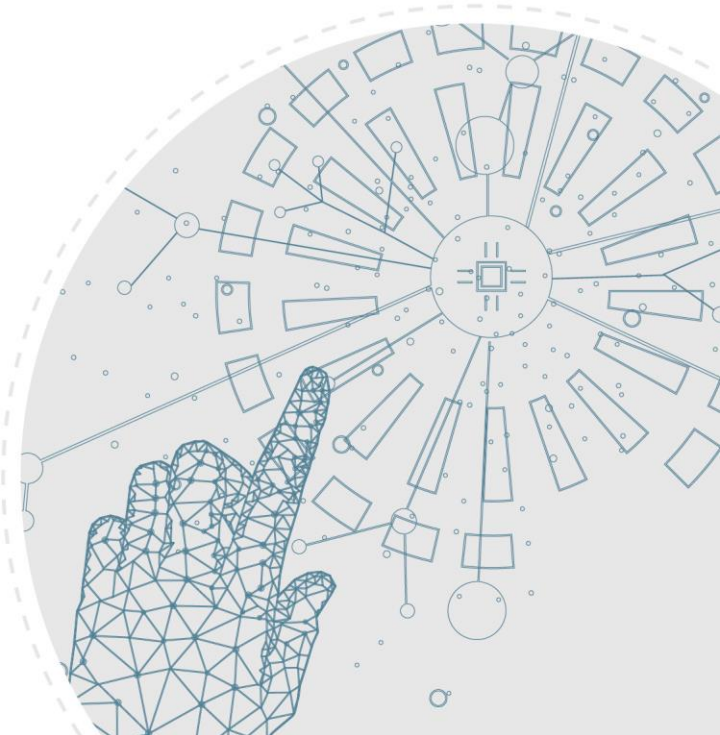
SYS DOCT 002 V1

Doctrine

Prise en compte des objets connectés dans le ferroviaire

23 octobre 2023



Sommaire

1. Introduction

1.1. Avant-propos

Ce document est le résultat d'un groupe de réflexion organisé par l'Établissement public de sécurité ferroviaire (EPSF) relatif aux objets connectés. Il est destiné à évoluer en fonction des avancées dans ce domaine. Il s'inscrit dans la période dynamique de digitalisation du secteur ferroviaire au cours de laquelle va potentiellement se développer l'utilisation d'objets connectés.

L'objectif de ce document est d'identifier les enjeux et risques associés à ces composants spécifiques et de réfléchir à leur impact sur la sécurité, en particulier dans le contexte ferroviaire, et de présenter des recommandations.

Ce document ne fournit pas de directives spécifiques sur le niveau de sécurité approprié pour chaque objet connecté.

1.2. Domaine d'application du présent document

Ce document regroupe un ensemble de recommandations relatives à l'utilisation des objets connectés dans les démonstrations de conformité aux exigences techniques et règlementaires applicables au domaine ferroviaire. Sa portée est générale et constitue une synthèse de réflexions.

Si les démonstrations de sécurité pour la certification et les autorisations sont plus particulièrement visées, ces préconisations se veulent suffisamment larges pour être utilisées dans d'autres cadres : expertise, recherche, développement, etc.

En revanche, ce document n'a pas vocation à s'inscrire dans une démarche d'ingénierie des objets connectés, allant de la conception à leur certification, mais bien à s'assurer que l'usage qui peut en être fait offre toutes les garanties d'obtenir des résultats conformes au comportement souhaité en service de l'objet connecté.

1.3. Définition d'un objet connecté

Selon la définition de l'Union internationale des télécommunications, un objet connecté est un équipement doté de capacités de communication et éventuellement de capacités de détection, d'actionnement, de saisie de données, de stockage de données et de traitement de données.

2. Contexte des objets connectés dans le ferroviaire

La diminution progressive du coût des composants sur le long terme, tels que des circuits, la généralisation d'internet, des réseaux de télécommunications, le développement de batteries à haute densité, le développement de l'intelligence artificielle, des capteurs à faible consommation, de protocoles de communication à faible énergie et longue distance, etc. concourent au développement

des objets connectés. Cette tendance facilite l'installation d'un grand nombre de ces dispositifs, améliorant ainsi la compréhension de l'état du système.

2.1. Apport des objets connectés

Les objets connectés ont la capacité de transmettre des informations depuis des zones auparavant inaccessibles pour l'homme. Cela permet une cartographie plus précise de l'environnement qui peut être potentiellement reproduite dans un jumeau numérique. Des composants existants peuvent être équipés de ces dispositifs pour communiquer. De plus, la transmission des informations peut se faire en temps quasi-réel.

La transmission des informations peut se faire en temps quasi-réel

Dans le secteur ferroviaire, l'usage de capteurs et de réseaux de communication n'est pas nouveau. Toutefois, auparavant, les fonctions étaient cloisonnées, opérant par sous-systèmes isolés. Les informations recueillies par différents sous-systèmes n'étaient pas partagées. De plus, pour un même composant, les données des capteurs étaient analysées de manière indépendante sans agrégation.

L'emploi d'objets connectés permet une maintenance en temps réel, avec la possibilité d'une intervention immédiate en cas de défaillance, et la mise en œuvre d'une maintenance prévisionnelle. Les réparations du matériel peuvent être planifiées au moment le plus opportun, c'est-à-dire lorsqu'elles ont un impact minimal sur la production.

2.2. Utilisation des objets connectés dans le ferroviaire

En ce qui concerne le ferroviaire, les applications potentielles actuellement identifiées ayant un lien avec la sécurité sont nombreuses :

- pour le matériel roulant les utilisations peuvent être des portiques d'analyses qui récupèrent les informations de capteurs embarqués afin de déclencher la maintenance en temps réel, la détection d'incendie, la détection de plats sur les roues, la détection d'échauffement de roulements ou de composants électriques, la prise en compte du kilométrage parcouru pour la maintenance, la détection d'un accostage brutal, la pose de capteurs sur le bogie pour identifier des vibrations anormales ou des montées en température, la détection de porte ouverte, etc. ;
- pour l'exploitation, les objets connectés peuvent être envisagés dans l'allumage automatique de lampes à l'approche d'un train ou d'un passage à niveau, la détection de quais encombrés, la revue d'aptitude au transport, la détection de bâches flottantes ou des pièces engageant le gabarit, la présence d'intrus, la localisation des trains, la détection de frein serré (frein digital), etc. ;
- pour l'infrastructure les objets connectés peuvent être utilisés pour la supervision de l'état des appareils de voie et la détection anticipée de la défaillance d'appareils de voie, le suivi des installations électriques et informatiques, de la défaillance de la géométrie de la voie, la présence de véhicules ou piétons aux passages à niveau, le suivi de la température affectant la dilatation des rails, la surveillance des ouvrages d'art, la surveillance du gabarit, la détection de crues, de montée de nappe phréatique, d'éboulement, la protection des opérateur travaillant sur la voie, etc.

2.3. Les contraintes et limitations des objets connectés

2.3.1 Contraintes environnementales

Les objets connectés sont généralement situés à proximité des composants qu'ils surveillent (in situ), aux conditions environnementales qui peuvent être inhabituelles pour les composants électroniques ferroviaires, et qui sont susceptibles de provoquer leur dégradation prématurée.

Ces dispositifs sont souvent conçus avec une capacité de calcul et de mémoire limitée, pour minimiser leur consommation d'énergie et préserver la batterie, en particulier lorsqu'ils ne sont pas connectés à une source d'électricité constante.

De plus, ils peuvent utiliser des protocoles spécifiques qui consomment très peu d'énergie et qui limitent la bande passante.

2.3.2 Implantation/contraintes

Les mesures effectuées présentent des incertitudes (notamment liées à la distance qui sépare le capteur de la source à mesurer) et peuvent être sensibles au vieillissement. Les mesures et informations doivent provenir de la source que l'on désire mesurer. Certains objets connectés seront répartis sur le terrain, dans des zones potentiellement difficilement accessibles.

Les objets connectés peuvent être alimentés par le réseau électrique, avec des batteries, ou en récoltant l'énergie dans leur environnement ou par plusieurs de ces sources. La durée de vie des batteries peut être insuffisante pour qu'elles restent fonctionnelles durant la période d'utilisation prévue. Si un objet connecté récolte l'énergie de l'environnement (solaire, vibrations, etc.), il existe des périodes où ces sources d'énergies ne seront pas disponibles.

2.3.3. Télécommunication

Les capteurs sont en mesure de dialoguer avec des serveurs possédant des capacités significatives en matière de traitement et de stockage de données, couramment situés dans le cloud. Plusieurs risques se dessinent alors : une possible rupture de liaison, des délais de transmission non négligeables, une bande passante potentiellement inadéquate.

La fréquence et le débit de transmission sont parfois intentionnellement réduits pour contrôler la consommation énergétique, risquant alors de s'avérer insuffisants pour assurer la fonction désirée. Les communications via réseau hertzien comportent des limitations et contraintes spécifiques. Ces contraintes sont typiques des réseaux de télécommunications : atténuation, portée, orientations, bande

passante, fréquences, présence d'obstacles, congestion, déconnexion, durée d'établissement de la connexion, etc.

L'établissement d'une liaison fiable entre l'émetteur et le récepteur est impératif, ce qui engendre des contraintes de polarisation, de directionnalité, de gain entre les composants. Ces exigences se traduisent par des contraintes en matière de conception et d'installation.

2.3.4. Compatibilité et interopérabilité

La compatibilité des équipements est un aspect important, notamment aux interfaces entre le matériel roulant et les infrastructures. En ce qui concerne les objets connectés, il faut donc tenir compte pour les équipements de leur interaction avec les véhicules venant sur le réseau ferroviaire. Des informations produites peuvent être ambigües. Ainsi, à titre d'exemple, une vitesse peut être la vitesse du train, de rotation d'un essieu, etc.

2.3.5. Gestion des données

Les objets connectés, par leur nature, produisent une multitude de données. Il est donc impératif que le système en place, ainsi que les agents assignés à cette tâche, soient à même de gérer ces informations de manière efficiente. Par ailleurs, une attention particulière doit être portée à la vérification de l'exactitude de ces informations, notamment en termes de pertinence temporelle ou face à leur vulnérabilité en termes de cybersécurité. Ainsi, il est important de prendre en considération la difficulté potentielle liée à l'utilisation de multiples données remontées, parfois de manière très précise, qui pourraient s'avérer difficilement exploitables. Le traitement du bruit, et sa distinction d'une éventuelle anomalie, représentent un enjeu majeur de l'analyse du signal. Une fonctionnalité ne doit pas être activée en réaction à un bruit de fond.

2.4. Spécificité des objets connectés dans le ferroviaire

En ce qui concerne les technologies, les objets connectés n'introduisent pas d'innovations radicalement nouvelles. Les domaines de l'électronique, des logiciels et des télécommunications sont bien établis depuis des décennies. Cependant, leur intégration envisagée dans le secteur ferroviaire présente des caractéristiques particulières qui pourraient engendrer de nouveaux risques. À ce stade, les particularités potentielles suivantes ont été identifiées :

- mise en œuvre de composants en environnement extérieur ;
- recours à l'intelligence artificielle ;
- multiplicité des composants ;
- évolution des protocoles de maintenance (maintenance assistée par les objets connectés, mise en place de la maintenance prédictive) ;
- substitution de la surveillance humaine par des dispositifs automatiques.

La majorité des objets connectés disponibles sur le marché ne sont pas conformes aux normes spécifiques au secteur ferroviaire. Par ailleurs, il est impératif de garantir que les objets connectés intégrés dans l'environnement ferroviaire peuvent l'être sans engendrer de nouveaux risques, tels que les perturbations électromagnétiques ou la chute de pièces, par exemple.

Les objets connectés sont souvent construits à partir de composants commerciaux à durée de vie relativement courte (matériel et/ou logiciel), généralement de quelques années, alors que les applications ferroviaires ont des durées de vie s'étendant sur plusieurs décennies

Il sera donc nécessaire de permettre la coexistence de ces objets avec des équipements ayant un cycle de vie beaucoup plus étendu. Par conséquent, l'obsolescence (qu'elle soit matérielle et/ou logicielle) se transformera en une problématique constante.

3. Cadre réglementaire relatif aux objets connectés

3.1. Le cadre règlementaire européen

Les développements technologiques numériques soulèvent des questions de compatibilité et accès au marché, sécurité, confidentialité ou encore de responsabilité. Ces problématiques peuvent être abordées au niveau européen lorsque des solutions communes sont nécessaires notamment dans le cadre du marché intérieur.

Même si les objets connectés sont un domaine récent pour lequel l'approche réglementaire reste pour l'heure limitée, depuis 2015, la Commission européenne a publié des documents d'analyse et stratégiques et proposé des initiatives législatives plus spécifiques dans plusieurs domaines ayant un impact, à titre différent, sur le développement des objets connectés.

La question de la sécurité des objets connectés n'est pas appréhendée en tant que telle mais se trouve *de facto* abordée par une réglementation plus générique qui s'applique également aux objets connectés. On constate aussi que, lorsqu'une législation horizontale est proposée sur ces thèmes, la Commission prend en compte les possibles spécificités sectorielles et les législation/structures/organismes/procédures déjà en place dans certains secteurs faisant déjà l'objet de règles concernant la mise sur le marché et la surveillance de systèmes et composantes (comme le ferroviaire). Il est particulièrement pertinent de suivre les développements dans des domaines tels que la cybersécurité, l'intelligence artificielle (IA) et les règles de responsabilité. En effet, des procédures législatives sont en cours auprès du Parlement européen et du Conseil de l'Union européenne sur des actes législatifs qui introduisent une approche horizontale à ces thématiques, mais qui ont ou pourraient avoir des suites au niveau sectoriel.

3.2. Cadre normatif

De nombreuses normes peuvent s'adresser aux objets connectés. En premier lieu, les normes ferroviaires doivent être prise en compte. Mais des normes d'autres domaines peuvent s'appliquer (télécommunication, etc.). L'entité devra analyser les normes potentiellement applicables, en termes d'environnement, de technologie et de domaine.

3.3. Conséquence pour l'EPSF de la réglementation des objets connectés

Les réglementations relatives à la cybersécurité, l'IA et les systèmes d'information ont et entraîneront indéniablement des conséquences importantes pour les acteurs du secteur ferroviaire. Toutefois, en

l'état actuel des textes, l'impact demeure limité pour l'EPSF dans le cadre de ses missions. En effet, en l'absence de réglementation prescriptive spécifique à l'Internet des objets (IoT), le schéma classique d'autorisation fondé sur les rapports des organismes notifiés (Nobo), des organismes désignés (DeBo) et des organismes d'évaluation de l'analyse des risques (Asbo) ainsi que sur une démonstration de sécurité seraient applicables en la matière. Ainsi, le texte central pour l'EPSF reste le règlement (UE) n° 402/2013 de la Commission du 30 avril 2013 *relatif à la méthode de sécurité commune relative à l'évaluation et à l'appréciation des risques*.

4. Gestion des défaillances

Les risques liés à l'utilisation des objets connectés peuvent être de diverses natures. Ils peuvent être fonctionnels, c'est-à-dire liés à la complexité de la mise au point de ces composants, ou dysfonctionnels, c'est-à-dire associés à des pannes.

4.1. Connaissance et détection des défaillances

Les défaillances à analyser concernent à la fois l'objet supervisé (tel qu'un essieu, par exemple) et l'objet connecté lui-même.

L'utilisation d'objets connectés ne permettra pas nécessairement d'identifier tous les modes de défaillance du composant surveillé. Certaines informations fournies par les objets connectés peuvent être perdues (à cause des perturbations électromagnétiques, perte d'alimentation, etc.).

Pour garantir qu'un objet connecté fournira l'information appropriée, il sera nécessaire d'avoir analysé les modes de défaillance, de comprendre les phénomènes de dégradation des composants supervisés. Cette démarche repose sur une analyse de ces modes de défaillance (approche de type sûreté de fonctionnement).

La détection des défaillances des objets connectés eux-mêmes représente un enjeu majeur. Certains ne sont pas utilisés en continu, et donc leur défaillance ne sera potentiellement détectée que lors de leur utilisation.

4.2. Modes dégradés

Traditionnellement, sur les systèmes ferroviaires, le mode dégradé est le retour à un état sûr. L'utilisation de très nombreux composants risque de conduire à un taux de défaillance important. Dans ce cadre, l'utilisation uniquement du mode dégradé « *Fail Safe* » peut conduire à une grande indisponibilité du système. La perte de liaison avec un capteur conduira par exemple à une déclaration d'une défaillance sur un essieu et potentiellement à un arrêt des circulations. Les modes dégradés à définir sont à repenser à la fois au niveau composant, mais aussi au niveau système. Et ce, tout en conservant un niveau de sécurité adapté.

À contrario, les objets connectés pourront permettre l'identification de défaillances qui ne l'étaient pas auparavant et améliorer ainsi le niveau de sécurité. Dans ce cas, quel mode dégradé sera à adopter ?

La conception doit envisager les pires cas de fonctionnement du système sans nécessairement lier ces états à une défaillance d'un composant. La mise en œuvre de limitations ou barrière peut être nécessaire afin de minimiser l'effet d'une défaillance. Ces limitations peuvent être locales (proche du composant) et/ou globales (au niveau système).

4.3. Système de système

La complexité des systèmes à base d'objets connectés crée un risque multiplié de pannes difficilement gérables. La défaillance d'un objet connecté peut impacter plusieurs fonctions. En effet, un capteur peut être utilisé dans plusieurs systèmes et/ou intégré successivement dans plusieurs fonctions. La complexité donne de l'imprévisibilité au système. Les systèmes deviennent tellement complexes qu'ils sont difficilement intelligibles, la capacité des agents à les comprendre est réduite. La modélisation de ces systèmes devient de plus en plus prégnante. Sachant que certains systèmes plus simples sont déjà difficilement modélisables.

Risques généraux

Des risques généraux ne sont pas toujours présents dans les analyses technologiques et sortent du périmètre traditionnellement couvert par l'EPSF. Les thématiques suivantes ont néanmoins été identifiées comme plus susceptibles d'affecter les objets connectés : la souveraineté, les risques climatiques, la consommation d'énergie.

5. Facteurs humains et organisationnels et gestion de la sécurité

5.1. Perte d'information

L'adoption des objets connectés implique que les opérateurs seront moins présents sur le terrain. Cependant, lors des interventions sur site, les agents peuvent observer des éléments que les capteurs ne détectent pas (tels que des signes de fuites, des odeurs, etc.). Ainsi, les opérateurs possèdent une vision globale de l'environnement. Un agent peut aisément identifier un incendie, tandis que pour des capteurs, il s'agit d'une déformation, d'une augmentation de température, d'un court-circuit, etc.

5.2. Gestion de crise

Les systèmes s'appuyant sur des objets connectés peuvent agir soit automatiquement, soit permettre à un opérateur d'enclencher une action, en se basant sur des informations brutes ou déjà traitées fournies par l'interface. L'opérateur interagit avec le système lorsqu'une situation particulière apparait, détecte une situation anormale, évalue la situation en utilisant les informations disponibles et en identifiant ou anticipant l'état du système. Il élabore ensuite une solution en fonction des contraintes et des risques encourus.

Les agents de maintenance ou d'exploitation peuvent être submergés par des informations ou alarmes trop nombreuses voire contradictoires. Si le système est disponible et fiable, les pannes avec un impact fort sur l'exploitation deviendront de plus en plus rares. L'exploitant devra réagir très rapidement face à

des défaillances qu'il rencontre très rarement. La possibilité de reprise en main du système par les opérateurs sera à déterminer face à de telles situations, ainsi que la formation nécessaire afin qu'ils soient en mesure d'y faire face le jour venu.

5.3. Compétences

Les objets connectés constituent une technologie naissante. De fait, il existe une pénurie de professionnels qualifiés dans ce domaine. Un fossé peut ainsi se creuser entre la technologie déployée et la capacité des employés à l'exploiter. Ce défi est d'autant plus complexe que plusieurs domaines de compétences sont requis, notamment en métrologie, en télécommunications et dans le numérique. La maintenance de ces systèmes sophistiqués pourrait représenter un défi majeur. Par ailleurs, il est essentiel d'intégrer la nécessité d'une formation continue, compte tenu de l'évolution constante de ces technologies.

5.4. Organisation/Responsabilités

L'implémentation des objets connectés pourrait entraîner un risque de désengagement des intervenants, qui pourraient se sentir moins impliqués dans des tâches comme la maintenance. En cas de défaillance, la maintenance devra intervenir, ce qui représente une rupture avec les méthodes de maintenance conventionnelles du secteur ferroviaire, qui reposent principalement sur des opérations de maintenance régulières.

5.5. Conséquences pour la gestion de la sécurité

L'intégration des objets connectés influence la gestion des systèmes de sécurité. Parmi les domaines impactés, on retrouve la gestion des compétences, la gestion des actifs, la gestion documentaire, ainsi que la surveillance.

6. Cybersécurité

La présente note n'a pas pour objectif de traiter de la cybersécurité dans le domaine du ferroviaire. Ce paragraphe rappelle néanmoins quelques notions qu'il peut être nécessaire d'avoir en tête à ce sujet.
Les aspects cybersécurité sont étroitement liés aux réflexions attenantes aux objets connectés. Sur la base du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 *relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications*, l'ENISA s'est vue attribuer un rôle central dans la mise en place d'un modèle de certification de cybersécurité.

Sur le sujet de la certification de cybersécurité, un autre acteur entrerait en compte en ce sens où il est prévu dans la réglementation un rôle important pour les autorités nationales de certification de cybersécurité. L'EPSF sera amené à collaborer et échanger avec cette autorité.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié en 2021 un guide « Recommandations relatives à la sécurité des (systèmes d') objets connectés (ANSSI-PA-087) ». Les

recommandations s'appliquent à tous objets connectés. Elles doivent être adaptées au niveau de sécurité à obtenir en fonction de l'application.

L'EPSF a publié un document élaboré en collaboration avec l'ANSSI, « Prise en compte des enjeux de cybersécurité au sein de la sécurité ferroviaire ». Ce document émet des recommandations de cybersécurité adaptées au domaine ferroviaire.

7. Recommandations

Compte-tenu des constats évoqués dans la présente note, à ce stade des réflexions, plusieurs recommandations peuvent être émises.

Recommandation pour l'EPSF

L'EPSF doit appréhender les risques inhérents à l'usage de ces technologies, de leur présentation au sein des dossiers de demandes d'autorisation, jusqu'à leur utilisation lorsqu'elle contribue à un processus de sécurité. Cette attention doit porter notamment sur le fait que ces composants peuvent être en évolution constante. La compréhension fine du fonctionnement des objets connectés pourra amener à la mise en place de formations spécifiques afin de faire évoluer les compétences des agents. L'impact en termes de système de gestion de la sécurité doit être analysé particulièrement en ce qui concerne les compétences nécessaires à l'exercice de ces tâches de sécurité.

***

Identification des défaillances critiques

Toutes les défaillances potentielles doivent être considérées, en particulier celles de l'objet connecté lui-même et celles de l'équipement surveillé. Un risque majeur est l'incapacité à détecter une défaillance considérée identifiable. L'entité devra s'assurer qu'elle a bien pris en compte ceci dans son organisation et dans ses modèles de risques.

***

Modes dégradés

Il est recommandé que les modes dégradés soient conçus en tenant compte du fait que toutes les défaillances ne seront pas nécessairement détectées. L'implémentation de restrictions ou de barrières pourrait s'avérer nécessaire pour garantir une gestion efficace de ces situations.

***

Implantation

Il convient de prêter attention au fait que des capteurs peuvent nécessiter un positionnement précis, qu'il peut être nécessaire de procéder à un étalonnage, et éventuellement à un réétalonnage, et que la précision des capteurs peut se détériorer dans le temps. L'accessibilité doit être analysée. Par ailleurs, l'impact de ces composants sur l'environnement ferroviaire doit être pris en compte (perturbations électromagnétiques, chute, etc.).

***

Responsabilités

Les rôles et responsabilités de chaque acteur doivent être clairement établis afin de garantir que toutes les actions nécessaires au maintien du niveau de sécurité des systèmes à base d'objets connectés soient bien exécutées.

***

Gestion de crise

Il convient de vérifier que l'organisation est apte à gérer les situations de crise potentielles, notamment en s'assurant que les informations remontées soient exploitables par les opérateurs et que ces derniers sont préparés et capables de gérer ces situations de manière efficace.

***

Compétences

L'organisation doit s'assurer que les opérateurs ont les compétences nécessaires à l'exploitation et à la maintenance des objets connectés qui comprennent plusieurs technologies de pointe.

***

Traitement des données

L'organisation doit s'assurer qu'elle est capable de gérer les informations fournies par les objets connectés. Cela concerne le fait que le volume de données reçues peut être potentiellement important, que les informations remontées peuvent être difficilement exploitables ou de s'assurer que ces informations puissent permettre d'accomplir la tâche requise.

***

Interopérabilité

La mise en œuvre d'objets connectés ne doit pas amener à des problématiques d'interopérabilité (par exemple dans le cas où des objets connectés sont présents dans des wagons qui sont assemblés pour former un train).

***

Consommation d'énergie

Il faut s'assurer que les objets connectés disposent de suffisamment d'énergie pour assurer leur fonction, ou que leur perte d'énergie ne compromette pas la sécurité.

***

Résilience face aux risques généraux

La mise en œuvre d'objets connectés doit être faite en analysant la résilience du système, c'est-à-dire son aptitude à résister aux chocs. Cette analyse doit comprendre les risques liés à une rupture d'approvisionnement, à une perte de souveraineté, à une défaillance d'un sous-traitant ou à l'obsolescence d'un composant. Des actions doivent être menées afin de réduire ce risque (constitution de stock, composants interchangeables, etc.).

***

Système de gestion de la sécurité

L'entité doit s'assurer que son système de gestion de la sécurité est adapté à la mise en œuvre d'objets connectés. Ceci concerne particulièrement la formation, des agents et de l'encadrement, la gestion de la configuration et du patrimoine de ces composants.

***

8. Remerciements

La rédaction de cette note s'est appuyée sur une analyse bibliographique conséquente. Par ailleurs, de nombreux entretiens ont été réalisés auprès de bureaux d'études, gestionnaire de l'infrastructure, *Start-up*, mainteneurs, fabricants d'objets connectés, etc. principalement du domaine ferroviaire.

L'EPSF tient à remercier l'ensemble de ces contributeurs.

Établissement public de sécurité ferroviaire

60, rue de la Vallée – CS 11758 – 80017 Amiens Cedex 1