

CYBERSÉCURITÉ

SYSTRA

Résilience des infrastructures de transport Pas de confiance sans cybersécurité



PROTÉGEZ VOS SERVICES ESSENTIELS



Les systèmes de transport sont complexes, fortement interconnectés et l'impact d'une cyber-attaque est potentiellement majeur aux niveaux humain, opérationnel, financier.

Concernant la sécurité des infrastructures existantes, il est de la responsabilité des opérateurs de transport et gestionnaires d'infrastructure de mettre en œuvre un processus d'amélioration continue de la sécurité. Il est nécessaire d'identifier les actifs existants, d'analyser les événements redoutés (indisponibilité, perte de contrôle, perte d'intégrité ou de confidentialité), puis de mettre en place les mesures organisationnelles et techniques pour réduire les risques. Les principaux défis à relever sont :

- La répartition géographique étendue des actifs le long de la ligne ferroviaire ;
- Un mélange croissant de systèmes anciens (souvent obsolètes et/ou isolés), et de nouvelles technologies connectées (ex : composants sur étagère, utilisant des protocoles standardisés, plates-formes open source, ICS accessibles à distance et IoT) ;
- Gestion complexe de la mise à niveau et de la protection de composants obsolètes dans des systèmes opérationnels sous garantie ;
- Éligibilité aux exigences de cybersécurité et de sûreté de fonctionnement.

Concernant la sécurité des projets de nouvelles infrastructures, l'enjeu est la prise en compte des exigences de cybersécurité dès la conception des systèmes et des architectures, de s'assurer de l'application de règles de sécurité par les fournisseurs, et finalement de donner une vision claire sur le niveau de conformité aux exigences et les risques résiduels.

La cybersécurité devient essentielle pour proposer des systèmes de transport à la fois plus connectés et plus résilients. De nombreuses infrastructures de transport sont aujourd'hui considérées comme critique par les certaines autorités, et soumises à des réglementations de sécurité telle que la Directive NIS en Europe ou des lois comme la LPM en France.

NIVEAU DE SÉCURITÉ CIBLE

La norme IEC 62443

« Sécurité des automatismes et des systèmes de contrôle industriels » définit quatre niveaux de sécurité :

SL1



Protection contre les menaces opportunistes

> *le minimum*

SL2



Protection contre les pirates et les cybercriminels

> *pour une meilleure disponibilité, détection et résilience*

SL3



Protection contre les activistes et organisations terroristes

> *pour une gestion centralisée de la sécurité*

SL4



Protection contre les organisations gouvernementales

> *pour une sécurité avancée*

Les gestionnaires et opérateurs d'infrastructures ferroviaires sont vulnérables aux cybermenaces : les mesures de gouvernance et de protection sont partiellement mises en œuvre tandis que les mesures de détection et d'intervention sont encore rarement implémentées.

La majorité des cyberattaques connues sur les systèmes ferroviaires sont de nature opportuniste, mais les moyens de journalisation et de détection ne sont pas suffisants pour élucider la question.

Quoiqu'il en soit, les gestionnaires et opérateurs d'infrastructures ferroviaires restent vulnérables à des menaces avancées (APT) qui cibleraient spécifiquement les technologies opérationnelles (OT).

RECOMMANDATIONS

- 1 > Cartographier les actifs, identifier les cibles critiques et évaluer les conséquences
- 2 > Identifier les menaces, les vulnérabilités et évaluer la vraisemblance des scénarios d'attaque
- 3 > Mettre à jour et durcir la configuration des systèmes, implémenter des solutions de protection des hôtes et de résilience : sauvegarde, gestion de stocks, etc.
- 4 > Segmenter les réseaux et appliquer des mesures de protection périmétriques telles que des pare-feux, des passerelles ou des diodes réseau
- 5 > Renforcer et unifier le contrôle d'accès physique et logique suivant une approche basée sur les rôles et responsabilités (RBAC) et le principe de moindre privilège
- 6 > Configurer la journalisation, implémenter des moyens de détection d'intrusion au niveau du réseau et des hôtes, et implémenter un système de collecte et stockage des journaux
- 7 > Déployer des outils de corrélation d'évènements et de gestion des incidents, et centraliser la supervision des réseaux et des systèmes dans un centre opérationnel de sécurité (SOC)
- 8 > S'assurer de la bonne répartition des rôles et responsabilités, mettre en œuvre des actions de sensibilisation et de formation auprès des collaborateurs pour diffuser les bonnes pratiques et prévenir les menaces internes

Les recommandations ci-dessus sont inspirées des normes de sécurité ISO 27001, CEI 62443 et des bonnes pratiques partagées par des agences de cybersécurité telles que l'ANSSI (France), l'ENISA (Europe) ou le NIST (USA).

Les implémentations doivent prendre en compte les spécificités OT et les normes de sécurité telles que CEI 61508 et les Common Safety Methods (CSM) définies par l'ERA.

Les exigences OT par ordre de priorité décroissant sont : intégrité et disponibilité puis confidentialité.

ASSURER LA SÉCURITÉ ET LA CONTINUITÉ D'ACTIVITÉ



2

OPÉRATIONS



Signalisation



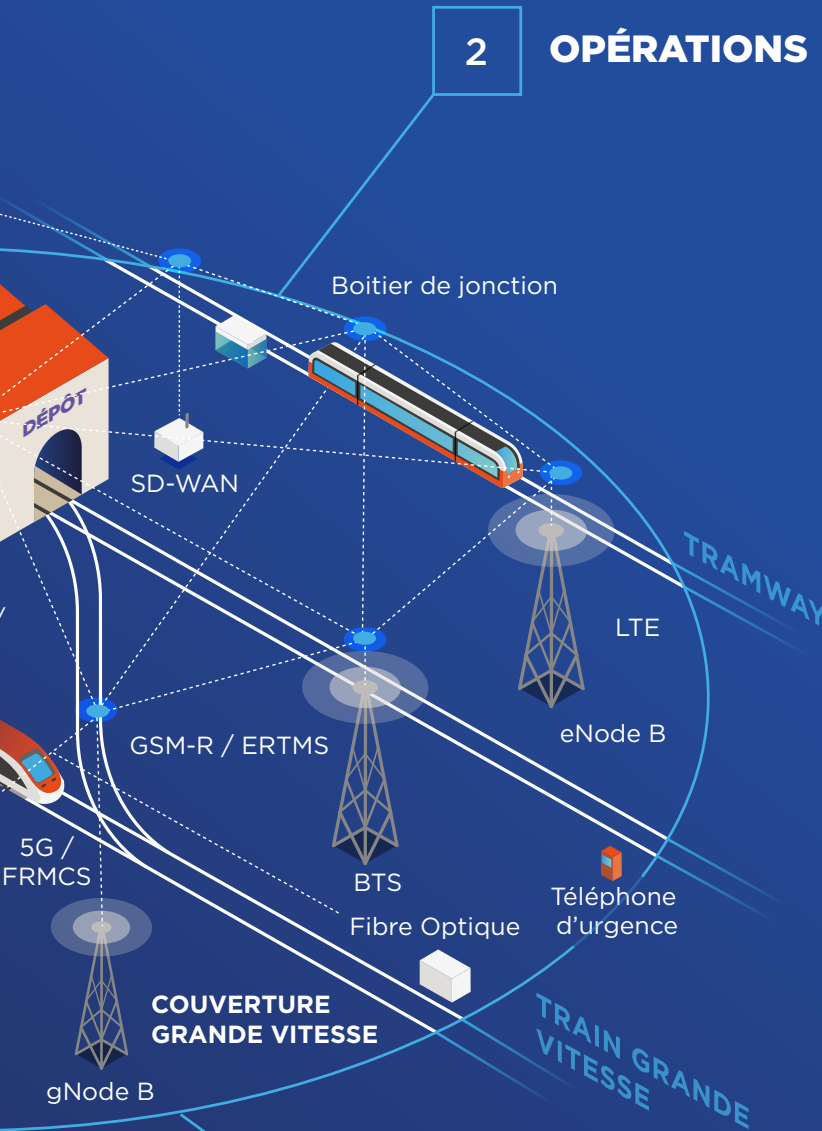
Contrôle-Commande



Télécom



Auxiliaire



3

SURETÉ, SÉCURITÉ & MAINTENANCE



Diagnostic



Détection incendie



Protection vidéo



Contrôle d'accès



Téléphonie d'urgence & Système d'alertes



Supervision réseau & Cybersécurité



Gestion d'actifs

NOS SERVICES POUR LES INFRASTRUCTURES EXISTANTES ET VOS PROJETS NEUFS

Nos équipes sont prêtes à accompagner vos projets

- Améliorer la continuité des activités
- Assurer la sécurité des passagers
- Protéger les données sensibles
- Gérer la conformité aux réglementations et aux standards

STRATÉGIE

Évaluation de maturité, conseil en stratégie,
puis support à la mise en œuvre
et au suivi de la feuille de route

ÉVALUATION & PROGRAMMATION

TRANSFORMATION

SENSIBILISATION & FORMATION

PROJETS

Accompagnement à l'intégration
de la cybersécurité dans le cycle de vie projet
et la chaîne d'approvisionnement

EXIGENCES

GESTION DES RISQUES

CONFORMITÉ

AUDIT

Cartographie des systèmes,
analyse et recommandations pour
l'amélioration de la cybersécurité
au niveau organisationnel et technique

PRÉPARATION

INVESTIGATION

RECOMMANDATIONS

SOLUTIONS

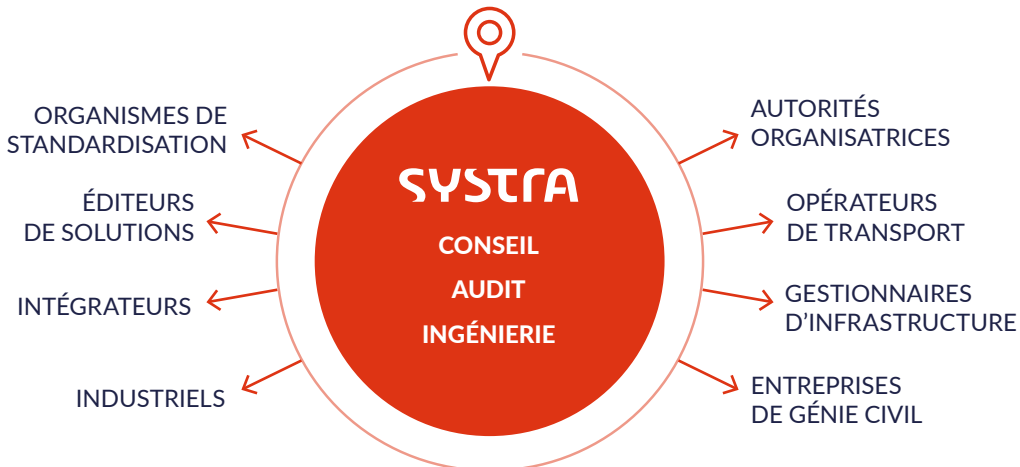
Veille technologique, études et conseil
sur le déploiement de solutions
de cybersécurité

VEILLE

ÉTUDES

DÉPLOIEMENT

NOTRE ÉCOSYSTÈME



ZOOM: GESTION AGILE DES RISQUES



La prise de décision nécessite d'avoir une vision claire des priorités s'appuyant sur un processus incrémental de gestion des risques.

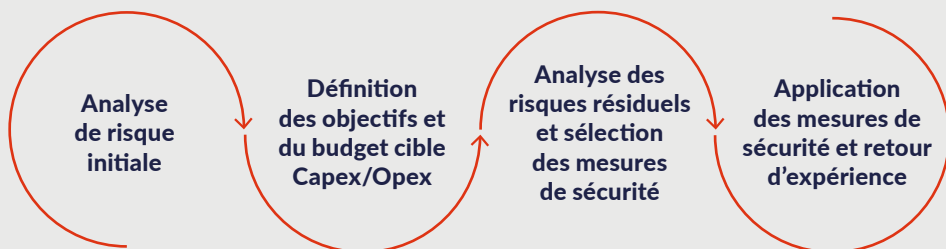
La méthodologie EBIOS Risk Management de l'ANSSI (conforme avec l'ISO 27005) promeut une approche dynamique et centrée sur les menaces, se focalisant sur l'analyse des scénarios stratégiques et opérationnels.

L'évaluation des niveaux de risque doit prendre en compte les conséquences (humaines, opérationnelles, financières, réputationnelles et légales) et la vraisemblance des scénarios menaces.

La vraisemblance peut être évaluée par l'analyse des cyberattaques passées et des nouvelles menaces.

De nouveaux exploits de sécurité sont rendus publics chaque mois révélant de nouvelles vulnérabilités sur les systèmes et les infrastructures de transport. Ils sont parfois industrialisés pour simplifier leur utilisation.

Alors que les évolutions technologiques s'accroissent (Ex: 5G, FRMCS, Cloud, IoT, etc.) avec des impacts importants sur la surface d'attaque, les mesures de sécurité doivent être adaptées le plus rapidement possible.



NOS RÉFÉRENCES



CARTOGRAPHIE ET MESURES DE SÉCURITÉ MINIMALES POUR LE SECTEUR FERROVIAIRE

CLIENT: ENISA (Agence européenne de cybersécurité), Europe

Dans le cadre du contrat cadre « Soutenir la cybersécurité pour les activités du secteur des transports - Lot 2 - cybersécurité pour le secteur ferroviaire », SYSTRA a réalisé une étude, un questionnaire et des entretiens pour aider l'ENISA à évaluer l'implémentation de la Directive NIS dans le secteur du transport ferroviaire. SYSTRA a soutenu l'ENISA dans les tâches suivantes :

- Analyse des normes et réglementations existantes (Ex: ISO 27001/2, CEI 62443, projet TS 50701, DIN VDE 831-104, NIST CSF, NIST 800-82, APTA, directives ANSSI ICS, Directive NIS, LPM)
- Revue des mesures de sécurité prédéfinies applicables aux systèmes ferroviaires
- Questionnaire auprès des gestionnaires et opérateurs d'infrastructures ferroviaires
- Rédaction d'un rapport de synthèse et d'un communiqué de presse



CHIFFREMENT DE LA SIGNALISATION POUR UNE LIGNE FERROVIAIRE EN AMÉRIQUE DU NORD

CLIENT: Opérateur ferroviaire, USA

SYSTRA conçoit et met en œuvre une PKI pour les communications radio PTC. SYSTRA effectue les tâches suivantes :

- Analyse des besoins et des contraintes du client
- Évaluation des menaces et des vulnérabilités, puis analyse de risques
- Rédaction des spécifications, puis développements logiciels
- Analyse du code source
- Plan de management des clefs et mise en place de la PKI pour les équipements bord et sol
- Implémentation d'un OTP pour la gestion des feux de signalisation
- Acquisition des actifs de bord et mise en œuvre dans la nouvelle gamme de produits de rames
- Tests en laboratoire, sur le terrain et démonstration dans le cadre du processus de certification
- Formation du personnel et services de conseil pour la mise à jour des procédures opérationnelles



SYSTÈME DE CONTRÔLE AUTOMATISÉ DES TRAINS

CLIENT: Autorité de Transport, Australie

SYSTRA a vérifié le design de l'infrastructure de télécommunication avec les exigences du système de signalisation (GSM-R, signalisation). Cela a consisté à analyser l'architecture actuelle et à identifier les améliorations afin d'augmenter les performances et la sécurité. SYSTRA a réalisé les tâches suivantes :

- Analyse de l'infrastructure actuelle et classification du réseau selon la norme EN 50159
- Analyse de risque de sécurité
- Directives de cybersécurité pour le réseau de télécommunication



SERVICES DE CONSEIL EN CYBERSÉCURITÉ POUR UN OPÉRATEUR DE MÉTRO

CLIENT: Opérateur de métro, Asie

SYSTRA agit en tant que consultant en gestion de projet sur les systèmes de métro (4 lignes, 37 stations). SYSTRA effectue les tâches suivantes :

- Analyse des réglementations locales
- Analyse des risques (selon ISO 27005)
- Revue du design et analyse des interfaces système
- Politique de sécurité (selon ISO 27001/2)
- Implémentation de la politique de sécurité et support de la gouvernance
- Définition de conformité et des procédures de test
- Définition de la stratégie de pentests et suivi d'exécution
- Études sur la mise en place d'un Centre d'opérations de sécurité



SERVICES DE CONSEIL EN CYBERSÉCURITÉ POUR UNE INFRASTRUCTURE TRAMWAY

CLIENT: Industriel, tramway, Asie

SYSTRA fournit des services de conseil et exécute les tâches suivantes :

- Revue du design
- Inventaire des actifs et analyse des interfaces des systèmes
- Audit de l'architecture des systèmes
- Analyse des réglementations locales
- Politique de sécurité et règles locales
- Analyse des risques initiale et détaillée (selon ISO 27005)
- Conseil sur le déploiement de la gouvernance
- Mise en œuvre de mesures techniques en coopération avec les autorités



NOTRE VALEUR AJOUTÉE

- Connaissance des systèmes de transport y compris télécom, contrôle-commande, signalisation, systèmes auxiliaires et services aux passagers
- Expertise en matière de cybersécurité pour l'OT
- Vision intégrée de la sécurité et la sûreté de fonctionnement
- Participation à des groupes de standardisation et de partage sur la sécurité ferroviaire dont CENELEC WG26 et ER-ISAC

www.systra.com
systems@systra.com

SYSTRA

SYSTRA Australie
Level 15 - Chifley Tower
2 Chifley Square
Sydney NSW 2000
AUSTRALIE

SYSTRA France
72-76, rue Henry Farman
75015 Paris
FRANCE
Tél. : +33 (0)1 40 16 61 00

SYSTRA Singapour
333 North Bridge Road
#05-01 KH KEA
Singapour 188721
SINGAPOUR

SYSTRA EAU
Al Masraf Tower
Dubai
ÉMIRATS ARABES UNIS

SYSTRA LTD Royaume-Uni
3rd Floor, 5 Old Bailey,
Londres, Angleterre, EC4M 7BA
ROYAUME-UNI

SYSTRA États-Unis
New York siège social
520 Eighth Avenue, Suite 2100
New York, NY 10018
ÉTATS-UNIS



LA CONFIANCE TRANSPORTE LE MONDE