DOCUMENT D'INFORMATION DE CYBERSÉCURITÉ DES STI

2026

Transport Canada Transports Canada

Canada

Ce document souligne l'importance d'investir dans la cybersécurité des infrastructures routières et offre des recommandations de haut niveau à cet égard.

Aussi disponible en anglais sous le titre : « ITS Cyber Security Briefing Document »

TP 15631F

Cat. T89-26/2025F-PDF

ISBN 978-0-660-76113-8

1 Résumé exécutif

Pour intégrer en toute sécurité les technologies émergentes telles que véhicules connectés et automatisés (VCA) à leurs systèmes de transport, les propriétaires et exploitants d'infrastructures doivent adopter des modèles de cyberrésilience toujours plus proactifs.

Investissements stratégiques requis

- Infrastructure et technologie : Concevoir et mettre en œuvre une infrastructure sécurisée dès sa conception et déployer des solutions de surveillance émergentes, telles que des systèmes centralisés ou basés sur l'IA.
- Capital humain : Recruter et former du personnel spécialisé capable de gérer une infrastructure numérique moderne et interconnectée.
- Gouvernance : Élaborer des processus, des procédures et des politiques intégrées et formalisées qui assurent la cohérence entre les technologies de l'information (TI) et les technologies opérationnelles (TO).

Plan d'action recommandé

Étape	Action	Objectif
1	Effectuer une autoévaluation	Utilisez l'outil d'auto-évaluation de la cybersécurité des STI de Transports Canada pour déterminer votre niveau de sécurité actuel et définir un objectif.
2	Cartographier l'environnement	Identifiez les vulnérabilités en comprenant la sensibilité et l'exposition des données sur votre réseau.
3	Adopter des normes	Modélisez vos politiques de gestion des risques selon les normes sectorielles et les cadres de conformité établis.
4	Tester les plans d'intervention	Créez, communiquez et testez régulièrement des plans d'intervention officiels en cas d'incident afin de minimiser l'impact d'une violation de données.
5	Surveillance continue	Intégrez la gestion des risques à vos opérations courantes pour anticiper les vulnérabilités « zero-day » et l'évolution des menaces.

Prochaines étapes

Pour obtenir des directives techniques détaillées sur la mise en œuvre de ces recommandations, veuillez consulter le site web Établir un programme de cybersécurité intégrée : Guide pour les propriétaires/exploitants d'infrastructures routières canadiennes et les professionnels des STI.

2 Introduction

Les technologies émergentes, telles que les systèmes de transport intelligents (STI) et les véhicules connectés et automatisés (VCA), transforment les systèmes de gestion du trafic (SGT) traditionnels. Ces innovations ont des capacités et des caractéristiques qui peuvent :

- réduire les impacts environnementaux des transports;
- améliorer la sécurité et l'efficacité
- améliorer l'expérience du voyageur grâce à plus de commodité, de confort et de satisfaction

Cependant, ces nouvelles innovations peuvent également introduire de nouveaux défis en matière de sécurité et de protection de la vie privée. Bien que les VCA soient encore en développement, le système de transport est composé de plus que simplement des véhicules. Il existe également de nombreux dispositifs et systèmes sous-jacents qui aident le TMS à fonctionner, des panneaux d'affichage intelligents aux feux de circulation en passant par les capteurs et les caméras.

Nous recommandons la lecture de ce document en parallèle afin de souligner l'importance d'investir dans des programmes de cybersécurité des infrastructures routières auprès des dirigeants et décideurs des sociétés canadiennes d'exploitation d'infrastructures routières et de transport. Ce document est complété par Établir un programme de cybersécurité intégrée : Guide pour les propriétaires/exploitants d'infrastructures routières canadiennes et les professionnels des STI, qui fournit des conseils détaillés supplémentaires sur la mise en place d'un tel programme.

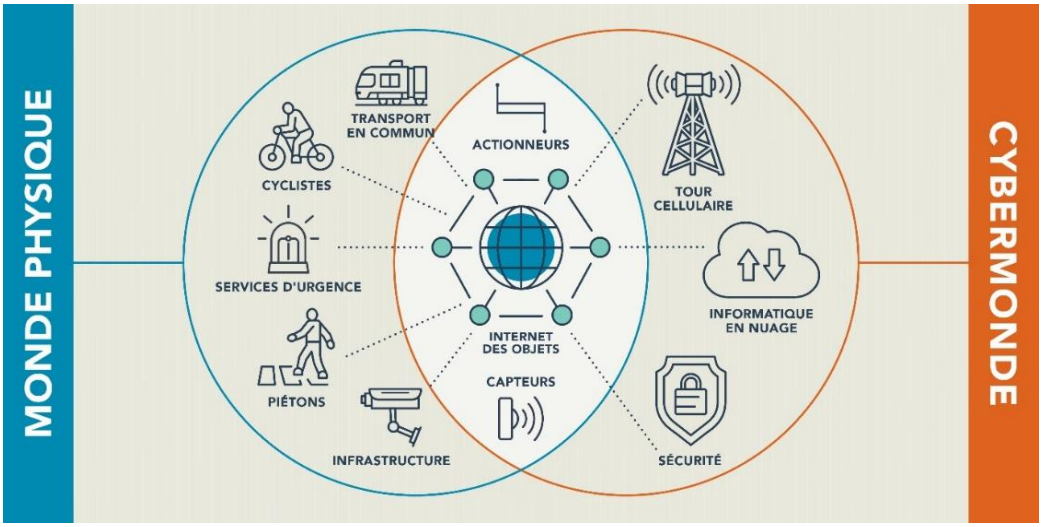
3 L'état actuel des systèmes de transport intelligents (STI) et des systèmes de gestion du trafic (SGT)

Les systèmes de gestion du trafic d'aujourd'hui sont constitués de systèmes de plus en plus interconnectés qui utilisent la technologie pour améliorer la circulation et la sécurité. Un effet secondaire de ces systèmes est un environnement de plus en plus connecté, ce qui expose les utilisateurs à des vulnérabilités potentielles en matière de cybersécurité. Vous trouverez ci-dessous trois facteurs qui introduisent une complexité dans la gestion et la sécurisation de l'infrastructure numérique et physique que vous devez prendre en compte lors de l'intégration d'un environnement de technologies opérationnelles traditionnellement séparé à un environnement informatique.

- **Convergence :** L'union des infrastructures de technologie de l'information (TI) et de technologie opérationnelle (TO) brouille le fossé entre le monde physique et le monde numérique, comme l'illustre la figure 1 ci-dessous. Dans ce contexte, les infrastructures et les composants des deux mondes sont connectés à l'Internet des objets. Une attaque localisée peut ainsi rapidement affecter l'ensemble du système, rendant difficile pour votre organisation la compréhension et la protection de l'environnement global.
- **Interopérabilité :** La combinaison d'anciens et de nouveaux systèmes et plateformes peut complexifier leur gestion et leur protection. La figure 2 illustre comment les systèmes existants et les nouveaux systèmes sont souvent incompatibles et peuvent nécessiter des mesures de protection distinctes.
- **Intégration et connectivité :** Dans le monde actuel, les différentes composantes des infrastructures critiques sont fortement interconnectées, comme l'illustre la figure 3. Par exemple, la gestion intelligente de l'eau et les transports intelligents font partie d'un écosystème de ville intelligente interconnecté par l'Internet des objets. Ces interconnexions présentent de nombreux avantages, mais les rendent également plus vulnérables aux cyberattaques.

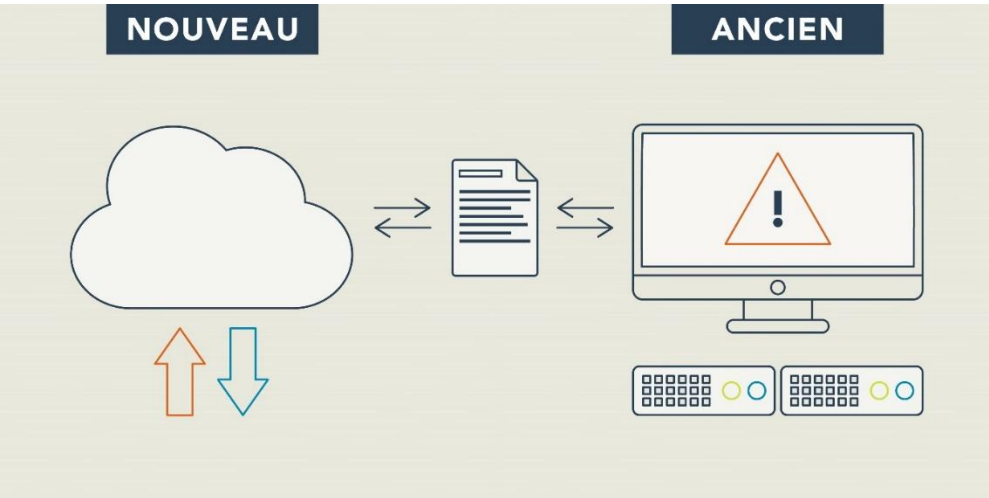
Convergence

FIGURE 1: FACTEURS CLÉS À CONSIDÉRER LORS DE L'INTÉGRATION D'UN ENVIRONNEMENT TECHNOLOGIQUE OPÉRATIONNEL SÉPARÉ À UN ENVIRONNEMENT DE TI



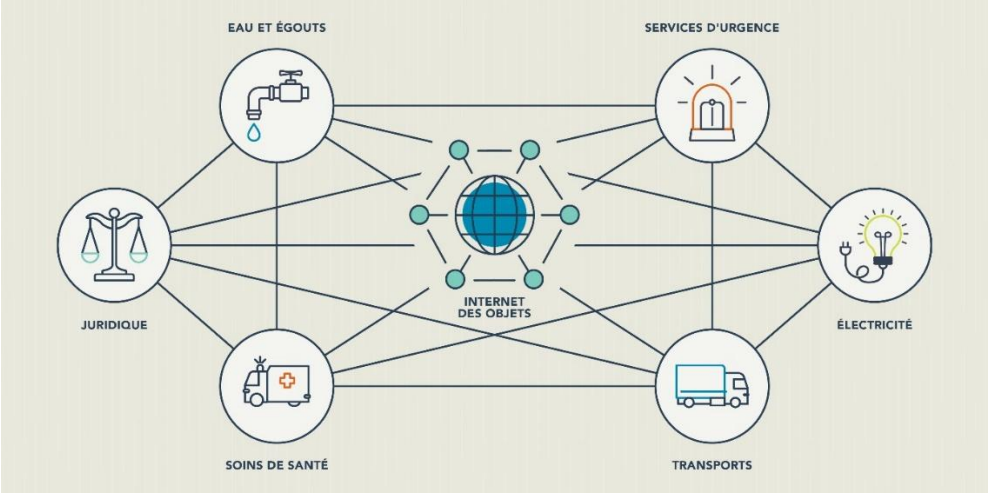
Interopérabilité

FIGURE 2: INTEROPÉRABILITÉ ENTRE LES NOUVEAUX SYSTÈMES MODERNES ET LES SYSTÈMES EXISTANTS



Intégration

FIGURE 3: INTÉGRATION ET CONNECTIVITÉ DES DIFFÉRENTES INFRASTRUCTURES ESSENTIELLES



Parallèlement à l'augmentation de la connectivité et de la complexité, la prolifération des appareils connectés offre aux attaquants d'innombrables points d'entrée pour compromettre les systèmes de transport ou tirer parti des vulnérabilités, ce qui augmente encore les risques.

4 Impacts des cyberattaques sur les STI

Les cyberattaques contre les systèmes de transport intelligents (STI) peuvent avoir un impact sur les propriétaires et les exploitants d'infrastructures. Les conséquences peuvent inclure le vol de données, la perturbation du réseau et l'exécution de logiciels malveillants. Voici les principaux domaines touchés par une cyberattaque réussie.

4.1 Sécurité

L'infrastructure impliquée dans la circulation et le transport est développée avec des mesures de sécurité pour protéger les usagers, les navetteurs et les travailleurs. Cependant, ces systèmes de sécurité peuvent devenir la cibles de cyberattaques, car ils peuvent être un outil puissant pour extorquer une organisation. Par exemple, en 2024, une cyberattaque à Hamilton, en Ontario, a paralysé le système de feux de circulation télécommandés de la ville. Si les systèmes de sécurité et leurs dispositifs de sécurité sont compromis, les navetteurs et les conducteurs pourraient être gravement blessés.

4.2 Opérations

Une attaque bien exécutée peut perturber l'infrastructure de transport de base. En tant que partie des infrastructures essentielles, le transport est interconnecté avec d'autres services publics, ce qui signifie qu'une attaque à grande échelle pourrait déclencher des effets d'entraînement. Par exemple, une attaque contre un système de contrôle de voie pourrait entraîner une augmentation de la congestion, un risque accru d'accidents de la route et des perturbations des principales voies de transport, ce qui aurait un impact sur la chaîne d'approvisionnement.

4.3 Réputation

Une atteinte ou une perturbation importante pourrait nuire à la perception du public à l'égard des STI et des organisations concernées (autorités routières, fournisseurs de technologie, etc.). Dans les situations où il y a atteinte à la protection des données personnelles (comme les noms, les adresses ou les données sur les numéros d'immatriculation), il y a des répercussions sur la vie privée du public qui pourraient nuire à la réputation de l'organisation visée.

4.4 Finances

Les cyberattaques ont des conséquences financières pour l'organisation touchée. Cela peut prendre de nombreuses formes, comme les coûts de rançon (dans le cas d'une attaque par rançongiciel), les frais juridiques, la diminution des revenus liés aux dommages à la réputation et les coûts

opérationnels et d'investissement pour atténuer l'attaque et réparer ou remplacer l'équipement endommagé.

5 Appel à l'action : Investir dans les programmes de cybersécurité

Face à la transformation rapide du secteur des transports pour s'adapter aux nouvelles technologies, vous devez investir dans la préparation et la réponse aux cybermenaces. Vous devez vous attendre à investir des ressources dans :

- la conception et la mise en œuvre de nouvelles infrastructures;
- élaborer de nouveaux processus et procédures
- embaucher et former du personnel pour gérer de nouvelles infrastructures;
- déployer des technologies émergentes liées à la cybersécurité (surveillance basée sur l'IA, solutions de surveillance centralisée, solutions automatisées de gestion de la conformité, etc.).

Vous devriez utiliser une approche flexible et évolutive pour naviguer dans ces changements. Pour gérer les coûts et maximiser les avantages de ce travail, vous devriez comprendre le profil de risque de votre organisation afin de pouvoir définir l'état de cybersécurité cible qui gère adéquatement ce risque. Pour aider votre organisation à y parvenir, le programme de promotion de la connectivité et de l'automatisation du système de transports (PCAST) de Transports Canada a élaboré un outil d'autoévaluation de la cybersécurité des STI pour vous aider à évaluer les risques et à vous y préparer.

Voici quelques aspects que vous devriez considérer pour développer la maturité numérique de votre organisation.

5.1 Comprendre l'environnement

Une bonne compréhension de votre environnement opérationnel et des risques qui y sont associés, y compris la sensibilité et l'exposition des données qui traversent le réseau, est essentielle pour bien planifier et mettre en œuvre de nouvelles technologies tout en gérant les risques.

Cette compréhension vous aidera à identifier les vulnérabilités et les risques qui peuvent survenir lorsque vous commencerez à intégrer de nouvelles technologies. Pour ce faire, votre organisation doit se tenir informée des dernières normes, cadres et directives disponibles.

5.2 Comprenez votre posture actuelle en matière de cybersécurité

Il est crucial de comprendre votre posture actuelle en matière de cybersécurité pour identifier les vulnérabilités, évaluer les lacunes et prioriser les améliorations afin d'atteindre votre posture cible en matière de cybersécurité.

L'outil d'autoévaluation de la cybersécurité des STI de Transports Canada vous aidera à évaluer votre posture actuelle en matière de cybersécurité. De plus, l'outil vous permettra de fixer un état cible et fournira des recommandations pour l'atteindre. Le profil cible est personnalisable, ce qui vous permet de mettre en œuvre des contrôles de sécurité qui reflètent votre évaluation unique des risques.

5.3 Utiliser des politiques et des pratiques exemplaires

Votre organisation devrait élaborer une approche intégrée et des politiques appropriées pour gérer la cybersécurité dans les actifs de TI et de TO. Utilisez les normes de l'industrie et les cadres de conformité pour évaluer et modéliser la politique de gestion des risques de votre organisation en ce qui concerne les actifs de SGT, les actifs de TI, les processus, les procédures et les fournisseurs.

Que votre organisation gère les TI ou les SGT, vous pouvez utiliser un cadre pour mettre en place les bonnes personnes, les bons processus, la bonne technologie et les bonnes pratiques de gouvernance afin de gérer les cyberrisques et d'améliorer la maturité en matière de cybersécurité.

5.4 Élaborer et mettre à l'essai des plans et des procédures d'intervention en cas d'incident

Toute organisation peut être victime d'une cyberattaque. La façon dont une organisation peut identifier, évaluer, réagir et se remettre d'un cyberévénement déterminera l'impact sur son organisation.

Vous devriez élaborer des plans officiels d'intervention en cas d'incident qui sont communiqués aux principaux intervenants, testés pour en assurer l'efficacité et mis à jour sur une base continue.

5.5 Continuer d'évaluer les cyberrisques

La gestion des cyberrisques est un processus continu qui doit être intégré à la fonction de gestion des risques de votre organisation. Avec des technologies et des risques en constante évolution, les organisations devraient rester à l'écoute des vulnérabilités du jour zéro (vulnérabilités que les fournisseurs ne connaissent pas) et des risques émergents, afin de pouvoir réagir en conséquence.

6 Conclusion

L'intégration des STI transforme fondamentalement l'infrastructure routière du Canada. Bien que ces technologies offrent des avantages importants en matière de sécurité et d'efficacité, elles introduisent aussi des vulnérabilités critiques en cybersécurité. Les impacts potentiels d'une attaque sont graves, menaçant la sécurité publique, les opérations critiques et la stabilité financière. Il est donc crucial que les propriétaires et exploitants d'infrastructures adoptent une approche proactive et continue la gestion des risques cybernétiques, en utilisant les outils et directives disponibles pour renforcer la résilience. Ce faisant, ils peuvent sécuriser leurs systèmes et s'assurer que les Canadiens bénéficient pleinement et en toute sécurité d'un réseau de transport moderne et connecté.

En plus de ce document, Transports Canada a élaboré Établir un programme de cybersécurité intégrée : Guide pour les propriétaires/exploitants d'infrastructures routières canadiennes et les professionnels des STI, qui propose des étapes précises à l'intention des propriétaires et des exploitants d'infrastructures routières pour établir ou améliorer un programme de cybersécurité et renforcer leur posture en la matière. Pour de plus amples renseignements et des ressources, veuillez consulter notre site Web sur la cybersécurité des infrastructures routières. Pour toute question, commentaire ou préoccupation, vous pouvez communiquer avec nous à l'adresse courriel suivante : tc.its-sti.tc@tc.gc.ca.