges**, Les boîtes noires du « deep learning » Les defis de l'intelligence artificielle - L'intelligence artificielle a connu des progrès spectaculaires. Mais toutes les questions techniques et éthiques qu'elle pose sont loin d'être réglées. [en ligne]. [Réf. du 27 Août 2018]. Disponible sur** Les boîtes noires du « deep learning » | Les Echos
Autres	**[238]**	ERTMS**, ERTMS Deployment Statistics – Overview. The figures indicate the lines and rolling stock in operation as well as contract signed by UNISIG companies. [en ligne]. [Réf. de Oct. 2020]. Disponible sur** Deployment Statistics - ERTMS
Article	**[239]**	Samuel Miller**, Alstom investit dans Cylus, spécialiste de la cybersécurité ferroviaire, et signe un accord de coopération stratégique, [en ligne]. [Réf. du 09 décembre 2020]. Disponible sur** Alstom investit dans Cylus, spécialiste de la cybersécurité ferroviaire, et signe un accord de coopération stratégique | Alstom
Article	**[240]**	Philippe Molitor, **Alstom investit dans le premier campus dédié à la cybersécurité au monde avec une composante ferroviaire, [en ligne]. [Réf. du 21 Juil. 2021]. Disponible sur** Alstom investit dans le premier campus dédié à la cybersécurité au monde avec une composante ferroviaire | Alstom
Article	**[241]**	CNFCE**, Conséquences d'une cyberattaque sur une entreprise [en ligne]. Disponible sur** Les conséquences d'une cyberattaque sur une entreprise - CNFCE
Guide	**[242]**	Deloitte**, Beneath the surface of a cyberattack. A deeper look at business impacts [en ligne]. [Réf. de Juin 2016]. Disponible sur** us-risk-beneath-the-surface-of-a-cyber-attack.pdf (deloitte.com)
Presentation	**[243]**	Olivier Devisscher**, European Railway Information Sharing & Analysis Center (ER-ISAC). Synthetic Presentation). [en ligne]. [Réf. de mars 2021]. Disponible sur** 8-initiatives-of-the-er-isac-devisscher.pdf (europa.eu)
Guide	**[244]**	Atsec**, Review by Airbus. CYRAIL , CYbersecurity in the RAILway sector. D6.1 – Protection Profiles Specifications. [en ligne]. [Réf. du 30 Sept. 2018]. Disponible sur** Microsoft Word - D6.1-Introduction.docx (cyrail.eu)
Article	**[245]**	François Quiquet, **Cartographie des acteurs étatiques du cyber en France [en ligne]. [Réf. du 06 Juin 2020]. Disponible sur** Cartographie des acteurs étatiques du cyber en France - Space & Cybersecurity Info (spacesecurity.info)
Article	**[246]**	**Secure 5G networks: Questions and Answers on the EU toolbox. [en ligne]. [Réf. du 24 Juil. 2020]. Disponible sur** Réseaux 5G sécurisés: la boîte à outils de l'UE (europa.eu)
Site	**[247]**	**Le Système européen de gestion du trafic ferroviaire [en ligne]. Disponible sur** European Rail Traffic Management System (europa.eu)
Article [3]	**[248]**	Earl Perkins **, Operational Technology Security – Focus on Securing Industrial Control and Automation Systems. [en ligne]. [Réf. du 14 mars 2014]. Disponible sur** Gartner Blog Network
Article	**[249]**	**David Legrand, SecNumCloud évolue. Le référentiel inclut notamment de nouvelles exigences en matière de protection des données à caractère personnel, fruit d'une coopération entre l'ANSSI et la CNIL, suite à l'entrée en vigueur du RGPD. [en ligne]. [Réf. du 18 oct. 2021]. Disponible sur** SecNumCloud : l'ANSSI adapte son référentiel au Cloud de confiance, qu'est-ce qui change ? (nextinpact.com)
Article	**[250]**	Sébastien Gavois**, ANSSI : la cybersécurité est « en pleine expansion » en France et en Europe [en ligne]. [Réf. du 01 Juil. 2021]. Disponible sur** ANSSI : la cybersécurité est « en pleine expansion » en France et en Europe (nextinpact.com)
Article	**[251]**	David Legrand**, SecNumCloud : l'ANSSI adapte son référentiel au Cloud de confiance, qu'est-ce qui change ? [en ligne]. [Réf. du 18 Oct. 2021]. Disponible sur** SecNumCloud : l'ANSSI adapte son référentiel au Cloud de confiance, qu'est-ce qui change ? (nextinpact.com)
Rapport Sénat français	**[252]**	Rapporteurs Denis BAUPIN, député, et Fabienne KELLER, sénatrice**. La multimodalité et l'intermodalité. Nouvelles mobilités et véhicules écologiques [en ligne]. [Réf. du 14 Janvier 2020]. Disponible sur** Le rapport final est en ligne (senat.fr)
Vidéo	**[253]**	**Table ronde de l'IMTD (Institut des Mobilités et des Transports Durables), avec** Dominique Riquet Député européen, Josef Doppelbauer, Directeur ERA , Nathalie Darmendrail de SNCF Didier Fernandes d'Alstom**, . Le ferroviaire au cœur des grands enjeux des transports. [en ligne]. [Réf. du 18 Févr. 2021]. Disponible sur** En https://www.youtube.com/watch?v=kezTSFXzxSA
Vidéo	**[254]**	**"Connecting Europe Express" : promouvoir le rail en Europe. [en ligne]. [Réf. de Sept. 2021]. Disponible sur** "Connecting Europe Express" : promouvoir le rail en Europe - YouTube
Article	**[255]**	European Parliament, **Digitalisation in railway transport. A lever to improve rail competitiveness. [en ligne]. [Réf. du 20 Févr. 2019]. Disponible sur** Digitalisation in railway transport (europa.eu)
Article	**[256]**	**Railway cybersecurity training. Cybersecurity training for railway undertakings (RU) and infrastructure managers (IM) [en ligne]. Disponible sur** Railway cybersecurity training - to keep passengers safe, trains protected, and the critical infrastructure secure. (railway-cybersecurity.com)
Livre blanc	**[257]**	Jana Pieriegud**, Digital transformation of railways [en ligne]. [Réf. du 12 avril 2018]. Disponible sur** Digital transformation of railways (stample.co)
Article	**[258]**	**Globalrailwayview, Digitalisation and rail's future: Q&A with Siemens Mobility's Gerhard Kreß. [en ligne]. [Réf. du 19 Juin 2019]. Disponible sur** Digitalisation and rail's future: Q&A with Siemens Mobility's Gerhard Kreß (globalrailwayreview.com)

Type	N°	Références
Article	**[259]**	Edouard Bedoucha**, Directive NIS renforcer le niveau de sécurité des réseaux et des systèmes d'informations essentiels (SIE) ainsi que d'améliorer le partage d'informations au niveau européen. [en ligne]. [Réf. du 07 mars 2019]. Disponible sur** Directive NIS 1/2 : Quels enjeux juridiques ? | Orange Cyberdefense
Site	**[260]**	SNCF**, Début des essais du prototype du Train Fret Autonome, un an après l'annonce de la création de deux consortiums dédiés au développement de prototypes de train autonome par SNCF et ses partenaires. [en ligne]. [Réf. du 04 Sept.2019 et 01 Oct. 2020]. Disponible sur** Train de Fret Autonome : la 1ère locomotive entre en atelier| SNCF
Site	**[261]**	LaFrenchCom**, Cellule de crise. [en ligne]. [Réf. de 2021]. Disponible sur** Cellule de crise : organisation et management | LaFrenchCom
Site	**[262]**	SNCF**, Stratégie RSE du groupe SNCF en détails. [en ligne]. [Réf. du 01 Juillet 2021]. Disponible sur** La stratégie RSE | SNCF
Rapport	**[263]**	**Déclaration de performance extra-financière, Engagement RSE de Transdev. [en ligne]. [Réf. de mars 2021]. Disponible sur** 2020-dpef_fr_version-seule_finale.pdf (transdev.com)
Article	**[264]**	Courrier International**, Pékin a ouvert sur son sol un nouveau tronçon de chemin de fer qui devrait faciliter l'accès au commerce maritime transitant par Rangoun. [en ligne]. [Réf. du 1er Sept. 2021]. Disponible sur** Du Sichuan à la Birmanie, la Chine s'offre une ouverture sur l'océan Indien (courrierinternational.com)
Article	**[265]**	Agnieszka Kumor**, La Chine tisse les « nouvelles routes de la soie » en Birmanie. [en ligne]. [Réf. du 16 Janvier 2020]. Disponible sur** La Chine tisse les «nouvelles routes de la soie» en Birmanie (rfi.fr)
Article	**[266]**	Sahar Entezari, **Connexion ferroviaire de l'Iran à la Chine par l'Afghanistan. [en ligne]. [Réf. du 16 mai 2021]. Disponible sur** Connexion ferroviaire de l'Iran à la Chine par l'Afghanistan - ISNA
Article	**[267]**	Rédaction Europe1**, Un train chinois arrivé en Iran fait revivre la route de la soie. [en ligne]. [Réf. du 15 Févr. 2016]. Disponible sur** Un train chinois arrivé en Iran fait revivre la route de la soie (europe1.fr)
Article	**[268]**	Sijie Ren et Frédéric Lasserre, **La stratégie ferroviaire chinoise en Asie centrale dans le cadre de la Belt and road initiative : concurrences, conflits et coopérations – [en ligne]. [Réf. de 2020]. Disponible sur** La stratégie ferroviaire chinoise en Asie centrale dans le cadre de la Belt and Road Initiative: concurrences, conflits et coopérations – Conseil québécois d'Études géopolitiques (cqegheiulaval.com)
Article	**[269]**	Xinhuanet, Baidu, **La connotation de « belt and road » est riche et de grande portée. [en ligne]. [Réf. de mars 2015]. Disponible sur** « belt and road » a une riche connotation et une signification profonde - xinhuanet
Site	**[270]**	ENISA**, Risk Management : Helping the EU Railways Catch the Cybersecurity Train [en ligne]. [Réf. du 25 Novembre 2021]. Disponible sur** Risk Management: Helping the EU Railways Catch the Cybersecurity Train — ENISA (europa.eu)
Article	**[271]**	Leedeo**, What Common Safety Methods (CSM-RA) are and when do they apply?. [en ligne]. [Réf. du 02 décembre 2019]. Disponible sur** ▹ What Common Safety Methods (CSMs-RA) are and when do they apply? (leedeo.es)
Site	**[272]**	ERA**, Technical Specifications for Interoperability [en ligne].Disponible sur** Technical Specifications for Interoperability | ERA (europa.eu)
Site	**[273]**	ART**, Du 1er au 4e paquet ferroviaire [en ligne]. Disponible sur** Du 1er au 4e paquet ferroviaire - ART (autorite-transports.fr)
Guide	**[274]**	**Règlement européen sur la protection des données personnelles se préparer en 6 étapes. [en ligne]. [Réf. du 11 avril 2017]. Disponible sur** pdf_6_etapes_interactifv2.pdf (cnil.fr)
Site	**[275]**	**What is Railway SIL Signaling System ? [en ligne]. [Réf. du 14 Janvier 2020]. Disponible sur** What is Railway SIL Signaling System? (raillynews.com)
Article	**[276]**	**La Rédaction Les Horizons, Train futuriste imaginé par Elon Musk et porté aujourd'hui par 3 grandes entreprises à travers le monde. [en ligne]. [Réf. du 18 Janvier 2020]. Disponible sur** Hyperloop • Les Horizons
Article	**[277]**	Christian Hohmann, **La continuité numérique, un facteur d'efficience, [en ligne].[réf. du 15 février 2015] Disponible sur *:*** continuité numérique | Blog de la Nouvelle Industrie (wordpress.com
Site	**[278]**	BEA**, Bureau d'enquêtes sur les accidents de transport terrestre. [en ligne]. [Réf. du 22 Août 2014 modifié le 13 septembre 2016]. Disponible sur*:*** Le Bureau d'Enquêtes sur les Accidents de Transport terrestre - BEA-TT (developpement-durable.gouv.fr)

II. LISTE DES EXPERTS ET THEMATIQUES ABORDEES

Nom et fonction	Période	Axe	Thématiques abordées
MIHAI CHIRCA Responsable Affaires Européennes - Transdev Group Expert Digitalisation et Mobilité Autonome | Affaires Européennes à l'UITP (International Association of Public Transport)	Juillet 2021	Vision normative, niveau européen	Challenges de la cybersécurité dans les transports Démarche de normalisation et gouvernance européenne … Véhicules autonomes Influencing pour l'établissement pour faire des lois et normes au niveau européen Difficultés pour rendre des synergies plus efficaces au niveau européen
SOPHIE BOUILLAND RSSI Transdev	Août - Novembre	Vision RSSI transverse	Cadre de la cybersécurité industrielle Les enjeux dans les transports
YSEULT GARNIER, Responsable cybersécurité industrielle, SNCF RÉSEAU, contributrice groupes de travail ENISA	Septembre et Octobre 2021	Vision cybersécurité industrielle d'un gestionnaire d'infrastructure	Risques convergences IT/OT Stratégie homologation et Respect du GAME Architecture modèles NIST/62443 SOC IT/OT Centre de Supervision et Contrôle Respect des fournisseurs de services IACS des Exigences IEC 62443-2-4 : 2017 et 'IEC 62443-3-3
LAURENT CEBULSKI Directeur Général de l'Établissement Public de Sécurité Ferroviaire EPSF (autorité nationale)	Octobre 2021	Vision autorité ferroviaire	Gouvernance ERA, EPSF, etc., normes, Audits et contrôles
QUENTIN RIVETTE Responsable cybersécurité industrielle SNCF Voyageur	Octobre 2021	Vision cybersécurité industrielle d'un Entreprise ferroviaire (Voyageurs)	Relation EF, GI RGPD France, Europe Risques UX Centre de Supervision et Contrôle et interactions avec le conducteur
JEAN-BAPTISTE RENAULT Responsable cybersécurité France - Alstom	Novembre 2021	Vision Manufacturiers, fournisseurs de produits et solutions (France)	Maîtrise risque de la chaîne d'approvisionnement Exigences constructeurs fournisseurs Security-by-design dans les projets Cybersécurité des produits et services Défense en profondeur Conformité NIST/62443/TS50701 : chaîne de sous-traitants et fournisseurs
EDDY THÉSÉE Vice- Président Cybersécurité Alstom	Novembre 2021	Vision Manufacturiers, fournisseurs de produits et solutions (Vision Monde)	Maîtrise risque de la chaîne d'approvisionnement Intelligence juridique Stratégie de partenariat avec Airbus Stratégie France et Europe, synergies Contribution aux normes TS 50701 Conformité NIST/62443/TS50701 : chaîne de sous-traitants et fournisseurs Innovations Influence et marché niveau mondial Pénétration marché Chine en particulier

Nom et fonction	Période	Axe	Thématiques abordées
JOEL NOIROT Responsable Sécurité Systèmes Informations des Infrastructures Techniques Directeur Numérique de la RED TEAM Groupe SNCF	Novembre 2021	Vision stratégie défensive versus offensive	Défense en profondeur Zéro-Trust et Confiance des actifs, * Qualification des risques d'infrastructure du point de vue de la sécurité des réseaux IT et OT. Protection, détection sans impact sur la productivité et la fiabilité, sans interférence sur les activités critiques Cartographie dynamique (Découverte automatique) des actifs OT (forces et faiblesses) CERT, CIRST,
AMAL EL FALLAH SEGHROUCHNI **Prof Émérite IA** **Présidente du Mouvement AI** **Titulaire de la chaire industrielle d'excellence Thales-SCAI Abu-Dhabi - Sorbonne** **Commission mondiale d'éthique des connaissances scientifiques et des technologies de l'Unesco (COMET)** **Experte internationale spécialisée en IA et systèmes multi-agent**	Novembre 2021	Vision monde de la Recherche sur l'Intelligence Artificielle et les transports	Trains autonomes, IA et systèmes industriels IA dans les transports intelligents (optimisation trafic, signalisation, dev durable) Cybersécurité de l'IA IA et Ethique (trains autonomes)
SADIO BA Coordinateur sectoriel "Transport" ANSSI	Octobre 2021	Vision Agence Nationale de la Sécurité des Systèmes d'Information	Gouvernance Articulation, ANSSI, EPSF, ENISA, etc. ANSSI et PASSI Audits et contrôles, homologation et cybertests industriels Accompagnement dans la et défense en profondeur résilience cyber des OIV Dispositif de Coordination et d'accompagnement en cas de crise majeure
ANTOINE ANCEL Directeur Cybersécurité du Groupe SNCF	Novembre 2021	Vision Management	Gouvernance, gestion risques cybersécurité ferroviaire et Challenges
THOMAS CHATELET Chef de projet ERTMS à l'ERA (European Railway Agency)	Novembre 2021	Vision Europe (ERA)	Gouvernance Européenne, ERTMS, Intermodalité, Budgets cybersécurité, Challenges au niveau européen, etc.

III. INTERVIEWS

III.1. Laurent Cébulski, D.G. de l'EPSF - Établissement Public de Sécurité Ferroviaire

Laurent CEBULSKI, est docteur-ingénieur en mécanique. Il a débuté sa carrière chez Alstom Transport où il a occupé diverses fonctions en bureau d'études et en R&D. Il a ensuite été responsable de majeure et enseignant au sein de l'ESIEE Amiens, puis responsable Recherche/Développement des applications électriques du groupe Carbone Lorraine / Mersen. Il est depuis 2012 directeur des autorisations au sein de l'Établissement Public de Sécurité Ferroviaire. Pendant sa formation à l'ESSEC Executive Education, il a rédigé un mémoire sur « l'impact de la transformation digitale du secteur ferroviaire sur le régulateur ».

Interview réalisée le 14 octobre-2021

VISION, STRATÉGIE, GOUVERNANCE, MISSIONS DE L'EPSF

M. CEBULSKI bonjour, comment s'articule la relation entre l'EPSF et les organisations autour de la sécurité ferroviaire (ETAT, ANSSI, l'armée, ERA, ENISA, UIC) ?

Au début des années 90, face à une part modale du fret ferroviaire en chute, l'Europe se saisit du sujet de l'interopérabilité, partant du constat que les transports ferroviaires qui traversent les frontières subissent les spécificités historiques et les différences de chaque réseau, tels que des écartements de rails, l'alimentation électrique, la signalisation, la barrière de la langue entre les conducteurs qui doivent changer à la frontière, et décide d'instaurer après la rédaction d'un livre blanc, ce qu'on appelle les paquets ferroviaires. Ce sont des jeux de directives de haut niveau que doit transposer chaque État. À terme, elles visent à harmoniser les règles inhérentes au transport ferroviaire entre tous les états européens, notamment les règles techniques pour justement éviter que les trains ne s'arrêtent à chaque frontière.

Il y a quatre paquets ferroviaires, c'est le deuxième qui « intéresse » l'EPSF. Il est sorti en 2004 et a été transposé en 2006. Il est dit que pour préparer l'ouverture à la concurrence le fret à partir de 2006, il faut que chaque état se dote d'une autorité de sécurité indépendante. La directive a été transposée par une loi de 2006 qui crée l'EPSF. Chaque état membre s'est doté d'une autorité de sécurité équivalente à l'EPSF. Le troisième paquet propose entre autres la possibilité de trafic international de voyageurs sans cabotage à partir de 2007, ainsi que l'harmonisation des licences de conducteurs. En 2019 arrive le quatrième paquet ferroviaire qui instaure plusieurs changements :

- Un transfert de compétences de délivrance de certaines autorisations à l'agence européenne ferroviaire (ERA) ; (les autorisations de matériel roulant et les certificats de sécurité d'entreprises ferroviaires) ;
- Toute autorisation internationale (faisant appel à au moins deux États membres) de cette nature est désormais prise en charge par l'ERA.

Si le matériel a une vocation nationale ou que l'entreprise a un rayonnement purement national, le demandeur peut choisir s'il veut être autorisé par son autorité nationale ou par l'agence européenne. En pratique, dans 100% des cas, les entreprises demandent à passer par l'EPSF, notamment parce qu'elles ont l'habitude de travailler avec nous. Le quatrième paquet ferroviaire comporte plusieurs volets, il y a le volet technique que l'on vient d'évoquer et il y a le volet des marchés qui préfigure l'ouverture à la concurrence, telle qu'on entend parler dans la presse, avec par exemple le premier marché remporté par

Transdev en région PACA. Ces nouveaux acteurs font aussi l'objet d'autorisations délivrées par l'EPSF. Après autorisation, on contrôle sur le terrain les acteurs, ce sont des contrôles de processus de sécurité, on notifie des écarts éventuels, et en fonction de leurs nombres et de leur importance, les entreprises peuvent être sanctionnées financièrement, ça peut aller jusqu'à la suspension de leurs autorisations voire dans les cas extrêmes elles leur sont retirées, il en résulterait la fin de l'entreprise.

Nous avons également une troisième mission qui est le suivi de la sécurité. Il y a un arrêté qui oblige tous les exploitants ferroviaires à remonter les événements de sécurité ferroviaire dans une base de données, soit entre 30 000 et 50 000 événements par an. Les analystes consignent ces événements et en tirent les grandes lignes pour organiser le retour d'expérience auprès du secteur et faire en sorte de faire avancer les réflexions sur l'amélioration la sécurité du réseau.

Est-que les 50000 d'événements couvrent tous les secteurs confondus ou seulement les entreprises et les gestionnaires d'infrastructures ?

Uniquement les exploitants ferroviaires (entreprises ferroviaires et gestionnaires d'infrastructure), sachant qu'aujourd'hui il y a près d'une cinquantaine d'entreprises ferroviaires autorisées et une petite vingtaine de gestionnaires d'infrastructure. Il y a au final 70 exploitants sur le réseau aujourd'hui.

Quels sont les autres organismes qui interagissent avec l'EPSF ?

Il y a deux clubs des autorités de sécurité à l'échelle européenne. Le premier réunit tous les trois mois toutes les autorités ferroviaires européennes pour discuter de sujets communs, de bonnes pratiques, comme la publication par l'EPSF des notes de cybersécurité, qui a notamment intéressé les Finlandais, avec qui nous échangeons à ce propos. Il y a également le besoin de passer des accords avec les autorités limitrophes de la France pour gérer les trafics aux sections frontières : dans le cadre du 4e paquet ferroviaire, la gestion des sections frontalières, jusqu'à la première gare pénétrée dans un pays, est dévolue directement entre autorités nationales de sécurité, et cela doit passer par des accords. Le second, le NSA (National Safety Authority) network est le club des autorités de sécurité sous l'égide de l'Agence Européenne qui s'occupe de tous les sujets d'harmonisation réglant les difficultés que l'on peut rencontrer dans nos pays respectifs.

Comment peut-on expliquer le manque d'anticipation des décisionnaires quant aux risques de plus en plus prégnants ?

Il y a deux niveaux, il y a le niveau attaque type rançongiciel ou on bloque tous les systèmes, tous les trains s'arrêtent et il n'y a « rien de mieux » qu'un train qui ne roule pas pour être en sécurité, donc quelque part il n'y a plus de problème de sécurité, sans prise en compte des impacts au niveau passager. Après il y a la vraie cyber attaque avec la prise de contrôle qui est beaucoup plus grave puisqu'elle peut conduire à un événement de sécurité, en fonction de la nature de l'attaque. Si c'est un rançongiciel qui bloque les systèmes de la SNCF, tout le monde va dire "mais que fait la SNCF pour se protéger ?", mais ce n'est pas de la sécurité ferroviaire, si c'est un train poussé contre un autre avec une prise de contrôle, là quelqu'un dira "mais qui est-ce qui vérifie ces trucs-là ?". J'espère que les choses bougeront véritablement afin d'éviter d'en arriver là.

L'ANSSI a beaucoup plus d'informations que nous sur ces sujets de cyber attaque et je pense que s'il y avait une menace imminente, ils tireraient probablement la sonnette d'alarme. Notre périmètre est constitué des risques ferroviaires, autrement dit que les trains freinent, ne se renversent pas, ne déraillent pas, on est encore assez loin de ces sujets de cybersécurité, car nous ne sommes pas mandatés pour cela, même si on imagine l'impact que cela pourrait avoir sur nous, cette dimension cyber.

Quel est le niveau de prises en compte des enjeux de cybersécurité ferroviaire au sein de l'Union européenne ?

Suite à mon intervention, la réunion avec l'ENISA, les Finlandais et les Allemands nous ont contactés , il y a trois ans j'étais en Australie à l'IRSC pour la grande conférence annuelle sur la sécurité ferroviaire, j'avais présenté la transformation digitale et abordé le sujet de la cyber, il y a vraiment eu un grand blanc, à l'époque certains de nos homologues étaient venus me voir en me disant " mais c'est vrai que c'est super intéressant, ça serait peut-être bien qu'on regarde ", mais quelque part il y a une certaine passivité dans certains États où on argue que "tant que la réglementation européenne ne le demande pas…". On a fait le choix de réfléchir un peu en avance de phase sous l'impulsion de l'ANSSI et de l'ERA.

Dans les réponses à appel d'offres des collectivités locales il n'y a peu voire pas de plan cyber, qu'est-ce que cela vous inspire ?

Ça dépend beaucoup de la sensibilité de l'autorité organisatrice, de ses compétences, c'est assez nouveau cette compétence chez elle on a été consulté sur les aspects sécurité ferroviaire, on a expliqué ce qu'était que la réglementation européenne, comment ça fonctionnait, on a répondu à beaucoup de questions, c'est vrai qu'on n'a jamais été questionné véritablement sur les aspects cyber, on n'a pas mis le sujet sur la table parce qu'on en a jugé que ce n'était pas dans notre périmètre, donc on n'était pas là pour préempter des sujets qui relèvent d'autres responsabilités, d'autres compétences, mais oui, il y a peut-être de la sensibilisation cyber à faire au niveau des AOM autorité organisatrice de mobilité, je pense que l'ANSSI doit en faire et en fait pas mal, mais ça c'est un pan qui m'échappe, je ne sais pas quelles actions sont conduites par l'ANSSI vis-à-vis des autorités.

Dans le projet TC Rail et le train autonome, comment est gérée la cyber sécurité dans ce type de solution complexe ?

TC Rail est un sous-ensemble du projet train autonome et dans le projet train autonome il y a un volet cyber qui est piloté par l'ANSSI, il est donc lié à des démonstrations de sécurité. En fait dans les projets de trains autonomes il y a un volet sécurité ferroviaire, démonstration de sécurité ferroviaire et il y a un volet cyber et pour l'instant ça reste deux directions qui avancent en parallèle, sans forcément se concerter, je pense que la consolidation est faite par la SNCF qui est porteur du projet, mais on ne va pas lorgner côté cyber pour l'instant.

AUDITS, CONTROLES, SANCTIONS

Quelle est la fréquence des contrôles internationaux opérés par l'EPSF ?

En fait ce sont nos équipes d'inspecteurs qui prennent contact avec les équipes des inspecteurs belges par exemple ou vice versa présentant le fait qu'une entreprise circule à la fois en France et en Belgique, qu'il est nécessaire d'organiser un contrôle en commun, et deux inspecteurs français et belge vont rencontrer cette entreprise, avec un questionnaire coconstruit et chacun produit son rapport en fonction des sujets, des problématiques nationales avec un tronc commun.

Est-ce que les contrôles concernent aussi le domaine de la cybersécurité ou restent-ils dans la sécurité ferroviaire ?

L'EPSF est la première en Europe à saisir réellement ce sujet. La partie cyber aujourd'hui n'est pas dans les prérogatives inscrites dans la loi et dans le code des transports. En 2017 Thomas Chatelet en charge de la cybersécurité à l'agence européenne, m'a contacté, "*il se*

passe des choses au niveau cybersécurité il y a des réflexions en cours pour l'adhérence entre la sécurité ferroviaire et la cybersécurité, il faudrait qu'on y travaille", qui a débouché sur la création d'un groupe de travail composé de SNCF Voyageurs, l'ANSSI, l'ERA et l'EPSF. Pendant deux ans on a travaillé sur un document qui a été publié et que j'ai présenté au séminaire de l'ENISA. Le risque était que la Commission européenne injecte des critères cyber dans les prérogatives des autorités de sécurité alors même que l'on n'a pas les compétences. Il faut que l'on se dote de ressources ou de formation pour être en mesure de pouvoir vérifier un système de gestion de la sécurité qui deviendrait un système de gestion de la sécurité informatique.

Il existe des auditeurs ISO 27000 pour les audits IT, leur pendant dans le domaine industriel, mais existe-t-il un organisme capable de contrôler une conformité à l'IEC 62 443 ?

La 62 443 est plutôt orientée cyber, aujourd'hui il n'y a pas de disposition cyber dans la réglementation d'interopérabilité de sécurité européenne donc nous sommes sur une base de volontariat sauf pour les organismes OIV ou OSE. Ça vient doucement, après l'articulation des normes techniques européennes il y a un chapeau qui s'appelle les STI (Spécifications techniques d'interopérabilité), ce sont des règlements européens qui s'appliquent à tous les états, il en existe sur le matériel roulant, sur les infrastructures, sur l'exploitation et sur les tunnels. Ce sont des règles de haut niveau qui elles-mêmes appellent des normes. Par exemple, on peut imaginer que sur la STI portant le contrôle commande et signalisation et que l'on injecte des critères de cybersécurité, celui qui demandera une autorisation en lien avec cette STI, devra également respecter la 62443 si elle est appelée par la STI. Il y a des organismes, qui s'appellent des organismes notifiés, en France ce sont CERTIFER et BUREAU VERITAS, qui regarde la conformité à chaque STI d'un demandeur d'autorisation, font un rapport qui est une donnée d'entrée pour que l'EPSF puisse instruire la demande.

Est-on en mesure d'auditer un organisme avec des solutions complexes mélangeant les deux domaines IT et OT ?

Il en existe et on est capable de le faire ; Alstom l'a fait sur une base de volontariat, je sais également que CERTIFER comprend dans ses ressources quelques experts en cyber. Suite aux demandes des industriels, CERTIFER réalise les audits cyber selon l'IEC 62 433. Ils ont une vision assez globale et sont capables de comparer les normes européennes et américaines.

Qu'en est-il de la stratégie d'homologation, qui est appliquée aujourd'hui à la SNCF, est ce que c'est le cas pour toutes les entreprises qui ont un certificat de sécurité ?

Non, c'était un de mes propos lorsque j'avais fait cette fameuse conférence : aujourd'hui il y a les gros acteurs SNCF qui ont les moyens et les compétences pour pouvoir mettre en place une dimension cybersécurité, par contre la petite entreprise de fret n'est pas en mesure d'appréhender la cybersécurité. Je me souviens d'un entretien avec un opérateur à qui j'avais demandé qu'avaient-ils mis en place en matière de cyber, et la réponse qui m'a été donnée est la suivante " on achète du matériel qui est conforme aux normes et pour l'instant on n'en fait pas plus. Nous sommes des exploitants et on ne gère pas directement la partie cyber sécurité du matériel roulant". C'était il y a trois ans maintenant, après nous sommes dans un système, qui lorsque ce n'est pas inscrit dans la réglementation, les entreprises ne vont pas le faire sur une base volontaire, sauf celles qui ont une taille induisant une surface d'attaque à la cyber importante.

On est vraiment sur du multifonctionnel, c'est-à-dire que la cyber représente la protection à un certain niveau matériel, mais aussi la protection de l'organisation, cela forme un tout.

Il y a tout un cadre à bâtir sur la façon dont on va contrôler l'aptitude d'une entreprise à se protéger des attaques que ce soit au travers de son matériel et de la mise à niveau régulière de son matériel et au niveau de son entreprise, éventuellement de l'ingénierie sociale qui peut être faite pour pouvoir pénétrer certaines organisations.

Dans un périmètre plus large, comment peut-on vérifier tous les liens de sous-traitance, et surtout comment vérifier que les sous-traitances ultérieures mettent en œuvre les moyens techniques nécessaires pour leur cyber sécurité ?

Ça pose effectivement un problème, une autorisation en matière de sécurité ferroviaire est figée, c'est-à-dire qu'une fois qu'on a approuvé un matériel roulant si vous ne le faites pas évoluer, son autorisation est valable at vitam aeternam. Par contre si demain, pour des raisons cyber, vous mettez à niveau la signalisation embarquée sous forme de patch par exemple, et que la somme des mises à jour finit par faire un changement substantiel et bien l'autorisation ne porte plus sur ce qu'est devenu le matériel. C'est un vrai sujet parce que cela veut dire qu'il faut repasser par un temps d'autorisation. Sauf qu'un temps d'autorisation ferroviaire, ça prend plusieurs semaines voire plusieurs mois. Quand il faut patcher un matériel parce qu'il est susceptible d'être attaqué on le fait le plus rapidement possible donc le temps ferroviaire et le temps cyber sont une question qu'on n'a pas encore résolue.

Est-ce qu'indépendamment de l'aspect cyber, l'EPSF dans ses contrôles, participent à des vérifications pour s'assurer que les stratégies d'homologation respectent la règle d'or, c'est-à-dire que la sécurité en continu est garantie et qu'il n'y a pas de régression potentielle ?

Non parce qu'aujourd'hui on n'est pas mandaté pour ces contrôles, on va regarder ce qui est dans le règlement sur les méthodes de sécurité commune des systèmes de gestion de la sécurité, cela concerne la gestion documentaire, les habilitations des personnels, la maintenance du matériel roulant ou de l'infrastructure, la politique de sécurité, le retour d'expérience et la remontée des événements. Ce sont des thèmes avec une liste d'une centaine de critères que l'on doit regarder. Demain s'il y a le critère de la politique de cyber sécurité de l'entreprise, on regardera, mais aujourd'hui ce n'est pas notre rôle et c'est d'ailleurs le gros sujet de débat avec l'ANSSI notamment pour savoir quelle est l'autorité compétente pour faire ça.

Aujourd'hui l'ANSSI fait certains types de contrôle et habilite des prestataires pour faire les mêmes types d'audit. L'EPSF spécialisé dans l'industriel ferroviaire a signé un accord avec l'ANSSI, qui est plutôt spécialisé dans le domaine IT, est-ce qu'il est prévu une stratégie d'homologation couvrant ces deux domaines ?

C'est toute la question d'interface et de recouvrement entre nos compétences respectives, c'est d'ailleurs ce qui a donné lieu aussi à ce « Think Tank » dont l'objet était de se demander si demain quelqu'un prend le contrôle d'un train ou d'un poste de signalisation et le balance contre un autre train, qui en serait le responsable ? Est-ce l'EPSF, l'ANSSI ? Ça reste un cadre à construire et pour ça il faut encore qu'on fasse beaucoup de sensibilisation notamment au niveau des décideurs étatiques, globalement çà peut être sous forme de coopération de contrôle commun. On peut aussi imaginer un CERTIFER ou BUREAU VERITAS qui eux vont faire l'audit, émettent également un rapport et ça reste aussi une donnée d'entrée dans l'autorisation, ou alors ça peut être directement l'autorité de sécurité qui le fait, tout est possible. La complexité, c'est que la sécurité ferroviaire tend à viser l'interopérabilité c'est-à-dire l'harmonisation européenne, tout le monde applique la même règle, au niveau cybersécurité pour tout ce qui concerne les domaines régaliens comme la sûreté, chacun a sa stratégie et n'a pas forcément envie de la partager avec son voisin. Il y a une certaine dichotomie entre la volonté d'organisation dans un domaine et

le secret défense dans l'autre domaine, rien que ça représente un frein pour pouvoir déployer cette stratégie d'homologation.

Si un opérateur est sous le coup d'une suspension d'autorisation d'opérer par manquement dans ses mesures de sécurité, comment serait gérée la période de transition entre sa notification et le démarrage d'un nouvel opérateur, en tenant compte du temps nécessaire à la mise en œuvre d'une nouvelle mise en concurrence ?

On peut imaginer que les entreprises qui obtiendront des autorisations dans le cas des appels d'offres seront très exigeantes en matière de sécurité. Elles sont suffisamment sérieuses pour ne pas arriver jusqu'au retrait d'autorisation, en tout cas dans l'histoire de l'EPSF, on n'est jamais arrivé à ce point. S'il y avait un danger grave et imminent identifié, nous le ferions sans réserve. Ça a d'ailleurs failli arriver une fois, mais l'entreprise s'est elle-même retirée, consciente de son impossibilité à mettre en œuvre le niveau de sécurité requis. Il existe un processus d'escalade, on réalise un premier contrôle, on notifie les écarts et au travers de ces écarts il y a un plan d'action qui est élaboré dans un délai plus ou moins court, l'entreprise doit démontrer qu'elle a corrigé la situation. Si effectivement lors d'un nouveau contrôle il s'avère que ces écarts n'ont pas été corrigés, à ce moment-là on passe à des avertissements plus contraignants, voire des restrictions de périmètre, on peut également suspendre des conducteurs, des trains, on émet ses sanctions pécuniaires qui peuvent atteindre 20 000 euros par écart. L'année dernière, j'ai dû en mettre un certain nombre. Il existe une liste de mécanismes en place qui permettent de s'affranchir d'en arriver là.

Les sanctions financières sont-elles assez dissuasives ?

C'est un processus assez récent, en effet ça semble dissuasif pour une petite entreprise de fret, pour la grande entreprise qui possède des fonds plus conséquents, ça le devient par la répétition des sanctions, 20 000 euros par écart, ça peut assez vite chiffrer, mais si ça ne suffisait pas la sanction la plus efficace reste la restriction de périmètre. Mais il y a différents niveaux d'écart, on peut par exemple notifier un écart sur la gestion de la documentation, qui est un écart de réglementation sans impact de sécurité immédiat, ça se traduirait par une sanction pécuniaire. Par contre, une entreprise qui ferait rouler des conducteurs non habilités, le risque est tout autre, dans ce type d'infraction on opterait pour une sanction de restriction, avec suspension des conducteurs, du trafic, etc. Il y a toujours de la mesure dans la façon dont on notifie la gravité de l'écart.

MANAGEMENT DES RISQUES DE SÉCURITÉ ET CYBERSÉCURITÉ

D'après vous qu'est-ce qui est le plus redouté entre la prise de contrôle d'un train et la prise de contrôle d'un passage à niveau ?

Pour moi il n'y a pas de compétition dans la gravité des événements si demain vous prenez un convoi exceptionnel que vous le mettez sur un passage à niveau avec un train qui arrive à 200 km/h, ce sera aussi catastrophique que de balancer un train contre un autre. Donc il n'y a pas de risque plus important au moins important. Bien sûr qu'il faut avoir une vue globale de la menace, mais je pense que sur l'aspect cybersécurité qui va préoccuper tout le monde, la prise de contrôle est la menace la plus redoutée ; lorsqu'un opérateur, censé opérer en toute sécurité, n'a plus le contrôle de son périmètre, que ce soit un train ou de son infrastructure, le pire est à craindre en effet.

On voit Alstom s'allier avec Airbus, et mettre en place des systèmes de sécurité qui englobent l'IT et l'OT. Pourvoir gérer les risques d'un système demande d'avoir établi une cartographie et un inventaire exhaustif des assets, dans le

cadre d'une entreprise comme la SNCF possédant un patrimoine informationnel de longue date, a-t-on les moyens techniques de réaliser cet inventaire ?

Là c'est une question de moyens, faire un inventaire de patrimoine, c'est d'ailleurs normalement une disposition de la réglementation de sécurité ferroviaire, chaque entreprise doit être en mesure de connaître son patrimoine. L'EPSF est plutôt sur de grandes mailles, c'est-à-dire le nombre de passages à niveau, le nombre de postes de signalisation, le nombre de cabines sur lesquels il y a du câblage électrique pilotant des équipements de sécurité et après la charge est à l'entreprise de mettre les moyens suffisants, les outils suffisants, l'organisation et les méthodes suffisantes pour ce faire la caisse et puis suivent son patrimoine dans me temps.

Quelle méthode d'analyse de risques est privilégiée dans le milieu ferroviaire, en IT on privilégie EBIOS RM, qu'elle est celle que vous utilisez ?

En général ce sont des APR (Analyse préliminaire des risques), on touche à du classique de type AMDEC (Analyse des modes de défaillance, de leurs effets et de leur criticité) par exemple, et puis il y a la matrice qui est similaire à celle d'EBIOS, on identifie la gravité d'un côté et l'occurrence de l'autre, sauf que dans les EBIOS on supprime l'occurrence et on met à la place la probabilité d'attaque, mais en gros les philosophies sont à peu près les mêmes. Une identification des risques et des barrières derrières pour couvrir ces risques, les barrières pouvant être une conformité à la réglementation. Il y a trois grands principes:

- Je suis conforme à la règle européenne, ça vaut la présomption de sécurité. Par exemple si mon frein est conçu selon la norme, je sais que mon train va freiner donc n'ai pas besoin de faire de démonstration supplémentaire ;
- Le deuxième principe c'est la comparaison à un système de référence, mon matériel est conçu exactement de la même façon qu'un autre matériel, qui est autorisé, donc je préjuge que ce matériel va se comporter de la même façon, donc ça vaut également barrière ;
- Le troisième principe, c'est la démonstration explicite, la règle n'existe pas, le système de référence n'existe pas, donc je fais une démonstration basée sur la sûreté de fonctionnement.

Est-ce que vous pensez qu'il y a une volonté de pouvoir mettre en place une méthode d'analyse de risque qui prenne en compte les deux domaines ?

Je pense que c'est le sens de l'histoire, mais que ça va prendre du temps, ne serait-ce que pour bâtir une méthode qui convienne à tout le monde et qui soit compatible à la fois avec la sécurité ferroviaire et puis l'aspect cyber. Je pense qu'il faut que ça vienne à la fois de l'Europe et des ministères qui sont à même de prendre ces réglementations. Après ma conviction personnelle, indépendamment du poste que j'occupe, c'est que comme dans beaucoup de systèmes, on est souvent dans du curatif et que le jour où il y aura un événement de sécurité, les choses s'accéléreront, mais tant qu'il ne se passe rien, tout ça va continuer un peu à vivoter.

CONCURRENCE INTERNATIONALE ET GUERRE ÉCONOMIQUE

Quid de l'espionnage étatique à des fins de suprématie concurrentielle ?

Il y a un axe qu'il ne faut pas négliger notamment côté Asie pour pénétrer l'Europe, on entre aussi par le biais des normes notamment en prenant le pilotage de certaines normes internationales, ce qui permet d'orienter la norme en fonction de vos compétences ; cet aspect normatif est important et c'est vrai que l'on a tendance à ne pas forcément y mettre toutes les ressources alors que c'est stratégique.

On voit que la Chine s'immisce de plus en plus dans les organismes de normalisation pour faire basculer la balance de son côté, est-ce que c'est quelque chose qui est visible au niveau européen ? Est-ce qu'au niveau de la France on fait ce qu'il faut pour rattraper le retard que l'on a pris ?

Je sais que ça préoccupe un certain nombre d'industriels, qui m'en parlent et qui sont attentifs au fait de prendre les bonnes places au sein des comités normatifs, pour garder la main. Ces normes sont bâties par les industriels eux-mêmes sous la supervision d'organismes comme le CEN-CENELEC. L'EPSF n'est pas élaborateur de normes, mais contributeur à l'élaboration de réglementations ; l'EPSF a un droit de regard pour dire "*là attention ce que vous écrivez ce n'est pas très « Safe » donc nous ne sommes pas d'accord*", mais sinon la balle est dans le camp de l'industrie.

Est-ce que les trains chinois entrent en France ? On a évoqué le fait que tous les trains qui viennent de pays hors Union européenne devaient avoir un certificat de sécurité pour pouvoir éventuellement entrer. Durant la COVID, l'augmentation du trafic des trains venant de chine pour ravitailler l'Europe a augmenté significativement. Est-ce qu'ils s'arrêtent aux portes de l'Europe ?

Je pense qu'il doit y avoir des problèmes de gabarits différents entre l'Europe et donc aux frontières le relais est pris par une entreprise européenne qui prend la suite de wagons et qui l'emmène à bon port.

Par contre il faut savoir qu'il y a deux ans, CRRC, le constructeur chinois a racheté Vossloh, les locomotives allemandes, ça lui a permis de mettre un pied en Europe même si aujourd'hui on ne les a pas encore vu en France. Et puis du côté Asie on a également un grand de la signalisation qui est Hitachi qui a racheté Ansaldo, fournisseurs majeurs du système de signalisation européen.

FORMATION, COMPÉTENCES

Qu'en est-il de la sensibilisation et de la formation au niveau de l'EPSF ?

On fait une première formation pilote en novembre donc 10 agents de l'EPSF, on s'est associé avec le Service Technique des Remontées Mécaniques et des Transports Guidés, un métro et un tramway sont aussi susceptibles d'être attaqués, on a des problématiques communes, on va faire une première formation pilote cette année, pour vraiment faire de la sensibilisation.

Y at-il des formations universitaires aujourd'hui qui abordent l'IT et l'OT ?

Il existe des boîtes qui proposent des formations, certaines sont homologuées par l'ANSSI et nous avons pris des contacts pour bâtir un programme sur mesure, on ne voulait pas d'une formation purement informatique, mais abordant toutes notions de risque et d'impact dans le domaine ferroviaire.

Outre les sujets déjà abordés, est-ce que vous entrevoyez d'autres challenges ?

Oui il y a tout ce qui touche aux nouvelles technologies numériques au sens large, tout ce qui est IoT avec déploiement massif sur le réseau. Je pense que l'aspect IA est un sujet important, par exemple celle utilisée pour reconnaître les obstacles ou la signalisation dont on viendrait modifier juste quelques pixels pour éventuellement biaiser le regard qu'elle a de l'obstacle. Tout ce qui lie à l'autonomie et la numérisation d'une manière générale, c'est plus de numérique qui se traduit par l'augmentation des surfaces d'attaque.

Merci beaucoup, Laurent, pour le temps que vous avez bien voulu nous consacrer.

III.2. Sadio BÂ, Coordinateur Sectoriel « Transport » - ANSSI

À l'ANSSI depuis 2014. Consultant pendant 5 ans chez Capgemini, Directeur de Projet à la SNCF, auditeur à l'IHEDN, Master à l'Ecole Centrale et un MBA Business Administration and Management, un Master en Electrical and Electronics Engineering.

« *J'ai pour principe structurant, la conviction que les technologies de l'information et de la communication sont le levier majeur de transformation des organisations au service de la performance et un contributeur prééminent au développement durable* ».

Entretien du 27-10-2021 et du 8-11-2021

CADRE D'INTERVENTION DE L'ANSSI

L'ANSSI a signé un accord avec l'EPSF, en quoi consiste cet accord et quelles sont les actions de l'ANSSI sur la montée en compétence de l'EPSF ?

L'accord signé en mars 2018, qui se nomme « lettre d'intention de coopération », entre l'autorité de sécurité des systèmes ferroviaires en France et l'autorité de cybersécurité en France, vise à rapprocher les deux autorités de sécurité et à mutualiser les approches, c'est aussi de faire en sorte que la cybersécurité puisse distiller les différents corpus réglementaires, les différentes références de sécurité à terme dans le transport ferroviaire. Il a été rédigé une note d'une vingtaine de pages dans laquelle nous avons apporté notre éclairage commun sur les enjeux de cybersécurité dans le ferroviaire et dans le but de faire passer le message suivant : « on ne peut plus considérer aujourd'hui la sécurité ferroviaire suivant les principes qui la régissent depuis 40 à 50 ans, on se doit d'intégrer aujourd'hui la cybersécurité dans la sécurité ferroviaire. » Aujourd'hui les choses avancent, ce discours commence à être intégré. Il est clair que la réglementation imposée pour les OIV et OSE, comme la LPM (loi de programmation militaire) et la NIS (Network and Information Security), ont aidé à cette évolution. L'explosion aujourd'hui des attaques cyber a aussi permis la prise de conscience, on ne peut plus faire juste de la sécurité et de la sûreté de fonctionnement classique sans y ajouter la cybersécurité et prendre en compte la malveillance.

Que ce soit dans le milieu de l'automobile avec l'autorité de sécurité qui s'appelle le CNRV (Centre National de Réception des Véhicules), que ce soit dans le transport guidé c'est-à-dire les tramways et des métros avec l'autorité de sécurité STRMTG (Service technique des remontées mécaniques et des transports guidés), ou dans le ferroviaire avec l'autorité de sécurité l'EPSF, l'ANSSI ne peut pas couvrir l'ensemble des champs d'activité, elle est certes compétente dans la cybersécurité, mais elle ne l'est pas de façon verticale. Il lui est impossible de couvrir l'ensemble des champs d'activité. La stratégie est de responsabiliser les autorités de sécurité qui délivrent les autorisations de mise en service afin qu'ils intègrent dans leurs référentiels la cybersécurité. L'objectif sera globalement atteint avec le CNRV en 2022, c'est en cours avec le STRMTG notamment pour les systèmes de transport autonome.

Aujourd'hui, pour le ferroviaire qui se distingue par la réglementation, des passerelles existent, le travail doit se poursuivre.

En se basant sur l'ouverture à la concurrence et à l'arrivée de nouveaux opérateurs dans les secteurs réglementés, comment et quand est revue la liste des OIV et des OSE ?

L'ANSSI n'est pas en charge de la désignation des OIV, ce sont les ministères coordinateurs, le SGDSN (Secrétariat Général de la Défense et Sécurité Nationale), et la PSE (Protection de la Sécurité de l'État) qui vont définir les OIV. Ce processus est extrêmement long et lourd. Il y a juste 2 rendez-vous annuels, les CIDS (Commissions Interministérielles de Défense et de Sécurité) qui se réunissent en juin et en décembre. Ces réunions, animées par un préfet, permettent de mettre à jour ces listes.

Quid de la distorsion de concurrence dans les réponses à appel d'offres du fait que certains opérateurs sont désignés comme OIV et d'autres non, avec du coup des contraintes financières différentes avec un avantage pour les non OIV ?

C'est un vrai sujet, nous sommes déjà confrontés à cette situation aujourd'hui. Il y a une distorsion potentielle de sécurité aujourd'hui, car pour les OSE (opérateurs de services essentiels) devant suivre la directive NIS (Network and Information Security) la désignation est dévolue à l'ANSSI avec un arrêté de désignation. Dans la version actuelle, l'ANSSI peut instruire cette désignation en 6 mois, de plus il n'y a pas la contrainte du Secret Défense, mais c'est bien les opérateurs qui émettent leur volonté de devenir OSE, pour des raisons diverses (justification budgétaire, politique, etc.).

Pour information, la liste des OIV est classifiée, par contre celle des OSE ne l'est pas, mais elle n'est pas diffusée.

Qui et comment sont définis les SIIV ?

Ce sont les opérateurs mêmes, qui identifient les systèmes d'information, en identifiant ce qui bloquerait l'entreprise en cas de compromission. Au niveau de la LPM, il existe un mécanisme, qui permet de définir les SIIV, au sein de ces secteurs, il y a des opérateurs qui ont été identifiés, privés comme publics, les opérateurs sont soumis depuis 2006-2007 à des règles de protection physique, suite aux attentats du 11 septembre. Toute une réflexion est née autour de ces problématiques, qui a débouché sur la création de points d'importance vitale (PIV). De fait chaque OIV a au moins un PIV, qu'il doit sécuriser. En 2013, le législateur voyant la menace cyber grandir décide d'ajouter un volet cybersécurité au volet sécurité physique. On s'est appuyé sur ces SAIV et les OIV, et le 18 décembre 2013 la loi de programmation militaire (LPM) a été promulguée, quatre articles concernent la cybersécurité dont l'article 22, le législateur décide que dorénavant on demandera aux opérateurs de protéger leurs systèmes d'information les plus sensibles et les plus critiques pour la Nation. Les décrets d'application sont sortis en 2015, et les arrêtés sectoriels sont sortis à partir de 2016. Pour identifier ces SIIV (systèmes d'information de la portance vitale) chaque secteur dispose d'une DNS (Directive Nationale de Sécurité) rédigée par les ministères coordinateurs et les ministères de tutelle, pour les transports terrestres, c'est le ministère des Transports. La DNS est une macroanalyse de risque réalisé par l'État sur le secteur, ça comprend les risques pandémiques, les risques terroristes et les risques cyber. Dans ce document se trouve un autre point important, les missions dites vitales. L'État définit les missions qu'il considère comme vitales par secteur pour la Nation. Tous ces documents sont classifiés SECRETS. Ces missions vitales vont servir à alimenter la réflexion de l'opérateur pour identifier ses systèmes d'information d'importance vitale.

La LPM précise qu'il faut sécuriser et appliquer des règles de sécurité, qui sont au nombre de 20, sur les systèmes les plus critiques et les plus sensibles, ce sont les SIIV qu'il est nécessaire d'identifier en amont. Cette identification repose uniquement sur l'opérateur, en aucun cas l'ANSSI désigne tel ou tel SI. L'opérateur réalise une analyse d'impact (et non une analyse de risque) qui lui permettra de définir quel système mettrait en péril la réalisation des services d'intérêt vital que doit fournir l'opérateur, s'il venait à être attaqué, il est alors défini comme Système d'Information d'Intérêt Vital. Dans les faits l'ANSSI en concertation avec l'opérateur peut avoir un avis éclairé qui peut se reposer sur l'expérience d'autres opérateurs, faire des commentaires. Dans cet arrêté il y a 4 annexes. Il y a une

annexe avec les règles de cybersécurité, qui est publique et accessible sur Légifrance[402]. Les 3 autres annexes sont en diffusion restreinte ; une concerne les délais d'application pour chacune des règles, une autre concerne les typologies d'incidents qu'il faut remonter à l'ANSSI et la dernière concerne les typologies de systèmes qui pourraient être SIIV.

La LPM propose aux OIV cette annexe. Elle leur permet d'ajouter des systèmes qui n'ont pas été recensés par contre s'il existe un système dans son environnement qui est listé dans l'annexe et qu'elle ne le définit pas comme SIIV alors elle doit justifier son choix et l'argumenter.

Comment dans un OIV, détermine-t-on le PIV[403] ?

Le PIV n'est pas de la cybersécurité, leur création date d'avant 2013, il y a des documents que doit rédiger l'opérateur, on appelle ça un PSO (Plan de Sécurité Opérateurs), en s'appuyant sur sa DNS (Directive Nationale de Sécurité), l'opérateur va rédiger son PSO, on lui fournit un plan générique, on lui demande de travailler et d'identifier ce PIV. Il est validé par l'État par le ministère coordinateur. Pour chacun de ces PIV, l'opérateur doit rédiger un PPP (Plan de Protection Particulier). Comme vous pouvez l'entrevoir, c'est une démarche lourde.

Il y a un arrêté sectoriel qui a été signé en 2016, à destination du secteur ferroviaire, suite à la loi de programmation militaire, est-ce que cet arrêté permet de renforcer la sécurité au plus haut niveau hiérarchique au sein des OIV ?

En effet cet arrêté, réalisé par l'ANSSI et entré en vigueur le 1er octobre 2016, concerne certaines catégories d'opérateurs publics comme privés que l'on nomme OIV (Opérateurs d'Importance Vitale), pour lesquels une réglementation qui peut déboucher sur du pénal si elle n'est pas respectée, la loi leur impose de sécuriser leurs systèmes identifiés comme les plus sensibles et les plus critiques, que l'on appelle les SIIV (Systèmes d'Information d'Importance Vitale). Cette réglementation est très horizontale, elle a été rédigée par l'ANSSI et coconstruite avec les secteurs. Elle ne concerne pas tous les opérateurs et ne concerne pas tous les systèmes. Ce n'est pas la réponse, c'est une réponse pour des raisons régaliennes, la loi parle de survie de la nation, elle parle de potentiel de guerre, elle parle de potentiel économique, elle parle de protection des populations, c'est une réglementation qui correspond à certains opérateurs pour certains systèmes. Il faut distinguer ce qui relève de l'obligation réglementaire du champ libre.

Qu'est-ce qui permet aujourd'hui, alors que les SIIV sont correctement sécurisés par la réglementation, de s'assurer que les écosystèmes autour de ces SIIV le soient aussi ? Les interfaçages entre ces SIIV ne permettent pas l'augmentation des surfaces d'attaque ?

Il est clair qu'en cybersécurité le risque zéro n'existe pas, il est difficile en cybersécurité d'établir des métriques opposables, donc mettre en place les moyens pour s'armer contre la cybercriminalité. Via en amont une analyse des risques, une architecture résiliente, une défense en profondeur, un système de supervision et de détection des attaques, un système de réponse à incident, des systèmes de tests de robustesse et d'audit. Pour les SIIV on va demander de mettre en œuvre des règles très classiques de cybersécurité, de gouvernance, d'homologation de systèmes, de maintien en conditions de sécurité, d'isolation, de détection, de corrélation, de journalisation, de réponse à incident, d'identification, d'authentification, d'administration, etc. Ce sont de bonnes pratiques à

---

[402] *RÈGLES DE SÉCURITÉ RELATIVES AU SOUS-SECTEUR D'ACTIVITÉS D'IMPORTANCE VITALE « TRANSPORTS TERRESTRES »* [En ligne]. [Réf. Du 11 aout 2016]. Disponible sur Article - Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale

[403] *Glossaire- ANSSI* [En ligne]. Disponible sur Glossaire | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

l'état de l'art. De fait ces SIIV sont protégés et travaillent avec d'autres systèmes d'information au sein de l'entreprise, si les choses ont été faites avec une protection périmétrique et en profondeur alors on garantit une bonne protection pour les SIIV.

CONFORMITÉ, SANCTIONS, AUDITS

A-t-on les moyens de contrôler la conformité de tous les OIV ?

Par le décret de 2009, l'ANSSI est l'autorité nationale de sécurité des systèmes d'information. Le décret de 2011 désigne l'ANSSI comme autorité nationale de défense des systèmes d'information. La LPM dit quatre choses :

- Identifier des SIIV que vous devez déclarer et que vous devez sécuriser ;
- Les OIV doivent sans délai H24 notifier l'ANSSI dans le cas de la survenue d'un incident de sécurité sur ces SIIV ;
- Le Premier ministre, en cas de force majeure dans le pays, peut demander aux OIV d'effectuer une opération d'urgence, typiquement couper leurs connexions Internet ;
- Et l'ANSSI peut contrôler de la conformité, ou des prestataires qualifiés par l'ANSSI pour vérifier le niveau de sécurité.

À date nous sommes plutôt sur un régime de bienveillance vis de certains opérateurs au regarde de lourdeur des transformations à opérer pour être conforme à la réglementation. Certains contrôles d'OIV ont déjà eu lieu. Après la crise sanitaire, nous avons un plan de contrôle pour 2021 qui a été mis en place et commencé. La loi précise bien, que les contrôles puissent être réalisés par l'ANSSI ou par un prestataire qualifié par l'ANSSI, ce sont les qualifications PASSI (Prestataires d'Audit de la Sécurité des Systèmes d'Information). L'ANSSI peut tout à fait s'adosser sur les prestataires qualifiés pour diligenter les contrôles.

Est-ce que le Top Management des OIV a pris en compte ces enjeux de cybersécurité ? Que se passe-t-il si un OIV ne respecte pas les obligations réglementaires de sécurité, quels sont les moyens de sanctions de l'ANSSI ?

En tant qu'autorité de régulation, la question ne se pose pas, un OIV se doit d'appliquer la loi. Il risque au pénal une amende pouvant aller jusqu'à 150 000 € par manquement observé, 750 000 € pour les personnes morales et 150 000 € pour les personnes physiques. Dans le transport ferroviaire, le dispositif est mis en place depuis le 1er octobre 2016, soit trois ans pour se mettre en conformité. Dans les Comex on constate clairement que le virage est pris et que tout le monde mesure parfaitement les enjeux encourus au niveau de la cybersécurité.

Puisqu'on agit dans le cadre de lois et réglementation, en cas de litige, c'est devant les tribunaux que cela finit par se régler. L'ANSSI à la différence de la CNIL n'a pas le pouvoir d'injonction ; ce sont bien les juges qui décideraient de sanctions pénales. Il y a une possibilité d'ajouter dans les missions de l'ANSSI, ce pouvoir d'injonction, lui permettant de sanctionner directement les opérateurs qui seraient en décalage avec la réglementation imposée aux OIV.

Quelle est la profondeur des audits réalisés au niveau du transport ferroviaire, s'arrête-t-on à la sécurité ou va-t-on jusqu'au niveau du logiciel ?

Il est évident que le sujet du ferroviaire est un sujet complexe, prenons l'exemple d'un opérateur qui propose un service de fret ou de transport de voyageurs, qui se base sur du matériel fourni par les fournisseurs, la loi s'applique à l'opérateur, l'exploitant. L'exploitant est tributaire d'un fournisseur de solutions (exemple Thales, Alstom, etc.), la

réglementation repose sur l'opérateur, l'exploitant. C'est à l'opérateur d'exporter les contraintes dans son cahier des charges au niveau du constructeur. Il n'y a pas encore dans le transport ferroviaire de réglementation sur la cybersécurité. La LPM répond au niveau horizontal aujourd'hui sur les exploitants et sur leurs contraintes. Demain il faudrait une réponse verticale qui puisse prendre en compte toute la chaîne composant l'organisation, etc. La seule exigence matérielle qu'impose l'ANSSI aujourd'hui, c'est la mise en place d'une sonde de détection qualifiée par l'ANSSI, c'est la règle 7 si de la LPM.

ANSSI et L'EUROPE : NORMES, INFLUENCING

Au niveau européen, quel est le rôle de l'ANSSI dans l'établissement des normes en cybersécurité, par exemple la TS 50 701 ?

L'ANSSI n'intervient pas directement, il y a des groupes qui sont constitués pour réaliser ce genre de mission. Il y a, au niveau de l'ANSSI, une personne qui suit les aspects normatifs, mais au vu de l'importance des tâches, l'ANSSI ne possède pas les ressources nécessaires pour participer à tous.

Au niveau européen, dans ces groupes de travaux, le lobbying est omniprésent, quel est le poids d'une autorité comme ANSSI par rapport aux poids lourds du secteur industriel ?

Dans le cadre de l'automobile, on a travaillé dans l'élaboration d'une réglementation pour l'homologation des véhicules qui a un caractère obligatoire, on a introduit un critère d'exigence en termes de cybersécurité. Dans le groupe dans lequel j'intervenais, il y avait évidemment du lobbying, on travaillait avec des délégations sectorielles, des constructeurs allemands, des équipementiers, et chacun essaie de favoriser des règles qui leur faciliteraient leur production. En tant que représentant de l'ANSSI, et par conséquent de la France, tout était assez transparent entre les parties contractantes. Contractant est l'autre nom des gouvernements. Évidemment les constructeurs, les fédérations, sont écoutés, mais il n'en reste pas moins que ce sont les parties contractantes qui votent ces réglementations.

Pour les normalisations, c'est beaucoup plus ouvert. On est dans l'élaboration d'un consensus entre les différentes parties prenantes.

Sur quel référentiel s'appuie l'ANSSI lorsqu'on lui propose une solution innovante soit pour l'homologation soit pour sa certification c'est-à-dire la validation d'un niveau fonctionnel réalisé ?

L'une des règles que l'on demande et qui est l'une des plus importantes est le besoin d'homologation de sécurité d'une solution. Elle correspond à l'autorisation de mise en service après avoir réalisé différentes actions de la part de l'industriel. Pour les OIV, ils ont l'obligation d'homologuer chacun de leur SIIV.

Pour ce qui est de la certification, elle est dévolue à un composant qui dispose d'une fonction de sécurité. On va évaluer la robustesse de cette fonction de sécurité et l'exactitude de ce qui est dit dans le mode d'emploi. Si c'est conforme, on délivre une certification. Pour ce faire on s'appuie sur des méthodes et des référentiels existants. Il est important au niveau européen et pour l'uniformisation que tout le monde s'appuie sur les mêmes méthodes des mêmes référentiels.

Pour la cybersécurité, il y a un cadre qui s'appelle les critères communs[404], c'est l'ISO 15 408, méthode utilisée depuis 40 ans et reconnue dans le monde entier qui permet de

[404] *CERTIFICATION CRITÈRES COMMUNS* [En ligne]. [Réf. Du 18 avril 2002]. Disponible sur Certification Critères Communs | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

certifier les composants ayant une fonction de sécurité. Il existe un organisme en Europe qui se nomme le SOGIS[405] (Senior Officials Group Information Systems Security) qui s'assure qu'une certification réalisée dans un pays de l'Union européenne soit valable dans un autre pays. Les niveaux d'assurance des critères communs en cybersécurité s'étalent du niveau EAL1 à EAL7[406]

Une fonction de sécurité certifiée EAL7 est une fonction qui a été testée jusqu'au niveau cryptographie : cela veut dire qu'elle fait l'objet de tests très poussés en termes de sécurité (en boîte noire, boîte grise et boîte blanche, pentests, analyse de code, etc.). Des laboratoires français appelés CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) qui sont agréés par l'ANSSI et accrédités par le COFRAC (Comité français d'Accréditation) sont en charge de l'évaluation des critères communs à minima ceux de niveau 1 (deux à trois points à respecter, plus de la gestion documentaire). Certains CESTI sont spécialisés en matériel et d'autres en logiciels. Une fois le dossier réalisé, le CESTI le remet à l'ANSSI, qui en tant qu'autorité de certification nationale, délivre ou non la certification.

L'avantage de cette certification différenciante, basée sur ces critères communs, est qu'elle est reconnue dans toute l'Union européenne. Néanmoins elle ne répond pas à tous les sujets de cybersécurité. Par exemple, il n'existe pas à ce jour de méthode pour certifier un train. Des travaux sont lancés au niveau européen afin d'élaborer une méthode de certification de solutions complexes.

CYBERSECURISATION DES TRAINS AUTONOMES

On peut imaginer qu'aujourd'hui il n'est pas possible de certifier des solutions pour les véhicules autonomes et encore moins pour les trains autonomes ?

Dans un véhicule aujourd'hui il existe 100 calculateurs, ce sont les ECU (Electronic Control Unit, unité de commande électronique). Ces ECU vont gérer l'injection, les essuie-glaces, gérer l'ABS, le freinage, etc. Il est impossible d'imaginer de pouvoir certifier les 100 ECU. Et même si on pouvait les certifier toutes unitairement, la question de certification des 100 ECU, une fois assemblée, reste entière. En effet rien ne nous dit qu'une fois montées ensemble, dans une même solution, nous n'aurions pas des problèmes de compatibilité qui induiraient des pertes d'efficience dans les fonctions de sécurité sur l'une ou l'autre de ces unités de commande. Il n'existe donc pas aujourd'hui de méthode permettant de certifier des solutions comme un train ou un véhicule dans sa globalité. Pour résoudre ce problème, aujourd'hui on passe par de la réglementation, on passe par de la normalisation, mais il manque aujourd'hui la preuve. Pour compenser ce manque, on travaille beaucoup sur des démonstrations de sécurité sur des « jumeaux numériques ». Comment s'assurer et faire une démonstration de sécurité d'un véhicule qui se meut grâce à de l'intelligence artificielle. Ce sont effectivement des sujets nouveaux, avec beaucoup de recherche dessus, il n'est plus possible d'avoir des approches classiques, avec des abaques. Nous sommes sur un sujet où il n'est pas possible de tester tous les chemins possibles et inimaginables de ce type de système. Il y a aujourd'hui beaucoup de travaux sur les véhicules autonomes et ce sujet-là est prégnant sans parler de la cybersécurité. Le véhicule autonome de niveau quatre n'est pas encore autorisé de toute façon.

Le premier train autonome a été mis en production en Allemagne au mois de septembre, en France des tests ont été réalisés dans le nord de la France. Sur qui peut s'appuyer l'industriel qui veut réaliser ce type de solution et s'assurer qu'il

[405] *Senior Officials Group Information Systems Security* [En ligne]. Disponible sur https://www.sogis.eu/index_fr.html
[406] *Les critères communs – CISA* [En ligne]. [Réf. Du 10 aout 2006]. Disponible sur The Common Criteria | CISA

a mis en place tout ce qu'il faut en termes de sécurité et de mesure de cybersécurité ?

L'ANSSI travaille sur deux projets qui ont débuté il y a trois ans avec une échéance en 2024 (TC Rails), réalisés par deux consortiums, il y en a un qui concerne le fret et qui s'appelle Convoi Fret, et un qui concerne le service voyageurs le TER. Ce sont deux projets parallèles à 27 millions d'euros chacun. Dès l'origine du projet l'ANSSI a dit qu'il faut accompagner ces projets sur le plan cybersécurité. On a commencé dans un premier temps par les ateliers d'analyse de risque, on a utilisé EBIOS RM sur les deux projets, il y avait un aspect architecture, mais ils ont fait appel à des sociétés faisant partie du consortium et spécialisées dans le domaine. L'ANSSI et la SNCF sont sur les deux projets, mais néanmoins restent étanches l'un envers l'autre. En 2023 il est prévu de réaliser un audit de sécurité sur le prototype final. On est au niveau Goa2 aujourd'hui. Dans ce domaine nous sommes encore dans l'expérimentation, il n'y a pas d'exigence réglementaire à date. Cet été trois codes ont évolué, le Code de la route, le code des transports et la responsabilité pénale, ces 3 codes ont été clarifiés sur des véhicules à délégation de conduite, c'est-à-dire les véhicules autonomes. Dans le Code de la route, il est précisé que vous devez toujours être derrière le volant et maîtriser votre véhicule, on parlait d'un homme, aujourd'hui on parle d'un homme ou d'un système. Pour le code du transport, c'est l'évolution permettant de faire évoluer sur la voie publique des véhicules sans conducteur. Et pour la responsabilité pénale on a introduit dans le droit, la responsabilité du système et non plus de l'être humain qui conduirait le véhicule. Donc, depuis cet été, la France à un corpus réglementaire qui permet de faire rouler des véhicules autonomes. Ce qui permettra demain en cas d'accident provoqué par le système de délégation de conduite, de pouvoir incriminer le système et par conséquent le constructeur et non plus le conducteur.

MENACES, CAPACITES OPERATIONNELLES GESTION DE CRISE

Quelles sont les typologies de menaces que l'ANSSI identifie ?

Il existe dans la littérature pléthore de catégorisations de menaces en tout genre. Nous avons pour habitude d'en comptabiliser 4 grandes menaces :

- La criminalité à but lucratif, faire de l'argent ;
- L'espionnage ;
- Celle la plus prégnante, à laquelle répond la LPM ; le sabotage et terrorisme ;
- La manipulation d'image, des opinions.

D'ailleurs à propos d'une cyber-attaque terroriste sur le ferroviaire avec des impacts humains peut être requalifiée comme un acte de guerre ?

Ce sont des questions qui ne sont pas encore stabilisées. Est-ce que si je me fais attaquer par du cyber, je peux me répondre par des actes physiques ? Ce n'est pas encore légiféré. Certains pays utilisent sans doute des cybercriminels pour réaliser certaines actions d'État. Ce sont de vraies problématiques auxquelles il faudra un jour répondre.

Il est intéressant de regarder depuis 5 ans l'évolution du cyber offensif, de l'intelligence et de l'espionnage, qui ne sont pas des modes opératoires de l'ANSSI qui est que dans le défensif et dans la sécurité. Mais il est certain qu'il est plus facile de se défendre quand on connait son agresseur, et que le partage des modes opératoires facilite la mise en œuvre de sa défense.

Nous avons une autre menace qui semble se profiler avec l'arrivée de la 5G. La « boîte à outils[407] » de l'UE pour la 5G et dans le cadre de Cybersecurity Act européen donne pouvoir et prérogative aux États ou les autorités habilitées d'Intervenir auprès des opérateurs de télécoms afin de vérifier la mise en œuvre de mesure de sécurité ou le cas échéant en mettre. Quelle est la nature et le périmètre d'intervention de l'ANSSI ?

Sur la 5G et sur les antennes, il existe un décret qui octroie à l'ANSSI la compétence pour autoriser le déploiement des antennes 5G sur le territoire national. Il est important de s'assurer que leur implantation ne menace pas sur certaines zones sensibles en étant physiquement installé trop près des installations. La nouvelle LPM, 2019-2024, étend les prérogatives de l'ANSSI et notamment envers les opérateurs de télécommunication. Elle prévoit la possibilité de positionner des sondes de détection chez les opérateurs Télécoms (et c'est à date notre périmètre d'intervention. Les cyberattaques passant par les flux réseaux, il devient vital de pouvoir les détecter au plus tôt et de permettre d'avoir de meilleures réponses, ce qui a poussé le législateur d'offrir cette prérogative à l'ANSSI.

Comment sont gérés au niveau européen en termes de responsabilité, les risques inhérents aux transports ferroviaires transfrontaliers ?

C'est identifié au niveau européen, dans la nouvelle directive SRI[408] (NIS), beaucoup de mécanismes et structures sont mis en place pour renforcer la coopération entre les états membres en termes de cyber sécurité au niveau opérationnel. Bien qu'il y ait eu des discussions sur la possibilité d'une super agence européenne, capable de projeter les équipes depuis Athènes, la France ne souhaite pas que ces structures interviennent au sein des états membres. La position de la France est la suivante : ces structures doivent être implantées en local près des opérateurs de chaque pays et de leur tissu économique. Cela permet aux États de développer leur capacité opérationnelle au niveau de leurs territoires et à même de projeter leurs équipes. La France et l'Allemagne sont plutôt en avance dans ce type d'organisation avec un bon niveau de maturité, ce qui n'est pas forcément le cas d'autres pays qui partent de beaucoup plus loin et pour lesquels s'est beaucoup plus compliqué. Pour résumer, nous ne sommes pas partisans de la mise en place de cybers pompiers européens.

Comment s'organise les interventions de l'ANSSI lors d'une crise cyber chez un OIV ? Est-ce que l'ANSSI peut intervenir sur les organismes importants malgré le fait qui ne soit pas OIV ?

N'oubliez pas que les OIV ont une obligation de déclaration de tout incident sur leurs SIIV sans délai auprès de l'ANSSI. Ce qui déclenche en fonction du niveau de gravité l'intervention avec ou sans projection d'équipes dimensionnées pour répondre à la crise. L'ANSSI est énormément sollicitée dans ce cadre même si l'organisme n'est pas OIV ou OSE, l'ANSSI a la même écoute, le même appui et propose le même soutien. Nous avons été maintes fois été sollicités par exemple par les hôpitaux, qui n'étaient des opérateurs régulés, l'ANSSI a projeté des équipes. On propose de l'accompagnement sur la remédiation, et maintenant les équipes réalisent même de l'analyse forensique pour aider à judiciariser les dossiers et accompagner dans la dépose des plaintes Quand c'est considéré comme important ou médiatiquement sensible et que l'on n'est pas en mesure

[407] *Secure 5G networks: Questions and Answers on the EU toolbox* [En ligne]. [Réf. Du 29 janvier 2020]. Disponible sur Réseaux 5G sécurisés : la boîte à outils de l'UE (europa.eu)

[408] *Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148* [En ligne]. [Réf. Du 16 décembre 2021]. Disponible sur Nouvelle directive sécurité des réseaux (NIS) (senat.fr)

d'intervenir par manque de ressources, l'ANSSI fait appel aux prestataires qualifiés PRIS[409] (Prestataire de Réponse aux Incident de Sécurité).

Un grand merci Sadio pour votre temps.

[409] *Prestataires de réponse aux incidents de sécurité qualifiés – ANSSI* [En ligne]. [Réf. 2021]. Disponible sur Prestataires de réponse aux incidents de sécurité PRIS

III.3. Antoine ANCEL, Directeur Cybersécurité - Groupe SNCF

Il a été le RSSI de **SNCF** Réseau de 2016 à Juin 2020.
À son actif des expériences dans, la banque, l'Armée et en SSII en tant que Directeur de projet, consultant, enseignant.
Antoine Ancel possède une expérience multiple, marquée par son expertise de la sécurité des SI.

GOUVERNANCE

Au sein du GI et entre le GI et les EF qu'en est-il de la gouvernance transverse en matière de cybersécurité dans le cadre de la convergence SIE et SII (IT/OT) ?

De manière générale dans le groupe, quels leviers à le BSSI pour créer de véritables synergies et renforcer la posture de cybersécurité dans l'ensemble du groupe ? Quelles sont les avancées notables ?

Il y a 3 questions dans ta question.

La première est bien la relation cyber sécurité au sein du GI pour adresser le thème de la continuité numérique (IT/OT). Cela implique de pouvoir maintenir une lecture continue de la chaîne de liaison afin de pouvoir rationnellement identifier le maillon le plus faible. Pour ce faire, il est indispensable d'assurer une gouvernance cyber sécurité unifiée, cela nécessite de développer des rattachements fonctionnels entre les acteurs IT et OT ce qui n'est pas natif dans la culture SNCF.

La relation entre le GI et les EF et CA, est bien une relation Clients / Fournisseurs avec des engagements réciproques de mise en œuvre des mesures de cyber sécurité nécessaires et suffisantes ainsi que de transparence en cas d'incident quelle que soit la gravité.

Enfin, ta troisième question est bien sur la dimension de la gouvernance cyber sécurité au sein d'un Groupe comme SNCF qui pour rappel est un Groupe international qui pèse tout de même près de 24 Mds €. Là le principe appliqué est un principe de collectif, de confédération. Toutes les SA sont responsables et autonomes dans leur prise de décision, mais le collectif aligne ses postures face aux différentes questions à adresser. Si l'une d'elle souhaite prendre un axe différent, cela est pris en compte et expliqué voire justifié. Cela peut notamment être induit de la bonne application de législation nationale qui ne s'applique pas au Groupe.

Est-ce que la création d'une forme d'entité technologique en Cybersécurité fédérant toutes les problématiques transverses de cybersécurité, gérer et faire évoluer les actifs cyber serait un accélérateur de synergies et pourrait rendre plus efficace les transformations ?

La Création de la Direction de la Cybersécurité (DCS) est sans nul doute un accélérateur de couverture, car cela permet d'assurer un niveau de service cyber sécurité plus large intégrant les petites structures de 10 à 100 personnes par exemple. Mais c'est aussi un facilitateur à la massification qui permet à terme d'assurer une internalisation des missions.

Enfin, un certain nombre de services et outillage peuvent être plus facilement intégrés et industrialisés par le Groupe que par une structure de taille moyenne. Le risque à une telle démarche étant bien sûr de développer un service minimaliste qui permettra aux filiales de se sentir protégée et donc de s'acheter un certificat de confiance. La contre mesure étant de toujours assurer un dialogue constant entre l'opérateur de services SSI interne et ses clients.

MANAGEMENT DE RISQUES

L'État de l'art présente la cartographie des actifs des SIE ou SII comme un préalable pour une véritable analyse de risque. Avec un patrimoine aussi immense et une visibilité restreinte des actifs quelle est la méthode pragmatique et efficiente pour mieux gérer les risques notamment industriels ?

Il n'y en a pas. Il faut aborder le sujet de l'Asset Management de manière très progressive, avec force et conviction afin de progressivement améliorer en continue la connaissance des assets. Mais ce n'est que la partie immergée de l'iceberg puisque ce qui importe encore plus est la chaîne de bout en bout, c'est-à-dire l'assemblage de ces assets.

L'exigence de sécurité dans le monde ferroviaire oblige des cycles d'homologation cyber assez lourd et long. Comment concilier cela avec l'agilité requise avec les besoins liés aux usages de mobilités ?

Le sujet n'est pas réellement spécifique au ferroviaire. Il est plutôt sur la convergence des temps entre l'IT et l'OT. L'OT conçoit, réalise et maintien sur un cycle de vie de 30 à 50 ans. Donc le sujet est bien l'échelle de temps. La mobilité, le CITZEN IT, et autres appellations marketing s'appuient elles sur un temps court de quelques mois. Il faut donc trouver des artifices pour assurer l'interface entre ces 2 mondes. Par exemple, des passerelles, des chaines de liaison dédiées…

Les actifs des SIE et SII sont des cycles de vie différents ? La retro-homologation semble être une gageure. On parle de gestion de risques raisonnée. Comment a minima garantir une bonne gestion d'obsolescence et un patch management prenant en compte les temporalités IT et OT complètement différentes.

cf. réponse précédente. La gestion de l'obsolescence sur l'OT ne se traduit pas de la même manière ; c'est encore une question d'échelle de temps. En OT nous parlons d'un contrôle commande, sa télé exploitation est souvent restreinte et donc cela nécessite souvent des déplacements, sur 30 000 km de voie… il faut trouver là encore d'autres solutions de protection micro périmétrique, de cloisonnement au niveau réseau et de vitrification d'un système afin de réduire sa surface d'exposition.

Est-ce bien raisonnable de penser à une méthode d'analyse de risques dites consolidée (rapprochant les risques IT de l'OT) ? Si oui, le domaine étant vastes, quels seraient les axes prioritaires ?

OUI, nous l'avons au sein de Groupe et elle est appliquée à SNCF Réseau afin de prendre en compte les contraintes de sûreté de fonctionnement dans l'IT et celles de cyber dans l'OT.

DÉFENSE EN PROFONDEUR

Malgré les difficultés de la cartographie des actifs, cartographie des flux, quels sont les piliers de la défense en profondeur par ordre d'importance qui ont encore besoin d'être consolidés fortement

La défense en profondeur ne s'arrête réellement jamais, d'une part le SI au sens large est un système vivant et donc même si l'on améliore la connaissance de l'ensemble de ses assets, cela représente toujours 90% du sujet seulement. De plus, les techniques d'attaques comme l'introduction de nouvelles approches de digitalisation remettent en cause les principes appliqués à date. Par exemple, nous avons longtemps considéré que les sauvegardes sont suffisantes pour la reconstruction alors que les ransomwares actuels ont pour première cible ces mêmes sauvegardes ; il faut donc changer de postulat.

On voit bien des choses faites sur la défense périmétrique, les segmentations et cloisonnement en respect des architectures en « zones et conduits », des moyens de protection, de détection de réaction face aux Incidents, etc., les notions de zéro-trust/network qui infusent de plus en plus .. Comment assurer une

segmentation et cloisonnement avec systèmes critiques, sensibles et non sensibles historiquement co-existant ? Comment garantir ces transformations de grande ampleur tout en impactant pas la production et prenant en compte les nouveaux besoins ?

Il est nécessaire de concevoir ces systèmes selon 3 blocs distincts, mais communiquant. Les services SI qui représentent des écosystèmes homogènes cohérents et confinables, les Endpoints utilisateurs et par là définir les exigences à appliquer suivant la sensibilité des écosystèmes accédés et enfin les infrastructures de cyber sécurité Surveillance & Contrôle notamment contextuel. Si l'on pousse le modèle à une granularité trop fine, on complexifie l'ensemble de la photo et cela devient rapidement ingérable. C'est un peu comme lorsque l'on voulait faire de la protection par le réseau en restreignant à une liste d'adresses MAC.

Revenons sur la Security-by-design au sein des projets ? Comment arriver à faire comprendre que le temps et le coût d'une cybersécurisation sont des gages de valeur aussi bien pour les services produits et pour l'entreprise ? D'ailleurs la notion de PV de sécurité avant une mise en service applicative ? Comme avoir un Radar de cybersécurité applicative ?

C'est une question de temps, de conduite du changement. C'est un travail qui s'opère par une « éducation » de l'ensemble des parties prenantes du SI (Métier, DSI, Exploitant,…)

Quels sont les leviers pour que le message de prise en charge dans leur budget des activités de gestion d'obsolescence et de décommissionnements est-il pris à bras le corps au plus haut-niveau des directions métiers et projets ?

Déjà ces sujets ne sont pas des sujets de Sécurité SI, mais ont des conséquences en termes de vulnérabilité et donc risques.

Le seul levier est de mettre les acteurs du SI en responsabilité.

RÉSILIENCE, MCS

La problématique de PCI, PCA des systèmes notamment critiques est un enjeu majeur Un rapport inquiétant de l'ENISA montre qu'on a moins de 15% d'entreprises qui ont des plans de résilience éprouvés, 42% qui l'ont partiellement éprouvé et, environ 40% qui l'ont lancé à peine. Quelle est la bonne démarche pour assurer une résilience minimale en cas de crise majeure ?

La communication, l'éducation, les exercices de crises, pour faire prendre conscience aux métiers de leur SI dépendance. C'est le principe du GPS dans la voiture, nous n'avons plus de carte…

Certains préconisent de pas opérer la convergence IT OT pour certains systèmes critiques afin de conserver les ruptures protocolaires, existantes en cas de crise majeure. Quelle est ton appréciation de cette posture.

Nous savons opéré la communication de bout en bout y compris vis-à-vis de système critique avec des ruptures protocolaires voire mieux des ruptures physiques.

La gestion de l'obsolescence peut être maîtrisée par une bonne gestion de risque. Le patch management peut lui devenir problématique notamment pour les IIoT). Comment maîtriser ce processus afin qu'ils ne génèrent pas de backdoors ou qu'il soit vecteur de compromission.

Rien à voir avec la gestion de risque, cela doit devenir un réflexe de passer son SI au contrôle technique pour obtenir son certificat de bon usage comme la voiture.

La pénurie des compétences dans le secteur est très préoccupante. Celle de compétences OT sensibilisées aux risques cyber l'est d'autant plus. Comment accélérer des mutualisations de compétences et notamment la mise en place de programme de formation en ce sens ? L'université de l'Ingénierie est-il

suffisamment dans la vision en termes de besoins de formation adaptée aux problématiques liées à la convergence IT –OT ?

Aujourd'hui je suis en recherche de la solution par une série d'expérimentations. La réflexion n'est pas encore aboutie.

POSTURE DE CYBERSÉCURITÉ

Dernière question, aujourd'hui le risque cyber se trouve classé dans le top 3 des risques d'entreprise. Bien que la prise de conscience de son importance sur la pérennité des activités du groupe ait été tardive, comme dans beaucoup d'entreprises, comment expliquer l'interdépendance des autres risques d'entreprise avec le risque cyber et que par ailleurs plus jamais le renforcement de la posture en cybersécurité est un puissant levier de croissance ?

OUI c'est un levier important de transformation des usages dans de bonnes conditions. Mais c'est un axe de responsabilisation des acteurs, tant métiers que IT et tout particulièrement utilisateurs.

III.4. Eddy THÉSÉE, Vice-président Cybersécurité chez Alstom

Portefeuille de produits et solutions

Entretien du 15-11-2021

SUPPLY CHAIN ET RISK MANAGEMENT

Le risque lié à la chaîne d'approvisionnement est considéré comme un risque majeur à plusieurs titres comme nous le verrons dans la suite. Nous souhaitons comprendre dans un premier temps comment Alstom gère cette problématique.

Nous avons lancé chez Alstom un programme de Gestion de la Supply Chain. Notre Supply Chain n'est pas vue comme un problème, mais un sujet de vigilance régulière et que nous abordons sur plusieurs angles :

Angle 1 (vis-à-vis de nos fournisseurs) :

- Capacité de nos fournisseurs à pouvoir gérer leurs secrets et leur cybersécurité
- Capacité à aligner les produits qu'ils nous livrent avec les exigences de cybersécurité. Ces exigences peuvent être spécifiques à un projet donné ou un produit particulier ou alors très génériques. Dans ce dernier cas typiquement, on va leur demander de faire de la MCS, et a minima fournir un bulletin de sécurité de façon régulière.

Angle 2 (vis-à-vis de notre entreprise elle-même) :

- Capacité d'Alstom à réagir face aux attaques cyber et de se protéger en sécurisant également les accès qu'ont certaines entreprises aux SI d'Alstom dans le cadre de la relation d'affaires que nous avons avec elles.

Est-ce que les produits des fournisseurs localisés hors d'Europe respectent les exigences de sécurité de type 62443 ?

C'est plus ce que nous livrent les fournisseurs et le niveau d'exigences de sécurité qu'ils intègrent qui importe quelle que soit leur localisation ou leur taille. Nous sommes vigilants sur le produit et le service fourni et leur capacité de s'intégrer dans notre architecture et leur niveau d'exposition au risque cyber.

ESPIONNAGE INDUSTRIEL, FUITE DES DONNÉES

Un produit peut respecter les exigences de sécurité, mais cacher des backdoors à des fins d'espionnage industriel. Comment Alstom peut-il s'en prémunir ?

Le risque zéro n'existe pas ; il nous est impossible comme pour tous les fournisseurs d'affirmer que nos produits ne sont pas espionnables. Tout ce que je peux dire, c'est que nous mettons tout en œuvre pour que nos chaînes de construction et d'approvisionnement soient sous contrôle. Nous avons aussi un peu d'Intelligence (au sens de veille) pour s'assurer que nous n'avons pas de fuite de données. On craint l'espionnage au sens de recherche active de l'information, mais aussi sur l'angle fuite de données par inadvertance et d'avoir également des données en libre-service sur Internet. La limite dans la maîtrise du risque est qu'on peut avoir à faire à une cascade de fournisseurs, et par conséquent on atteint la limite d'intrusion qu'on peut avoir. Ce dont on s'assure c'est que le fournisseur s'engage bien à garantir à aller au bout de la démarche de cyber-sécurisation. Nous

sommes conscients qu'il y a souvent des limites à ces engagements en raison de la taille de certains fournisseurs et leur capacité à démontrer l'effectivité des processus, la présence de bonnes ressources et l'application des réflexes appropriés.

Outre la menace d'espionnage industriel, Alstom doit porter la responsabilité de toutes les solutions et produits qu'elle commercialise quelle que soit la chaîne d'approvisionnement. Quelle est la démarche d'Alstom pour développer son intelligence juridique de manière générale ?

Aujourd'hui nous avons un service juridique en charge de veiller aux clauses contractuelles aussi bien avec les fournisseurs en rand 1, rang 2 er rang 3 et pour protéger les produits d'Alstom. Une grosse partie du travail contractuel d'Alstom est relatif à l'IP (Intellectual Property). Les clauses commerciales sont plus ou moins déjà bien fixées et ont déjà une longue vie et sont plus ou moins éprouvées. Ce que nous sommes en train d'améliorer est surtout de la responsabilité en cas de cyberattaque ou incident de cybersécurité. Cela nécessite de clarification en amont : qui va être responsable de quoi et à quel niveau de la couche qu'on utilise. C'est un travail qui est en cours, car assez nouveau pour nous et plus globalement dans le secteur. Par exemple que se passe-t-il si l'un des clouders où sont stockées les données collectées par les produits ou solutions de nos fournisseurs est hacké et que nos données sont exfiltrées ? Il faut déterminer qui porte la responsabilité.
Dans chacun des contrats qu'on signe on doit s'assurer qu'il y a bien cette revue qui a été faite préalablement avec une dimension légale et comment nous Alstom nous nous protégeons de la divulgation de notre Propriété Intellectuelle ou d'une éventuelle utilisation frauduleuse.

Quelle est votre appréciation du risque lié au stockage des données des solutions dans le cloud et par rapport à leur localisation ?

On signe des clauses de localisation dans une région spécifique et dans 90% de nos contrats avec nos clients, les données sont stockées on-premise. Le reste c'est souvent pour des clients qui n'ont émis aucune exigence. De manière générale, il y a une frilosité parfois légitime des clients de stocker des données sur des environnements qu'ils ne maîtrisent pas. Et dans le cas ferroviaire on peut avoir des données personnelles (sur les conducteurs, badges, etc.), les exigences de RGPD doivent s'appliquer de bout en bout.

GESTION INCIDENT, SOC

Quel type de SOC dans le ferroviaire ?

Pour moi chaque SOC ferroviaire doit se démarquer de la valeur ajoutée ferroviaire qu'il embarque. Le choix doit être drivé par deux choses : premièrement, comment on arrive à interpréter un incident de cybersécurité dans le contexte ferroviaire, qui n'a rien à voir avec un incident de sécurité dans une voiture, un bâtiment, ou dans un écosystème et deuxièmement quelle est la démarche adaptée pour résoudre cet incident dans un tel contexte.

Faut-il avoir un SOC mutualisé ou des SOC distincts IT et OT

Il y a deux choses : d'un côté la théorie qui nous sert de colonne vertébrale pour réfléchir et ensuite il faut se confronter au réel. C'est comme quand les gens font la guerre. Il y a ce qu'on apprend à l'Ecole de Guerre et ce qu'on vit sur le terrain et qui revient à l'Ecole de Guerre. C'est une bonne chose de séparer le SOC corporate du SOC industriel. Par contre pour le SOC industriel, il est important de réunir au même endroit des personnes IT et OT pour mutualiser les connaissances et compétences et surtout avoir une force d'analyse et de réaction rapide et la plus globale possible en cas d'incident. D'un autre

côté, il y a de petites entreprises qui ne peuvent pas se payer le luxe d'avoir un SOC ou plusieurs SOC. Pour ce genre de client, un abonnement à un service qui leur remonte des infos avec une visu sur ce qui se passe sur leurs réseaux, des alertes en cas d'incidents ou comportements anormaux, du support si besoin et l'accompagnement pour remettre l'exploitation en route leur suffit

Oui pour le cloisonnement ou la segmentation même des SOC en sachant concilier avec la priorité de l'opérationnel, mais l'information doit circuler. Si on a un système trop cloisonné on ne l'opère plus.

CONVERGENCE IT OT

Quid de la convergence IT OT qui fait couler beaucoup d'encre et les risques inhérents ?

Dans le terme, convergence IT OT, on veut plus parler de l'informatique de gestion ou d'entreprise qui veut se connecter à l'OT pour connaître la position des trains, valoriser les assets, etc. Les capteurs intelligents sont partout dans les trains, sur la voie. L'informatique, ça fait lus de 20 ans qu'on l'a dans le ferroviaire, déjà les SCADA c'est de l'IT. La question actuelle est comment on sécurise les interfaces et les échanges entre l'IT d'entreprise et les Systèmes d'information industriels. Avec les IoT, on ne va pas réinventer tout, même si la topologie a changé. Le système de « zones et conduits » est quelque chose d'assez puissant. L'IoT est un composant dans une zone particulière.

Vouloir protéger un système qui n'a pas été prévu pour ça, requiert des compétences de concepteur ferroviaire dans l'âme. Un Alstom, Thalès, Siemens peuvent faire de l'Analyse même sur des systèmes qu'ils n'ont pas conçus eux-mêmes, mais dont ils comprennent les mécanismes et peuvent garantir une Safety case ou une homologation. Ce qui semble risqué pour des entreprises non spécialistes du métier pur ferroviaire. C'est un point de vigilance à avoir.

PARTENARIAT STRATÉGIQUE

Vu d'Alstom, y a-t-il en France ou En Europe une volonté de développement des grands pôles en cybersécurité ferroviaire comme en Asie, Israël par exemple ?

Quand on met en place des pôles c'est pour servir deux besoins :

- Soit un besoin de conception (ingénieur, pour designer des trains et des systèmes de signalisation, pentests). On a monté des pôles d'excellence en France, aux États-Unis, Bangalore)
- Soit pour des besoins de services (monitoring de sécurité, etc.). Des réflexions sont en cours avec quelques opérateurs ferroviaires pour fournir un service de monitoring de sécurité dans les assets ferroviaires et des SOC à valeur ajoutée ferroviaire.

POSITIONNEMENT INTERNATIONAL, VISION PROSPECTIVE, INFLUENCE EUROPEENE

Quel est le positionnement de la France sur l'expertise ferroviaire et sa démarcation par rapport aux autres pays

La France aidée par son écosystème législatif et la LPM a une longueur d'avance sur le ferroviaire. A part Singapore et l'Australie, je n'ai pas constaté une attention particulière aussi poussée qu'en France. Ici on a quand-même un délégué spécial au transport qui s'occupe du ferroviaire (c'est aussi le cas à Singapore et en Australie). Le fait que les

opérateurs ferroviaires aient commencé à traiter du sujet de la cybersécurité combiné à l'encadrement législatif (les deux se complétant) est un accélérateur.

Les États-Unis sont en retard et ont commencé à bouger véritable que depuis quelques mois

Pouvons-nous craindre nous faire damer le pion par d'autres pays ?

La cyber évolue très vite. Ce qui ne pas changer si vite c'est l'avance qu'on a sur les produits dont l'expertise et la maturité ne s'acquièrent pas en quelques mois.

Par contre, il n'est pas exclu par exemple que les États-Unis malgré le retard, mais avec les mesures drastiques qu'ils ont prises et une force financière ne rattrapent leur retard sur les services, la formation l'accompagnement, la prise de conscience. La crainte qu'on pourrait avoir c'est qu'on n'accélère pas. Ce que je crains pour le ferroviaire français et européen est qu'on en reste au stade de se poser des questions. Il faut accepter que la cybersécurité ait un coût comme la Safety a eu un coût à un moment donné. Il ne faut plus être dans une logique « comment je réduis les coûts pour avancer, mais comment j'avance en réduisant les coûts » En ayant une roadmap en termes d'objectifs de cybersécurité avec des exigences réalistes et atteignables aussi bien des opérateurs que vis-à-vis de nos fournisseurs

Quid de l'influencing des gros acteurs du ferroviaires (opérateurs, comme manufacturiers) ?

Je ne peux pas dire qu'il y ait un groupe d'influence européen. Il a fallu du temps (4 ans) et cela s'est fait que très récemment qu'en tant que manufacturier nous soyons admis dans le cercle fermé des discussions entre les opérateurs. Des échanges inclusifs sont quelque chose à encourager et qui nous feront avancer. Notre contribution est légitime d'autant plus que c'est nous qui fabriquons les produits.

Il y a un ER-ISAC (European Railway ISAC) dans lequel nous participons depuis quelques mois et qui nécessite une réactivation et un restaffing suffisant. Il nous faudrait aussi définir une stratégie claire. Le seul élément fédérateur à mon sens à date, est la contribution d'un grand nombre d'opérateurs, de manufacturiers pour l'élaboration de TS 50701 qu'on souhaite faire adopter comme norme internationale.

Dernier message personnel ?

Il y a trois choses que j'aimerais rappeler pour terminer :

1- Personne n'arrivera tout seul en cybersécurité ; c'est un sujet qui se travaille en commun et pour lequel le partage des informations et la connaissance sont capitales
2- Personne n'y arrivera sans plan. Fournisseur, client, manufacturier, chacun doit faire l'effort d'établir un plan et accepter que le plan se ressource, qu'il faut des moyens financiers, mais surtout humains avec des personnes dédiées et non faire dans l'épaisseur du trait en fonction des disponibilités.
3- Autre point, il faut investir dans des outils adéquats et entrer dans une démarche de revue permanente et d'amélioration continue paradigme dont n'est pas forcément habitué le monde ferroviaire.

Merci beaucoup Eddy pour votre disponibilité

III.5. Jean-Baptiste RENAULT – Resp. Cybersécurité Alstom France

Responsable des activités cybersécurité sur les appels d'offres et projets en France pour l'ensemble des produits et des solutions du portfolio d'Alstom,

Interview réalisée le 03 Novembre 2021

Bonjour, pouvez-vous nous parler brièvement des services au ferroviaire que vous proposez ?

Nous proposons des solutions clé en main, Génie civil, électrification, pose de voie. Aide à l'exploitation et à la Maintenance, etc.

POSITIONNEMENT D'ALSTOM DANS LE RENFORCEMENT DE LA PRISE EN COMPTE DU RISQUE CYBER

Alstom est-il moteur pour entraîner les clients dans le « wagon » Cybersécurité ? Si oui de quelle manière ? Côté Transport aérien, un Conseil en Cybersécurité du Transport Aérien (CCTA) a été créé avec l'impulsion de Airbus Cybersecurity, pourquoi pas une telle initiative pour le ferroviaire ?

Je suis pro-actif avec mes clients. Je suis en contact avec tous les RSSI industriels et équivalents.

AU niveau des Grandes lignes et métro, le sujet est beaucoup pris en compte et un peu moins dans les agglomérations comme Nantes Anger avec les Tramways. Ces derniers ont peut-être une faible prise en compte du risque cyber. Plusieurs raisons évoquées : problèmes de compétences, ou de moyens ou ils pensent peut-être qu'il est plus avantageux pour un malveillant d'attaquer une grande ligne ou métro qu'un Tramway. De par mes fonctions, je suis aussi très actif dans la création d'un groupe de travail cyber ferroviaire dans le cadre du Campus avec l'ANSSI (Sadio Bä), la SNCF (Yseult Garnier, Quentin Rivette) qui sont moteurs. Alstom est aussi reconnu comme moteur lors de l'AG du cyber campus qui a eu lieu le 01/11.

Pour l'équivalent du CCTA dans le ferroviaire, ça ne m'étonne pas qu'on n'en soit pas là. Ça va prendre du temps, mais c'est quelque chose qui peut se faire et qui se fera dans le cadre du Campus Cyber

En 2020 7,8 milliards de dollars ont été injectés dans les sociétés de cyber sécurité, alors même que 45,1 milliards de dollars ont été mis dans les biothèques et 26,8 milliards de dollars dans les Fintech. Au vu de ces éléments pensez-vous que l'industrie de la cyber sécurité a pris la mesure réelle des enjeux du domaine ? Comment Alstom se positionne dans ce segment ?

La question est plutôt est-ce que l'industrie ferroviaire a pris la mesure des risques cyber ?

Ce n'est pas en injectant des milliards qu'on va résoudre le risque cyber. Ce que je remarque c'est que les personnes qui travaillent sur le risque cyber chez Alstom ou les

opérateurs (SNCF) n'ont pas suffisamment de capacité d'influence auprès des grands dirigeants d'entreprise. Les budgets ne sont pas à la hauteur. Ou alors prennent du temps à être débloqué (certains parlent d'un an pour un budget de traitement de vulnérabilité) ce qui peut être problématique dans la gestion des vulnérabilités. On a l'impression qui faut être attaqué pour débloquer rapidement un budget.

Quid des AO sans budget cyber ? La cyber est-elle incluse systématiquement dans les contrats d'Alstom ?

On ne peut pas imposer la cybersécurité à nos clients, sinon on perdrait aussi des marchés. Nous avons des contrats avec des exigences cyber et d'autres pas. Pour ceux qui n'en ont pas, on essaie quand-même d'avoir un devoir de conseil à minima d'interpeller le commanditaire de la raison de non prise en compte des exigences cyber si nous entrevoyons cela.

Quelles autres actions menez-vous au niveau national et européen ?

Outre le fait d'être forces de proposition pour la création d'un groupe cybersécurité ferroviaire au sein du campus cyber en France, nous sommes moteurs sur la création de normes (cas de la TS 50701)

Notre challenge est d'amener nos clients décideurs à mieux appréhender les risques cyber et aussi à attirer leur attention sur la nature des offres alléchantes du marché, car dans beaucoup de cas le prix du marché n'est pas souvent à la hauteur du travail à fournir s'il faut être sérieux. Ce n'est pas parce qu'on a fait un bon dossier d'analyse de risques qu'on va garantir un bon niveau de cybersécurité.

Il y a 10j, nous avons fait un webinar mondial pour présenter nos produits. On est moteur pour promouvoir la cybersécurité partout avec une démarche pro-active vis-à-vis de nos clients pour partager les visions.

DÉFENSE EN PROFONDEUR

Quel est l'état des lieux de la mise en œuvre réelle dans vos activités ?

La cybersécurité demande une grande flexibilité. Côté Ingénierie, les choses sont mises en place. Côté logistique, il y a encore des points à fixer. Côté maintenance, production et exploitation, cela va prendre un peu plus de temps. Ces derniers secteurs sont assez sensibles aux changements Par exemple, pour des mainteneurs habitués à se loguer avec des identifiants simplistes, leur dire de passer à une authentification forte multi-facteurs est déjà en soi une transformation pas simple à opérer.

Est-ce que le virage de la Security-by-design est une réalité chez Alstom ?

Alstom a des produits sur étagère avec une temporalité qui dépend des produits que ce soit pour le TGV, le Train Régional ou le système de signalisation. On intègre dans toutes nos solutions la norme CEI 62443. La robustification en profondeur est bien une réalité. Et cela passe par l'amplification des règles d'hygiène en cybersécurité de l'ANSSI. En plus de de cette robustification en profondeur, on rajoute de vrais équipements de sécurité complètement intégrés dans nos systèmes en périphérie et par où convergeront tous les flux : Firewaling, Antivirus, Active Directory Centralisé. Notre tactique est claire, nos équipements de sécurité les plus puissants sont mis sur les parties les plus exposées.

Pouvez-vous préciser le choix d'architecture que vous adoptez ?

On n'a pas implémenté toutes les exigences de sécurité dans nos systèmes. C'est un parti pris que nous assumons et que nous avons éprouvé. Les zones les plus exposées sont celles où les plus fortes exigences (norme 62443) ont été mises en œuvre. Et les équipements les plus sensibles sont dans les zones les moins exposées et les principaux équipements de sécurité dans les zones les plus exposées et qui vont attirer les flux de communication, flux d'entrées/sorties et forcer toutes le communications (normales ou malveillantes) par ce biais

Une barrière de sécurité principale au sol ou à bord contrer tous les produits et produits de cybersécurité et qui va laisser une flexibilité aux équipements de cyber pour traiter les vulnérabilités. On va prioriser les vulnérabilités sur les parties les plus exposées.

Ce qui laisse un peu plus de flexibilité sur les SI sœur. L'autre avantage de cette démarche est que le niveau de risque d'une vulnérabilité sur un SI critique, moins exposé, même s'il est élevé sur le produit reste bas au niveau du projet (par exemple TGV) et maîtrisable. Des équipements cyber et contre-mesures ayant mises pour le mitiger.

Nous pensons que c'est la meilleure manière d'intégrer la cybersécurité dans le milieu industriel.

Le risque cyber sur les composants critiques étant généralement couvert par les défenses périmétriques même en cas de découverte de vulnérabilité, c'est à l'exploitant d'évaluer le coût-bénéfice d'un tel traitement de vulnérabilité. Il peut y avoir plus de contraintes d'exploitation d'installer le correctif que de gain. C'est au RSSI et au Responsable d'exploitation d'évaluer la pertinence.

MENACES, RISQUES

À date que peut-on entrevoir comme grandes menaces réalistes ?

Je pense à autres choses …. Mais en tout cas pas de prise contrôle d'un train. ON a de la chance, dans l'industrie ferroviaire, la plupart des attaques sont circonscrites dans l'environnement IT. Je n'ai pas de connaissance d'attaques cyber sur nos environnements industriels.

Est-ce possible de compromettre la sécurité du cantonnement ? L'information transmise par la balise est-elle falsifiable ?

C'est la Safety qui gère ça. Il n'est pas possible de faire entrer dans un canton déjà occupé. Pour que cela soit possible il faudrait éteindre tout le système.

Et dans les trains autonomes ou les grandes lignes c'est le système ETCS qui est utilisé avec les balises et des communications en GSM-R

On ne peut pas falsifier l'information transmise par la balise de par sa nature inerte. Il faut se mettre au milieu entre le satellite et l'antenne du train pour pouvoir envoyer une fausse information. Néanmoins cette information est doublée en sécurité avec l'info de la balise liée au feu et au canton d'avant. Il y a une histoire de shuntage de rail (qui est un contact métal à métal) et c'est du physique pas du numérique là. Les signaux aujourd'hui sont transmis par des câbles en cuivre et ce n'est pas falsifiable.

Demain avec ETCS 3 et l'utilisation du Wifi ou la 5G est ce que potentiellement le risque pourrait augmenter ?

Fonctionnellement il n'y a pas de crainte à avoir. On utilise déjà cela dans les métros et on est sur du SIL3. Le train autonome et la grande ligne c'est encore plus exigeant c'est du SIL4. L'autre différence c'est que pour le métro les accès aux voies sont difficiles alors que sur les grandes lignes on est sur des centaines de km avec des passages d'animaux. On sait déjà faire rouler des trains sans conducteur

Que pensez-vous du cyber-espionnage ?

On est vigilant. Le groupe Alstom se sécurise là-dessus. C'est pris en charge par l'entité Alstom IT.

Quid de la menace et attaque Internes ?

C'est une bonne question. On fait beaucoup de sensibilisation et on applique les politiques de moindre privilège et restreignant les accès. Après il y a un volet confiance au personnel intervenant sur les systèmes.

Par ailleurs, il faut aussi savoir que la Safety se base sur des données dont la génération est hypersécurisée. Une compromission d'un système ferroviaire requiert des connaissances approfondies des mécanismes et dispositifs d'une part. D'autre part, lorsqu'une donnée est compromise la Safety par des algorithmes complexes arrivera à suspecter une situation anormale et arrêtera le Trafic. Les données métriques sont des données qui sont relevées sur la voie par laser, auxquelles s'ajoutent les données générées par le système. Outre le système, il y a de vraies personnes dans des équipes Safety qui vérifient à chaque fois si on n'est dans un état consistant de Safety.

Pour qu'un risque de type prise de contrôle d'un équipement de circulation se manifeste vraiment, il faudrait une combinaison d'événements complexes à aligner.

Mais encore une fois, l'humain qui assure la génération et le contrôle est un élément crucial dans le dispositif de confiance. Personnels d'Alstom comme les exploitants doivent avoir un niveau de confiance très élevé.

La différence entre IT et OT est qu'en IT on essaie de compromettre la confidentialité, mais en OT ce sont les critères d'intégrité et de disponibilités qui priment.

On peut avoir une personne de confiance, mais qui fait l'objet de pression et finit par céder. Comment le système peut-il sécuriser ce risque ?

J'ai une ébauche de réponse : si on a une combinaison d'alertes venant de nos systèmes et qui passent par un SIEM pour être analysées potentiellement au niveau du SOC, ce dernier pourrait suspecter par expérience un comportement potentiellement déviant.

STRATÉGIE ET CONCURRENCE INTERNATIONALE

Quid du partenariat avec Airbus et Cylus

Airbus nous a aidé au démarrage pour monter en maturité sur la Security-by-design nous a proposé un partenariat dans le cadre de leurs solutions éprouvés de services managés en SIEM et SOC.

Nous menons également conjointement des réflexions sur le traitement de la vulnérabilité (avec la capitalisation des expériences de chacun Airbus dans l'aéronautique et Alstom dans le ferroviaire).

Les partenariats sont aussi tactiques pour nous. Nous n'envisageons pas développer des expertises cyber par exemple de type SIEM

Pour Cylus, notre partenariat est axé autour de la sonde CylusOne pour faire de la détection et la cartographie dynamique des actifs. Cette solution offre okus de flexibilité qu'une solution équivalente connue du marché, car intégrable à tout moment alors pour la solution concurrente, il faut le prévoir dès la conception.

Comment Alstom voit-il la concurrence des pays d'Asie, Chine, Israël sur le secteur de la cybersécurité ferroviaire en l'occurrence ?

En Europe, Alstom participe aux travaux sur l'ERTMS, Sfift2Rail, la nome 62443 puis la TS 52701. Alstom ne se positionne pas pour créer un groupe en cybersécurité comme Airbus Cybersecurity.

Je ne sens pas de décalage entre la France, l'Europe par rapport à Israël pour ne citer que ce pays. Alstom a l'ambition de proposer pour se démarquer des solutions utilisables dans tous les pays respectant les standards en vigueur et à même de passer toutes les homologations quelques soit la législation la réglementation de ces pays. De plus nous avons une bonne expertise pour accompagner dans la gouvernance, l'analyse de risque et produire des rapports d'évaluation. À cela s'ajoute la compétence ferroviaire d'Alstom que les autres concurrents n'ont pas forcément et cela ne s'acquiert pas du jour au lendemain. Et cela nous permet de proposer des solutions clés en main.

Merci beaucoup Jean-Baptiste pour votre disponibilité et les éclairages précieux.

Le train à très grande vitesse Avelia Horizon d'Alstom remporte le prix German Design Award | Le Rail[410]

[410] Le train à très grande vitesse Avelia Horizon d'Alstom remporte le prix German Design Award | Le Rail

III.6. Yseult GARNIER - Responsable Cybersécurité Industrielle -RCS-I - SNCF RÉSEAU

Experte en protection des entreprises et intelligence économique (INHESJ)

Contributrice des groupes de travail de l'ENISA, ER-ISAC et CEN CENELEC TS 50701

Interviewée en Octobre 2021

Quelles sont les grands principes éprouvés pour parer aux risques découlant de la convergence IT/OT ?

Concernant l'analyse de risque, pour la partie cyber c'est la méthode SNCF issue d'EBIOS qui est utilisée, et pour la partie industrielle, nous respectons le principe de "zones et conduits" de la norme 62443. Sur le plan de l'architecture plus précisément : rupture matérielle et filtrage : passerelle sécurisée pour les interconnexions IP, architecture en 3 zones de criticité cyber différente.

Comment est assurée la sécurité du "voyage au sein de la donnée industrielle" ? L'RIoT qui est une réalité (cas calculs de cantons et la géolocalisation sur des perches caténaires et inspection de leur poids et dilation, etc.) Le risque d'envoi de flux pouvant compromettre ces IoT est-il maîtrisé ?

Tous les projets IOT en expérimentation ou en industrialisation sont accompagnés en cybersécurité, une note SSI a été publiée afin d'avoir une liste d'exigences SSI selon les enjeux cyber de l'IOT.

La convergence IT OT donne accès au système de production industriel encore fermé il y a quelque temps. On parle de ségrégation, de cloisonnement. Le respect des directives ou normes NIST, 62443 est-il possible sans interférence et impact sur la productivité ? Qu'en est-il de la mise en œuvre de passerelles unidirectionnelles pour éviter des prises de contrôle ?
Nous utilisons Seclab et pas en mode diode, solution de rupture matérielle CSPN ANSSI

La mise en place de zone Sécurité Plus et Zone homologuée suit cette logique de « zones et conduits ». Pouvez-vous nous en décrire le fonctionnement en termes de mode de communication, sécurisation de flux et des accès ? Quels retours d'expérience a-t-on puisque SNCF fait figure de proue en la matière ?

Techniquement les interconnexions se font avec Seclab et FW (filtrage). Nous n'avons pas de REX, la cybersécurité industrielle a été amorcée à partir de 2018, donc il n'y a pas longtemps.

Concrètement, quels les sont les dispositifs mis en œuvre pour empêcher un cybermalveillant de prendre le contrôle d'un poste d'un centre de contrôle et de régulation et envoie une commande de signalisation (passage au vert par exemple alors que devrait être rouge) ou de freinage ?

Nous appliquons les pratiques d'usage : à savoir passerelle sécurisée pour les accès externes au réseau fermé, le réseau IP industriel où sont déployés par ex les postes d'aiguillage est fermé au sens 50 159. De plus, la cyber est intégrée dans les nouveaux développements de poste d'aiguillage, et de centre de contrôle et régulation. Il faut rappeler que l'agent de conduite reste maître de la vitesse de son train, en respectant la signalisation latérale. Le KVB est une boucle de rattrapage et peut déclencher le freinage

du train en cas de survitesse. Pour les LGV où il n'y a pas de signalisation latérale, c'est le système ETCS qui affiche la vitesse à bord et la contrôle. Au niveau sécurité, nous sommes alignés avec les exigences élevées SIL 4. Par ailleurs, pour les échanges entre le sol et le bord Le subset 037 précise le protocole de communication. Dans tous les cas la sécurité est au rendez-vous.

On a tendance à ne regarder que des attaques via des protocoles standards ouverts. Les protocoles propriétaires du monde industriel sont de plus en plus connus et certains visibles et accessibles sur des sites étrangers (Chinois par exemple). Comment se prémunir contre des menaces liées à ces protocoles à l'origine non sécurisés et des compromissions potentielles de firmware de PLC (utilisé pour la commande ou la régulation d'une installation) *?*
Ma réponse rejoint celle donnée précédemment, on dans une architecture de réseau industriel fermé au sens 50159, et des exigences de chiffrement notamment pour les flux les plus critiques.

Les Automates de sécurité font-ils l'affaire ? Le package Pare-feu, système d'authentification centralisée par exemple via des protocoles RADIUS et VPN est-il une garantie pour des niveaux de sécurité SIL4 ?
La règle c'est l'intégration d'exigences cyber dans le Cahier de Charges, SIL 4 ne veut pas dire cyber compliant. Des protections matérielles peuvent être mises en œuvre. Les soumissionnaires de solution sont tenues de respecter le besoin métier en termes de cybersécurité.

NIST n'est pas normatif, IEC 62443 est considérée comme lourde et complexe à mettre en œuvre et assez généraliste pour les systèmes industriels, la TS 50701 adaptée au système ferroviaire est disponible, mais pas encore officiellement publiée. Dans le cas de SNCF RÉSEAU. L'arrêté sectoriel couvre-t-il les thématiques des normes citées ?
La TS 50701 a été publiée mi-juillet, maturité à éprouver, V2 et V3 à venir, l'arrêté sectoriel couvre les grandes thématiques, SNCF réseau a également des exigences cyber en plus de l'arrêté afin de couvrir toutes les thématiques.

Qu'est-il prévu pour évaluer continuellement le niveau de maturité de la mise en œuvre de directives en matière de cybersécurité ?
Il n'y a pas d'évaluation de la maturité à date. La démarche de cybersécurité industrielle ferroviaire est récente. Il est déjà difficile d'avoir cette démarche pour les systèmes IT, l'envisager pour les SI industriels requièrent préalablement une maturité dans la cybersécurité industrielle éprouvée...

La stratégie d'homologation devrait in fine permettre entre autres de s'assurer du principe de "GAME" (Niveau de Sécurité « Globalement Au Moins Équivalent »). Comment garantir une analyse de risque suffisamment pertinente avec des actifs patrimoniaux non suffisamment cartographiés ?
Le GAME n'est pas un principe cyber. Par contre les équipes cyber et projet travaillent en collaboration afin de garantir qu'un nouveau composant ou solution IT interagissant avec le réseau ne dégrade le niveau de sécurité précédent et n'apporte pas un risque supplémentaire à moins qu'il soit résiduel et accepté. Tout projet se lançant avec de potentiels modifications dans le SI critique est sensibilisé sur le délai long d'homologation (environ 18 mois)

Comment garantir par les fournisseurs le respect des Exigences IEC 62443 ?

Nous ne le demandons pas dans nos Cahiers de Charges. Par contre des exigences en cybersécurité relatives à chaque besoin projet sont incluses dans les appels d'Offre. C'est au soumissionnaire de s'assurer du respect des exigences conformément à l'État de l'art. L'attributaire doit également apporter la preuve des tests qu'il a dû effectuer. La SNCF effectue aussi ses propres tests

Comment garantir le MCS et MCO IT et OT ? Quid des systèmes industriels ?

La démarche de MCS repose sur une veille et une contextualisation des vulnérabilités, de la vraisemblance au travers d'une qualification de la menace et de l'exposition. En cas de vraisemblance élevée un plan d'actions et de mesures sera instruit.

Un dernier mot ?

La sensibilisation des utilisateurs est capitale. On peut mettre toutes les protections possibles, sans application des règles d'hygiène minimales de cybersécurité, les utilisateurs deviennent des maillons faibles.

Merci Yseult pour ton accompagnement et tes éclairages

III.7. Quentin RIVETTE - Responsable Cybersécurité Industrielle - SNCF Voyageurs

Entretien du 28 Octobre 2021

Qu'est-ce qui nous permet de parler de cybersécurité industrielle chez SNCF Voyageurs ? La production des horaires, la signalisation, l'aiguillage, la maintenance, etc. étant côté Gestionnaire d'infrastructure ?

Une EF dispose de systèmes d'informations industriels qu'il convient de cybersécuriser tels que les Systèmes informatiques embarqués dans les trains et les outillages qui servent pour la maintenance. On parle de SI industriel pour des SI avec impact dans la vie réelle, dans le monde cyberphysique. Ce type de produits peut embarquer un certain nombre d'automatismes, de la sûreté de fonctionnement, impliquer des équipements spécifiques, des OS plus ou moins spécifiques. La cybersécurité industrielle et la cyber IT ont des parallèles, notamment, des technologies issues de l'IT (Ethernet, linux, ...) sont de plus en plus utilisées dans le monde industriel. Ce qui diffère c'est la capacité des systèmes à faire et la capacité des systèmes à gérer l'évolutivité notamment du fait de leur durée de vie longue ou de la nécessité de réaliser des démonstrations fonctionnelles (liées à la dimension sûreté de fonctionnement qui peut exister pour les systèmes de contrôle et commande ; ce qu'on ne retrouvera pas dans une appli web IT traditionnelle).

Quelles sont les grandes menaces de cybersécurité chez une EF ?

Elles sont variées en fonction des systèmes dont on parle, leurs fonctionnalités, leurs expositions. Les impacts peuvent être sécurité des personnes, exploitation, image de marque. Les risques sont adressés par la démarche de maîtrise des Risques Cyber du Groupe (appelée ZEN). Selon les enjeux identifiés en préqualification, la profondeur d'analyse et d'exigence pour la définition des requis et pour leurs vérifications est établie de manière proportionnée. Une analyse de risques et/ou des pentests peuvent être menés.

Les systèmes embarqués dans les rames sont, je suppose de la responsabilité de l'EF. C'est exact ? Peut-on imaginer une interférence avec le système industriel du GI ? Un mot sur la réalité des trains communicants et les enjeux en termes de sécurité

Tout à fait. Les systèmes embarqués sont de la responsabilité des EF. Aujourd'hui il n'y a pas un train qu'on achète ou modifie sans une exigence de cybersécurité. Les mesures sont prises pour le faire fonctionner dans des conditions de cybersécurité suffisante en fonction des enjeux pour le système concerné. La connectivité / l'exposition des systèmes n'est pas une spécificité de la cybersécurité industrielle, plus on connecte plus les menaces et les risques augmentent. Pour les trains communicants, la cybersécurité est adressée en prenant en compte les besoins de sécurité des systèmes et données manipulées, les liens utilisés, les spécifications ou standards pouvant exister. Des interfaces avec le GI existent notamment pour les systèmes de contrôle-commande-signalisation tels que ERTMS. Des interfaces existent également avec l'EF pour les systèmes de responsabilité de l'EF tels que le télédiagnostic, l'information voyageurs, ...

Sauf erreur de ma part le sens des informations de commande est plutôt du système de production ou du centre de contrôle et de commande vers la locomotive et/ou à destination du conducteur et non dans l'autre sens. Est-ce exact ? Qu'est-ce qui garantit la fiabilité des informations transmises au conducteur par exemple ? Existe -t-il des boucles de vérification suffisamment rapides permettant de garantir l'exactitude et le caractère sûr des informations qui lui sont transmises ? Ou cela relève-t-il de la responsabilité du GI en charge du CCR ? (Cas des boucles de rattrapage pour le KVB, mais quid du TGV)

La communication des trains n'est pas monodirectionnelle et ne se limite pas à un dialogue CCR vers le train. Pour plusieurs systèmes, la communication est aussi du train vers le sol (télédiagnostic, géolocalisation, …) ou bidirectionnelle selon les systèmes concernés. La cybersécurité de ces échanges est adressée en prenant en compte les besoins de sécurité des systèmes et données manipulées, les liens utilisés, les spécifications ou standards pouvant exister.

S'agissant des communications entre le GI et le conducteur, elles peuvent être informatiques (par exemple via des autorisations ERTMS s'affichant en cabine), mais aussi traitées par la signalisation latérale complétée si besoin d'une communication orale par téléphonie. Cela va dépendre de la technologie de la ligne et du train concernés.

Si l'on considère le cas des systèmes de sécurité ferroviaire que sous-tend la question, ce qu'il faut retenir en substance, c'est qu'il y a les systèmes qui varient selon les lignes et les trains. Ces systèmes de sécurité ferroviaire et sûreté de fonctionnement contribuent à la robustesse globale du système. Les équipements de sécurité appliquent des règles strictes limitant les opérations du conducteur (si le conducteur sort de ces limites, les équipements de sécurité arrêtent le train, si l'équipement ne sait pas déterminer si on est dans une situation sûre, le train s'arrête) .

Beaucoup de données personnelles transitent par le réseau Wifi opéré par la SNCF Voyageurs. Un mot sur la confidentialité et le respect de la RGPD ?

Pour les réseaux Wifi embarqués dans les trains, SNCF Voyageurs s'appuie sur des acteurs du marché qui assurent le rôle de FAI (incluant les obligations associées de conservation des traces de connexion, etc.). La prestation est contractualisée d'un point de vue cybersécurité, incluant les aspects RGPD.

Quels sont les contrôles auxquels est assujetti SNCF Voyageurs ? Quid des contrôles d'interfaces avec les systèmes de production ferroviaire ? Qu'est-ce qui drive la couverture de périmètre des contrôles PASSI (Architecture, Organisationnel et physique, Tests d'intrusion, audit de configuration, audit de code ?)

En contrôle externe les autorités de tutelle, en contrôle interne niveau 3 la DAIG, en contrôle interne niveau 1&2 les équipes SSI en lien direct avec les projets au travers des accompagnements de projet et des pentests. On applique les réglementations qui s'appliquent à nous. Concernant la profondeur de réalisation des audits, elle est fonction des enjeux (proportionnalité). Un audit cyber, que l'on parle du scope ou de la durée de tests, ne peut jamais être considéré comme absolu. Il convient donc d'adapter cela aux enjeux du projet. Pour les interfaces et les tests afférents, comme pour le fonctionnel, chaque partie prenante a sa part de responsabilité.

Quels sont les référentiels utilisés chez SNCF voyageurs ? Et côté PSSI, comment se font les contrôles de sa bonne application ?

Il existe une PSSI groupe. La déclinaison industrielle est adaptée du fait de la complexité des systèmes industriels. Il est notamment fait usage des référentiels IEC62443, TS50701, et guides ANSSI. Le suivi de leurs bonnes applications passe par des contrôles des exigences, suivi SSI des projets et pentests selon enjeux.

Quelle est la démarche de CTI dans le cadre d'une convergence IT OT ? L'accélération des nouveaux usages avec le RIoT demande une agilité de prise en compte et de remédiation à laquelle le monde industriel n'est pas familier. Comment se concilie le besoin de sécurité et l'impérative nécessité de contrecarrer dans les meilleurs délais les menaces et attaques potentielles ?

La convergence IT OT fait couler beaucoup d'encre. La CTI est beaucoup plus utilisée dans l'IT. Pour L'OT il convient d'abord d'améliorer la capacité de superviser les réseaux OT c'est

la priorité, ensuite la CTI sur des kill-chain à surveiller suivra. Il y a des marches à franchir. L'IoT est un mot dont la définition est parfois peu uniforme (on a tendance à associer IoT avec des produits tels qu'un capteur, un smartphone, une box qui communique avec des SI tiers ou opérés ; mais parfois tout ce qui est communiquant, même les systèmes complexes ou distribués sont considérés comme du périmètre IoT). Si l'on considère la définition de l'IoT comme étant un produit unitaire (tels qu'un capteur communicant), associé à un modèle économique faible coût et/ou jetable, alors on ne fait pas de sûreté de fonctionnement avec l'IoT. Pour autant, cela n'affranchit pas de cybersécuriser les solutions déployées, tant pour la donnée transportée que pour l'IoT en lui-même.

Quelles sont les difficultés actuelles dans la mutualisation des expertises sécurité et cybersécurité ?

On a des organisations et des processus différents. Mais les synergies et mutualisation sont en marche. Chez SNCF Voyageurs Matériel, il y a un processus qui concerne "l'autorisation /admission du matériel roulant" dont le but est d'obtenir/de conserver une autorisation de rouler, sorte de carte grise qui dépend de l'état technique du train. Si on modifie l'état technique du train, on doit faire modifier la carte grise du train. Ce processus est systématique et requiert un dossier plus ou moins lourd selon la modification réalisée et son impact sur l'exploitation ferroviaire. Des échanges avec les équipes en charge de l'admission ont donné lieu à la mise en place de liens entre le processus cyber (ZEN) et le processus d'admission/autorisation du matériel. Ces liens ont été établis selon des principes de proportionnalité et de fluidité. Ainsi, le processus admission peut permettre de déclencher le processus cyber selon critères (si celui-ci n'a pas déjà été lancé) ; les deux processus peuvent vivre en parallèle avec leurs modalités de traitements spécifiques ; et le retour d'information vers l'admission est établi également selon critères pour limiter au maximum les cas de blocages.

La cybersécurité est intégrée dans les projets SI Industriels de SNCF Voyageurs avec proportionnalité, pragmatisme et respect des réglementations. La règle d'or est Safety first, et la cybersécurité une composante de la maîtrise globale de la sécurité ferroviaire.

Merci Quentin pour l'échange et la disponibilité

III.8. Pr. Amal EL FALLAH SEGHROUCHNI, membre du COMEST – UNESCO.

Responsable du mouvement IA chez UM6P – Centre international d'intelligence artificielle du Maroc. Professeur à l'Université de la Sorbonne, spécialisé en intelligence artificielle, agents autonomes et systèmes multi-agents.

Je suis titulaire de la chaire d'Excellence Industrielle « Thales- SCAI Abu Dhabi » – 2020-2025 – Abu Dhabi / Paris. Le sujet de la chaire porte sur les radars cognitifs et collaboratifs, l'IA hybride et les jumeaux numériques ». Mes sujets de recherche sont l'intelligence artificielle, les agents intelligents et les systèmes multi agents appliqués dans plusieurs domaines tels que les villes intelligentes, les assistants intelligents et la défense. Je suis membre de la Commission mondiale sur l'éthique des connaissances scientifiques et de la technologie COMEST – UNESCO.

Entretien du 01-11-2021

Quelles sont les grandes tendances de l'IA actuelle ?

On est sur le triptyque : données – objets connectés – robotique. L'un des soucis majeurs est lié la collecte des données et les problématiques de la Data Privacy. Concernant le domaine du développement durable et notamment dans le domaine industriel des transports, l'utilisation massive des IoT et aussi de l'IA pose la question de la *consommation énergétique qui en découle*

Quelques domaines d'application ?

Les thématiques comme la maintenance prédictive sont assez citées dans la littérature

Nous pouvons citer l'apport de l'IA dans la surveillance. Plusieurs expérimentations ont été menées avec des résultats intéressants pour la sécurisation des rails (vol de câbles par exemple qui un impact sur la production ferroviaire et financier) par l'utilisation des drones et l'imagerie satellitaire.

Des outils de simulation à base d'IA avec des systèmes multi-agents sont aussi utilisés pour la gestion des portes de trains en vue de la fluidification et l'optimisation du trafic.

Quels sont les risques que vous entrevoyez du fait de l'utilisation des trains autonomes ?

La question de la responsabilité en cas d'accident se pose déjà pour la voiture autonome. Avec le train on est sur une tout autre échelle avec des impacts qui peuvent très vite être considérables en termes de pertes humaines, mais aussi psychologiques au sein de la population et durablement.

Y voyez-vous des questions d'éthique ?

Bien sûr l'IA questionne et interpelle parfois les consciences sur le modèle de société. Dans le cas des entreprises, il ne faut pas négliger la conduite de changement à mener. Quel que soit l'apport de l'IA l'humain doit être au centre et maître du jeu.

III.9. Thomas CHATELET – Projet ERTMS - ERA - Agence Européenne des Chemins de Fer

Entretien du 24-11-2021

GOUVERNANCE

L'ERA et les autorités nationales se sont partagés les rôles concernant les autorisations de circulation et d'exploitation. Comment s'opèrent les contrôles de l'ERA vis-à-vis de ces autorités étant donné qu'on pourrait avoir des disparités d'exigence dans les différents pays ?

L'ERA a, selon le 4ème paquet ferroviaire (réglementation ferroviaire votée par le Parlement européen et le Conseil européen), la compétence exclusive de délivrer les autorisations pour les véhicules circulant dans au moins 2 états membres, en vérifiant la conformité au cadre réglementaire ferroviaire européen (Directives d'interopérabilité et de sécurité ferroviaire [(EU) 2016/797 - (EU) 2016/798], Spécifications Techniques d'Interopérabilité (TSI), Méthodes Communes de Sécurité (CSM)). En ce sens, les autorités nationales délivrent les agréments de sécurité aux gestionnaires d'infrastructure, ERA a les compétences exclusives pour les Certificats Uniques de Sécurité des Entreprises Ferroviaires opérant dans deux états membres ou plus. ERA exerce aussi une mission de contrôle sur le déploiement de l'ERTMS par les Gestionnaires d'Infrastructure. Les vérifications de l'ERA se font par rapport au cadre législatif européen, les vérifications des agences nationales peuvent prendre en compte certaines normes nationales si elles sont justifiées et acceptées par l'Agence. En outre, l'Agence surveille les performances et le processus de décision des autorités nationales de sécurité par le biais d'audits et d'inspections, au nom de la Commission.

Il est à noter que le cadre réglementaire ferroviaire européen ne comporte, pour le moment, pas de requis spécifique à la cybersécurité à l'exception de :

- Une référence indirecte dans les CSM à la norme CENELEC EN 50126 dans laquelle le « Safety Case » est lié à la prise en compte du risque cyber
- Des règles de base pour les TSI TAP/TAF (Télématique Passager/Fret) et des requis plus spécifiques pour la TSI CCS (Contrôle-Commande et Signalisation) pour assurer l'authenticité et l'intégrité des messages ETCS (European Train Control System) ainsi que le PKI y étant associé

Quelles sont les répartitions de rôles entre l'ERA, l'UIC et l'ENISA ? Et les spécificités

Nous constatons qu'il existe des Livres blancs, Guides écrits par chacun des organismes sur le même sujet de cybersécurité dans le transport ferroviaire

L'ERA et l'ENISA étant des agences de l'Union européenne, le partage des compétences EU/états membres tel que défini par le traité de Lisbonne s'applique à elles aussi. Ainsi la compétence de la sécurité (au sens du terme anglais « security »), une compétence partagée, ne peut être définie uniquement par les institutions européennes. Sur le sujet de la cybersécurité ERA et ENISA ne peuvent par conséquent qu'émettre des recommandations, et/ou définir conjointement avec les états membres la politique à mettre en place. ENISA s'occupe principalement de cybersécurité, conseille la Commission Européenne, dresse un état des lieux de la menace cyber secteur par secteur, propose des guidelines pour tous les acteurs concernés, y compris ferroviaire. ERA s'occupe principalement d'interopérabilité et de sécurité ferroviaire (sans inclure la sécurité physique), conseille la Commission Européenne, propose des évolutions du cadre réglementaire ferroviaire européen (TSI/CSM). L'UIC est une association ferroviaire qui propose, entre autres, des guidelines et des standards ferroviaires à ses membres (certains

de ces standards étant repris dans certaines TSI). UIC offre aussi du support à ER-ISAC (European Railway – Information Sharing and Analysis Center), groupe de partage et de confiance entre différents acteurs ferroviaires sur le sujet cyber.

La complémentarité de ces 3 acteurs est nécessaire pour avoir un niveau de recommandation en direction des acteurs ferroviaires pour prendre en compte la menace cyber et les solutions à y apporter.

ENJEUX MAJEURS

Josef DOPPELBAUER lors de la table ronde organisée par l'IMTD le 18 novembre 2021 évoquait les enjeux majeurs d'interopérabilité. On serait passé de 14632 règles à 868 règles. Quels sont les pays qui ont encore des efforts à faire pour s'aligner sur l'harmonisation des normes ? Quels sont les freins à l'accélération ? Et comment activer les leviers ?

Actuellement, il n'a pas été porté à la connaissance de l'ERA de règle spécifique sur la cybersécurité dans un état membre. Les règles en matière de cybersécurité ferroviaire ne sont pas définies par le réglementaire ferroviaire européen, mais plutôt par la transposition de la Directive NIS et/ou par les lois de programmation militaire (notamment en France et en Allemagne). D'après notre analyse, ces règles ne présentent pas de risque pour la sécurité ou l'interopérabilité ferroviaire et concourent à une meilleure prise en compte du risque cyber. L'introduction dans le cadre réglementaire ferroviaire européen de plus de requis cyber nécessite une analyse bénéfice/risque qui est en cours (e.g. pour chaque nouveau requis d'interopérabilité ou de sécurité ferroviaire au niveau européen, une vérification par un Notified/Assessment Body est demandée, ce qui entraîne une complexification/renchérissement du coût de certification).

On parle aussi d'intermodalité et de multimodalité qui seraient l'avenir du transport ferroviaire de demain. Quelle a date l'appréciation de l'ERA sur les avancées concrètes sur cette thématique ?

L'ERA a un groupe de travail dédié aux aspects d'intermodalité et de multimodalité qui reflétera dans les TSI les propositions du secteur ferroviaire pour une meilleure facilitation des échanges rail-route. En ce qui concerne l'échange de données entre les acteurs du ferroviaire pour les aspects télématiques passager ou fret, des exigences de cybersécurité sont détaillées dans les TSI TAP/TAF pour le format et la sécurité des échanges.

BUDGET

On parle de 25 Mds annuels et un plan pluriannuel sur 7 ans de plus 170 Mds qui seront investis dans le transport et dont 80% dans le ferroviaire. Cet argent comment est-il redistribué et comment sera évalué le retour sur investissement ? La problématique des répartitions équitables selon les projets, les initiatives ne risquent pas de ralentir l'Europe par rapport aux autres pays ?

L'ERA n'étant pas compétente pour la gestion des financements, nous suggérons d'adresser la question à CINEA (Climate, Infrastructure and Environment Executive Agency : https://cinea.ec.europa.eu/index_fr).

Et d'ailleurs quelle sera la part de budget alloué à la cybersécurité dans tout ça ? (Quel est généralement le % dédié à la cybersécurité pour les différents projets ou programmes lancés par l'ERA ?)

L'ERA prend très au sérieux la sécurisation de ses propres systèmes d'information (i.e. registres sur les données d'interopérabilité ferroviaire, One Stop Shop) et alloue des budgets en proportion. Par ailleurs, l'ERA est soutenue dans ces activités par CERT-EU.

RISQUES et MÉTHODES

Quels risques majeurs entrevoyez-vous dans la filière ferroviaire à date ? et demain avec l'ERTMS 3 ?

L'ERA ne réalise pas de threat landscape, mais a un très bon partenariat avec l'ENISA, qui va prochainement en réaliser un pour le secteur ferroviaire. Le principal système à protéger du point de vue de l'ERA est l'ERTMS, pour sa dimension d'interopérabilité (les systèmes de billettique sont probablement tout aussi importants, mais n'entrent pas dans le champ d'application du cadre réglementaire ferroviaire européen). Certaines études, notamment de l'université de Birmingham ont souligné les risques théoriques associés à l'ERTMS. La consultation avec le secteur ferroviaire nous laisse plus optimiste que ces études, mais le risque cyber est néanmoins pris en compte et fera l'objet de renforcement dans les prochaines versions des TSI[411]. L'ETCS de niveau 3 ne présente en soi pas plus de risque que celui de niveau 1 ou 2, chaque niveau reposant sur des aspects techniques précis pouvant faire l'objet d'attaque (par exemple la signalisation latérale en niveau 1 ou le GSM-R en niveau 2). Le niveau 3 devrait voir l'introduction du concept de canton mobile basé sur l'intégrité du véhicule. Si ce dernier était réalisé par le biais d'un système de géolocalisation, l'authenticité des informations fournies par ce dernier devrait faire l'objet d'un examen très attentif.

L'IA est de plus en plus utilisée, dans l'industrie ferroviaire. Quelle est la position de l'ERA en termes de responsabilité juridique ou pénale si un asset ferroviaire serait à l'origine d'un incident de sécurité et dû aux algorithmes d'IA ?

L'ERA met en place un jeu de règles communes pour la sécurité ferroviaire (CSM) qui confère aux opérateur une grande responsabilité en termes d'évaluation du risque. L'utilisation de l'IA et ses conséquences juridiques devrait faire partie de cette évaluation.

Avec la convergence IT-OT ? La réflexion autour d'une méthode européenne d'analyse de risque combinant les méthodes d'analyse de risque IT et les méthodes d'analyse de sécurité spécifique au monde ferroviaire est-elle à l'ordre du jour ? Si oui sous quelle échéance pourrait-on envisager un atterrissage ?

En ce qui concerne une méthode commune d'analyse du risque cyber dans le monde ferroviaire, l'ERA suit avec attention les développements du groupe de normalisation WG26 de CENELEC, ainsi que les futures évolutions de la spécification technique 50701. Si cette norme venait à devenir un standard européen, l'ERA se montrerait très intéressée de la référencer dans ses règles communes (CSM) pour que le risque cyber soit partie prenante de l'évaluation du risque (« Safety Case »).

NORMES, REGLEMENTATIONS

L'ENISA a sorti la TS 50701, quel rôle jouera l'ERA pour promouvoir cette TS afin qu'elle se transforme en norme ? Quelles sont les circuits et prochaines étapes à franchir ?

La TS 50701 a été publiée par CENELEC en juillet 2021. La promotion de cette norme passera par un référencement dans le guide d'application de la Méthode Commune de Sécurité pour l'analyse de risque (CSM-RA). La transformation de cette spécification en norme est, d'après nos informations, prévue au sein du groupe de travail CENELEC.

On sait que le lobbying dans les comités de normalisation et dans la Commission Européenne est déterminant pour la suite en termes de propositions de solutions, de produits et services.

[411] Technical Specification Interoperability

Comment arriver à activer les leviers afin que les parties prenantes manufacturiers, constructeurs et opérateurs européens soient forces de proposition et pèsent les instances de normalisations et réglementations ?

Dans le cadre de ses activités de mise à jour des TSI/CSM, l'ERA dispose de nombreux groupes de travail où sont représentés tous les acteurs ferroviaires européens (Gestionnaires d'Infrastructure, Entreprises Ferroviaires, Industrie, Syndicats). La mise à jour de la CCS TSI pour renforcer les risques liés aux attaques cyber et menée suite aux propositions émanant de recherche (Shift2Rail) et soutenue par l'industrie (UNISIG).

GRANDS MESSAGES de l'ERA

Quels sont les grands messages de l'ERA pour garantir un transport ferroviaire durable et de confiance ?

L'ERA s'assure de la mise à jour proportionnée du cadre réglementaire ferroviaire européen pour contribuer à établir l'espace ferroviaire unique au niveau européen. Nous sommes conscients du potentiel du rail pour contribuer aux objectives de réduction de l'impact environnemental du transport, et aussi de son atout comme le moyen de transport terrestre le plus sûr. Nous contribuons activement par notre collaboration avec la Commission Européenne, l'ENISA et le secteur ferroviaire, à une meilleure prise en compte du risque cyber par tous les acteurs, pour que leur responsabilité dans ce domaine soit pleinement assurée.

Merci beaucoup Thomas pour ta prompte disponibilité et les éclairages apportés.

IV. ANNEXES - LEXIQUE

Anomalie - Une anomalie est un terme décrivant l'incidence lorsque le résultat réel sous un l'ensemble d'hypothèses est différent du résultat attendu.

Atout - Une application majeure, un système de support général, un programme à fort impact, une usine physique, système critique, du personnel, de l'équipement ou un groupe de systèmes logiquement liés.

Attaque - Une tentative d'obtenir un accès non autorisé aux services, ressources ou informations du système, ou une tentative de compromettre l'intégrité du système.

Atténuation des risques - Prioriser, évaluer et mettre en œuvre les risques appropriés réduire les contrôles/contre-mesures recommandés à partir du processus de gestion des risques.

Canton - Il consiste à espacer les trains roulant dans le même sens afin de respecter les distances de freinage. Un système de signalisation des infrastructures ferroviaires qui permet d'assurer la circulation de plusieurs trains sur une même voie tout en évitant les risques de rattrapages.

Contre-mesure – Action, dispositif, procédure ou technique qui réduit une menace, une vulnérabilité, ou les conséquences d'une attaque en l'éliminant ou en la prévenant, en minimisant le préjudice qu'il peut causer, ou en le découvrant et en le signalant afin que des mesures correctives puissent être pris.

Contrôle d'accès - Le processus d'accorder ou de refuser des demandes spécifiques pour : 1) obtenir et utiliser des informations et des services de traitement d'informations connexes ; et 2) entrer des données physiques spécifiques (p. ex., édifices fédéraux, établissements militaires, entrées frontalières).

Cryptage - Conversion de texte en clair en texte chiffré grâce à l'utilisation d'un algorithme.

Cyber- résilience – La capacité d'anticiper, de résister, de se remettre et de s'adapter aux conditions, contraintes, attaques ou compromissions sur les ressources informatiques.

Faux négatif - Une instance dans laquelle une technologie de détection et de prévention des intrusions échoue pour identifier une activité malveillante comme telle.

Faux positif - Une instance dans laquelle une technologie de détection et de prévention des intrusions identifie à tort une activité bénigne comme étant malveillante.

Intrusion - Acte non autorisé consistant à contourner les mécanismes de sécurité d'un système.

Malveillant - Matériel, micrologiciel ou logiciel qui est intentionnellement inclus ou inséré dans un système dans un but préjudiciable.

Menace - toute circonstance ou événement susceptible d'avoir un impact négatif sur l'organisation opérations (y compris mission, fonctions, image ou réputation), actifs organisationnels, SIGC (Industrial Automation and Control System), ou des personnes qui, contrairement à la politique de sécurité, empêcher intentionnellement ou non l'accès aux données ou provoquer la destruction, la divulgation ou modification des données.

Résilience – La capacité de se préparer et de s'adapter aux conditions changeantes et de résister et récupérer rapidement des perturbations. La résilience comprend la capacité de résister et de se remettre de attaques délibérées, accidents ou menaces ou incidents naturels.

Risque de cybersécurité non atténué – Niveau de risque de cybersécurité présent dans un système avant que des contre-mesures de cybersécurité soient envisagées.

Risque résiduel – Le risque qui subsiste après la prise en compte des contre-mesures.

Risque tolérable - Niveau de risque jugé tolérable pour une organisation afin que le même un avantage ou une fonctionnalité particulière peut être obtenu.

Risque - une combinaison de la probabilité d'une menace d'exploitation d'une vulnérabilité existante et de l'impact résultant de cette situation indésirable.

Signature - Un motif reconnaissable et distinctif associé à une attaque, tel qu'un binaire chaîne dans un virus ou un ensemble particulier de frappes utilisées pour obtenir un accès non autorisé à un système

Source de menace - soit une exploitation intentionnelle d'une vulnérabilité, soit une situation imprévue qui peuvent accidentellement exploiter une vulnérabilité.

Systèmes converger proposée par le groupe de travail Cigref Les systèmes industriels font partie du système d'information (données) de l'entreprise qui peut être redéfini comme l'ensemble des équipements matériels et logiciels générateurs de données, capables de transmettre ces données et de les traiter via un standard de communication (couche d'interface).

Système de détection d'intrusion - Produit matériel ou logiciel qui recueille et analyse informations provenant de diverses zones au sein d'un ordinateur ou d'un réseau pour identifier une éventuelle sécurité les violations, qui comprennent à la fois les intrusions (attaques extérieures aux organisations) et les abus (attaques internes aux organisations).

Système de détection et de prévention des intrusions - Logiciel qui automatise le processus de surveiller les événements se produisant dans un système ou un réseau informatique et les analyser pour signes d'incidents possibles et tenter d'arrêter les incidents potentiels détectés.

Système de prévention des intrusions - Système(s) pouvant détecter une activité intrusive et pouvant également tenter d'arrêter l'activité, idéalement avant qu'elle n'atteigne ses objectifs.

Systèmes d'information d'entreprise (SIE) / Information Technology (IT) « L'ensemble des technologies de traitement de l'information, y compris les logiciels, le matériel informatique, les technologies de communication et les services connexes. En général, le service informatique n'inclut pas les technologies intégrées qui ne génèrent pas de données pour une utilisation en entreprise. » Glossaire IT Gartner.

Systèmes d'information industriels (SII) / Operation Technology (OT) « Le matériel et les logiciels dédiés à la détection ou à la modification de processus physiques via la surveillance et/ou le contrôle direct de périphériques, processus et événements physiques dans l'entreprise (technologie orientée équipement physique). » Glossaire IT Gartner.

Vulnérabilité - faiblesse d'un système d'information, procédures de sécurité du système, des contrôles ou une mise en œuvre qui pourraient être exploités ou déclenchés par une source de menace.

V. ANNEXES - L'INDUSTRIE FERROVIAIRE

V.1. SEGMENTS D'ACTIVITES

Les principaux segments d'activités relevant de l'exploitation industrielle sont[3] :

- La gestion des infrastructures ferroviaires ;
- La gestion du matériel roulant ;
- La gestion de la circulation : cette activité est d'une importance capitale dans la gestion au quotidien de la circulation des trains ;
- La gestion des horaires :
  - **L'horairiste** conçoit et adapte le plan de transport pour permettre à des milliers de trains de circuler quotidiennement et faire cohabiter toutes les entreprises ferroviaires sur le réseau. L'horairiste consolide les besoins de tous les clients du gestionnaire d'infrastructure et adapte les circulations si une infrastructure n'est pas disponible en raison d'une maintenance ou d'un incident. L'horairiste produit un plan d'horaires et est souvent amené à gérer des demandes circulations de dernières minutes.

- La signalisation :
  - Pour transmettre au conducteur des ordres et informations liées à la sécurité des circulations, il est fait usage de signaux412.
  - Outre les signalisations manuelles, la plupart des signaux sont des signaux au sol ou directement transmises sur le tableau de bord en cabine de conduite.
  - Les signalisations actuelles s'appuient sur des dispositifs au sol remplissant les fonctions suivantes :
    - Protection : destinée à interdire l'accès à un itinéraire, à une aiguille, à un passage à niveau (PN) ;
    - Cantonnement : pour assurer l'espacement des circulations de même sens ;
    - Arrêt, indication de marche, limitation de vitesse, indication de direction.

Plus concrètement la signalisation contribue à[413] :

- Contrôler la vitesse train pour interdire le dépassement de la vitesse limite et donc éviter tous risques de déraillement ;
- Contrôler le rattrapage train pour garantir l'espacement physique entre les trains et donc interdire les collisions avec ceux qui sont situés en aval ou en amont ;
- Contrôler la prise en écharpe train pour interdire les itinéraires incompatibles et donc éviter les collisions avec des trains convergents ;
- Contrôler la sécurité des croisements » pour interdire les collisions des trains avec des véhicules routiers.

V.2. L'AIGUILLAGE

- L'aiguillage peut être mécanique ou électrique. L'aiguilleur du rail veille à la régularité des trains, mais aussi la sécurité aussi bien du matériel roulant, des passagers et des équipes de maintenance qui travaillent sur les voies. Il est tenu de faire rouler à l'heure et dans la stricte application des règlements. Les opérations d'aiguillage se font le plus souvent à distance dans un poste d'aiguillage. La manœuvre d'aiguillage s'opérant depuis un ordinateur[414].

- Une erreur dans l'aiguillage a pour conséquence des retards voire des accidents de trains.

[412] EPSF - *Les signaux. Les régimes d'exploitation des lignes. Les systèmes d'espacement des trains* [En ligne]. [Réf. du 05 Juil. 2017]. Disponible sur https://securite-ferroviaire.fr/sites/default/files/users/reglementations/pdf/document-pedagogique-signaux-regimes-exploitation-v1.pdf
[413] *Le contrôle-commande ferroviaire* [En ligne]. [Réf. Du 10 décembre 2020]. Disponible sur Techniques de l'Ingénieur
[414] *Gestion des circulations* [En ligne]. [Réf. Du 15 juin 2020]. Disponible sur SNCF RÉSEAU

V.3. LA SUPERVISION, SURVEILLANCE ET MAINTENANCE

- La surveillance du réseau ferré est assurée par des engins, des trains de mesure, et des équipes techniques. C'est une fonction de veille sur les installations de signalisations électriques ou mécaniques, les aiguillages, les caténaires ainsi que les installations informatiques et de télécoms.
- L'entretien sert à maintenir les infrastructures de transport dans un état convenable afin de retarder d'importants travaux de rénovation et de réduire ainsi les coûts d'exploitation. La maintenance des installations du système ferroviaire est un élément vital de la continuité des activités[415]. Elle se base soit sur des modèles purement statistiques (base sur l'historique de fonctionnement d'un grand nombre de systèmes identiques ou équivalents et on en tire une base d'expérience pour l'identification des seuils critiques que l'on utilise ensuite sur le système sous observation) ou par apprentissage via une technologie d'intelligence artificielle à base par exemples de réseaux de neurones.

V.4. LE SYSTEME INDUSTRIEL FERROVIAIRE

Le transport ferroviaire est qualifié de système industriel, en ce sens qu'il est basé sur un système informatisé/numérique réalisant de manière automatique des traitements, à partir d'informations collectées par des capteurs, ayant pour effets des actions sur des organes physiques. Il se combine avec les systèmes d'information classiques (systèmes "IT") en charge des traitements des données.

Le système industriel comporte deux composantes :

- Une composante opérative (qui exécute les actions)
- Une composante commande qui transmet des instructions à la composante opérative. ICS : Industrial Control System ou Industrial Automation Control System (IACS) ; SACOPI [416](Systèmes Automatisés de Contrôle de Procédés Industriels)

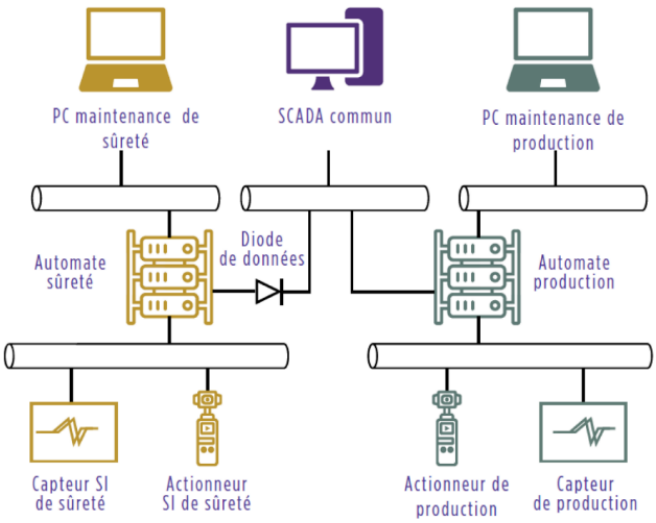


Schéma de cloisonnement SI Industriel / SI de Sûreté (SIS)

Plusieurs terminologies désignent les "systèmes industriels" :

- Le Système de Contrôle Industriel (ICS : Industrial Control Systems ou Industrial Automation Control System (IACS) ou OCC (Operations Control Center) ;
- Systèmes Automatisés de Contrôle de Procédés Industriels (SACOPI) ;
- Systèmes Numériques Industriels.

Par raccourci, le terme SCADA est utilisé pour désigner les systèmes industriels. Mais concrètement les systèmes industriels ne se résument pas au système SCADA tel qu'illustré dans le schéma ci-dessus.

---

[415] *Solutions techniques pour le rail opérationnel - UIC* [En ligne]. [Réf. du 10 Mai 2021]. Disponible sur https://uic.org/IMG/pdf/uic-solutions-techniques-pour-le-rail-operationnel.pdf

[416] *Les systèmes industriels* [En ligne]. [Réf. De septembre 2019]. Disponible sur Mémo CERTITUDE - Les systèmes industriels (certitudenumerique.net))

V.5. LES SYSTEMES ERTM/ ETCS

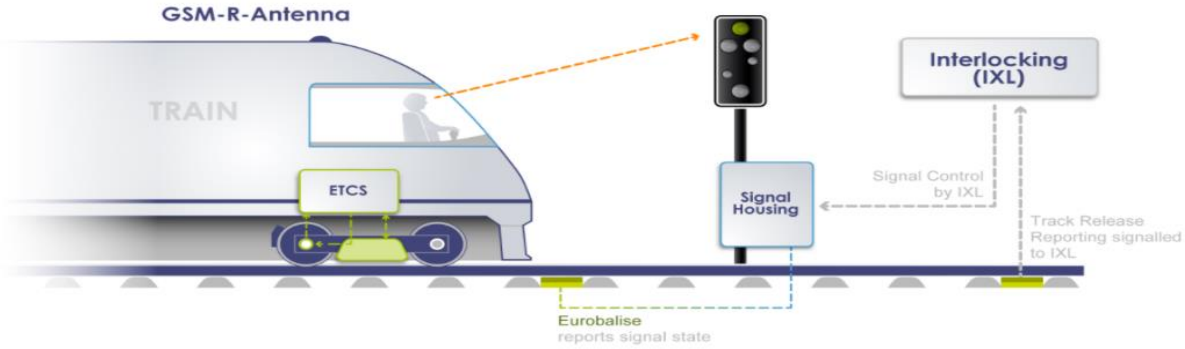
V.5.1. LES SYSTEMES ETCS[417]

European Train Control System (ETCS) | Thales Group

ETCS est la composante majeure de signalisation et de contrôle des trains de l'ERTMS (European Rail Traffic Management System), le système européen de gestion du trafic ferroviaire. ETCS calcule en permanence, pour chaque train, une vitesse maximale de sécurité avec signalisation en cabine à l'intention du conducteur et met en œuvre des systèmes embarqués qui reprennent le contrôle en cas de dépassement de la vitesse autorisée. Il y a, dans le cadre d'ETCS, normalisation des équipements au sol et des systèmes embarqués à bord des trains en respect des différents niveaux que connaît l'ETCS.

Thales offre une gamme complète de solutions ETCS pour des projets clés en main, mais aussi pour des installations sur emplacements neufs (« green field ») ou sur terrains construits (« brown field », aussi appelées friches industrielles). Nous ne nous contentons pas de couvrir uniquement les domaines évidents, tels que les équipements au sol ou des installations ferroviaires embarquées. Parallèlement, nous nous chargeons d'autres domaines horizontaux tels que la cybersécurité ou des fonctionnalités spéciales autres que des spécifications internationales. Par exemple, DAS, ATO, une communication radio à base d'IP et des diagnostiques sophistiqués.

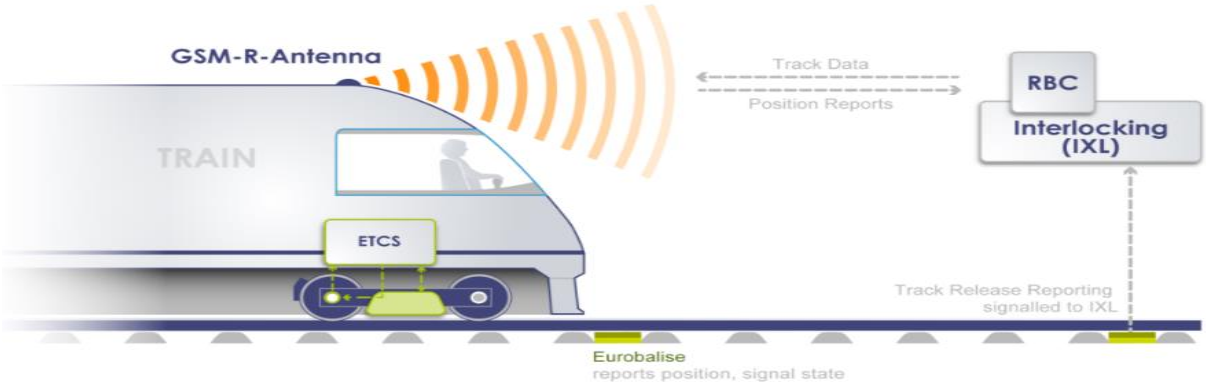
L'ETCS Niveau 1 se superpose facilement sur le système de signalisation national existant et assure une signalisation en cabine. Les autorisations de circulation peuvent être accordées par des Eurobalises fixes et commutables. Elles envoient également des données d'itinéraire à l'unité embarquée. Sur la base des données reçues il y a, à tout moment, calcul de la vitesse maximale ainsi que les courbes de freinage. Il est possible, en plus d'Eurobalises, de mettre en œuvre Euroloop (loop infill = remplissage par boucle) ou une solution radio (remplissage par radio ou sans fil) qui transmet des données en continu sur une distance plus importante.



ETCS est installé au sol et embarqué à bord du train. Les données sont échangées par transmission ponctuelle du sol (voie) au train par le biais de balises ETCS.

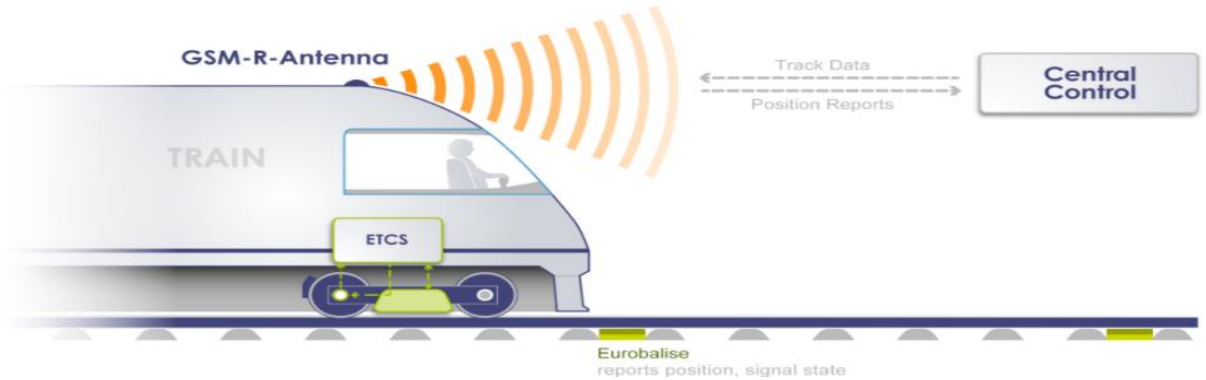
L'ETCS Niveau 2 est un système basé sur la radio (sans fil) qui affiche en cabine la signalisation et les autorisations de circulation. Le train ne cesse d'envoyer des données au RBC (Radio Block Center = centre de bloc radio) pour rapporter sa position exacte et sa direction. Les eurobalises font office de balises de positionnement passives. Les trains affinent leur position à l'aide de capteurs et systèmes additionnels tels que les accéléromètres, odomètres ou radar.

[417] *European Train Control System (ETCS) – THALES* [En ligne]. Disponible sur European Train Control System Etcs



Niveau 1 étendu, avec transmission de données ETCS en continu par GSM-R. Au sol, un RBC contrôle tous les mouvements de trains dans la zone couverte.

L'ETCS niveau 3 est un système entièrement basé sur la radio, sans aucun équipement au sol. Le centre de bloc radio (RBC) reçoit en permanence le positionnement de chaque train et calcule à tout moment la plus petite distance possible entre les trains. Ainsi, la voie n'est plus séparée en blocs fixes, mais en "blocs mobiles". En même temps, il est vital que les trains garantissent leur intégrité, car il n'y a pas d'équipement au sol disponible pour fournir cette information. L'ETCS L3 est actuellement encore en cours de normalisation.



L’équipement de voie a disparu. Le positionnement du train et son intégrité ne reposent pas sur des équipements au sol (signaux, des circuits de voie ou des compteurs d'essieux), mais sont gérés par le train et le RBC.

Le réseau de communication est généralement une infrastructure complexe souvent hiérarchisée, hautement disponible (redondé) et de grande performance que ce soit en matière de latence de propagation des données (temps réel) ou de bande passante. Une norme internationale ferroviaire IEC 61375 précise aujourd’hui les aspects de l’architecture du réseau TCN (Train Communication Network) du système de contrôle/commande.

L’apport de l’informatisation du contrôle/commande a permis :

- Un gain d’encombrement lié principalement à la suppression des armoires à relais
- L’amélioration de l’efficacité économique grâce à sa facilité d’installation ;
- L’amélioration de la souplesse d’adaptation et la flexibilité de déploiement.

Mais certaines fonctionnalités ne sont pas encore pilotées par des systèmes informatiques et conservent la logique câblée c’est le cas de la distribution de l’alimentation électrique dans le train ou l’implémentation de boucles de sécurité à haute intégrité ;

Le TCMS est principalement composé entre autres :

- D'un ordinateur centralisé sur lequel s'exécute l'application logicielle de mission du train et qui supervise l'ensemble des composants constitutifs ;
- D'un dispositif de visualisation homme/machine permettant de restituer à un opérateur les états du système et de le contrôler ;
- D'une infrastructure informatique de communication de données qui connecte numériquement les contrôleurs d'entrées/sorties aux superviseurs applicatifs ;
- D'une infrastructure de communication entre le train et le sol

Le système TCMS est hautement disponible et il est, par construction, robuste à la simple panne, ce qui signifie que n'importe quelle panne simple de communication ou d'exécution n'hypothèque pas la mission du train. Il possède de plus des caractéristiques de fiabilité très élevées de manière à limiter les activités de maintenance et de remplacement et on parle de MTBF supérieur à 100 000 heures (Mean Time Between Failure).

VI. ANNEXES - ENJEUX DE CYBERSECURITE ET MENACES DANS LE SECTEUR FERROVIAIRE

VI.1. DEFENSE EN PROFONDEUR

La notion de ligne de défense permet de regrouper des barrières pour un aspect "communication" et de les corréler avec les niveaux de gravité. Une ligne de défense correspond alors à une transition entre deux niveaux de gravité et implique une réaction planifiée correspondante.

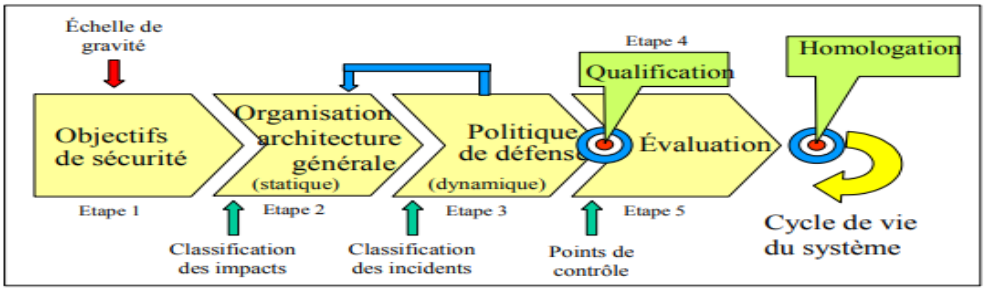


Fig 1. Exemple de démarche de défense en profondeur

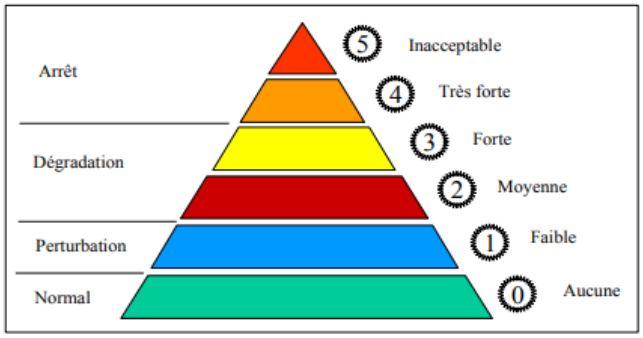


Fig 2. mementodep-v1-1.pdf (ssi.gouv.fr)

VI.2. UN PLAIDOYER POUR UNE CYBERDEFENSE EN PROFONDEUR

Message fort et emblématique de la norme CEI 62443, le principe de défense en profondeur revient à sécuriser chaque sous-ensemble du système et s'oppose à la vision d'une sécurisation du système uniquement en périphérie.

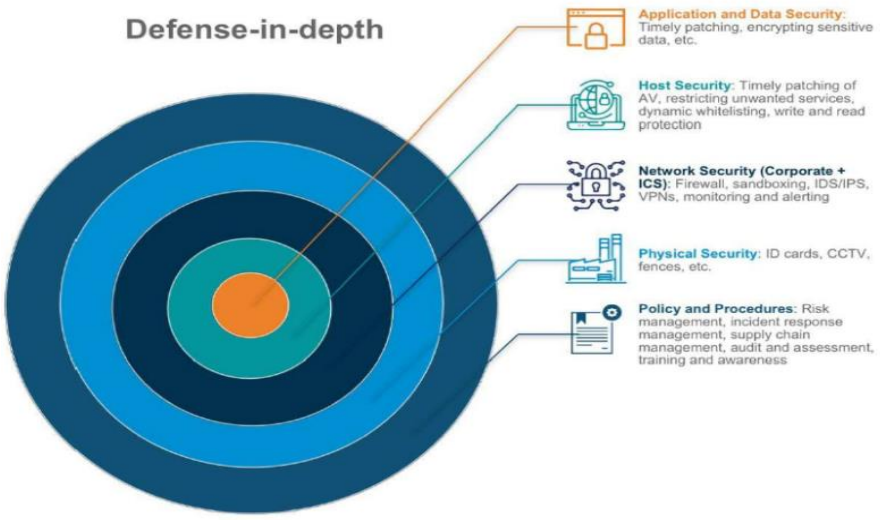


Fig 3. Notions de défense en profondeur

L'attaque Stuxnet de 2010, largement médiatisée, a largement contribué à rendre crédible la menace aux yeux des responsables concernés. Cette attaque, a mis en œuvre une construction informatique malveillante, un malware, d'une complexité jamais rencontrée, était directement ciblé sur un type d'équipements, des automates Siemens en l'occurrence, avec l'objectif, assez largement atteint, semble-t-il, de créer des dommages aux centrifugeuses de l'usine d'enrichissement d'uranium de Natanz en Iran, dont des automates de ce type pilotaient les moteurs.

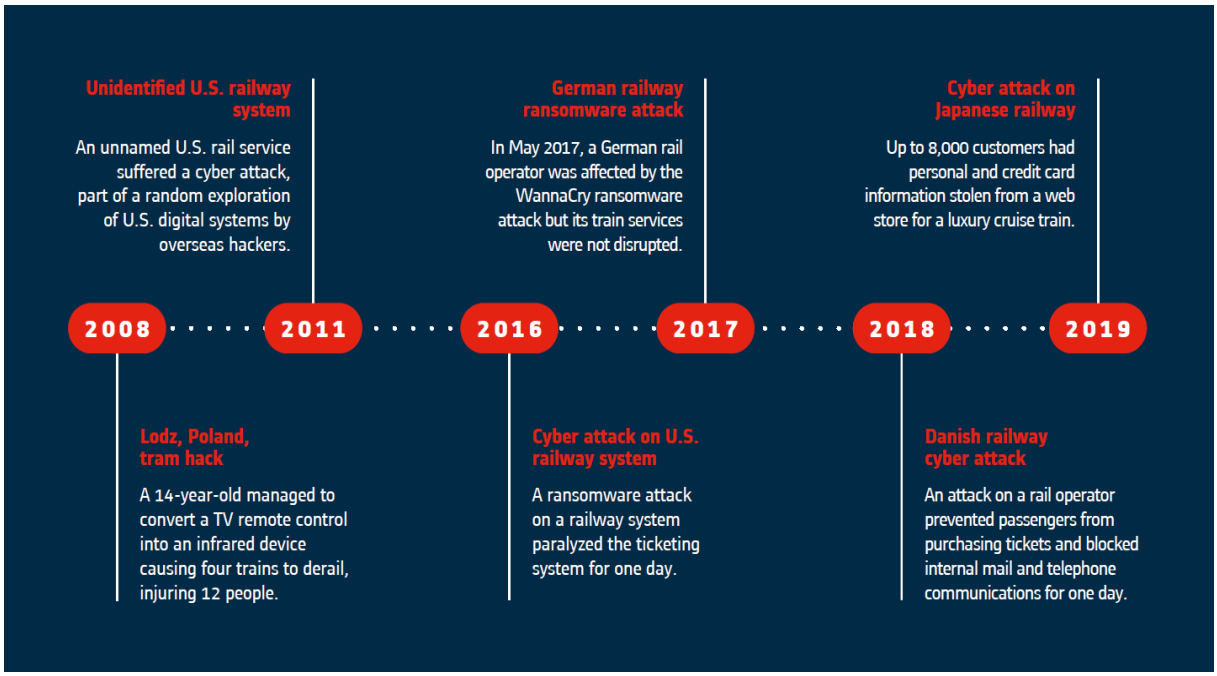


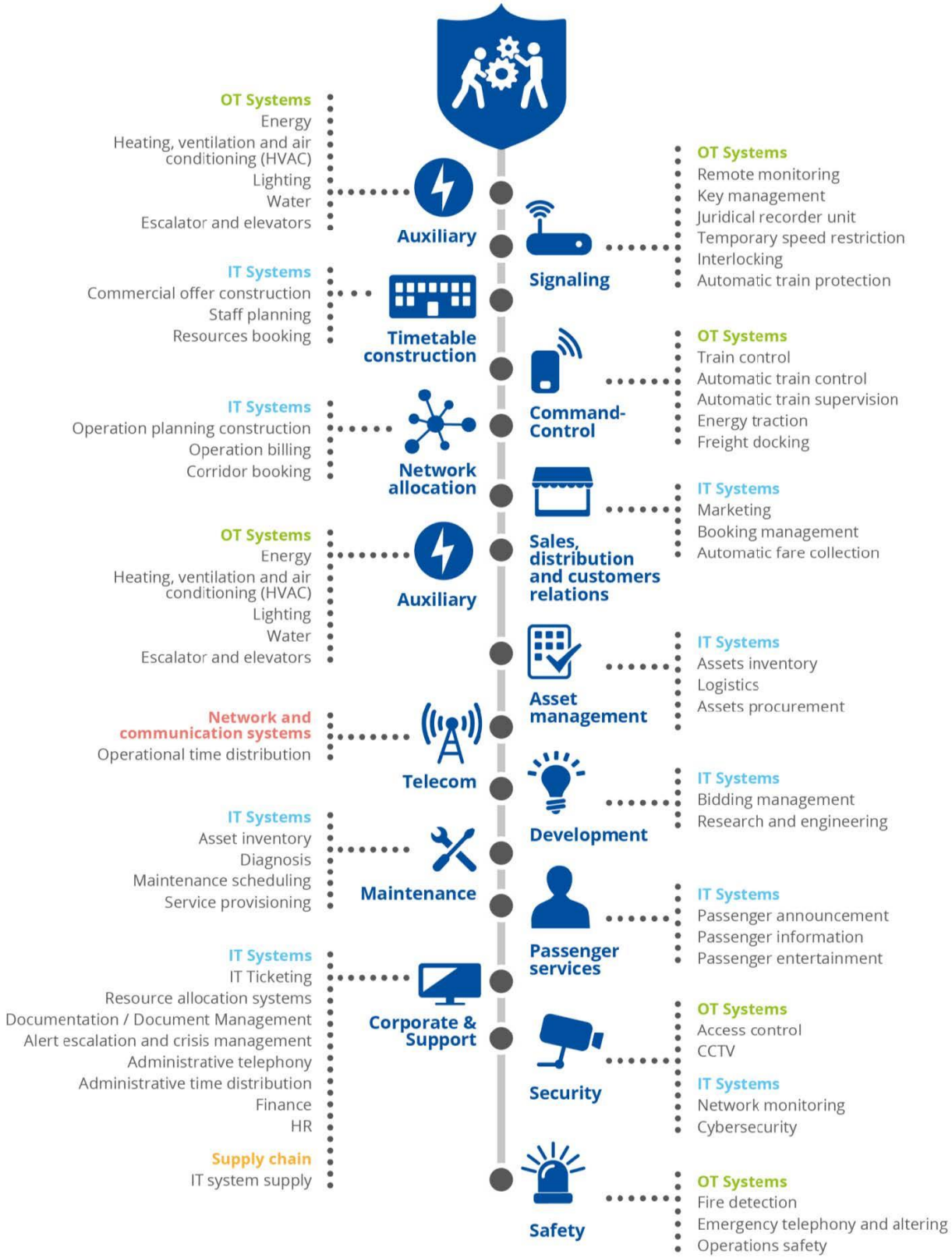
Fig 4. Whitepaper Cybersecurity.pdf (alstom.com)

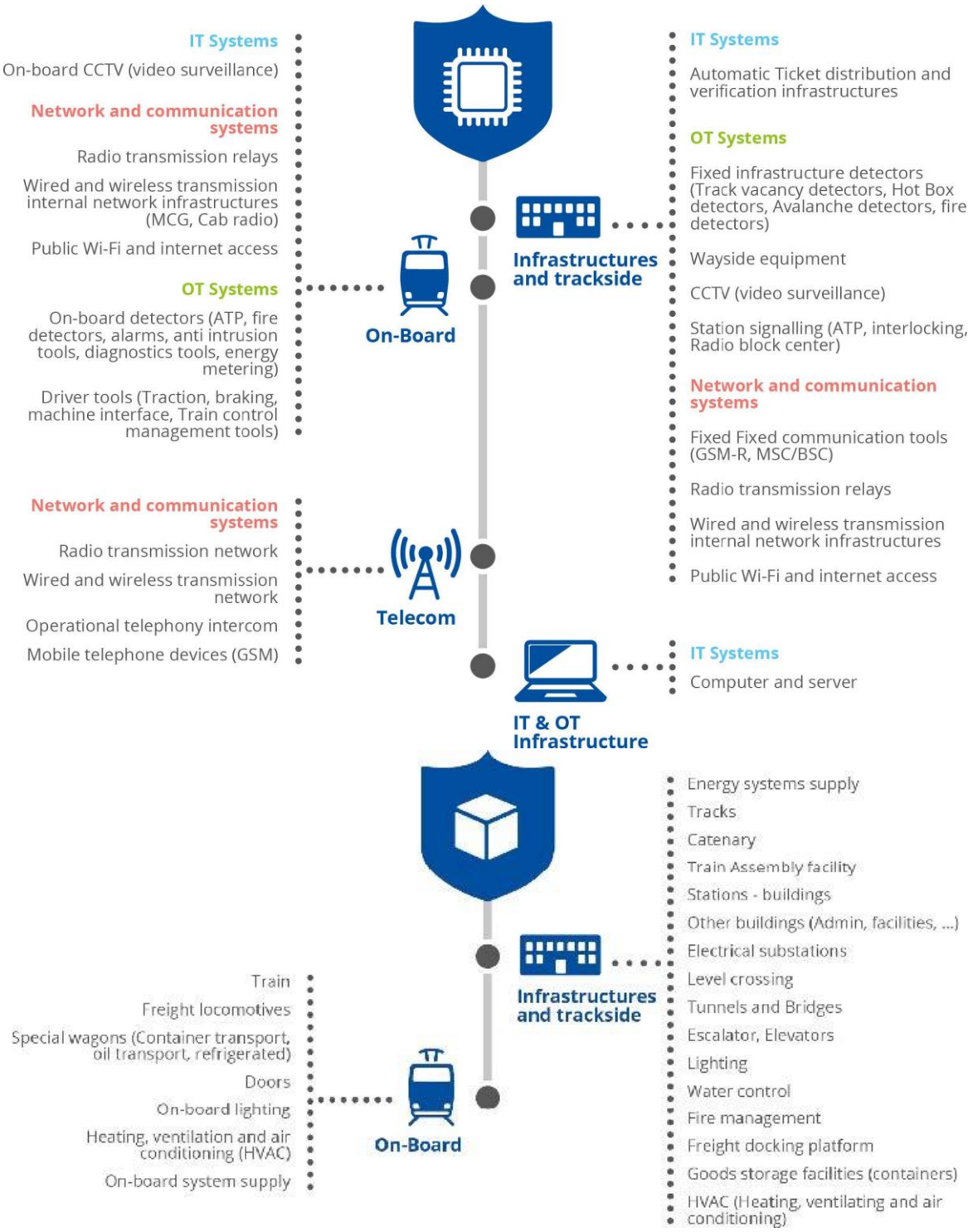
La liste ci-dessous présente des événements considérés comme des incidents de sécurité SI selon l'annexe IV de l'arrêté sectoriel « Transports terrestres » de l'ANSSI (concerne uniquement les SI déclarés à l'ANSSI) :

- Transmission illicite de données entre un système d'information d'importance vitale (SIIV) et un autre système d'information.
- Maintien illicite dans un SIIV.
- Accès illicite à un SIIV.
- Mise en œuvre d'un code malveillant installé sur un SIIV.

- Atteinte à la disponibilité d'un SIIV d'origine inconnue ou malveillante.
- Modification illicite d'un site internet nécessaire au fonctionnement d'un SIIV.
- Collecte illicite de données permettant d'obtenir des droits d'accès privilégiés à un SIIV.
- Dysfonctionnement d'un SIIV, lié notamment à une panne matérielle ou logicielle, susceptible d'affecter significativement la sécurité ou le fonctionnement du SIIV.
- Utilisation illicite des ressources d'un SIIV.
- Manquement à la politique de sécurité d'un SIIV susceptible d'affecter significativement la sécurité ou le fonctionnement d'un SIIV.
- Tentative d'attaque informatique ciblant un SIIV et présentant un caractère particulièrement inhabituel.
- Tentative d'attaque informatique ciblant un SIIV et menée de façon répétitive pendant une période de temps limité.
- Tentative d'attaque informatique s'avérant particulièrement complexe et conçue pour cibler spécifiquement un SIIV.
- Fraude ou tentative de fraude.
- Diffusion illicite d'informations de l'entreprise (Déontologie / RH)

VI.3. TAXONOMIE DES MENACES SUR LES IOT IDENTIFIEES PAR L'ENISA




IT Systems
On-board CCTV (video surveillance)
Network and communication systems
Radio transmission relays
Wired and wireless transmission internal network infrastructures (MCG, Cab radio)
Public Wi-Fi and internet access
OT Systems
On-board detectors (ATP, fire detectors, alarms, anti intrusion tools, diagnostics tools, energy metering)
Driver tools (Traction, braking, machine interface, Train control management tools)
On-Board
Network and communication systems
Radio transmission network
Wired and wireless transmission network
Operational telephony intercom
Mobile telephone devices (GSM)
Telecom
IT Systems
Automatic Ticket distribution and verification infrastructures
OT Systems
Fixed infrastructure detectors (Track vacancy detectors, Hot Box detectors, Avalanche detectors, fire detectors)
Wayside equipment
CCTV (video surveillance)
Station signalling (ATP, interlocking, Radio block center)
Network and communication systems
Fixed Fixed communication tools (GSM-R, MSC/BSC)
Radio transmission relays
Wired and wireless transmission internal network infrastructures
Public Wi-Fi and internet access
Infrastructures and trackside
IT Systems
Computer and server
IT & OT Infrastructure
Train
Freight locomotives
Special wagons (Container transport, oil transport, refrigerated)
Doors
On-board lighting
Heating, ventilation and air conditioning (HVAC)
On-board system supply
On-Board
Energy systems supply
Tracks
Catenary
Train Assembly facility
Stations - buildings
Other buildings (Admin, facilities, ...)
Electrical substations
Level crossing
Tunnels and Bridges
Escalator, Elevators
Lighting
Water control
Fire management
Freight docking platform
Goods storage facilities (containers)
HVAC (Heating, ventilating and air conditioning)
Infrastructures and trackside

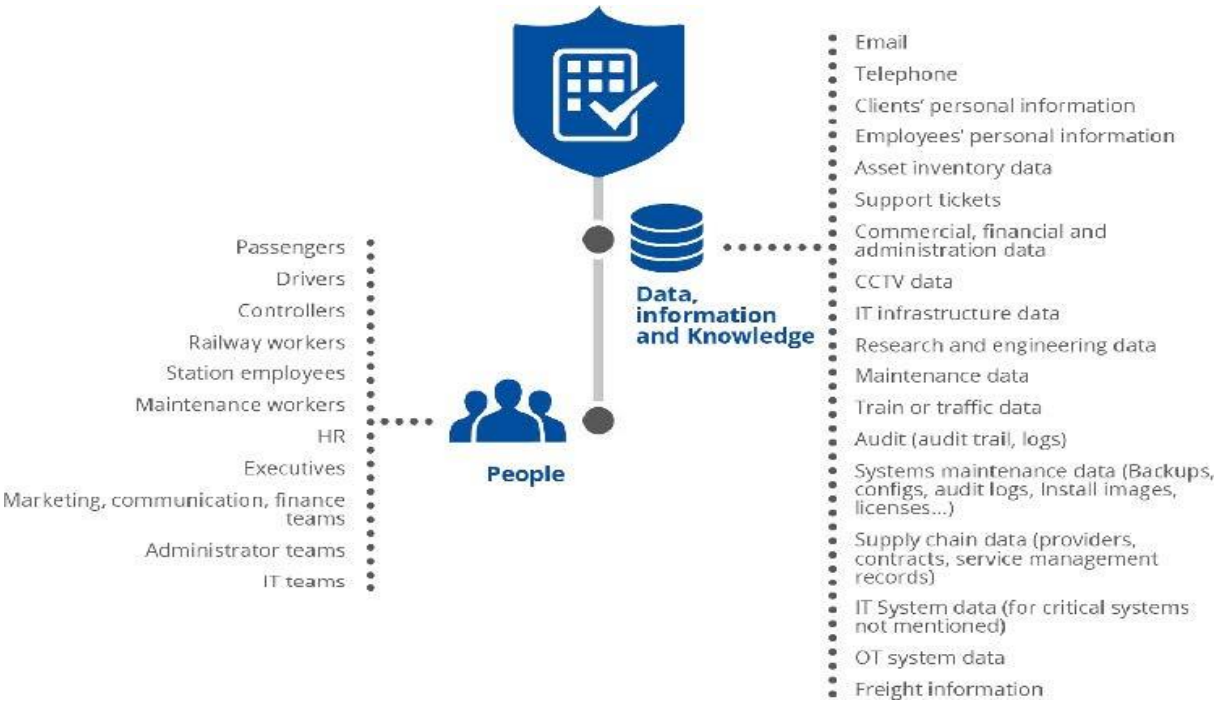


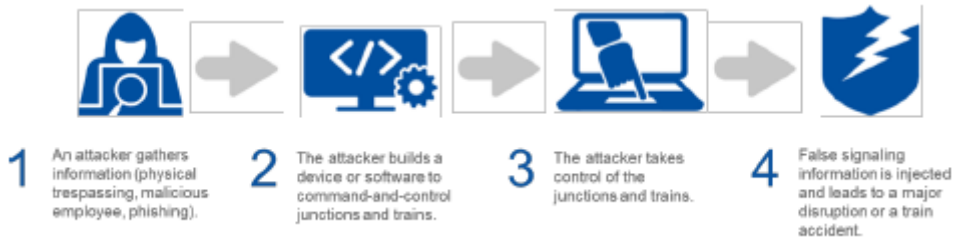
Fig 5. Menaces sur les IoT identifiées par l'ENISA[418]

VI.4. SCENARII D'ATTAQUE ENISA

Ci-dessous 3 des 7 scénarios identifiés par l'ENISA dans son dernier rapport de novembre 2021[419]

Scénario 1 - Compromission d'un système de signalisation ou d'un système de contrôle automatique des trains, entraînant un accident de train

Compromission d'un système de signalisation ou d'un système de contrôle automatique des trains, entraînant un accident de train.



Ce scénario nécessite une forte motivation de l'attaquant et une connaissance approfondie des systèmes et réseaux ferroviaires. Il est considéré comme un scénario à faible probabilité. Il a été inclus, car l'impact potentiel peut être très élevé et c'est l'une des principales préoccupations des parties prenantes du secteur ferroviaire lorsqu'elles examinent les cyber risques. Un incident similaire a eu lieu dans la ville de Lodz, en Pologne, en 2008, lorsqu'un attaquant a réussi à pirater un système de tramway.

[418] *ENISA Report - Railway Cybersecurity - Good Practices in Cyber Risk Management* [En ligne]. [Réf. 2021]. Disponible sur railway-cybersecurity-good-practices-in-cyber-risk-management
[419] *Gestion des risques : Aider les chemins de fer européens à prendre le train de la cybersécurité - ENISA* [En ligne]. [Réf. Du 25 novembre 2021]. Disponible sur Risk Management: Helping the EU Railways

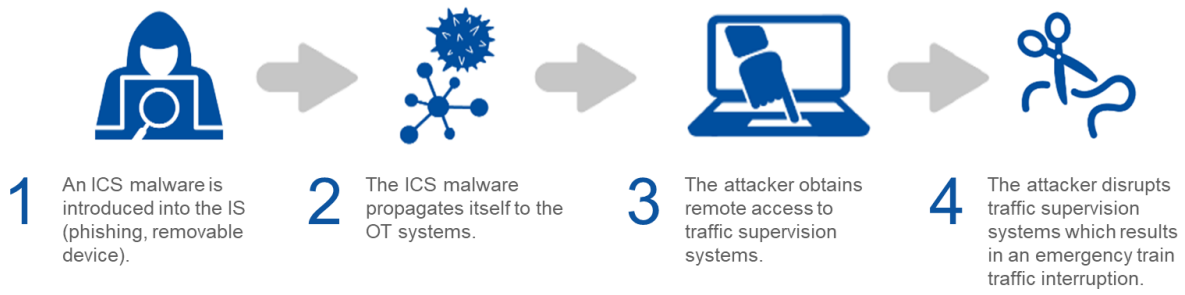
Détails de l'attaque		

• Un attaquant recueille des informations (type de requêtes, adresse IP, etc.),
  ○ Soit l'intrusion dans les installations de l'entreprise ferroviaire (par exemple, dépôt, centre de maintenance,etc.),
  ○ Ou d'un employé malveillant,
  ○ Ou l'utilisation du phishing pour voler des informations à un employé ;
• Un attaquant construit un dispositif ou un logiciel pour commander et contrôler les carrefours et les trains enfonction des informations recueillies ;
• Un attaquant utilise l'appareil pour contrôler les carrefours et les trains ;
• Un attaquant fournit de fausses informations au système, entraînant une perturbation majeure, voire unaccident de train.		

Impacts	**Parties prenantes**	**Actifs affectés**
• Victimes du train • Victimes humaines • Perturbation de l'activité • Perte de réputation	Entreprise ferroviaire Gestionnaire d'infrastructure	• Système de contrôle automatique des trains • Systèmes d'emboîtement • Voies, trains • Passagers
Mesures de sécurité		
Mesures de sécurité de haut niveau	**Exemples de mesures spécifiques**	
• NIS - PR.10 - Sécurité physique et environnementale NIS - GV.6 Sécurité des ressources humaines • NIS - PR.4 • Cryptographie NIS - PR.8 Droit d'accès • NIS - DF.3 Corrélation et analyse des logs	• NIST - Sensibilisation et formations PR.AT (1, 2, 3, 5) • CLC/TS50701 SR 1.2 - Processus logiciel et identification et authentification des dispositifs	

Scénario 2 - Sabotage des systèmes de supervision du trafic, entraînant l'arrêt de la circulation des trains

Sabotage des systèmes de supervision du trafic, entraînant l'arrêt du trafic ferroviaire



Ce scénario est une attaque ciblée utilisant un logiciel malveillant spécifique aux systèmes de contrôle industriel (ICS) pour perturber les systèmes de supervision du trafic, entraînant ainsi un arrêt urgent de la circulation des trains. Un tel incident ne s'est pas encore produit dans le secteur ferroviaire. Ce scénario pourrait également être appliqué aux systèmes d'accostage des marchandises, et ainsi perturber ou interrompre l'activité de fret.

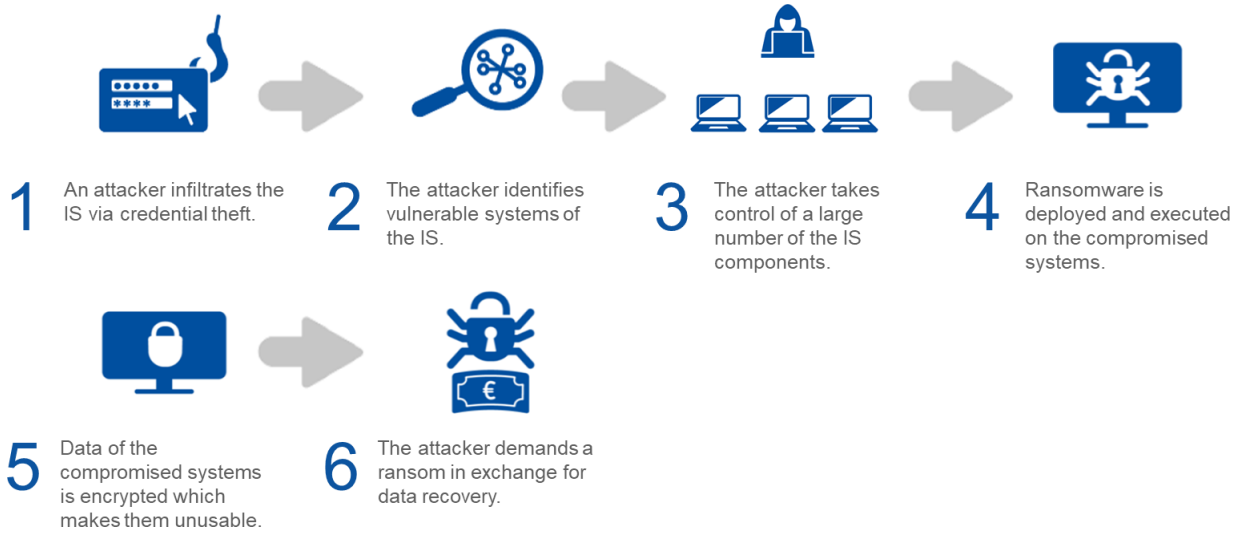
Détails de l'attaque
• Un attaquant introduit un logiciel malveillant ICS, par le biais de courriels d'hameçonnage envoyés aux employés ou aux dispositifs amovibles utilisés sur les systèmes OT ; • Le logiciel malveillant ICS se propage, prend le contrôle du système et obtient un accès à distance ; • Le malware permet aux attaquants de communiquer facilement avec les systèmes de supervision du trafic et de manipuler à distance la mémoire du système pour y injecter des shellcodes, et finalement injecter une charge utile qui perturbe les systèmes de supervision du trafic ; • Les systèmes de supervision du trafic s'arrêtent, empêchant leur surveillance et entraînant un arrêt urgent de la circulation des trains.

Impacts	Parties prenantes	Actifs affectés
• Perturbation de l'activité • Perte de réputation	• Entreprise ferroviaire Gestionnaire d'infrastructure	• Surveillance à distance • Restriction temporaire de la vitesse • Emboîtement • Contrôle des trains • Protection automatique des trains • Mise à quai du fret

Mesures desécurité	
Mesures de sécurité de haut niveau	**Exemples de mesures spécifiques**
• NIS - GV.6 Sécurité des ressources humaines NIS - PR.9 Procédure de maintenance de la sécurité informatique NIS - GV.5 Audit de sécurité • NIS - DF.1 Détection • NIS - DF.3 Corrélation et analyse des logs	• NIST - Sensibilisation et formations PR.AT (1, 2, 3, 4, 5) • CLC/TS50701 - SR 3.2 - Protection contre les codes malveillants • CLC/TS50701 - SR 3.3 - Vérification de la fonctionnalité de sécurité • CLC/TS50701 - SR 3.4 - Intégrité des logiciels et des informations

Fig 6. Attaque par ransomware, ENTRAÎNANT une perturbation des activitÉs

Scénario 3 : Attaque par ransomware, entraînant une perturbation des activités



En 2021, les attaques par ransomware sont considérées comme le premier scénario de menace et visent le secteur des transports. Dans ce cas, l'attaquant s'infiltre dans le système d'information, exploite une vulnérabilité et déploie un ransomware sur une grande quantité d'actifs. Un incident similaire s'est produit en mai 2017 lorsque l'infrastructure ferroviaire de la Deutsche Bahn en Allemagne a été infectée par le ransomware WannaCry22, entraînant l'apparition de messages sur les écrans d'information des gares.

<table>
<tr><th colspan="3">Détails de l'attaque</th></tr>
<tr><td colspan="3">• Un attaquant s'infiltre dans le système d'information par hameçonnage ou vol d'informations d'identification ;
• Ils analysent le réseau à la recherche de vulnérabilités, pour les exploiter et recueillir des informations ;
• Ils découvrent les vulnérabilités des systèmes (par exemple, en raison d'une gestion inadéquate des correctifs) ;
• Ils déploient un ransomware qui crypte les données de tous les systèmes vulnérables ;
• Les systèmes et appareils infectés ne peuvent plus être utilisés ;
• Ils exigent une rançon en bitcoins dans un délai limité en échange du décryptage des données.
• Ils extorquent en outre les employés et les clients en les menaçant d'exposer des données personnelles ou confidentielles.</td></tr>
<tr><th>Impacts</th><th>Parties prenantes</th><th>Actifs affectés</th></tr>
<tr><td>• Perturbation de l'activité
• Perte de données et d'informations
• Perte de réputation
• Perte financière</td><td>• Entreprise ferroviaire Gestionnaire d'infrastructure</td><td>• Systèmes informatiques dans les services et les appareils
• Données, Informations et connaissances</td></tr>
<tr><th colspan="3">Mesures de sécurité</th></tr>
<tr><th>Mesures de sécurité de haut niveau</th><th colspan="2">Exemples de mesures spécifiques</th></tr>
<tr><td>• NIS - PR.9 Procédure de maintenance de la sécurité informatique NIS - PR.2 Séparation des systèmes
• NIS - PR.3 Filtrage du trafic
• NIS - GV.6 Sécurité des ressources humaines NIS - DF.1 Détection
• NIS - DF.3 Corrélation et analyse des logs</td><td colspan="2">• CLC/TS50701 - SR 3.2 Protection contre les codes malveillants
• CLC/TS50701 - SR 3.4 - Intégrité des logiciels et des informations
• CLC/TS50701 - SR 5.2 Protection des limites de zones
• CLC/TS50701 - SR 5.1 Segmentation du réseau NIST - PR.AT Sensibilisation et formations (1, 2, 3, 4, 5)</td></tr>
</table>

[22] Voir https://www.railtech.com/digitalisation/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/

VI.5. ÉVALUATION DES RISQUES DANS LE FERROVIAIRE

VI.5.1. LES METHODES D'ANALYSE DE RISQUE

- **ISO 27005, L'ANALYSE DE RISQUE SUIVANT LES STANDARDS INTERNATIONAUX[420]**

La norme se décline en 6 étapes principales

- Établissement du contexte de l'analyse des risques ;
- Définition de l'appréciation des risques SSI :
  - ✓ Appréciation des risques :
    - ✓ Identification des risques ;
    - ✓ Estimation des risques ;
  - ✓ Évaluation des risques ;
- Choix pour le traitement du risque SSI ;
- Acceptation du risque ;
- Communication et concertation relative aux risques SSI ;
- Surveillance et revue du risque en SSI.

- **EBIOS RM, MÉTHODE MISE AU POINT PAR L'ANSSI[421]**

Les étapes de la méthode (en 5 ateliers) :

- Définir le périmètre métier et technique (atelier 1)
- Identifier les biens supports (ateliers 1, 4 et 5)
- Évaluer la gravité des événements redoutés (ateliers 1 et 3)
- Identifier et caractériser les sources de risque (atelier 2)
- Construire la cartographie de menace numérique de l'écosystème (atelier 3)
- Définir des mesures de sécurité pour l'écosystème (atelier 3)
- Élaborer des graphes d'attaque (atelier 4)
- Évaluer la vraisemblance des scénarios opérationnels (atelier 4)
- Structurer les mesures de traitement du risque (atelier 5)

- **NIST 800-30 [422]**

NIST Risk Management Framework en 6 étapes :

- ✓ Catégorisation des systèmes d'information ;
- ✓ Sélection des contrôles de sécurité ;
- ✓ Mise en œuvre des contrôles de sécurité ;
- ✓ Évaluation des contrôles de sécurité ;
- ✓ Autorisation des systèmes d'information ;
- ✓ Surveillance des contrôles de sécurité.

- **AMDEC - ANALYSE DES MODES DE DÉFAILLANCE, DE LEURS EFFETS ET DE LEUR CRITICITÉ[423]**

AMDEC en 7 étapes :

- ✓ Définition du périmètre de l'étude ;
- ✓ Identification des défaillances redoutées ;

---

[420] *Information technology — Security techniques — Information security risk management* [En ligne]. [Réf. 2021]. Disponible sur ISO - ISO/IEC 27005:2018

[421] *La méthode EBIOS Risk Manager – Le Guide* [En ligne]. [Réf. De décembre 2018]. Disponible sur La méthode EBIOS Risk Manager

[422] *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [En ligne]. [Réf. De décembre 2018]. Disponible sur SP 800-37 Rev. 2, RMF: A System Life Cycle Approach for Security and Privacy | CSRC (nist.gov)

[423] *Qu'est-ce que l'AMDEC ?* [En ligne]. [Réf. Du 3 février 2020]. Disponible sur AMDEC Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (piloter.org)

- ✓ Évaluation des défaillances redoutées ;
- ✓ Sélection des défaillances critiques ;
- ✓ Recherche d'actions correctives ;
- ✓ Validation
- ✓ Mise en œuvre.

- **ANALYSE QUANTITATIVE DES RISQUES**

AQR en 6 étapes :

- ✓ Identification et Recueil des données relatives au système évalué
- ✓ Choix des événements redoutés
- ✓ Évaluation des conséquences et des fréquences des événements
- ✓ Agrégation en un modèle EQR (Évaluation Quantitative des Risques)
- ✓ Étude de sensibilité
- ✓ Utilisation et évaluation du modèle
- ✓ Rapport d'Évaluation du modèle

- **FAIR - FACTOR ANALYSIS OF INFORMATION RISK**

FAIR en 10 étapes réparties en 4 phases :

- ➢ Phase 1 : Identifier les éléments du scénario :
  - ✓ Identifier l'actif à risque ;
  - ✓ Identifier la communauté de menaces envisagée ;
- ➢ Phase 2 : Évaluation de la fréquence des pertes (FEP) :
  - ✓ Estimer la fréquence probable des événements de menace (TEF) ;
  - ✓ Estimer la capacité de la menace (TCap) ;
  - ✓ Estimer la force de contrôle (CS) ;
  - ✓ Déterminer la vulnérabilité (Vuln) ;
  - ✓ Déterminer la fréquence des événements de perte (FEP) ;
- ➢ Phase 3 : Évaluation de l'ampleur des pertes probables (PLM) :
  - ✓ Estimer la perte la plus défavorable ;
  - ✓ Estimation de l'ampleur des pertes probables (PLM) ;
- ➢ Phase 4 : Déterminer et formuler le risque :
  - ✓ Dériver et articuler le risque.

La matrice des risques donne une vision graphique de l'évaluation du niveau des risques d'un système au cours d'une étude de sécurité. Ses versions successives tracent l'évolution de l'exposition aux risques du projet et le déploiement des mesures nécessaires pour leur réduction le cas échéant.

Dans le domaine ferroviaire, c'est l'EN50126 qui donne les bases applicables de définition et d'utilisation de la matrice de criticité.

Le principe est de combiner vraisemblance et impact pour établir à un niveau de risque, en en ayant préalablement déterminé le niveau de risque acceptable.

VI.5.2. ÉVALUATION DU RISQUE

L'évaluation des risques d'un système consiste à :

- ➢ Évaluer les vulnérabilités du système et les menaces auxquelles il est confronté ;
- ➢ Analyser les conséquences probables ou les risques associés aux vulnérabilités ;
- ➢ Mettre en œuvre et maintenir des contre-mesures qui réduisent les effets du risque sur un niveau acceptable.

Dans le domaine de la cybersécurité, les risques inacceptables sont :

- ➢ Le piratage ayant pour objectif la prise de contrôle d'un train ;
- ➢ L'atteinte à l'intégrité aux informations envoyées au conducteur de la locomotive (information de signalisation étant d'anticiper les risques de rattrapage).

VI.5.3. CRITERES D'EVALUATION DES RISQUES

Pour classifier les différents scénarios de risque dans un périmètre donné, des seuils d'acceptation du risque et des niveaux de sécurité à atteindre en cas de non-acceptation doivent être définis.

Niveau de vraisemblance	Ordre	Description	Fréquence
Minime	F1	Cela ne devrait pas se (re)produire.	1 / 10 ans
Significatif	F2	Cela pourrait se (re)produire.	1 / 2 ans
Fort	F3	Cela devrait se (re)produire un jour ou l'autre.	1 / 6 mois
Maximal	F4	Cela va certainement se (re)produire prochainement.	1 / mois

Échelle de vraisemblance

Niveau de gravité	Ordre	Description des impacts					
		Financier	Juridique	Organisationnel	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	Éventuellement une personne légèrement blessée
Significatif	2	Affecte l'entreprise 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 l'entreprise 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 l'entreprise ou l'exploitant surle plan financier sur plus de 3 ans.	Infraction entraînant une sanction pénale	Arrêt total	Intervention gouvernement ale / 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.

Échelle de gravité

VI.5.4. ANALYSE DE RISQUE EN SECURITE IEC 62 443

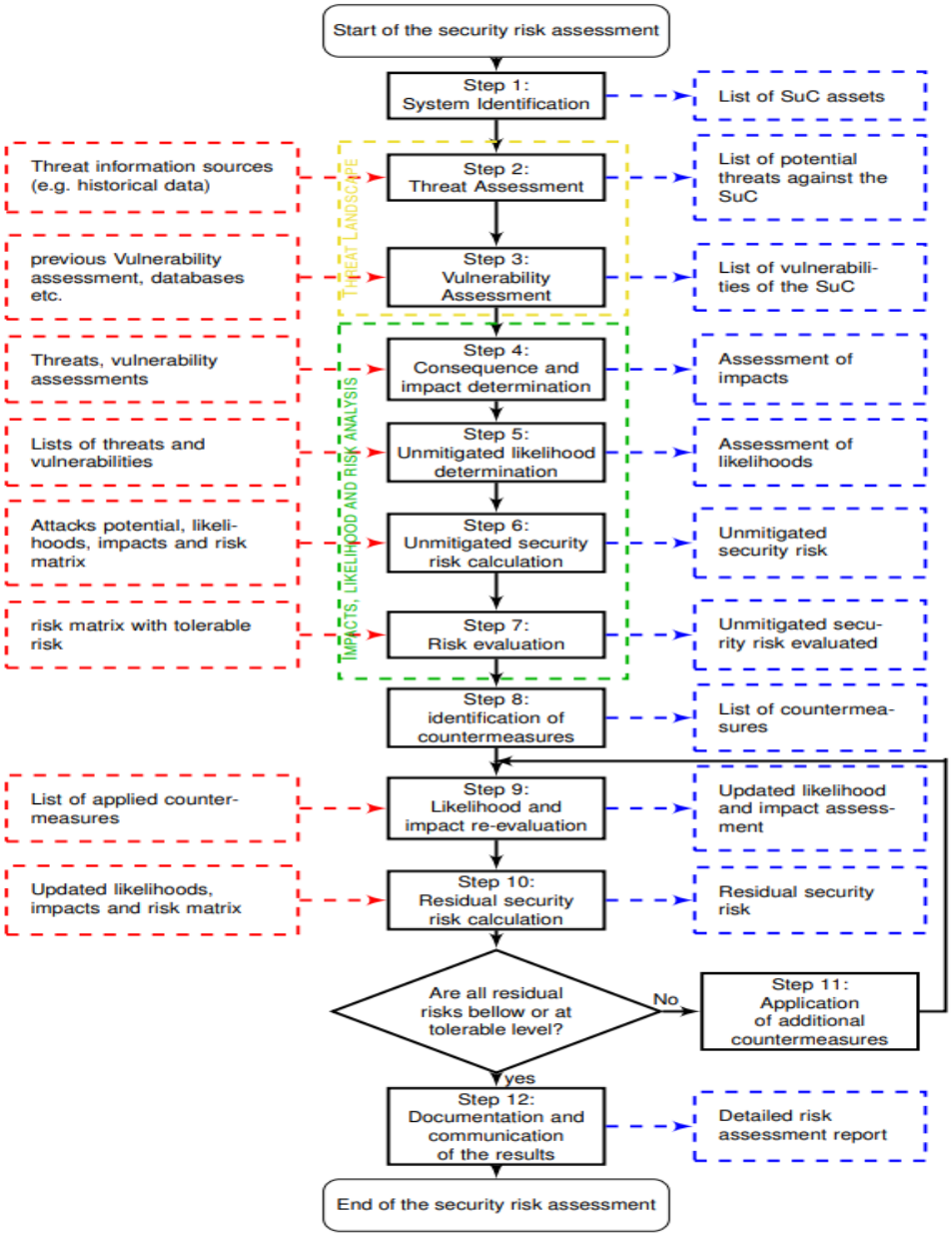


Fig 7. ISA/IEC-62443 security risk assessment methodology[424]

Approche générale de l'ISA99

VI.6. DIRECTIVE (UE) 2016/ SUR LA CYBERSECURITE

Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 – COM (2020) 823 final du 16/12/2021

Contrôle de subsidiarité (article 88-6 de la Constitution)

[424] Mouna Rekik , Christophe Gransart , Marion Berbineau, *Évaluation du risque de sécurité cyber-physique pour les systèmes de contrôle et de surveillance des trains*, [Communication dans un congrès], [Réf du 1 Janvier 2018] Disponible sur Cyber-Physical Security Risk Assessment for Train Control and Monitoring Systems (core.ac.uk)

La proposition de directive COM (2020) 823 s'inscrit dans le cadre de la nouvelle stratégie de cybersécurité de l'Union présentée le 16 décembre dernier, qui vise à renforcer la résilience des entités publiques et privées européennes face aux cybermenaces, dans un contexte de numérisation et d'interconnexion croissante des activités, en Europe et dans le monde.

Destinée à remplacer la directive sur la sécurité des réseaux de 2016 (directive « SRI »)1(*), elle en reprend les principales dispositions (obligation pour les États membres d'adopter une stratégie nationale de cybersécurité, de désigner des autorités compétentes et de veiller à la mise en place d'exigences particulières en matière de cybersécurité par les entités publiques et privées qualifiées d'« opérateurs de services essentiels » (OSE)2(*) ; mise en place de structures de coopération et d'échanges d'informations entre États membres), et l'approfondit, afin de tenir compte de l'évolution du contexte, et des menaces en matière de cybersécurité. À cette fin, la proposition prévoit notamment :

- ✓ Une extension du nombre de secteurs concernés, avec des obligations différenciées - par ailleurs rationnalisées3(*) - pour les entités des secteurs dits « essentiels » et « importants » ;
- ✓ Une prise en compte de la sécurité des chaînes d'approvisionnement ;
- ✓ Le renforcement des mesures de surveillance par les autorités nationales et de la coopération et du partage d'information entre États membres ;
- ✓ Une harmonisation partielle du régime de sanctions administratives entre les États membres - sans préjudice pour ces derniers de la possibilité d'infliger des sanctions pénales ou administratives en cas de violation des dispositions nationales transposant la directive.

La Commission se fonde sur l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), qui vise au rapprochement des règles nationales aux fins de bon fonctionnement du marché intérieur. En effet, l'évaluation de la directive SRI de 2016, adoptée sur la même base juridique, a montré d'importantes divergences entre les législations nationales adoptées pour la transposer. En outre, en raison du manque de clarté de certaines dispositions de la directive, les systèmes de surveillance des entités et de partage d'information entre États membres prévus par la directive ont été insuffisamment appliqués.

Il résulte de cette inégale application de la directive SRI d'importantes charges et une insécurité juridique pour les entités exerçant des activités dans plusieurs États membres, qui peuvent entraver la liberté d'établissement et de prestation de service au sein du marché unique.

En outre, et de ce fait, la Commission observe des degrés de résilience variables en fonction des États membres et, plus globalement, un degré de résilience insuffisant des entités européennes, ce qui est d'autant plus dommageable qu'en raison de l'interdépendance croissante des systèmes et réseaux informatiques européens et de la nature de plus en plus transfrontière des menaces cyber, une mise en œuvre insuffisante dans un État peut avoir des répercussions importantes dans un autre État. Il apparaît donc évident que seule une action au niveau de l'Union est de nature à pouvoir remédier à ces problèmes4(*).

Il faut en outre souligner que la directive serait d'harmonisation minimale (art. 3), et garantirait notamment la possibilité, pour les États membres, de recenser des entités essentielles ou importantes supplémentaires, par rapport à celles déterminées sur les critères de la directive.

La proposition précise également qu'elle serait « sans préjudice des compétences des États membres concernant la préservation de la sécurité publique, de la défense et de la sécurité nationale » (art. 2, 3.), et que les États membres ne seraient pas tenus, dans le cadre des mécanismes d'échanges d'informations, de « fournir des renseignements dont la divulgation serait contraire aux intérêts essentiels de [leur] sécurité intérieure » (considérant 6).

En conséquence, la proposition ne paraît pas porter atteinte au principe de subsidiarité ; le groupe de travail sur la subsidiarité a donc estimé qu'il n'était pas nécessaire d'intervenir plus avant sur ce texte au titre de l'article 88-6 de la Constitution.

* 1 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

* 2 Entités publiques et privées de sept secteurs (énergie, transports, banque, infrastructures de marchés financiers, soins de santé, fourniture et distribution d'eau potable, infrastructures

numériques), ainsi que places de marchés en ligne, moteurs de recherche en ligne et services d'informatique en nuage.

* 3 Avec la possibilité, notamment, d'utiliser les certificats de cybersécurité introduits par le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications.

* 4 De manière complémentaire, les importants risques que peuvent faire courir les incidents cyber à la protection des données personnelles, droit consacré à l'article 8 de la Charte, peut également justifier l'action de l'Union.[425]

[425]Eric Marsden, *La relation contrôleur-contrôlé dans les activités industrielles à risque*, [Livre], [Réf du 21 mars 2019] Disponible sur La relation contrôleur-contrôlé dans les activités industrielles à risque ... - Eric Marsden - Google Livres

FIN DU DOCUMENT

Top of the Document