ITS CYBER SECURITY BRIEFING DOCUMENT

2026

Transport Canada Transports Canada

Canada

This document highlights the importance of investing in road infrastructure cyber security and offers high level recommendations to do so.

Aussi disponible en français sous le titre : « Document d'Information de cybersécurité des STI »

TP 15631E

Cat. T89-26/2025E-PDF

ISBN 978-0-660-76112-1

1 Executive summary

To safely integrate emerging technologies like connected and automated vehicles (CAVs) into their transportation systems, infrastructure owners and operators (IOOs) must transition to increasingly proactive cyber-resilient models.

Required strategic investments

- Infrastructure & Technology: Design and implement secure-by-design infrastructure and deploy emerging monitoring solutions, such as AI-enabled or centralized systems
- Human Capital: Recruit and train specialized staff capable of managing modern, interconnected digital infrastructure
- Governance: Develop formal processes, procedures, and integrated policies that bridge the gap between Information Technology (IT) and Operational Technology (OT)

Recommended action plan

Step	Action	Objective
1	Perform Self-Assessment	Use Transport Canada's ITS Cyber Security Self-assessment Tool to identify your current posture and define a target state.
2	Map the Environment	Identify vulnerabilities by understanding the data sensitivity and exposure across your specific network.
3	Adopt Standards	Model risk management policies after established industry standards and compliance frameworks.
4	Test Response Plans	Create, communicate, and regularly test formal incident response plans to minimize impact during a breach.
5	Continuous Monitoring	Embed risk management into ongoing operations to stay ahead of "zero-day" vulnerabilities and evolving threats.

Next steps

For detailed technical guidance on implementing these recommendations, you can refer to the web page Establishing an Enterprise Cyber Security Program: A Guide for Canadian Road Infrastructure Owners/Operators and ITS Professionals.

2 Introduction

Emerging technologies, such as intelligent transportation systems (ITS) and connected and automated vehicles (CAVs) are transforming traditional traffic management systems (TMS). These innovations have abilities and features that can:

- reduce the environmental impacts of transportation
- enhance safety and efficiency
- improve traveller experience through greater convenience, comfort and satisfaction

However, these new innovations can also introduce new security and privacy challenges. Although CAVs are still developing, the transportation system is made of more than just vehicles. There are also many underlying devices and systems that help TMS operate, from smart message boards and traffic lights to sensors and cameras.

We recommend that this document be read in parallel to highlight the importance of investing in road infrastructure cyber security programs to executives and decision-makers of Canadian road and transportation IOOs. This document is supplemented by Establishing an Enterprise Cyber Security Program: A Guide for Canadian Road Infrastructure Owners/Operators and ITS Professionals, which provides additional detailed guidance on setting up a cyber security program.

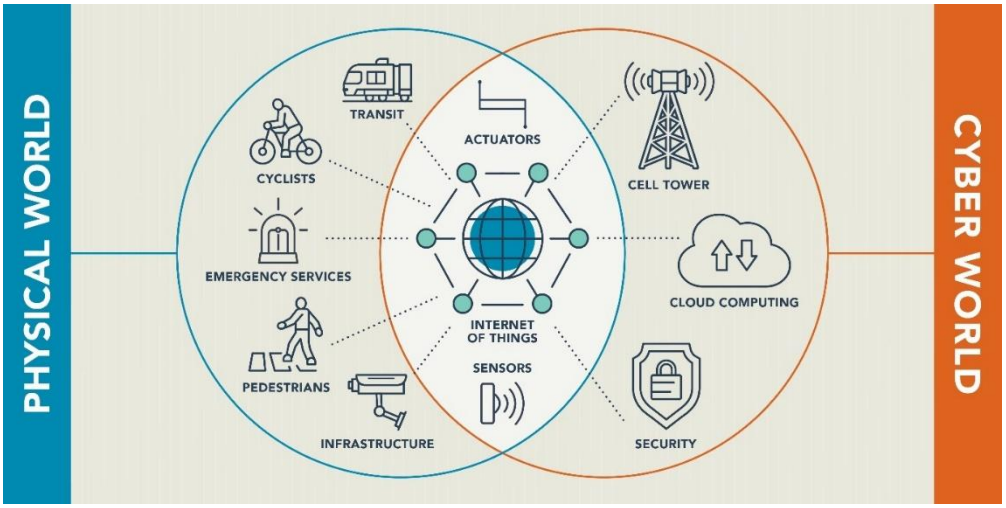
3 The current state of intelligent transportation systems (ITS) and traffic management systems (TMS)

A by-product of such a system is an increasingly connected environment that exposes potential cyber security vulnerabilities. Below are three factors that that introduce complexity in managing and securing digital and physical infrastructure which you should consider when integrating a traditionally segregated operational technology (OT) environment with an information technology (IT) environment.

- **Convergence:** The union of IT and OT infrastructures blurs the divide between the physical and cyber worlds, as illustrated in figure 1 below, where infrastructure and components in the physical and cyber worlds are all connected to the Internet of Things. This could cause an attack on one area to quickly affect the entire system, making it hard for your organization to understand and protect the whole environment
- **Interoperability:** Combining old and new systems and platforms can make it more complicated to manage and protect. Figure 2 illustrates how legacy systems and new systems are often non-interoperable and may require separate protection measures
- **Integration and connectivity:** In today's world, different components of critical infrastructure are highly interconnected with each other, as illustrated in Figure 3. For example, smart water management and smart transportation are both part of a smart city ecosystem that are interconnected through the Internet of Things. These interconnections bring many benefits but also makes them more vulnerable to cyber attacks

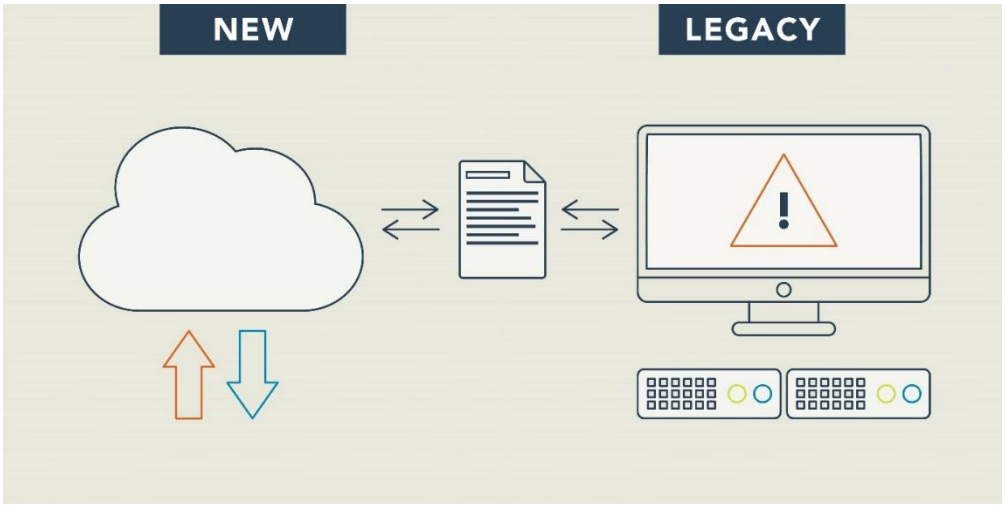
Convergence

FIGURE 1: KEY FACTORS TO CONSIDER WHEN INTEGRATING A SEGREGATED OPERATIONAL TECHNOLOGY ENVIRONMENT WITH AN IT ENVIRONMENT



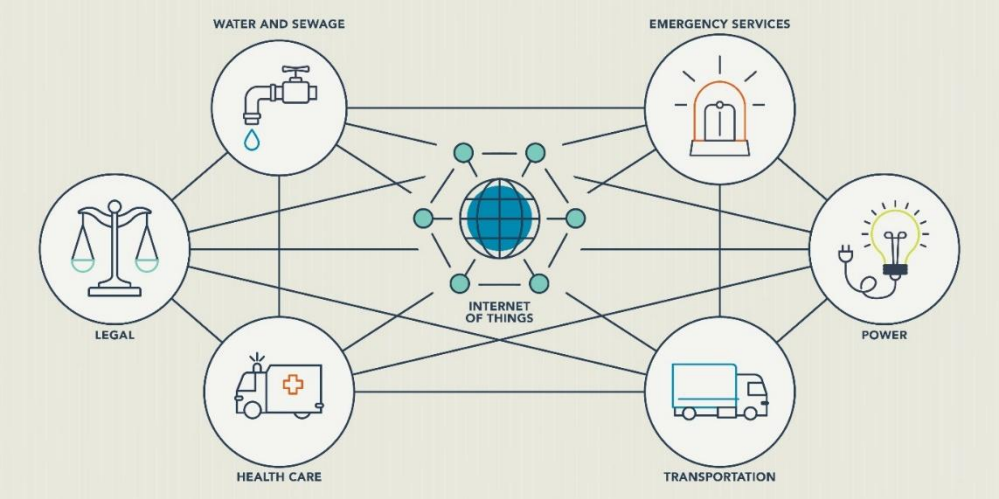
Interoperability

FIGURE 2: INTEROPERABILITY BETWEEN NEW MODERN SYSTEMS AND LEGACY SYSTEMS



Integration

FIGURE 3: INTEGRATION AND CONNECTIVITY OF DIFFERENT CRITICAL INFRASTRUCTURE



Alongside increased connectivity and complexity, the proliferation of connected devices can provide attackers with multiple entry points to potentially compromise transport systems or to exploit vulnerabilities, further increasing the risks.

4 Impacts of cyber attacks on ITS

Cyber attacks on Intelligent Transportation Systems (ITS) can impact Infrastructure Owners and Operators (IOOs). The consequences could include data theft, network disruption, and malware execution. Below are key areas affected by a successful cyber attack.

4.1 Safety

Transportation infrastructure is designed with embedded safety measures to protect riders, commuters, and workers. However, these safety systems can become targets of cyber attacks, because they can be a powerful tool for extorting an organization. For example, in 2024, a cyberattack in Hamilton, Ontario, paralyzed the city's remote-controlled traffic light system. If safety systems and their fail-safes are compromised, commuters and operators could be seriously injured.

4.2 Operations

A well-executed attack may disrupt the core transportation infrastructure. As a part of critical infrastructure transportation is interconnected with other public services, meaning that a large-scale attack could trigger ripple effects. For example, an attack on a lane control system could lead to increased congestion, a higher risk of traffic accidents, and disruptions to major transport routes.

4.3 Reputation

A significant breach or disruption could damage the public's perception of ITS and the organizations involved (IOOs, technology suppliers etc.). In situations where there's a personal data breach (like names, addresses or plate number data), there are privacy implications for the public that could cause reputational damage to the organization being attacked.

4.4 Finances

Cyber attacks have financial consequences for the affected organization. This may come in many forms, such as ransom costs (in a ransomware attack), legal costs, decreased revenue from reputational damage, and operational and capital costs to mitigate the attack and repair/replace damaged equipment.

5 Call to action: Investing in cyber security programs

As the transportation sector rapidly transforms to accommodate emerging technologies, your organization should invest in preparing for, and responding to, cyber threats. You should expect to invest resources into:

- designing and implementing new infrastructure
- developing new processes and procedures
- hiring and training staff to manage new infrastructure, and
- deploying cyber security related emerging technologies (AI enabled monitoring, centralized monitoring solutions, automated compliance management solutions, etc.)

You should use a flexible and scalable approach to navigate these changes. To manage the costs and maximize the benefits of this work, you should understand your organization's risk profile so you can define the target cyber security state that adequately manages that risk. To help your organization do this, Transport Canada's Program to Advance Connectivity and Automation in Transportation Systems (ACATS) has developed an ITS Cyber Security Self-assessment Tool to help you assess and prepare for risks.

5.1 Understand the environment

A solid understanding of your operating environment and its associated risks, including the sensitivity and exposure of data traversing the network, is essential to properly plan and implement new technologies while managing risk.

This understanding will help you identify vulnerabilities and risks that may arise as you begin to integrate new technologies. To accomplish this, your organization should stay informed on the latest standards, frameworks, and guidance available.

5.2 Understand your current cyber security posture

Understanding your current cyber security posture is crucial for identifying vulnerabilities, assessing gaps, and prioritizing improvements to reach your target cyber security posture.

Transport Canada's ITS Cyber Security Self-Assessment Tool will help you assess your current cyber security posture. In addition, the tool will enable you to set a target state and provides recommendations to achieve it. The target profile is customizable, so you can implement security controls that reflect your unique risk assessment.

5.3 Use policies and best practices

Your organization should develop an integrated approach and appropriate policies to manage cyber security across IT and OT assets. Use industry standards and compliance frameworks to assess and model your organizations' risk management policy as it relates to TMS assets, IT assets, processes, procedures, and vendors.

Whether your organization manages IT or TMS, you can use a framework to put the right people, process, technology, and governance practices in place to manage cyber risk and improve cyber security maturity.

5.4 Develop and test incident response plans and procedures

Any organization may experience a cyber attack. The way an organization can identify, assess, respond, and recover from the cyber event will dictate the impact to their organization.

You should develop formal incident response plans that are communicated to key stakeholders, tested to ensure efficacy, and updated on an ongoing basis.

5.5 Continue to assess cyber risks

Managing cyber risks is an ongoing process that needs to be embedded into your organization's risk management function. With constantly evolving technologies and risks, organizations should stay attuned to zero-day vulnerabilities (vulnerabilities that vendors don't know about) and emerging risks, so they can react accordingly.

6 Conclusion

The integration of ITS is fundamentally changing Canada's road infrastructure. While these technologies offer significant benefits in safety and efficiency, they also introduce critical cyber security vulnerabilities. The potential impacts of an attack are severe, threatening public safety, critical operations, and financial stability. Therefore, it is crucial that infrastructure owners and operators adopt a proactive and continuous approach to cyber risk management, using available tools and guidance to build resilience. By doing so, they can secure their systems and ensure Canadians fully and safely benefit from a modern, connected transportation network.

In addition to this document, Transport Canada has developed Establishing an Enterprise Cyber Security Program: A Guide for Canadian Road Infrastructure Owners/Operators and ITS Professionals, which offers specific steps for IOOs to set up or improve a cyber security program and increase their cyber security posture. For more information and resources, please visit our website

on road infrastructure cyber security. If you have any questions, comments or concerns, you can reach us at tc.its-sti.tc@tc.gc.ca.