Executive Summary

Driving Towards a Secure Future: Automotive Cyber Security in Ontario

Quarterly Specialized Report

Introduction

Cyber attacks are becoming increasingly pervasive as everyday processes and products are digitalized. In the automotive industry, cyber security is gaining increased focus as vehicles—which can now feature more lines of code than a 747 jet—become increasingly complex and digital. While the digital technology underpinning modern vehicles is advancing safety, efficiency, and sustainability goals, it has also increased the number of attack vectors—or ways to gain unauthorized access to a system.

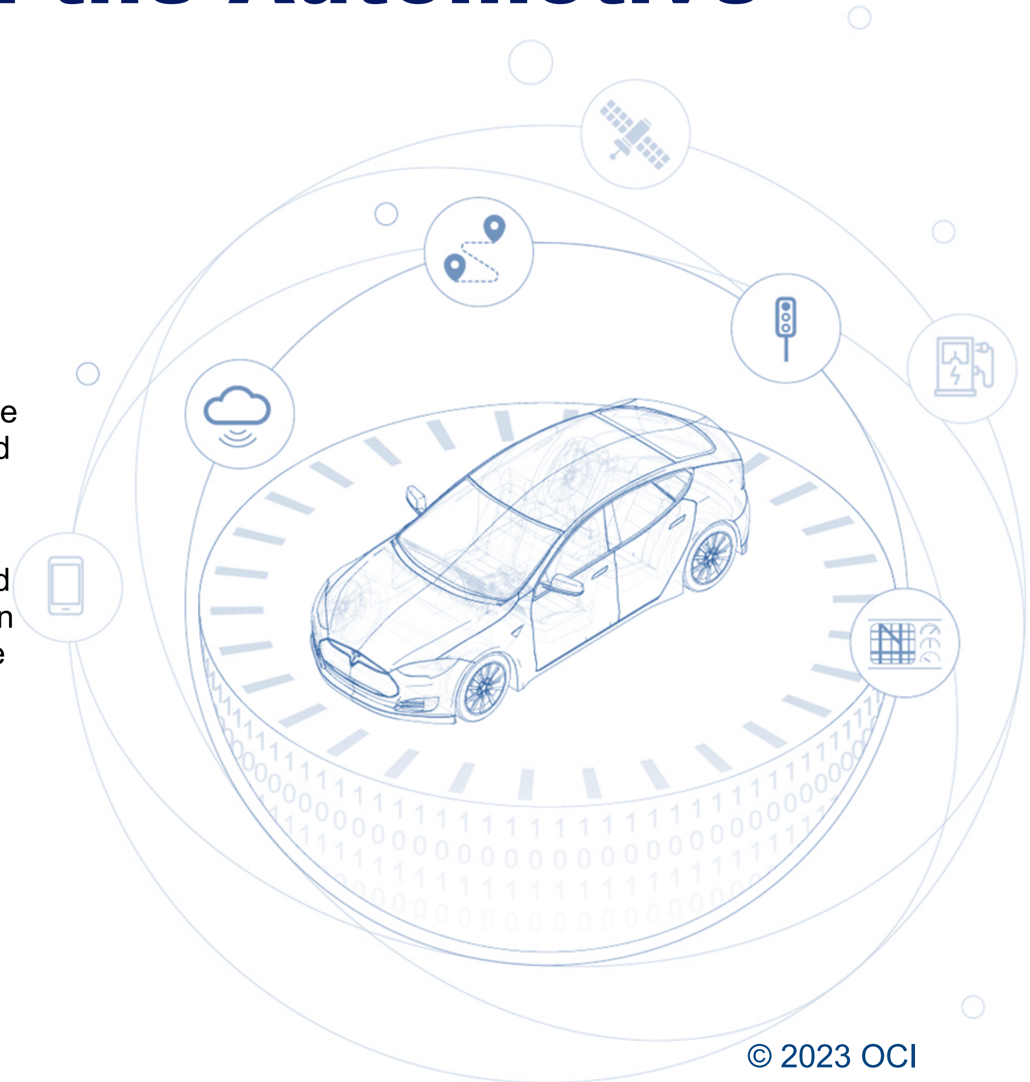
Organizations across Ontario are playing a leading role in the development of cyber security solutions. Ongoing projects at world-class automotive cyber security research labs and partnerships between the private sector and academia are facilitating Ontario-made cyber security innovations. Additionally, several university, college, and training programs are preparing future generations for careers in automotive cyber security, with an understanding that these roles will become more important as digital transformation continues. The province, through the Ontario Vehicle Innovation Network (OVIN), is also promoting awareness about the importance of automotive cyber security while ensuring that small- and medium-sized enterprises (SMEs) in Ontario have access to state-of-the-art facilities and research at the province's Regional Technology Development Sites (RTDS).

With these strengths and its thriving automotive sector, Ontario is uniquely positioned to continue pioneering advances in automotive cyber security. This report presents an overview of cyber security in the automotive industry, including the advanced transportation systems that are vulnerable to cyber threats, some common types of cyber attacks, the role of cyber security in protecting against attacks, and key international and national guidelines and standards for automotive cyber security. This report also identifies some opportunities to continue advancing automotive cyber security within Ontario.

Cyber Security in the Automotive Industry

The use of computerized and connected technology in vehicles has introduced new concerns related to cyber security. Vehicles are increasingly reliant on a range of advanced transportation systems that enable improved efficiency, safety, and sustainability. However, as this technology is increasingly incorporated into vehicles, the number of attack vectors—or ways to gain unauthorized access to a system—grows and vehicles become more vulnerable to cyber threats.

The following section provides an overview of advanced transportation systems, introduces some of the common types of cyber attacks used against them, highlights the importance of automotive cyber security in protecting against these threats, and presents some of the main guidelines and standards that inform automotive cyber security.



Advanced transportation systems

Automotive and mobility technology can be divided into three primary categories: connected vehicle systems, autonomous vehicle systems, and intelligent transportation systems. Technologies in all three systems are used to outfit cars and infrastructure with advanced features that improve transportation.

Intelligent transportation systems

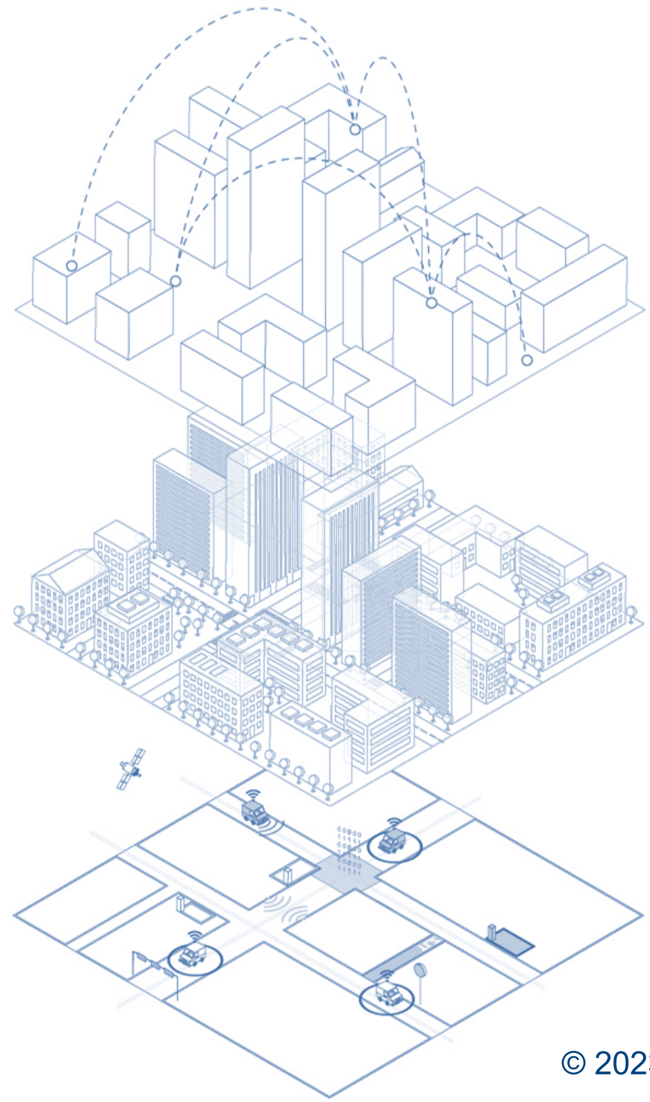
Intelligent transportation systems (ITS) support the move towards a fully integrated surface transportation management system. ITS rely upon advanced hardware and software that can detect, identify, and analyze objects. ITS include adaptive traffic signal control, variable message signs, and high-speed toll collection.

Connected vehicle systems

Connected vehicle systems facilitate communication between cars and other objects. These communication systems are frequently referred to as V2X systems, or vehicle-to-everything systems.

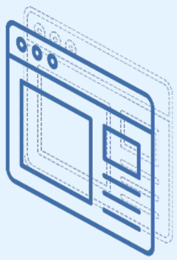
Autonomous vehicle systems

Autonomous vehicles rely on a range of systems that automate the driving process and eliminate (to varying degrees) the need for a driver. Autonomous vehicle systems handle actuation, perception and object analysis, localization and mapping, decision making and more using a variety of sensors, computer hardware, and operating systems.



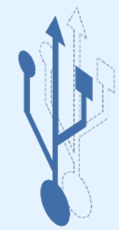
Cyber attacks

Attacks across the automotive ecosystem are growing both in number and in sophistication. While the motivations or actors behind cyber attacks vary, all attacks pose potential threats for the safety of road users, the operations of transportation infrastructure, and the reputation and finances of organizations involved. As vehicles continue to include increasingly complex digital systems, the number of attack vectors—or ways to gain unauthorized access to a system—is growing. Some types of attack vectors associated with modern vehicles are presented below.

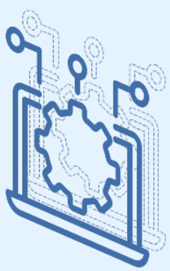


Infotainment and connectivity

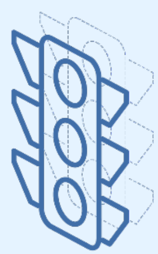
Sensors



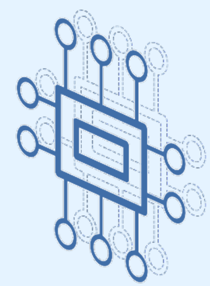
Vehicle buses and interfaces



Supply chain



V2X communication systems



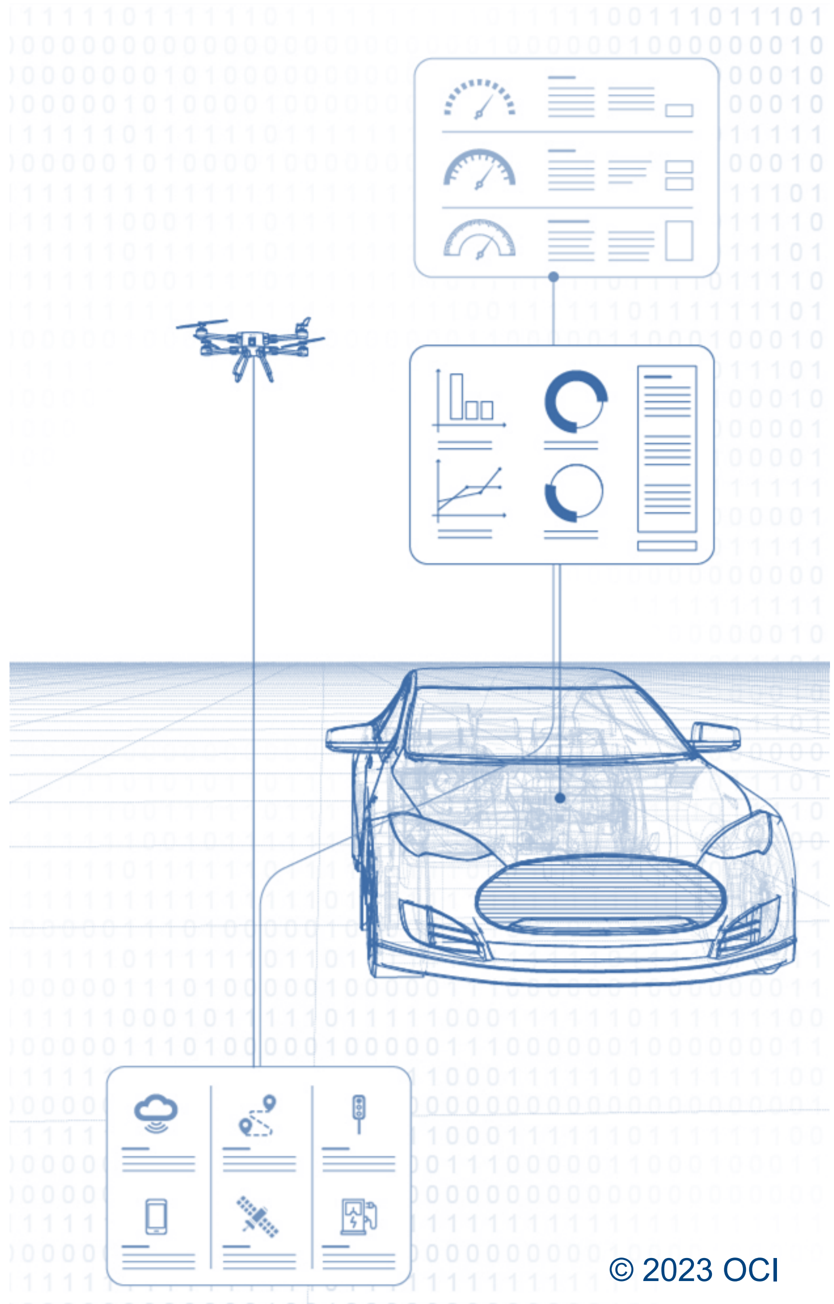
Hardware components

Cyber security measures

The advent of advanced transportation systems and the consequent introduction of new cyber attack vectors has increased the need for strong vehicle cyber security. By protecting communication networks, data, software, and other vulnerable systems from cyber attacks, cyber security enables the safe implementation of advanced transportation systems that reduce accidents, improve efficiency, and increase sustainability.

To adequately protect vehicles from cyber attacks, cyber security measures must be implemented across the entirety of a vehicle's lifecycle, from design through end of service. At all stages, a risk-based approach enables the prioritization and management of risk in acknowledgement of the fact that eliminating all cyber security risks is unrealistic. Additionally, it is imperative that cyber security risk assessments cover the entire automotive supply chain and that cyber security practices are implemented by all original equipment manufacturers (OEMs), suppliers, sub-contractors, and third-party vendors.

Given the increasing importance of cyber security, several Ontario-based companies have been developing cyber security technologies to help OEMs and other members of the automotive supply chain protect their assets.



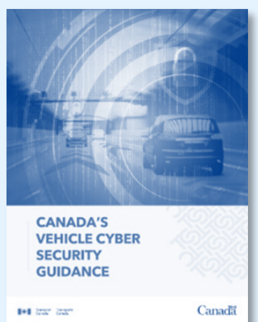
Guidelines and standards

A range of international and national guidelines, standards, strategies, and frameworks have been published to help manage new vehicle cyber security threats. A selection of widely used documents is presented below.

International Organization for Standardization (ISO)/Society of Automotive Engineers (SAE) 21434: Road Vehicles – Cybersecurity Engineering

UNECE WP 29.R156 Software update and software update management systems

UNECE WP 29.R155 Cyber security and cyber security management system

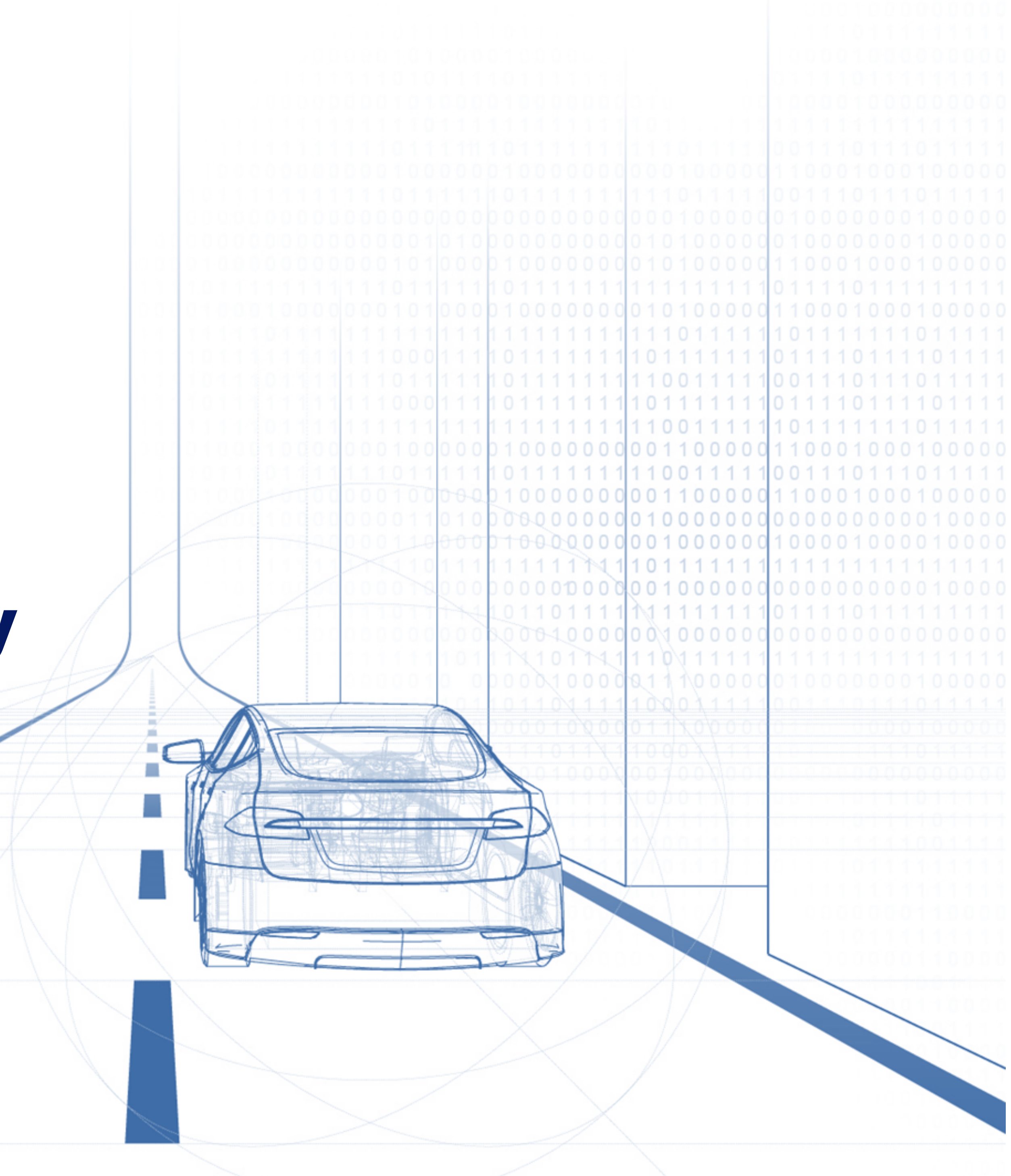


Canada's Vehicle Cyber Security Guidance

Transport Canada's Vehicle Cyber Security Strategy

Canada's Safety Framework for Automated and Connected Vehicles

Continuing to Advance Automotive Cyber Security in Ontario



Investing in talent and workforce development

Advances in automotive cyber security depend upon a highly-trained workforce with the skills necessary to develop and implement new cyber security features. In Ontario, several university, college, and training programs are preparing students for future careers in automotive cyber security. Additionally, Ontario—through OVIN—is helping ensure that the demand for professionals with cyber security skills is met though continued funding aimed at talent and workforce development.

Enabling comprehensive testing

Automotive cyber security solutions must undergo rigorous testing before being introduced to the market. OVIN's Regional Technology Development Sites (RTDS) enable Ontario companies to trial and advance their cyber security solutions in safe and secure environments. Moving forward, OVIN will continue to promote awareness about the importance of automotive cyber security while ensuring that SMEs in Ontario have access to state-of-the-art facilities and research at the province's seven RTDS.

Continued support of research initiatives

Cutting-edge research initiatives will play a vital role in maintaining Ontario's position as a leader in automotive cyber security. Already, Ontario is home to several research labs that are advancing the safety and security of new mobility technologies. OVIN continues to provide support for research in this domain through its R&D Partnership Fund which provides co-investment to support the development, testing, and demonstration of projects in the CAV and smart mobility space.

Ensuring quick recovery

Cyber security incidents are inevitable. For this reason, it is important that organizations develop plans for recovery in addition to implementing strong cyber security measures and processes. Canada's Vehicle Cyber Security Guidance advocates for post-incident analysis to identify vulnerabilities, develop remedies, and document lessons learned. The Guidance also notes the importance of partnership building and information sharing for the development of adequate cyber security defences. OVIN can play an increasing role in facilitating collaboration opportunities between various stakeholders—including OEMs, suppliers, research groups, and government bodies—to support knowledge sharing in the realm of cyber security.

About OVIN

The Ontario Vehicle Innovation Network (OVIN) is a key component of Driving Prosperity, the Government of Ontario's initiative to ensure that the automotive sector remains competitive and continues to thrive. The Government of Ontario has committed $56.4M for OVIN over four years to support research and development (R&D) funding, talent development, technology acceleration, business and technical support, and testing and demonstration sites. OVIN programs support small- and medium-sized enterprises (SMEs) to develop, test, and commercialize new automotive and mobility products and technologies, and cultivate the capacity of a province-wide network to drive future and green mobility solutions, reinforcing Ontario's position as a global leader.

OVIN, led by Ontario Centre of Innovation (OCI), is supported by the Government of Ontario's Ministry of Economic Development, Job Creation and Trade (MEDJCT) and Ministry of Transportation (MTO).

The initiative comprises five distinct programs and a central hub.

The OVIN programs are:

- Research and Development Partnership Fund
- Talent Development
- Regional Technology Development Sites
- Demonstration Zone
- Project Arrow

The OVIN Central Hub is the driving force behind the programming, province-wide coordination of activities and resources, and Ontario's push to lead in the future of the automotive and mobility sector globally. Led by a dedicated team, the Central Hub provides the following key functions:

- A focal point for all stakeholders across the province;
- A bridge for collaborative partnerships between industry, post-secondary institutions, broader public sector agencies, municipalities, and the government;
- A concierge for new entrants into Ontario's thriving ecosystem; and
- A hub that drives public education and thought leadership activities and raises awareness around the potential of automotive and mobility technologies and the opportunities for Ontario and for its partners.

To find out the latest news, visit www.ovinhub.ca or follow OVIN on social media @OVINhub

OVIN Objectives

- Foster the development and commercialization of Ontario-made advanced automotive technologies and smart mobility solutions.
- Showcase the Province of Ontario as the leader in the development, testing, piloting and adoption of the latest transportation and infrastructure technologies
- Drive innovation and collaboration among the growing network of stakeholders at the convergence of automotive and technology
- Leverage and retain Ontario’s highly skilled talent, and prepare Ontario’s workforce for jobs of the future in the automotive and mobility sector
- Harness Ontario’s regional strengths and capabilities, and support its clusters of automotive and technology

Meet the OVIN Team

Raed Kadri
Vice President, Strategic Initiatives, and Head of the Ontario Vehicle Innovation Network at OCI.
rkadri@oc-innovation.ca

Mona Eghanian
Director. Strategy and Programs. Automotive and Mobility.
meghanian@oc-innovation.ca

Amanda Sayers
Director. Skills, Talent, and Workforce Development.
asayers@oc-innovation.ca

Shane Daly
Portfolio Manager. Automotive and Mobility.
sdaly@oc-innovation.ca

Christine Stenton
Project Lead. Talent Initiatives.
cstenton@oc-innovation.ca

Shirin Sabahi
Team Coordinator.
ssabahi@oc-innovation.ca

Kathryn Tyrell
Manager. Automotive and Mobility Strategy.
ktyrell@oc-innovation.ca

John George
Sector Manager. Electric Vehicles.
jgeorge@oc-innovation.ca

Asad Farooq
Director. Sector and Cluster Development.
afarooq@oc-innovation.ca

Maruk Ahmed
Innovation Strategy Specialist.
mahmed@oc-innovation.ca

Shannon M. Miller
Project Lead. Strategic Partnerships.
smiller@oc-innovation.ca

Natalia Lobo
Project Manager.
nlobo@oc-innovation.ca

Natalia Rogacki
Portfolio Manager. Automotive and Mobility.
nrogacki@oc-innovation.ca

Ghazal Momen
Manager. Implementation and Delivery.
gmomen@oc-innovation.ca

Alèque Juneau
Project Lead. Workforce Development.
ajuneau@oc-innovation.ca

Rodayna Abuelwafa
Project Lead. Skills Development.
rabuelwafa@oc-innovation.ca

Disclaimers

This report was commissioned by the Ontario Centre of Innovation (OCI) through a Request for Proposals titled "Ontario Vehicle Innovation Network (OVIN) – Annual Comprehensive Sector Report & Quarterly Specialized Reports," dated April 26, 2022, and has been prepared by Arup Canada Inc. It is one of five reports covering an analysis of Ontario's automotive technology, electric vehicle and smart mobility landscape while incorporating implications for the sector's skills and talent landscape.

This report contains general information only, and by means of this communication, OCI is not rendering professional advice or services. Accordingly, readers are cautioned not to place undue reliance on this report and to perform their due diligence, investigations, and analysis before making any decision, relying on the report, or taking any action that may affect readers' finances or business.

No representations, warranties, or undertakings (express or implied) are given as to the accuracy or completeness of the information in this report. OCI shall not be liable or responsible for any loss or damage arising directly or indirectly in connection with any person relying on this report.

Copyright images cannot be used without explicit written consent and must be treated as general illustrations only and not relied upon to accurately describe the scheme.