FICHE DE POSITION STRATÉGIQUE

STRANE

STRatégie d'Action de l'EPSF au Niveau Européen
en concertation avec le secteur français

GT2
Cybersécurité

STRANE : **STR**atégie d'**A**ction de l'EPSF au **N**iveau **E**uropéen en concertation avec le secteur français

Fiche de position stratégique

GT2 : Cybersécurité

Date / version : 07/01/2026 – V2.0

Organisations représentées :

- AFRA
- AGIFI
- ALSTOM GROUP
- ANSSI
- CERTIFER
- EPSF
- HEXAFRET
- Lisea
- RLE
- SNCF Réseau
- SNCF SA
- SNCF Voyageurs
- UTPF

1. Introduction et contexte

La cybersécurité constitue un enjeu croissant dans le secteur ferroviaire, en particulier en matière de sécurité ferroviaire, parallèlement aux évolutions technologiques et plus généralement à la numérisation. Dans un objectif d'amélioration de la sécurité, de la compétitivité, des performances et du développement de nouveaux services, de plus en plus de systèmes sont aujourd'hui interconnectés et reposent sur l'utilisation de nouvelles technologies (cloud, IA, ...), de systèmes informatiques et des réseaux. Ces évolutions entraînent de nouvelles vulnérabilités qui peuvent fragiliser à la fois la sécurité des personnes et des biens et la continuité des opérations.

Dans ce contexte, de nouvelles réglementations européennes (dont la directive NIS2[1] et le règlement CRA[2]) émergent et s'appliquent transversalement aux activités et aux produits sans nécessairement prendre en compte les spécificités propres au domaine ferroviaire comme la durée de vie très longue des équipements. Les infrastructures et le matériel roulant ferroviaires intègrent des technologies dont l'obsolescence est accélérée du fait des évolutions techniques rapides et des menaces de cybersécurité en constante évolution. Cela induit un désalignement entre les dispositifs actuels

[1] NIS2 : DIRECTIVE (EU) 2022/2555 Network and Information Security, directive publiée au Journal Officiel de l'Union européenne en décembre 2022

[2] CRA : REGULATION (EU) 2024/2847 Cyber Resilient Act entré en vigueur le 10 décembre 2024

d'évaluation de la conformité réglementaire et la fréquence nécessaire de mise en œuvre de mesures d'atténuation (évolutions de procédures, configurations, correctifs, ...).

La question d'un cadre réglementaire efficace, compatible et proportionné, appliqué au secteur ferroviaire se pose. Aussi, il est indispensable de proposer une vision claire et de poser un cadre durable et réaliste. Ceci doit notamment passer par une réflexion sur les schémas de certification des matériels et des équipements (démonstration de conformité) ainsi que par un mécanisme de notification des incidents de cybersécurité optimisé. Par ailleurs les imbrications toujours plus étroites entre les constructeurs/fabricants et les opérateurs/exploitants, notamment en termes de maintenance, représentent également un défi pour la cybersécurité de la chaine de valeur. Enfin, la multiplication des acteurs avec l'ouverture à la concurrence complexifie les rôles et responsabilités des Gestionnaires d'Infrastructures et des Entreprises Ferroviaires alors que le système ferroviaire est toujours plus intégré (ERTMS, CBTC). Les travaux en cours pour l'élaboration d'une norme dédiée à la cybersécurité du ferroviaire ou à venir avec la mise à jour des Spécifications Techniques d'Interopérabilité (STI) doivent aller dans ce sens pour contribuer à un cadre réglementaire efficace et économiquement soutenable.

2. Etat des lieux et pistes de réflexion

- Mille-feuille réglementaire, cohérence d'ensemble et démonstration de la conformité, périmètre cybersécurité des STI

En première approche, la réglementation ferroviaire ne semble pas intégrer la cybersécurité : il est difficile de trouver dans une STI ou une MSC le mot cybersécurité écrit en toutes lettres. Pourtant, des exigences peuvent apparaître :

- Dans la STI CCS[3], la citation de la révision 2018 de la norme EN 50129[4] introduit des éléments de cybersécurité.
- De même, une lecture assez large du règlement (UE) 2018/7625 pourrait amener à examiner la politique de cybersécurité d'une organisation dans le cadre de la délivrance d'un certificat de sécurité ou d'un agrément, avec le risque d'introduire des exigences hétérogènes.

Les processus d'autorisation (véhicules et installations fixes) prévoient qu'un demandeur mène un processus de collecte des exigences au-delà des exigences purement ferroviaires. Le demandeur doit ainsi attester qu'il a pris en compte des réglementations diverses susceptibles de s'appliquer.

Ainsi, des réglementations cyber non ferroviaires "transverses » s'appliquent aux organisations : gestionnaires d'infrastructure, entreprises ferroviaires et à leurs systèmes (notamment NIS2, REC[6], CRA et RED[7]). Dans le cas des directives, leur nécessaire transposition en droit national peut introduire des disparités entre les Etats Membres.

[3] Règlement d'exécution 2023/1695/UE «Contrôle Commande et Signalisation»
[4] Applications ferroviaires - Systèmes de communication, de signalisation et de traitement
[5] Conformément à la directive 2016/798 et à l'arrêté du 4 janvier 2016 relatif à la nomenclature de classification des événements de sécurité ferroviaire.
[6] Directive 2022/2557/UE sur la résilience des entités critiques
[7] Directive 2014/53/UE concerne la mise sur le marché des équipements radioélectriques

Comment naviguer dans ce paysage réglementaire ? La réglementation ferroviaire vis-à-vis de la cybersécurité est balbutiante. A l'inverse, les réglementations "cybersécurité" proposent un ensemble de mesures, parfois non coordonnées, qui visent à accroitre le niveau de cybersécurité appliquée au domaine ferroviaire. Il est essentiel de s'assurer de la compatibilité des deux approches, ferroviaires et cybersécurité, au service d'un système plus sûr et plus performant. En cas d'évolution ou de conflit réglementaire, le choix des mesures devra s'appuyer sur une évaluation des contraintes spécifiques au secteur ferroviaire, en tenant particulièrement compte des principes de Sécurité ou Méthode de Sécurité Commune, de la longévité des équipements ainsi que des enjeux de faisabilité technique et industrielle. Cette approche permettra d'assurer une réglementation adaptée aux réalités du système ferroviaire et de l'industrie.

Les activités de cybersécurité ne s'arrêtent pas avec l'obtention d'une autorisation : la menace évolutive nécessite une approche par les risques ainsi qu'une surveillance continue, afin d'assurer l'adaptation des mesures mises en œuvre. Les réglementations ferroviaires ou cybersécurité exigent la notification des incidents et, le cas échéant, la production d'un rapport. Si un incident touche à la fois la sécurité ferroviaire et la cybersécurité, ou d'autres aspects, l'exploitant peut devoir procéder à de multiples déclarations qu'il conviendrait de rationaliser.

- Composants cyber-critiques/Cyber critical assets : garantir l'innocuité pour accélérer les correctifs

Un système considéré comme cybersécurisé à un instant donné peut devenir vulnérable dès le lendemain, nécessitant des correctifs ou des mesures d'atténuation rapides. Cependant, ces interventions doivent être conciliées avec les délais d'analyse réglementaires, souvent incompatibles avec l'urgence des mises à jour, notamment en raison des méthodes d'évaluation rigoureuses appliquées aux modifications des sous-systèmes ferroviaires.

Une voie possible pour éviter cet écueil consiste à définir en amont une liste des composants critiques en matière de cybersécurité (Cyber Critical Assets), selon des critères à définir. Ces composants, par leur conception et l'architecture des systèmes, doivent garantir une innocuité vis-à-vis de la sécurité ferroviaire, quel que soit le correctif qui leur est appliqué (par exemple la montée de version d'un firewall sans impact sur la qualification des calculateurs fonctionnels qui l'encadrent). Ce principe rejoint d'ailleurs les préconisations des normes EN 50129[4] et EN 50159[8], en matière d'architecture des systèmes, visant à séparer les aspects de sécurité fonctionnelle et ceux de cybersécurité. Les critères permettant de définir ces composants critiques pourraient être développés par les acteurs du secteur au niveau européen au moyen d'un groupe de travail et en concertation avec les autorités. Ainsi, le déploiement de correctifs de cybersécurité pourrait être réalisé par l'industriel ou l'opérateur et en application de la réglementation transverse cybersécurité, selon des dispositions définies par anticipation dans le dossier de demande d'autorisation ou de certification.

[8] Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

- Clarification des compétences et de la coordination pour la cybersécurité ferroviaire

L'évolution du contexte réglementaire de la cybersécurité impose une clarification des rôles entre les autorités compétentes en sécurité des systèmes d'information (ANSSI en France) et en sécurité ferroviaire (EPSF en France). Faut-il faire évoluer le rôle des ANS ferroviaires (Autorités Nationales de Sécurité) en leur attribuant des compétences spécifiques en matière de cybersécurité ?

Par ailleurs, la présence d'acteurs multiples occupant des rôles divers au sein du système ferroviaire accentue la nécessité d'une coordination renforcée et d'une clarification des responsabilités, notamment pour sécuriser les échanges entre des entités dont les capacités et la maturité en matière de cybersécurité peuvent être hétérogènes.

Enfin, la démonstration du respect des exigences de la directive NIS2 et du règlement CRA doit prendre en compte le fait que les principaux sous-systèmes ferroviaires sont constitués d'un assemblage de produits, et aboutir à des modalités d'application opérationnelles. Une réglementation sectorielle cohérente, et une définition plus précise des modalités d'application de ces réglementations transverses pourraient répondre à ce besoin.

3. Synthèse : Position du secteur ferroviaire français face aux évolutions réglementaires en cybersécurité

Dans un contexte de renforcement des exigences européennes en matière de cybersécurité, le secteur ferroviaire français adopte une approche stratégique articulée autour de trois principes fondamentaux pour garantir la conformité, la pertinence opérationnelle et l'efficacité documentaire.

1. Assurer une compatibilité réglementaire

L'objectif est de construire une cohérence entre les différents cadres réglementaires. La directive **NIS2** et le **Cyber Resilience Act (CRA)** se complètent en matière de cybersécurité :

- La **NIS2** s'adresse principalement aux **entités** et à leur **organisation** (opérateur, constructeur, industriel), en mettant l'accent sur la **gouvernance**, les **processus internes**, la **chaîne d'approvisionnement** et la **gestion des risques** liés aux systèmes d'information.
- Le **CRA**, quant à lui, s'adresse aux fournisseurs de produits et agit comme un **levier technique**, en ciblant les **produits** et leur **sécurité intrinsèque**. Il permet de démontrer la **conformité technique** des équipements et logiciels.

Cette répartition des rôles permet une **gestion plus efficace des risques de cybersécurité** : les entreprises peuvent s'appuyer sur les exigences du CRA pour **identifier et atténuer les vulnérabilités** dans leurs produits et services, facilitant l'atteinte des objectifs de la NIS2 à savoir **protéger leurs réseaux et systèmes d'information** contre les cybermenaces.

Les STI[9] doivent être **compatibles avec le CRA** voire avec la directive NIS2. Afin d'assurer une interopérabilité sécurisée à l'échelle européenne, les exigences de cybersécurité que pourraient comprendre de futures évolutions des STI doivent être alignées avec les réglementations cybersécurité transverses et mettre en évidence l'articulation vis-à-vis des exigences issues de celles-ci.

2. Prioriser les efforts et optimiser la mise en œuvre des mesures de cybersécurité

Face à la complexité des systèmes et à la diversité des actifs, le secteur souhaite prioriser ses efforts en :

- **Se concentrant sur les CCA (Cyber Critical Assets)** : qu'il s'agisse d'actifs existants (legacy) ou de composants critiques dans les projets récents/futurs, les CCA sont au cœur des démarches de sécurisation (Maintien en Condition de Sécurité – MCS) et doivent à ce titre être précisément identifiés. Cela inclut notamment la gestion des correctifs, qui doit se faire dans le cadre du CRA pour garantir une sécurité continue et documentée.
- **Donnant la priorité aux COTS (Commercial Off-The-Shelf)** : les produits sur étagères, parfois utilisés comme CCA, sont un levier de déploiement de la cybersécurité par effet de volume.

Pour éviter les redondances et maximiser l'efficacité, le secteur préconise :

- **D'utiliser les normes cybersécurité ferroviaire IEC 63452** (en cours d'élaboration) **et TS 50701** : ces standards permettent de produire des livrables **réutilisables directement** dans les démarches de conformité CRA et NIS2, évitant ainsi la duplication documentaire.

3. Permettre une cybersécurité efficace articulée avec la maîtrise de la sécurité ferroviaire

- **Optimiser les démarches de démonstration**

L'anticipation des conditions de déploiement cybersécurité dans un contexte de sécurité ferroviaire est un point clef que le secteur doit considérer afin de garantir la réactivité nécessaire au traitement d'une problématique cybersécurité. Des conditions et critères de traitement cybersécurité clairement définis (autour notamment de l'approche CCA) en adéquation avec les nécessités de maîtrise de la sûreté de fonctionnement devraient permettre de déployer des correctifs cybersécurité en limitant les démonstrations de sécurité ferroviaire et *a fortiori* d'obtenir une nouvelle autorisation de la part d'une ANS.

- **Encadrer les démonstrations par une approche sectorielle harmonisée**

Les conditions et critères de déploiement cybersécurité doivent être définis par les experts sécurité de fonctionnement et cybersécurité du secteur, et en relation avec les autorités de sécurité respectives (ERA/ANS pour la sécurité ferroviaire, ENISA pour la cybersécurité) afin

[9] Dont les STI OPE (Règlement d'exécution 2019/773/UE «Exploitation et gestion du trafic du système ferroviaire», STI TAF Règlement d'exécution 2021/541/UE **« Applications télématiques au service du fret »** et STI TAP Règlement d'exécution 2011/454/UE « Applications télématiques au service des voyageurs » sont exclues.

d'aboutir à une application harmonisée et efficace pour l'ensemble des projets et de la chaîne d'approvisionnement du secteur ferroviaire européen.

- **Matériel ancien**

La transformation du secteur ferroviaire vers des systèmes plus cybersécurisés appliquera les principes de transition et de priorité pour les matériels anciens (legacy) leur permettant de rester en service tout en progressant vers la conformité en proportion des risques identifiés ou par opportunité lorsqu'une modification est réalisée.


STRANE