Les enjeux de la cybersécurité dans le domaine ferroviaire

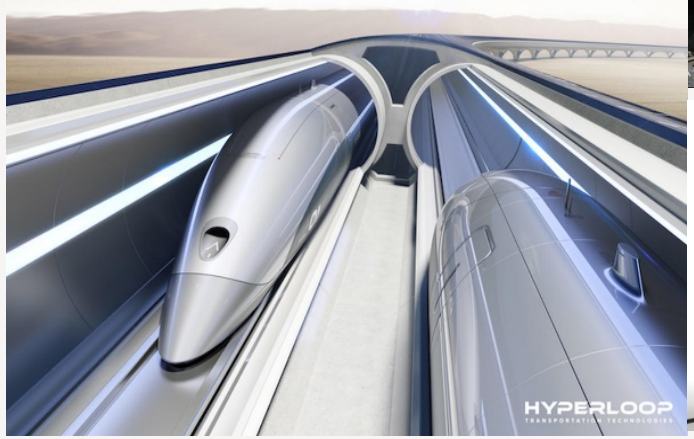
Tchilabalo Dong HAINGA, C|EH, GCIH, CCNA, CCNP, CCDP

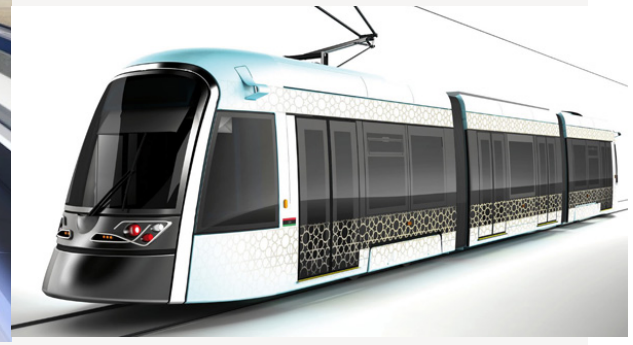
Agenda

- Systèmes de contrôle industriels
- Évolution numérique
- Cyber-retard
- Pourquoi voudrait-on attaquer les systèmes de contrôle industriels?
- Quoi faire?
- Notre équipe
- Questions

Systèmes de contrôle industriels (SCI)

- L`ensemble trains, voies, leur systèmes de surveillance, opération et maintenance font partie des SCI.
- Rôles des SCI: automatisation des processus industriels et machines.
- Historiquement les SCI étaient isolés:
  - Commandes à boucle unique
  - Appareil autonome
  - Pas d'Ethernet (pas de réseaux)
  - Pas de communication





Évolution numérique

- Intégration numérique avec évolutions
  - Ethernet partout
  - Le sans fil
  - Possibilité de configurer à distance
  - Système exploitation Windows et Linux
  - Logiciels propriétaires commerciaux sont adoptés
- Objectif: productivité, efficacité, sûreté
- Sécurité négligée

Évolution numérique avec cyber-retard

- Du point de vue cybersécurité, ces systèmes présentent un énorme défi.
- Ils sont exploitables. Les SCI ont subis plusieurs attaques ces dernières années.
- Le risque est réelle: Les cyberattaques se sont fortement intensifiées

SNC·LAVALIN ATKINS Member of the SNC-Lavalin Group

Example de cyber-attaques: Tramway Polonais

- Date: Jan 2008
- Cible: Tramway Polonais
- Outil: Télécommande de télévision modifiée
- Impact: déraillé quatre véhicules de train. Douze personnes ont été blessées dans l'un des incidents.
- Description: Il a étudié les tramways et les voies pendant longtemps, puis a construit un dispositif qui ressemblait à une télécommande de télévision et l'a utilisé pour manœuvrer les tramways et les voies.

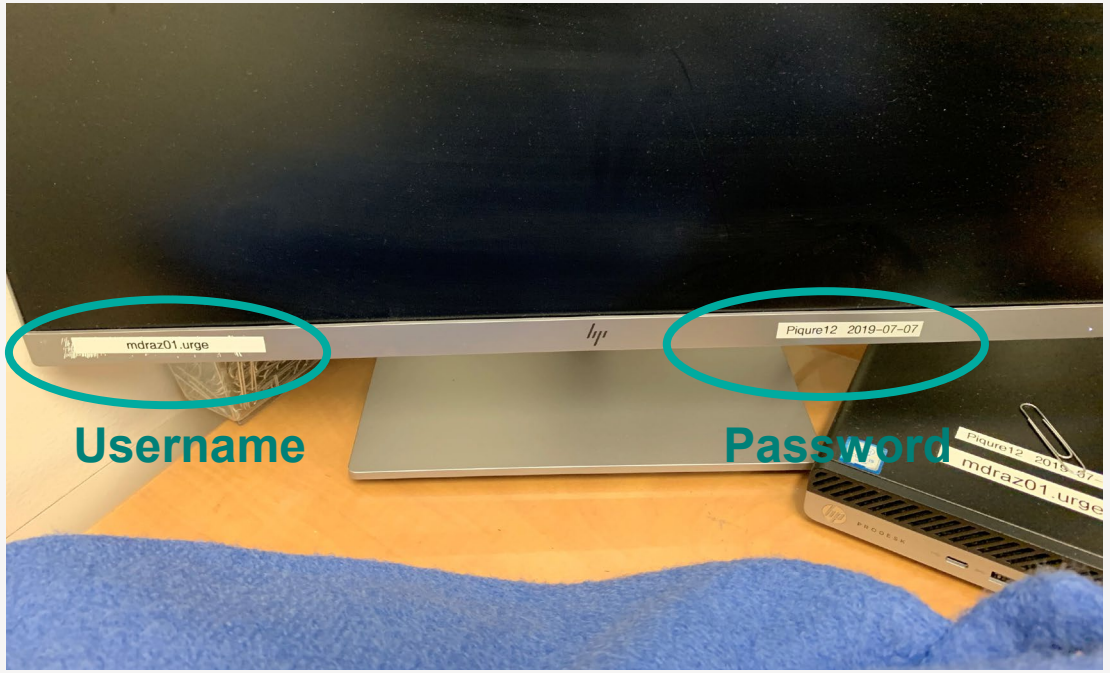
Example de cyber-attaques: Stuxnet

- Découvert en juin 2010
- Cible: Les installations nucléaires de l'Iran
- Source d'introduction: Clé USB (Réseau fermé)
- Impact: destruction de nombreuses centrifugeuses
- Description: Le logiciel malveillant spécifiquement conçu pour prendre le contrôle des machines industrielles et les faire fonctionner en dehors de leur performance normale causant des dommages dans le processus. Ce logiciel s'est propagé à travers une machine (Microsoft Windows) et a ciblé le logiciel s7 de Siemens utilisé pour contrôler et surveiller les automates. Le logiciel malveillant atteint l'automate, met à jour son code et modifie les commandes et les contrôles échangés par l'automate.

Example de cyber-attaques: Séance vidéo

Pourquoi voudrait-on attaquer les systèmes de contrôle industriels?

- Erreur humaine
- L’espionnage d’entreprise ou industriel
- Espionnage et cyberguerre entre États
- Gain financier (ou ruiner)
- Activités terroristes
- Le hacktivisme
- Piratage éthique mal guidé
- Pour la reconnaissance éducative



Quoi faire?

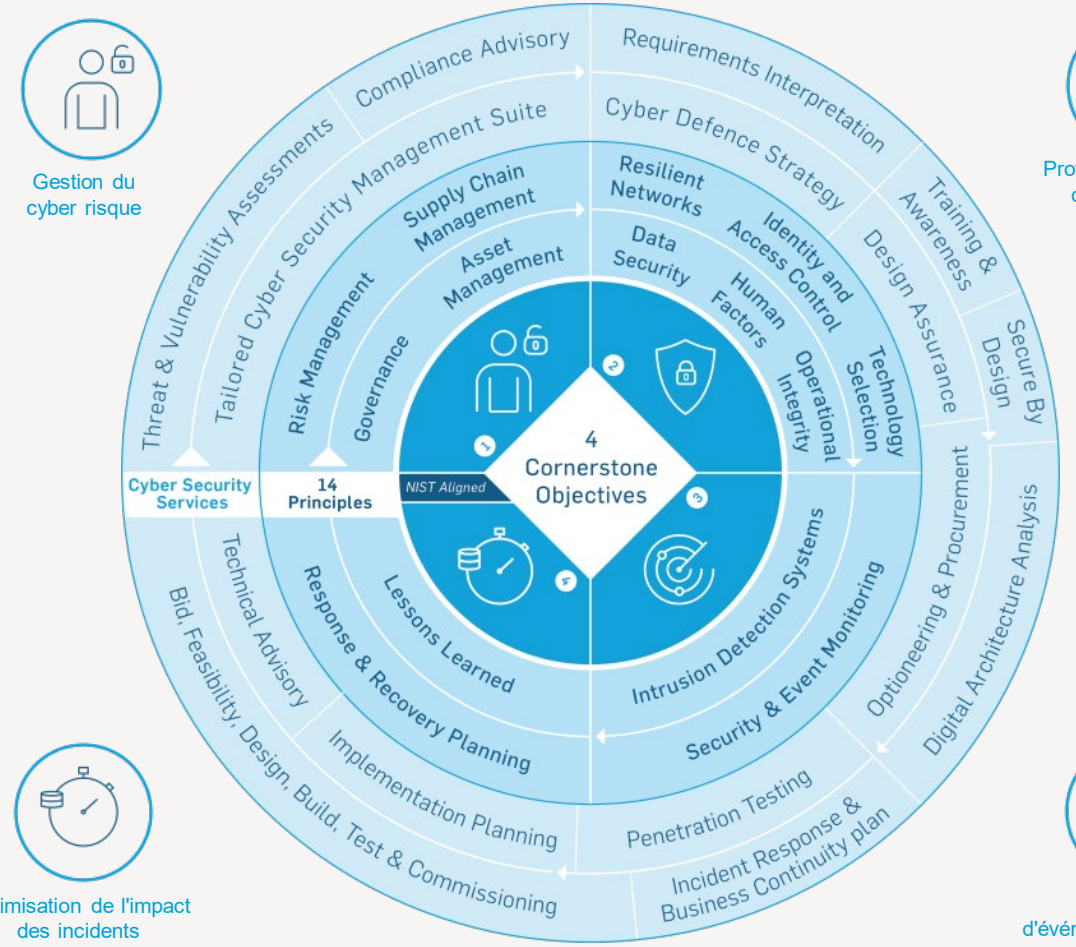
- C'est l'ensemble des mesures de protection techniques et non techniques, qui permettent à un système de résister à des événements susceptibles de compromettre:
  - la disponibilité,
  - l'intégrité
  - la confidentialité
  - ou les preuves associées (identité, authenticité, traçabilité), des données stockées, traitées ou transmises.

SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

La cybersécurité des systèmes de contrôle Industriel (ferroviaire)

- La cybersécurité doit être appréhender comme une démarche globale. Elle ne dépend pas seulement de mesures techniques mais aussi de mesures organisationnelles : sensibilisation, formation, procédures.
- Dans le contexte ferroviaire, l'approche de la cybersécurité doit être guider par les démarches suivantes:
  - La sécurité à la source
  - La défense en profondeur
  - La cyber résilience



SNC·LAVALIN ATKINS Member of the SNC-Lavalin Group

Équipe de cyber sécurité transports collectifs et ferroviaires

Chris Johnson, ***N+***

Lead - Cyber Security

Martine Chlela, ***BSc MSc PhD***

Cyber Security Consultant

Gurinder Kaur, ***Eng***

Cyber Security Engineer

Pat Chartrand, ***CISSP***

Cyber Security Specialist

Tchilabalo Dong Hainga,

CCNP, CCDP, CEH, GCIH

Cyber Security Analyst

Justin Nguyen, **Jr. Eng**

CCNA, CCSA, CCSE. NSE4/7

Cyber Security Analyst

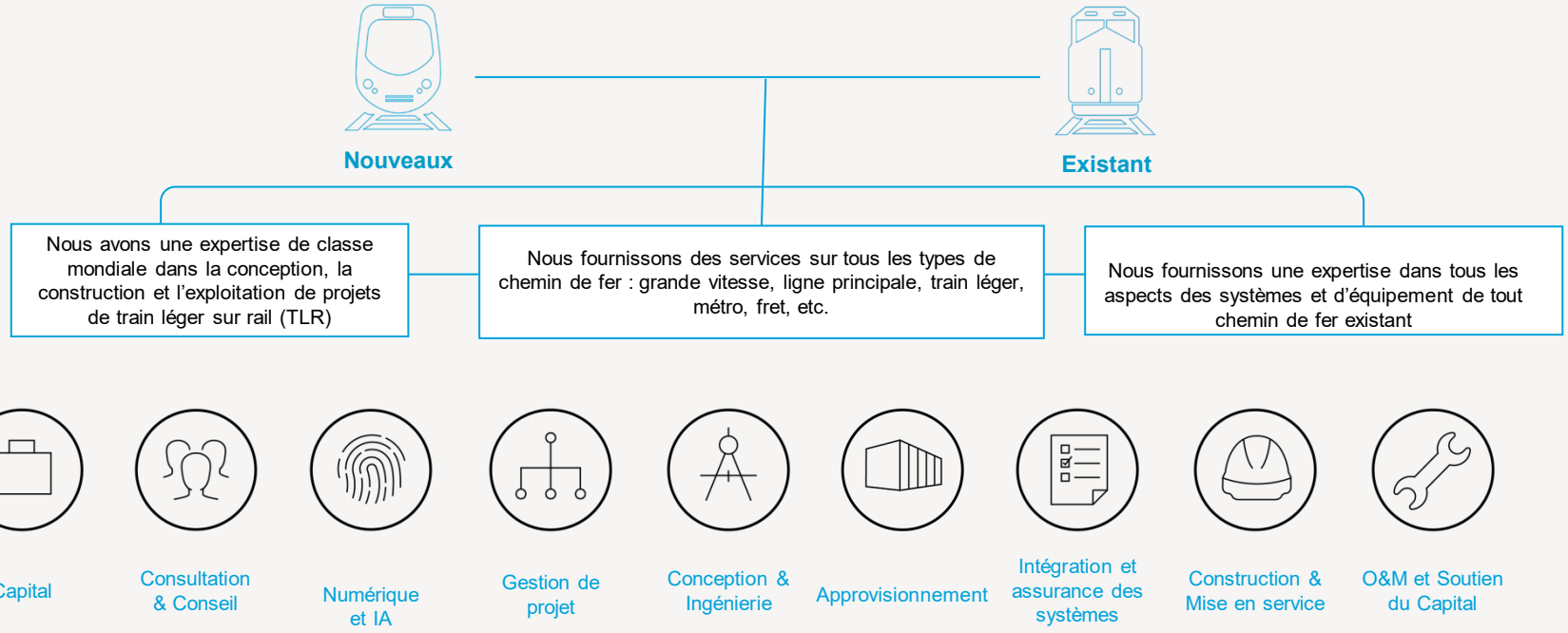
SNC·LAVALIN

ATKINS

Member of the SNC-Lavalin Group

Capacités ferroviaires et transits de bout en bout

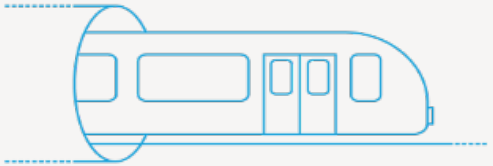
Nous fournissons des services tout au long du cycle de vie des projets ferroviaires, existants ou nouveaux.



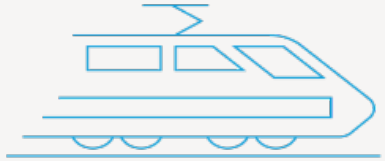
SNC·LAVALIN ATKINS Member of the SNC-Lavalin Group

Nous supportons tous les types de systèmes ferroviaires

Train léger



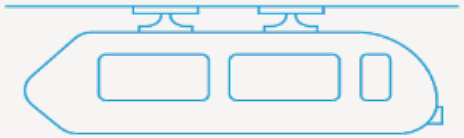
Métro



Mainline

Grande Vitesse

Fret



Autres modes

SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Nos Projets

SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Projets – Réseau Express Métropolitain (REM)

- Interprétation et gestion des exigences en matière de cyber sécurité.
- Analyse de l'architecture de conception du réseau et déploiement d'équipements afin de prendre en compte les considérations de sécurité, de performance et de redondance.
- Optioneering d'appareils de sécurité, de technologies et de solutions à déployer pour une résilience améliorée.
- Production du plan de gestion de la cyber sécurité décrivant tous les jalons en aval, les activités et les parties responsables, par exemple:
  - Évaluations des menaces et vulnérabilités
  - Conseil technique en approvisionnement
  - Aide à la construction et à la mise en œuvre
  - Base de configuration sécurisée

SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Projets – NouvLR Data Confidentiality Directive

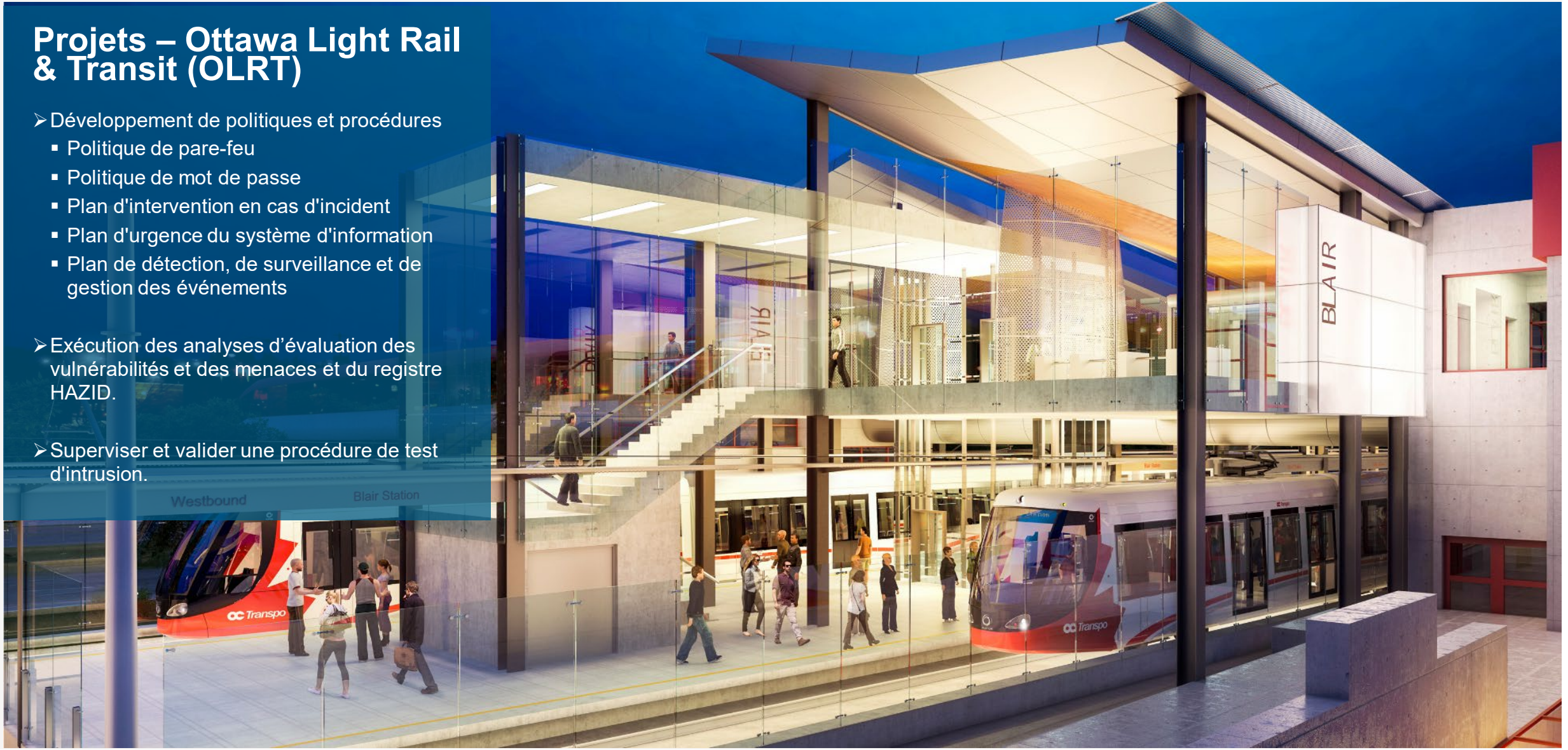
- Fourniture d'une directive sur la sécurité des données et la confidentialité pour la gouvernance du projet, comprenant:
  - Gestion des interfaces du projet
  - Outils et méthodes utilisés pour accéder, transférer et échanger les données sensibles d'un projet
  - Responsabilités et tâches définies pour atteindre la clôture
  - Matériels de formation et de briefing produits et distribués aux responsables du projet

SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Projets – Ottawa Light Rail & Transit (OLRT)

- Développement de politiques et procédures
  - Politique de pare-feu
  - Politique de mot de passe
  - Plan d'intervention en cas d'incident
  - Plan d'urgence du système d'information
  - Plan de détection, de surveillance et de gestion des événements
- Exécution des analyses d'évaluation des vulnérabilités et des menaces et du registre HAZID.
- Superviser et valider une procédure de test d'intrusion.



SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Projets – Eglinton Crosstown Light Rail & Transit (ECLRT)

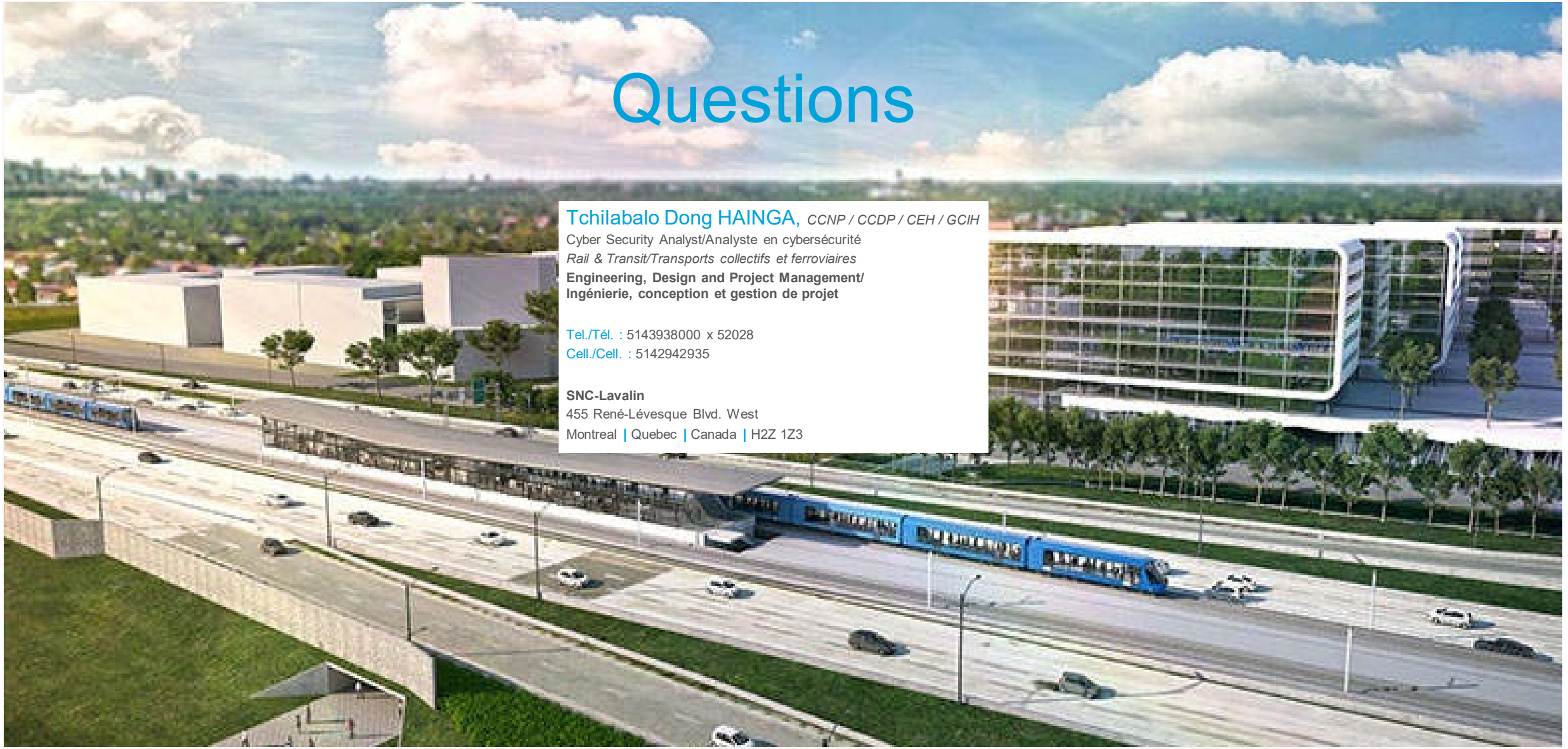
- Plan de gestion de la cyber sécurité
  - En conformité avec les meilleures pratiques du NIST, de l'APTA et du CPNI
  - Mise en place de processus étape par étape pour l'identification et la gestion des risques pour la durée de vie du rail

- Spécification du réseau de communication dorsale
  - Capture des dispositifs de sécurité et des caractéristiques d'architecture dans la spécification ECLRT BCN pour appel d'offres
  - Définition de la fonctionnalité et de l'emplacement du pare-feu
  - Solutions virtualisées à des fins de sauvegarde et de redondance

SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Questions



Tchilabalo Dong HAINGA, *CCNP / CCDP / CEH / GCIH*

Cyber Security Analyst/Analyste en cybersécurité

Rail & Transit/Transports collectifs et ferroviaires

Engineering, Design and Project Management/
Ingénierie, conception et gestion de projet

Tel./Tél. : 5143938000 x 52028

Cell./Cell. : 5142942935

SNC-Lavalin

455 René-Lévesque Blvd. West

Montreal | Quebec | Canada | H2Z 1Z3

SNC·LAVALIN

ATKINS

Member of the SNC-Lavalin Group