CENTRE D'INNOVATION CENTRE

SGDDI nº 18422356

# PCAST – Cybersecurité des STI des administrations routières - Mars 2022

## PROGRAMME DE PROMOTION DE LA CONNECTIVITÉ ET DE L'AUTOMATISATION DU SYSTÈME DE TRANSPORT (PCAST) INITIATIVES DE CYBERSÉCURITÉ

Chris Nowak, agent, Recherche et Développement, Transports Canada


Transport Canada Transports Canada

Canada

# ORDRE DU JOUR

- Pourquoi la cybersécurité des infrastructures est-elle importante?
- Convergence de la cybersécurité des infrastructures routières
- Facteurs à considérer en matière de cybersécurité
- Projet de cybersécurité des infrastructures
- Infrastructure cybersecurity project
  - Aperçu
  - État
- Système de gestion des certificats de sécurité (SGCS)

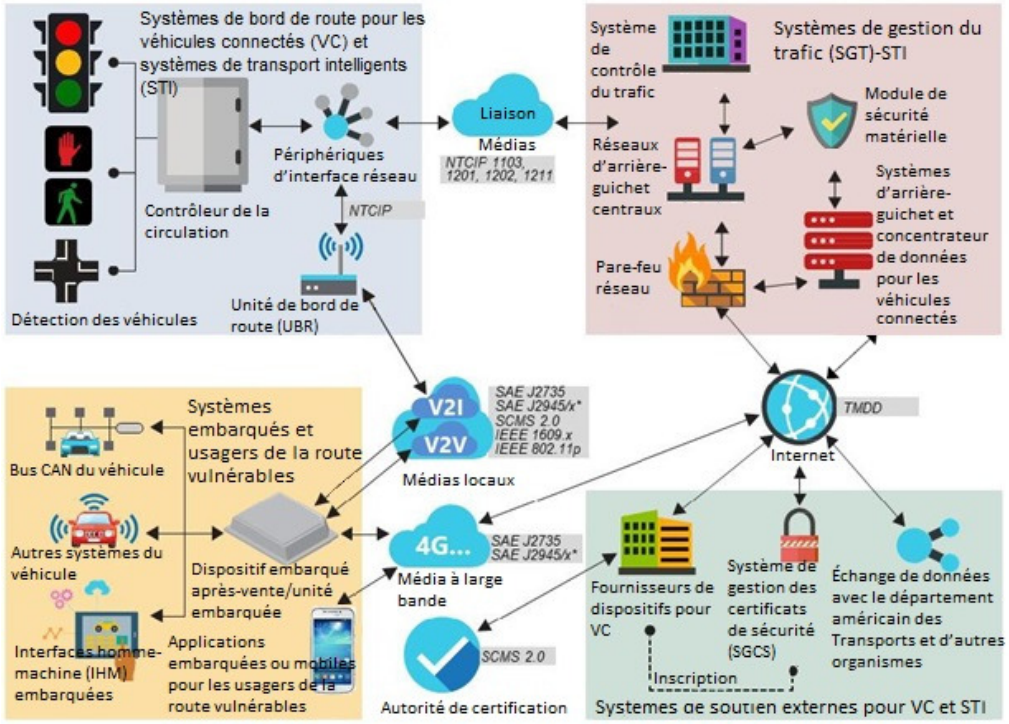
# CONTEXTE – POURQUOI LA CYBERSÉCURITÉ DES INFRASTRUCTURES EST-ELLE IMPORTANTE?

Le paysage des systèmes de gestion du trafic (SGT) dans le cadre de l'intégration accrue des infrastructures de transport routier, des véhicules et des communications est connu sous le nom de systèmes de transport intelligents (STI).

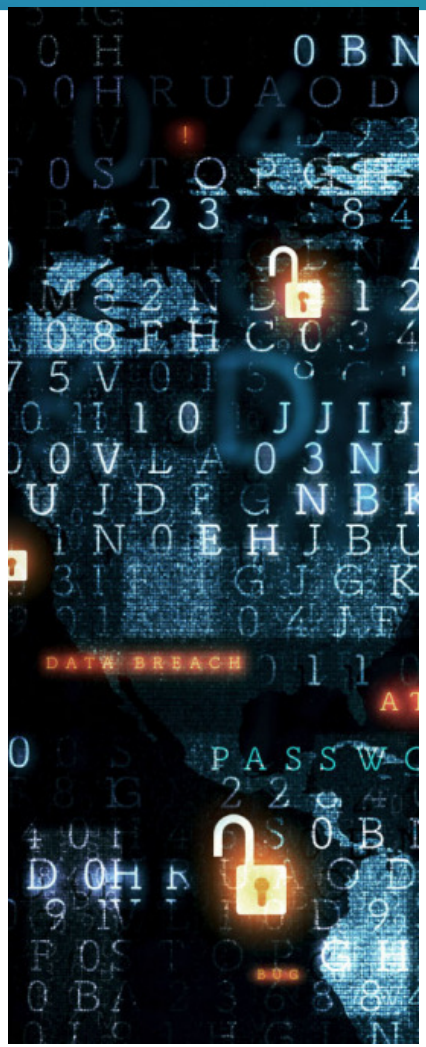
Les SGT traditionnels sont composés de plusieurs composants, notamment :

- **Contrôleurs de signalisation** - coordination des feux de circulation
- **Capteurs de circulation** - surveillance des volumes de trafic
- **Surveillance des systèmes de surveillance par télévision en circuit fermé (CCTV)** - systèmes de surveillance du trafic
- **Signalisation numérique** - affichage des avertissements et des messages aux usagers de la route

Bien que l'intégration ait engendré de nouvelles possibilités d'optimisation et de rendement, elle a également créé de nouvelles occasions pour les acteurs de menaces de se connecter au SGT et de l'exploiter.



# CONVERGENCE DE LA CYBERSÉCURITÉ DES INFRASTRUCTURES ROUTIÈRES




- La cybersécurité des infrastructures de transport est un système essentiel émergent qui nécessite une gestion active des risques.
- La convergence des technologies de l'information (TI, par exemple les technologies de STI) et de la technologie opérationnelle (TO - par exemple, les feux de signalisation, les panneaux de signalisation) crée de nouveaux vecteurs d'attaque pour le SGT.
- Le SGT jouera un rôle important en permettant des niveaux plus élevés d'automatisation des véhicules grâce à la connectivité entre l'infrastructure et le véhicule en fournissant des avertissements de sécurité, des données cartographiques et des informations sur la synchronisation des feux de circulation, etc.
- L'écosystème des véhicules connectés et automatisés (VCA) ne peut être aussi sécurisé que le composant le plus vulnérable.
- Soutenir les autorités des infrastructures routières pour améliorer la cyberrésilience afin de *cerner* les menaces, s'y *protéger*, les *détecter*, y *réagir* et de se *rétablir* de celles-ci.

# FACTEURS À CONSIDÉRER EN MATIÈRE DE CYBERSÉCURITÉ

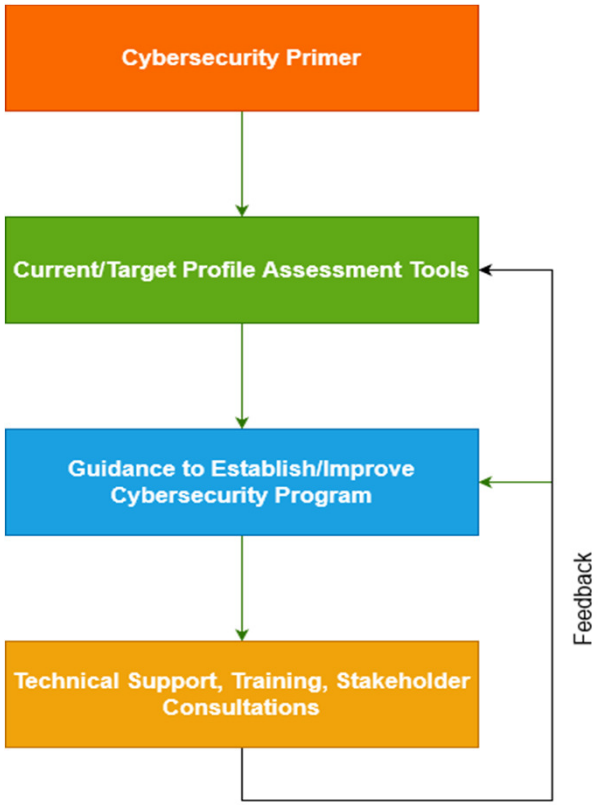
- Renforcer le milieu et les capacités de la cybersécurité
  - Forte demande et faible offre d'experts en cybersécurité, en particulier dans le secteur des transports
  - Collaborer avec l'industrie, le milieu universitaire et le gouvernement

- Améliorer l'état de la cybersécurité de l'écosystème des STI grâce au :
  - Renforcement des capacités en matière de cybersécurité et sensibilisation
  - Soutien de la conception d'outils, de cadres et de directives en matière de cybersécurité

# PROJET DE CYBERSECURITÉ DES INFRASTRUCTURES - DELOITTE

**Améliorer la préparation à la cybersécurité des propriétaires ou des exploitants des infrastructures routières du Canada en vue d'une meilleure connectivité et automatisation.**

1. Concevoir un **abécédaire de la cybersécurité** de l'infrastructure routière et des **documents d'information** à l'intention du personnel et des gestionnaires assumant divers rôles (Opérations, Finances, RH, Politique, etc.).
2. Élaborer des **outils d'auto-évaluation de la cybersécurité** pour les autorités chargées des infrastructures routières afin d'évaluer leur état de préparation actuel et leur état de préparation à l'égard des cibles en matière de cybersécurité.
3. Élaborer des **directives sur l'utilisation des outils** et la création/l'amélioration d'un programme de cybersécurité adapté aux opérations du SGT et à l'infrastructure connexe.
4. Assurer une **formation et un soutien technique pratique** pour les autorités chargées des infrastructures routières dans la réalisation d'évaluations de la cybersécurité et l'élaboration de programmes de cybersécurité.
5. Fournir une **analyse de la cybersécurité et des conseils stratégiques** au besoin concernant les problèmes de cybersécurité émergents dans les infrastructures de transport.
6. Effectuer une **analyse de la vulnérabilité des infrastructures** du secteur des transports au besoin pour éclairer la gestion des risques émergents en matière de cybersécurité.



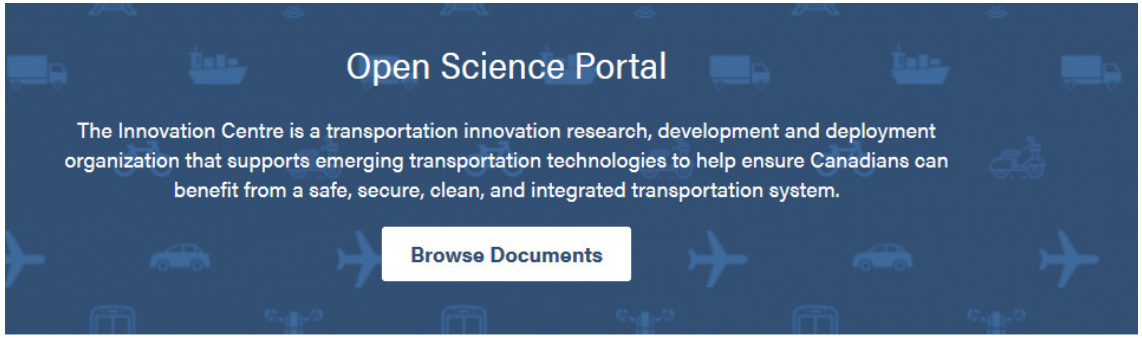
CENTRE D'INNOVATION CENTRE

# PROJET DE CYBERSECURITÉ - ÉTAT

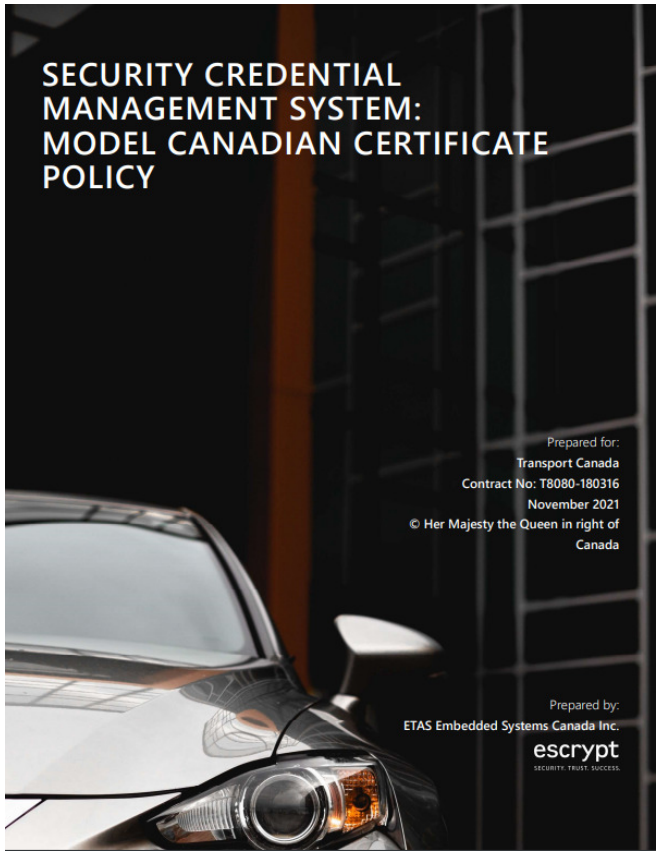
- Contrat débuté en septembre 2021
- Durée du projet - 18 mois
- Travaux du Comité directeur et du Comité consultatif en cours
- Conception d'un abécédaire de la cybersécurité, de documents d'information sur la cybersécurité et d'outils d'auto-évaluation en cours
- Futures séances de formation et webinaires - possibilité de fournir de la rétroaction et des commentaires

# SYSTÈME DE GESTION DES CERTIFICATS DE SÉCURITÉ (SGCS)

Système de gestion des certificats de sécurité (SGCS) – Modèle de politique de certification (PC) du Canada - (30 novembre 2021) : https://tcdocs.ingeniumcanada.org/




Security Credential Management System (SCMS) - Model Canadia...
Cybersecurity | Nov 30, 2021




- Rapport : lien vers la PC du SGCS/ (en anglais seul.)

CENTRE D'INNOVATION CENTRE

# SYSTÈME DE GESTION DES CERTIFICATS DE SÉCURITÉ (SGCS)

| Document | Objectif |
|---|---|
| Analyse des exigences<br>Lien du rapport | Examen de la documentation technique, de la législation canadienne sur la protection des renseignements personnels, évaluation des besoins/considérations des intervenants canadiens |
| Analyse des options<br>Lien du rapport | Déterminer les options pour exploiter et gouverner un SGCS coordonné au niveau national, recueillir les commentaires des intervenants |
| Élaboration du modèle d'exploitation et de gouvernance recommandé<br>Lien du rapport | Concevoir le modèle d'exploitation technique recommandé (y compris l'architecture de haut niveau) pour les opérations pilotes et de production du SGCS au Canada, élaborer un modèle de gouvernance |
| Modèle de politique de certification<br>Lien du rapport | Conformément au modèle d'exploitation, élaborer des procédures et des politiques d'exploitation détaillées pour assurer l'uniformité et l'interopérabilité entre les fournisseurs du SGCS |
| Analyse des mauvaises utilisations du spectre<br>Lien du rapport | Recherche sur l'utilisation de l'architecture du SGCS pour détecter et signaler les cas d'utilisation abusive du spectre |

# Merci!

Pour de plus amples renseignements, veuillez communiquer avec :

**Chris Nowak, ing.**
Agent, Recherche et Développement
Centre d'innovation – PCAST
Transports Canada

Tél. : (343)571-4961
chris.nowak@tc.gc.ca