OVIN
AUTONOMOUS • CONNECTED • ELECTRIC

Ontario

OCI
Where Next Happens

OVIN INSIGHTS
Specialized Series

Driving Towards a Secure Future: Automotive Cyber Security in Ontario

Quarterly Specialized Report

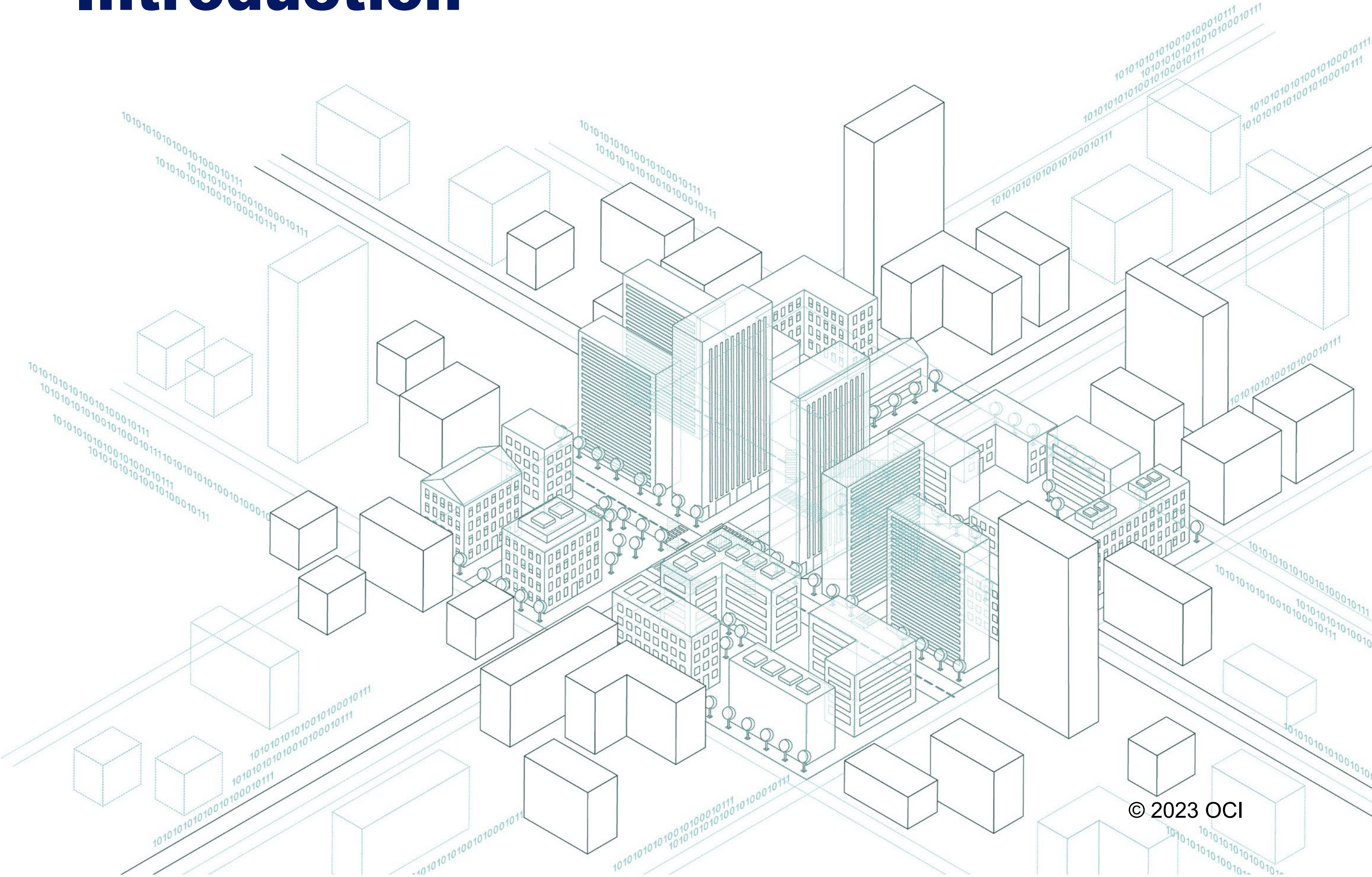
Table of contents

Acronyms

AI	Artificial Intelligence
AV	Autonomous Vehicle
AVRIL	Autonomous Vehicle Research and Intelligence Lab
CAV	Connected and Autonomous Vehicle
CV	Connected Vehicles
DSB	Danish State Railways
EV	Electric Vehicle
ISO	International Organization for Standardization
ITS	Intelligent Transportation Systems
LiDAR	Light Detection and Ranging
NSERC	Natural Sciences and Engineering Research Council
OEM	Original Equipment Manufacturer
OTA	Over-the-air
OVIN	Ontario Vehicle Innovation Network
KPI	Key Performance Indicator

R&D	Research and Development
RTDS	Regional Technology Development Site
SAE	Society of Automotive Engineers
SME	Small - and Medium-Sized Enterprises
SSP	Service Specific Permission
TTC	Toronto Transit Commission
UNECE	United Nations Economic Commission for Europe
VCAT	Canada’s Vehicle Cyber Security Assessment Tool
V2C	Vehicle-to-cloud
V2G	Vehicle-to-grid
V2I	Vehicle-to-infrastructure
V2P	Vehicle-to-pedestrian
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything
WP.29	World Forum for Harmonization of Vehicle Regulations

Introduction



Cyber attacks are becoming increasingly pervasive as everyday processes and products are digitalized. In 2021, nearly one-fifth of Canadian businesses (and over one-third of large businesses) reported a cyber security incident.[1] The costs associated with cyber attacks are growing as well: according to Statista, the average cost of a data breach in Canada in 2022 was $7.3M, up from $6.8M in 2021.[2]

As cyber attacks are increasing in number and scale, so is spending on cyber security. Canadian businesses spent approximately $10B on cyber security measures in 2021, with 61% of businesses reporting paying for protection.[3]

In the automotive industry, cyber security is gaining increased focus as vehicles—which can now feature more lines of code than a 747 jet[4]—become increasingly complex and digital. While the digital technology underpinning modern vehicles is advancing safety, efficiency, and sustainability goals,[5] it has also increased the number of attack vectors[6]—or ways to gain unauthorized access to a system. Attacks on the automotive industry have broadly resulted in data and privacy breaches, car theft, fraud, and business disruption.[7]

Given the major safety, financial, operational, and reputational impacts that can stem from cyber attacks in the automotive ecosystem,[8] it is critical that cyber security be prioritized by both the public and private sectors.[9] Furthermore, 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.[10]

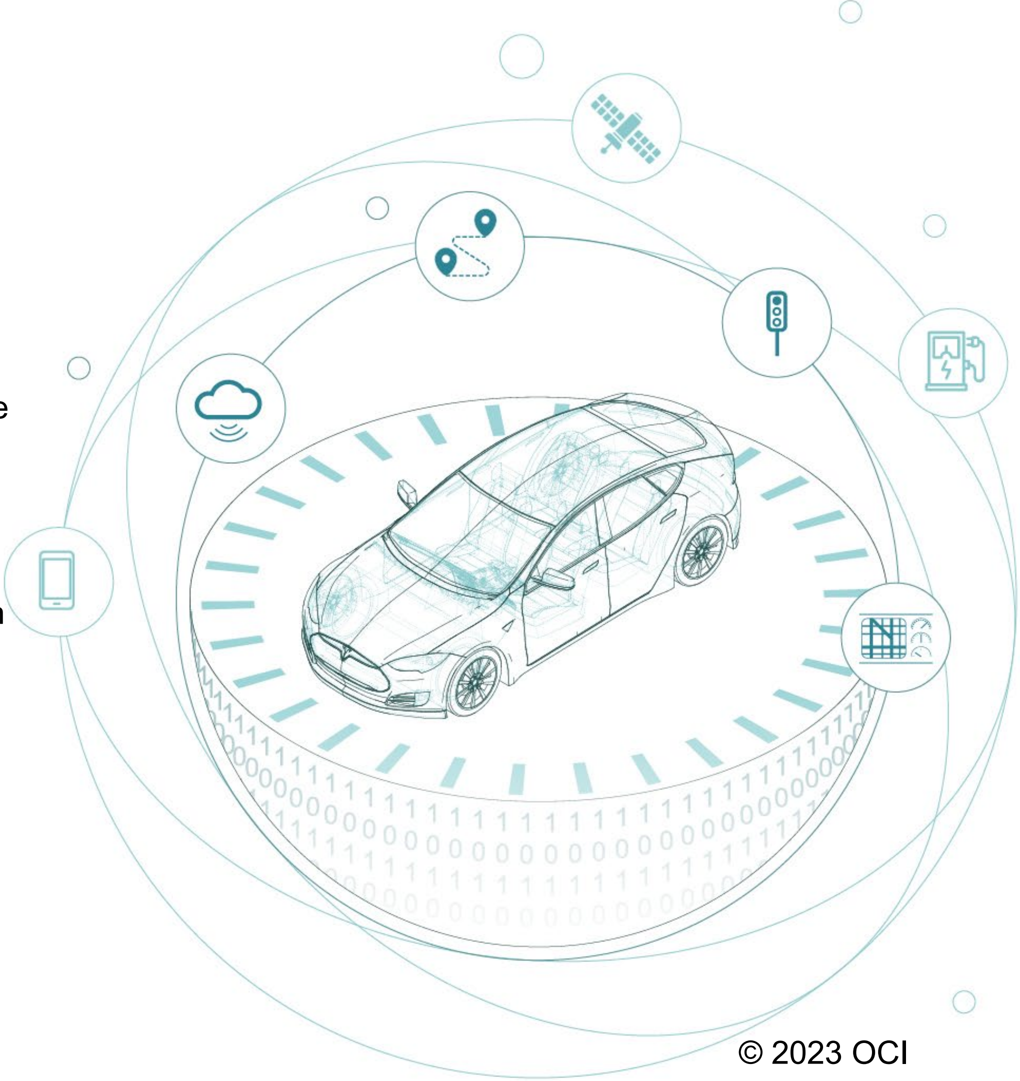
Organizations across Ontario are playing a leading role in the development of cyber security solutions. Ongoing projects at world-class automotive cyber security research labs and partnerships between the private sector and academia are facilitating Ontario-made cyber security innovations. Additionally, 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.[11] 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.[12]

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.



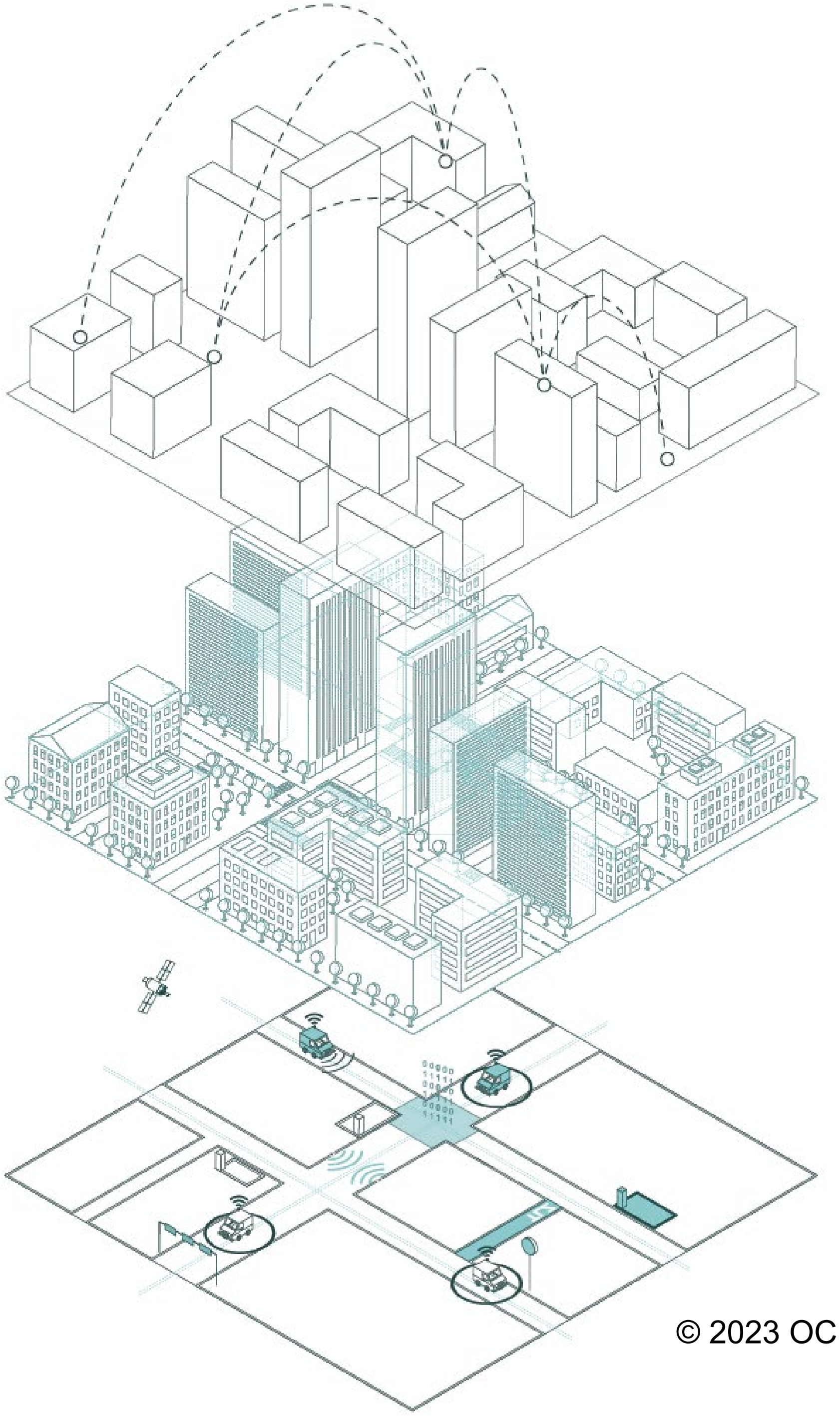
© 2023 OCI

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. For example, a combination of connected vehicle systems and autonomous vehicle systems enable platooning (a method of driving vehicles together in groups to increase efficiency). Similarly, a combination of connected vehicle systems and intelligent transportation systems enable transit vehicle signal priority.[13]

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.[14]



© 2023 OCI

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. Some of the specific communications systems under the V2X umbrella include:[15]

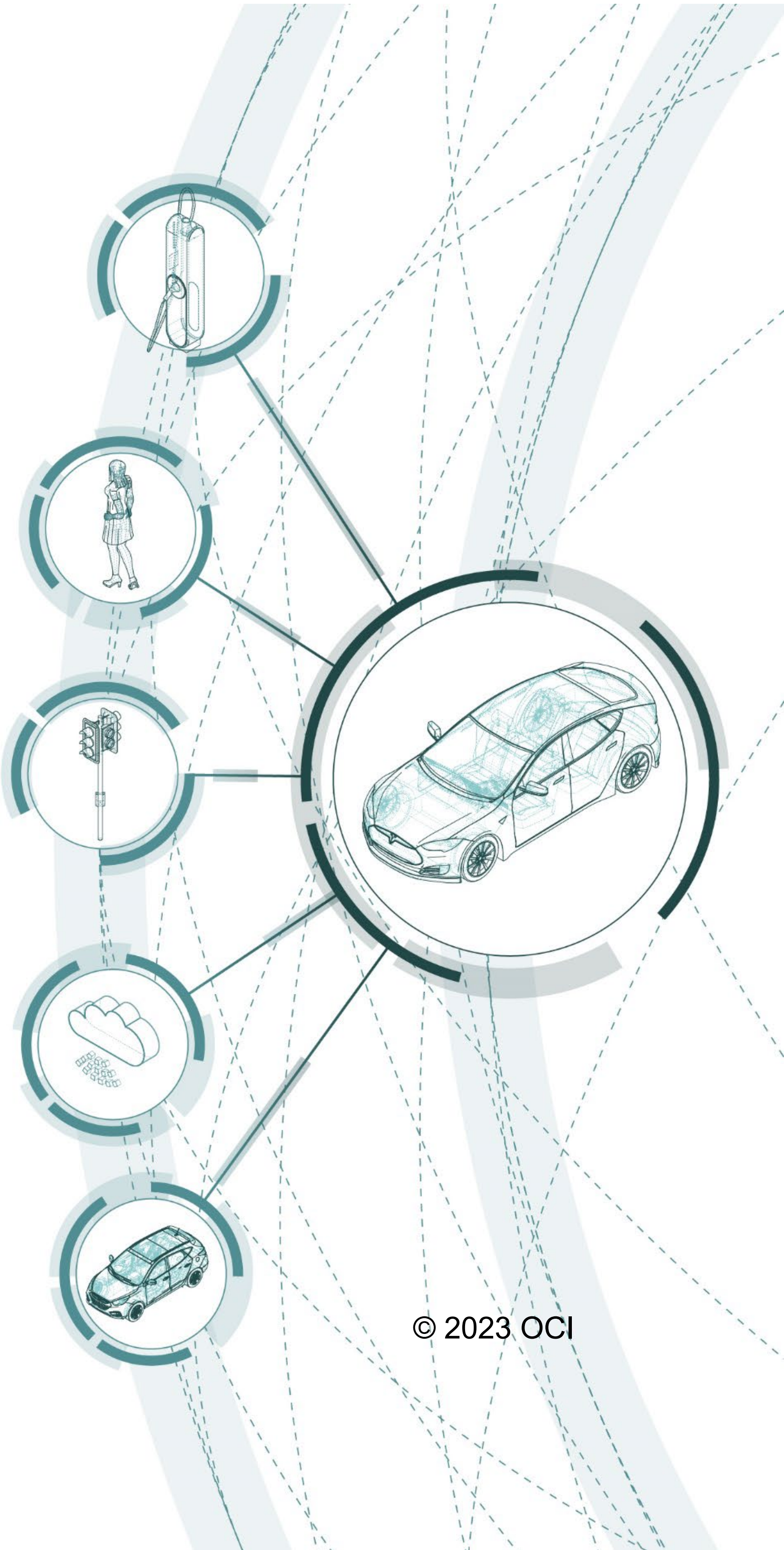
Vehicle-to-grid: Vehicle-to-grid (V2G) communication facilitates interactions between electric vehicles (EVs) and the power grid, enabling the balancing of loads and reduced utility bills.

Vehicle-to-pedestrian: Vehicle-to-pedestrian (V2P) communication connects vehicles and pedestrians, helping to ensure that vehicles are aware of the presence of active travellers and ensuring their safety.

Vehicle-to-infrastructure: Vehicle-to-infrastructure (V2I) communication allows vehicles to interact with nearby infrastructure, such as traffic lights or parking meters.

Vehicle-to-cloud: Vehicle-to-cloud (V2C) communication connects vehicles with the cloud, enabling remote vehicle diagnostics or over-the-air (OTA) vehicle software updates.

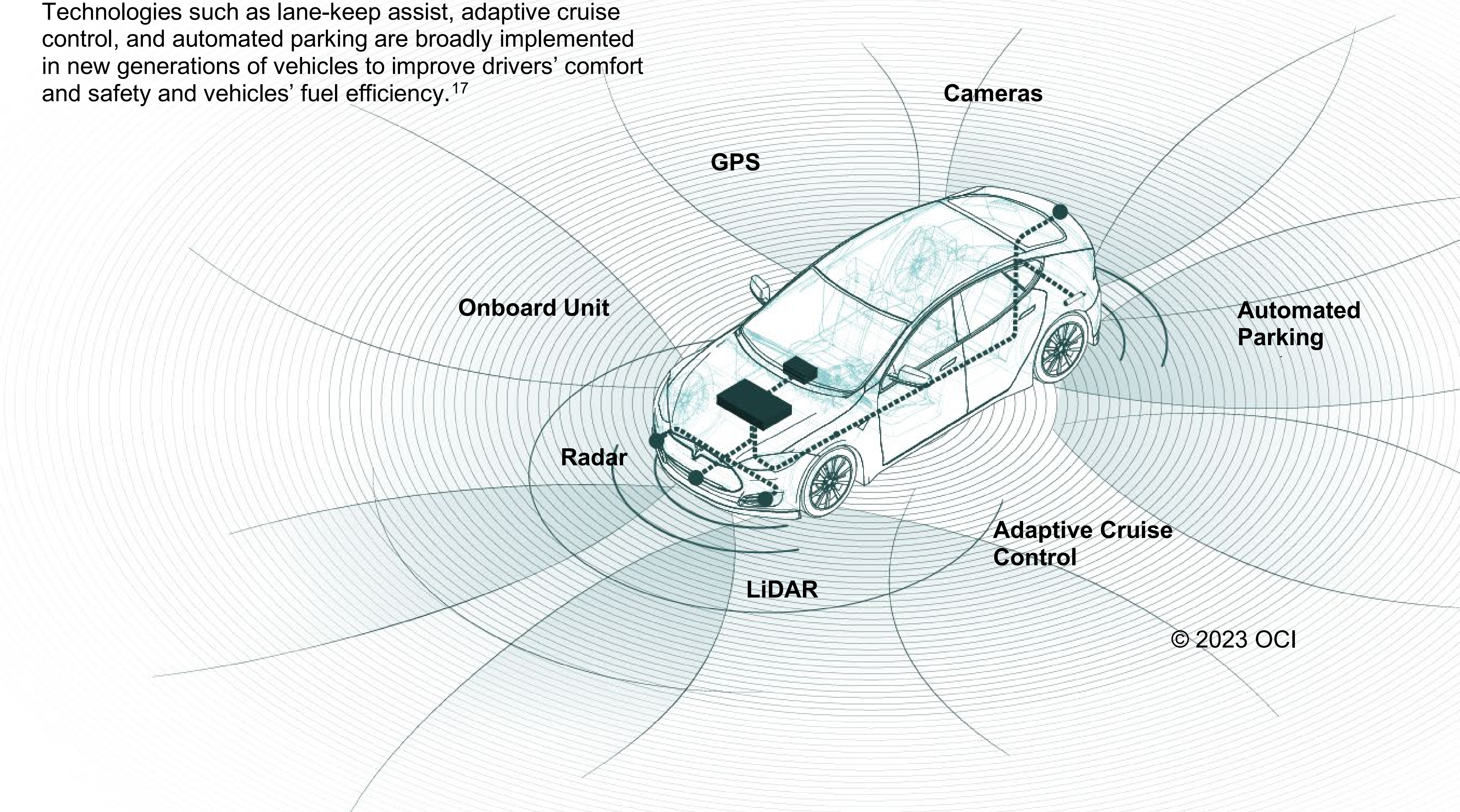
Vehicle-to-vehicle: Vehicle-to-vehicle (V2V) communication allows vehicles to share information such as their speed, location, and direction with other vehicles, enabling safer operations.



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.[16]

Technologies such as lane-keep assist, adaptive cruise control, and automated parking are broadly implemented in new generations of vehicles to improve drivers' comfort and safety and vehicles' fuel efficiency.[17]



© 2023 OCI

Cyber attacks

Attacks across the automotive ecosystem are growing both in number and in sophistication.[18] 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.[19]

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.[20] Some types of attack vectors associated with modern vehicles are described below.

Infotainment and connectivity

Infotainment systems can be attacked by hackers to enable the transfer of information from computers to vehicles and can be susceptible to interconnectivity vulnerabilities when accessing the internet. Researchers have also shown that vulnerabilities can enable access to various vehicle systems via Bluetooth or cellular connections.[21]

Sensors

Autonomous vehicles use sensors such as radar and LiDAR to recognize objects such as other vehicles and pedestrians and to avoid collisions. These sensors could be jammed (preventing features like automatic braking) or spoofed (made to think nonexistent objects are in the vicinity).[22]

Vehicle buses and interfaces

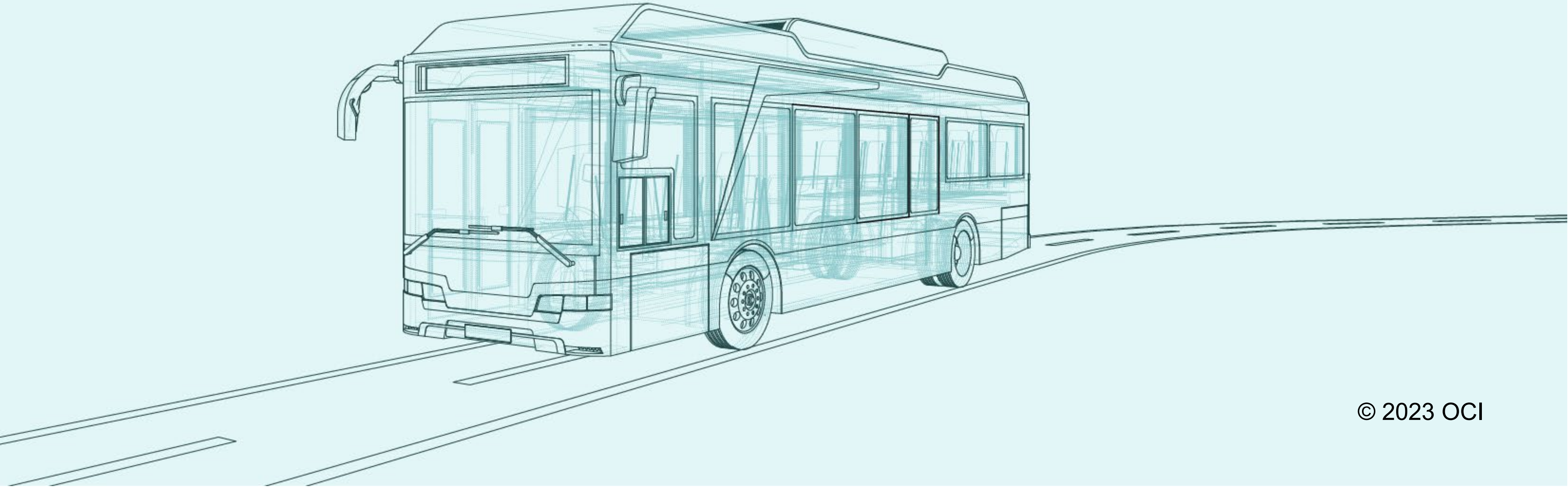
Vehicles buses enable connections between various electronic devices in a vehicle. There is a risk of attackers manipulating vehicle systems by directly splicing into vehicle buses or by gaining access through external electronic control units like the tire pressure monitoring system.[23]

Real-world cyber attacks: Toronto Transit Commission

The Toronto Transit Commission (TTC) announced that it was the victim of a ransomware attack in October 2021. The attack, which was identified by IT staff after detecting unusual network activity, impacted the online Wheel Trans booking service, internal TTC email service, next-vehicle information, and the TTC's Vision system, which enables communication between vehicle operators and Transit Control.[24]

In early November 2021, the TTC announced that the personal data (including names, addresses, and Social Insurance Numbers) of up to 25,000 current and former employees had also been stolen during the attack.[25] Shortly after the attack, the Toronto Star reported that the TTC had hired legal experts in cyber security to help coordinate the agency's response.[26]

The TTC Chief Executive Officer Rick Leary noted in a statement about the attack that the attackers belonged to an extremely well-organized enterprise[27] but did not comment on whether any ransom demands were made.[28] Although there was no indication that any of the stolen personal data was misused, the TTC provided credit monitoring and identity theft protection to those impacted.[29]



Supply chain

The software and hardware components required to make connected and autonomous vehicles (CAVs) are provided by a wide variety of third-party vendors. All suppliers of vehicle components must prioritize the cyber security of their products to ensure that the entirety of the vehicle ecosystem is secure.[30]

V2X communication systems

V2X makes it possible for vehicles to communicate with other vehicles, infrastructure, and the cloud. Vulnerabilities in the communication systems could enable hackers to compromise the safety of the vehicle by, for example, sending malicious over-the-air software updates.[31]

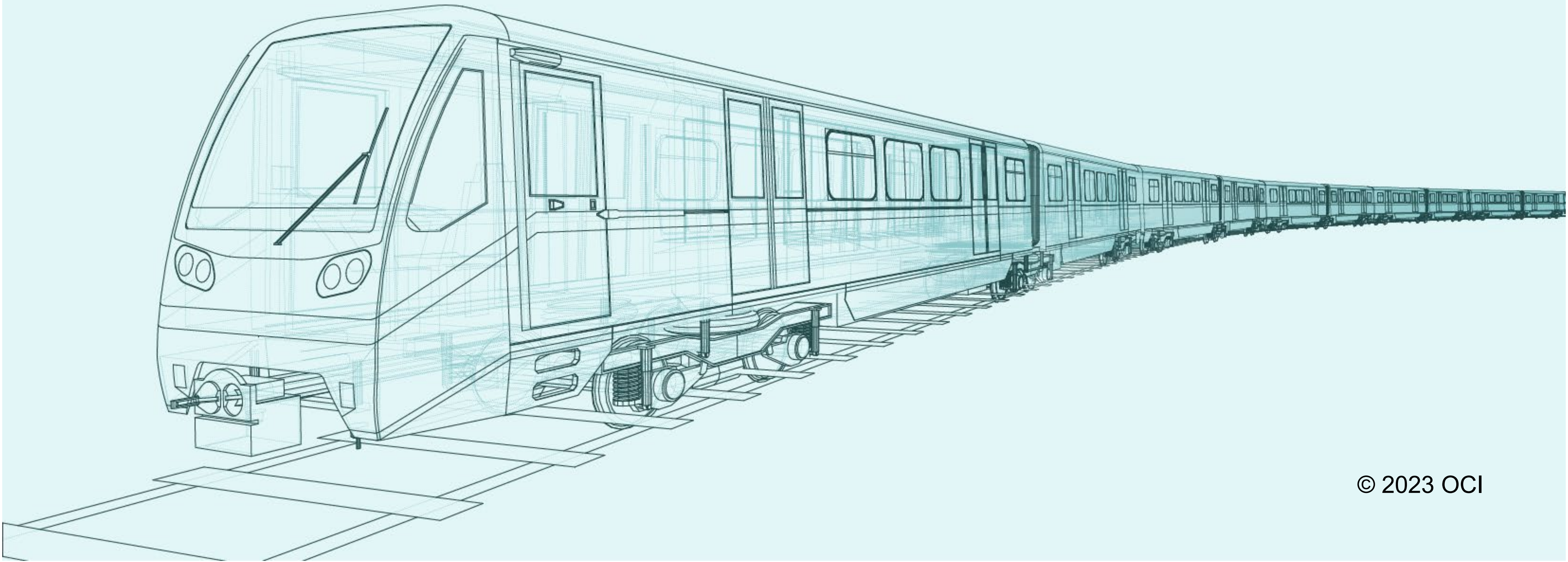
Hardware components

Physical manipulation of vehicle hardware can allow attackers to launch "man-in-the-middle" attacks in which messages sent to or from vehicles are disrupted or altered. One example of a man-in-the-middle attack is sending false information to roadside units to impact traffic conditions.[32]

Real-world cyber attacks: Danish State Railways

All trains operated by DSB (Danish State Railways), Denmark's major train operator, came to a complete stop on October 29, 2022, due to a security incident at an IT subcontractor, Supeo. The incident—which was described by a DSB representative as "economic crime"—forced Supeo to shut down its servers, and as a result, the application used by DSB's train drivers ceased to function. Trains were forced to stop operations when the application went offline and drivers could no longer access critical information, such as speed limits.[33]

Following the attack, DSB's chief of security announced that Supeo's testing environment had been compromised by criminal hackers.[34] While no information about the threat actors has been released, the attack highlights how supply-chain vulnerabilities can have major impacts for the safety and security of final products, services, and operations.



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.

The responsibility for effective cyber security is shared across the public and private sector. In Canada, all levels of government work collaboratively to support vehicle cyber security. Their responsibilities include fostering alignment on the development of standards, best practices, and regulatory frameworks; enforcing traffic laws; and implementing CAV-supportive infrastructure.[35] Examples of public-sector cyber security initiatives in Canada include CyberSecure Canada (a national cybersecurity certification program for SMEs),[36] the Canadian Centre for Cyber Security's Alerts and Advisories webpage,[37] and Ontario's Cyber Security Centre of Excellence (an initiative to educate public-sector organizations on cyber security through awareness campaigns, events, and online learning modules).[38] Individual organizations shoulder the responsibility for managing cyber security risks; protecting the vehicle ecosystem; detecting and responding to cyber attacks; and, following attacks, ensuring quick recoveries.[39]

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. A multi-layered approach that considers security controls, data security, internal and external communication, software development and updates, identity management and access control, and supporting infrastructure and services can help create security redundancy and reduce the likelihood of a successful attack. 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.[40]

Given the increasing importance of cyber security, a suite of cyber security technologies has been developed to help OEMs and other members of the automotive supply chain protect their assets. For example, Toronto-based Cybeats Technologies' SBOM Studio helps to track and manage all third-party components integrated into software products, enabling the identification of risks and insights regarding software security and quality.[41] Vehiqilla, an automotive cybersecurity firm based in Windsor, offers a range of services and solutions including cyber-risk assessments, fleet incident management services, V2X authentication and encryption technologies, and a Vehicle Security Operation Center to help monitor, detect and respond to cyber threats.[42] Based in North York, QA Consultants has provided software testing services to over a dozen automobile brands and has partnered with the Automotive Centre of Excellence at Ontario Tech University to develop a comprehensive testing environment for physical and software testing.[43]

CYBERNETIQ

Company Spotlight: CybernetIQ

Ottawa-based CybernetIQ helps organizations see the cyber security world on a deeper level, during a time when digital products and processes are under continued threat from cyber attacks. CybernetIQ's flagship product, CLAW, serves as a real-time lens into the cyber security of any network, presenting an accurate picture of what is in a network and why it matters.

With support from OVIN, CybernetIQ sought to prove that, regardless of the type of the network, CLAW's reports could reduce the time it takes for cyber security operators to respond to a cyber security event, one of the key performance indicators (KPIs) in the cyber security industry. The project successfully demonstrated that CLAW can provide Canada and the Province of Ontario with a view of autonomous vehicle networks, their supporting technologies, and the teams that defend them. These tools and tradecraft will shape the future of the automotive industry and the defense of its technologies to ensure that Ontarians are well protected now and in the future.

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[44]

This document details engineering requirements for cyber security risk management throughout concept development, production, operation, maintenance, and decomissioning of electrical and electronic systems in road vehicles, including their components and interfaces.

UNECE WP 29.R156 Software update and software update management systems[45]

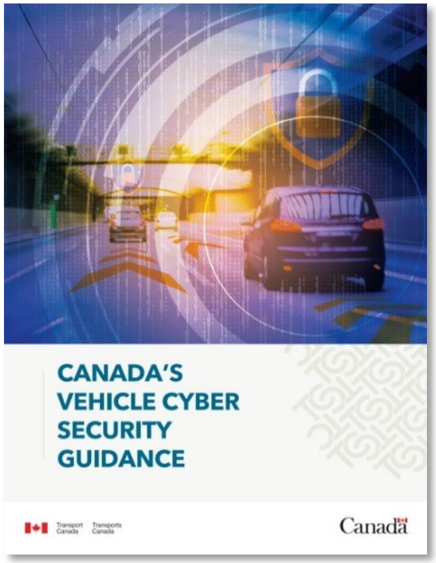
United Nations Economic Commission for Europe's (UNECE) World Forum for the Harmonization of Vehicle Regulations (WP.29) covers through Regulation No. 156 requirements for post-production software update procedures.

UNECE WP 29.R155 Cyber security and cyber security management system[46]

United Nations Economic Commission for Europe's (UNECE) World Forum for the Harmonization of Vehicle Regulations (WP.29) describes through Regulation No.155 the need to create a Cyber Security Management System that covers all phases of a vehicle's lifecycle.

Canada's Vehicle Cyber Security Assessment Tool (VCAT)[47]

This voluntary self-assessment tool can be used by vehicle manufacturers and Tier 1 and 2 suppliers to assess the cyber security performance and resilience of their vehicles and vehicle components.

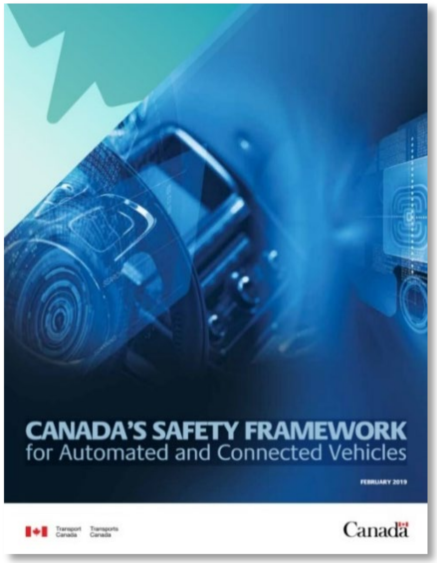


Canada’s Vehicle Cyber Security Guidance[48]

- Provides technology neutral and non-prescriptive guiding principles to strengthen cyber security throughout the vehicle lifecycle
- Encourages organizations to identify, manage, respond to and safely recover from cyber security events, while protecting the vehicle ecosystem

Transport Canada’s Vehicle Cyber Security Strategy[49]

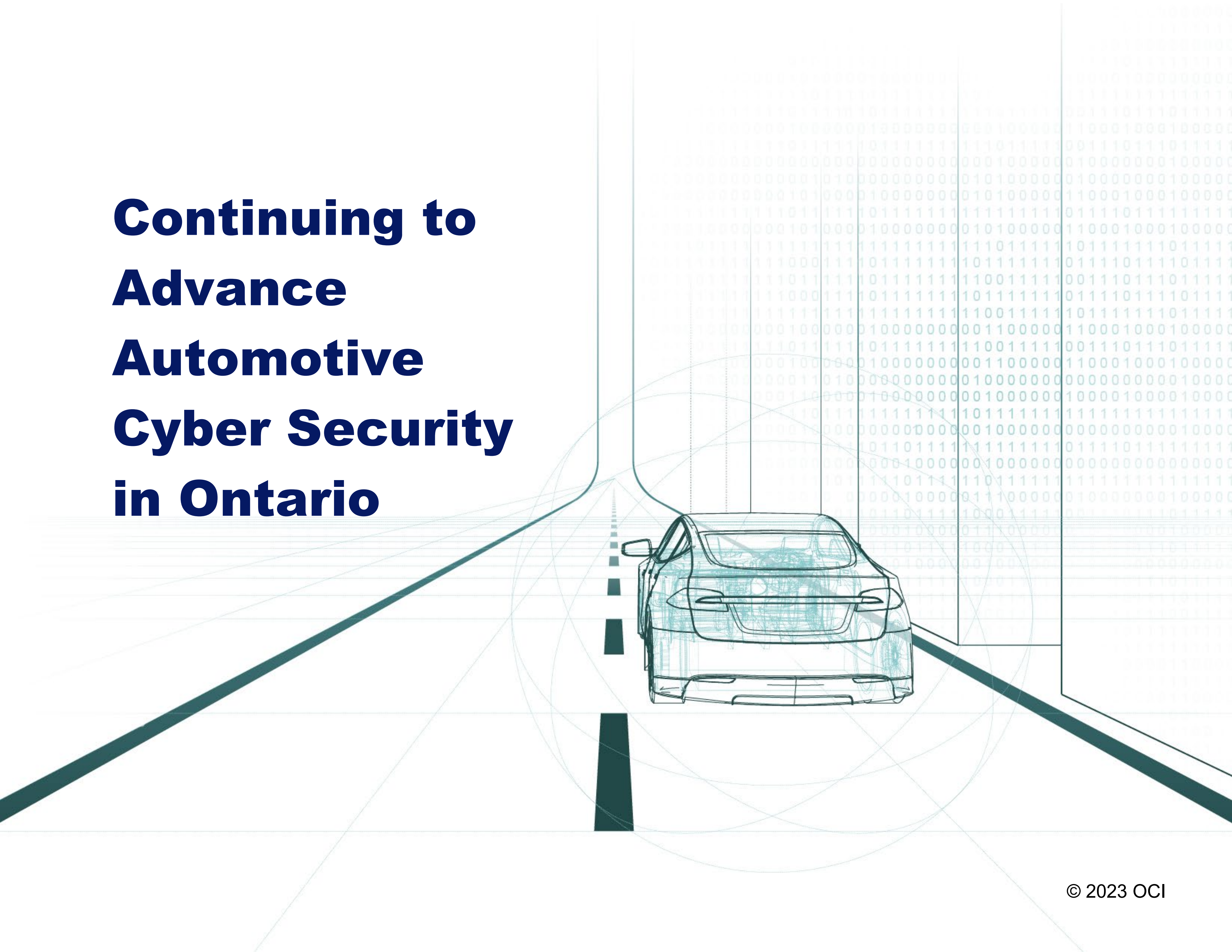
- Presents three vehicle cyber security goals around incorporating vehicle cyber security into policy and regulations, promoting awareness, and addressing emerging issues in the vehicle cyber security landscape
- Identifies areas in which to further develop policy guidance, and tools and undertake research and testing


CANADA'S SAFETY FRAMEWORK
for Automated and Connected Vehicles
FEBRUARY 2019
Transport Canada
Transports Canada
Canada

Canada’s Safety Framework for Automated and Connected Vehicles[50]

- Provides an overview of current legislation, and existing and emerging policy tools that will be used by Transport Canada to support Automated Vehicles’ (AVs) and Connected Vehicles’ (CVs) safety and security
- Sets a stable policy direction for safely deploying AV/CVs on Canada’s public roads

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.

At the University of Windsor, the SHIELD Automotive Cybersecurity Centre of Excellence—Canada's first centre focused on researching and teaching automotive cyber security—provides students with skills in artificial intelligence, machine learning, and advanced analytics. The University of Windsor also offers a two-course Certificate in Cybersecurity as part of its Continuing Education program.[51]

Last year,[52] St. Clair College began offering several graduate programs in cybersecurity, including a two-year Cybersecurity - Automobility program[53] and a one-year Cybersecurity Analytics - Automobility program[54]. Both programs prepare students for future jobs with automotive firms, with classes focused on topics including secure vehicle architecture, vehicle to everything cybersecurity, and cyber-physical vehicle system security.

In February 2023, Toronto Metropolitan University's Rogers Cybersecure Catalyst announced a new six-month program that will grant participants two globally-recognized cyber security certifications. Delivered in partnership with SANS Institute, the part-time program will offer students career mentorship and networking opportunities, in addition to the training.[55]

Additionally, Ontario’s Cyber Security Centre of Excellence provides public-sector organizations (including universities, hospitals, school boards, etc.) with advice, guidance, services, and information related to digital resilience. The information includes education and awareness materials such as online learning modules that can help employees of public-sector organizations build capacity in cyber security.[56]

Ontario is helping ensure that the demand for professionals with cyber security skills is met though continued funding aimed at talent and workforce development. Through OVIN, Ontario supports the Regional Future Workforce Program, which provides applicants up to $500K to implement education programs that support students in kindergarten through Grade 12 to develop the skills needed to succeed in the automotive and mobility sector.[57] OVIN's TalentEdge Fellowship[58] and Internship[59] Programs provide continued work-integrated learning opportunities for undergraduate and graduate students and post-doctoral fellows by providing funding to support internships and fellowships in the automotive and mobility sector.

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 North America's first automotive cyber security organization, the SHIELD Automotive Cybersecurity Centre of Excellence.[60] Located in Windsor, the automotive capital of Canada, researchers at SHIELD are developing Canadian-made cyber security solutions that keep pace with the introduction of new technology and new threats.[61] Funding from SHIELD's sponsors (including the Ontario Centre of Innovation)[62] supports projects focused on cyber security for connected, autonomous, shared, and electric vehicles. Some of SHIELD's ongoing projects are investigating the impact of quantum computation on hardware security for automotive applications, the detection of hardware trojans using machine learning, and hardware security issues associated with using electric-vehicle fleets with battery exchange infrastructure.[63]

The University of Waterloo's Autonomous Vehicle Research and Intelligence Lab (AVRIL) is also advancing automotive cyber security research. As part of a five-year, $1.6M partnership with the Natural Sciences and Engineering Research Council (NSERC) of Canada and Magna International that began in 2021, AVRIL will help identify ways to develop complex automotive software for connected and autonomous vehicles. Ultimately, Magna International will use this research to develop secure features and products and to identify ways to re-purpose older software in an effort to shorten development times of new products.[64]

More recently, TELUS announced a $5M investment to create a 5G connected campus and commercial lab at the University of Windsor. The investment will support research into new applications of 5G technology in the fields of agriculture, advanced manufacturing, and connected and autonomous vehicles (CAVs). One of the lab's initial projects, which is being undertaken in collaboration with Mitacs, focuses on the development of new cyber security applications for CAVs by using artificial intelligence (AI) and deep learning to identify potential CAV vulnerabilities.[65]

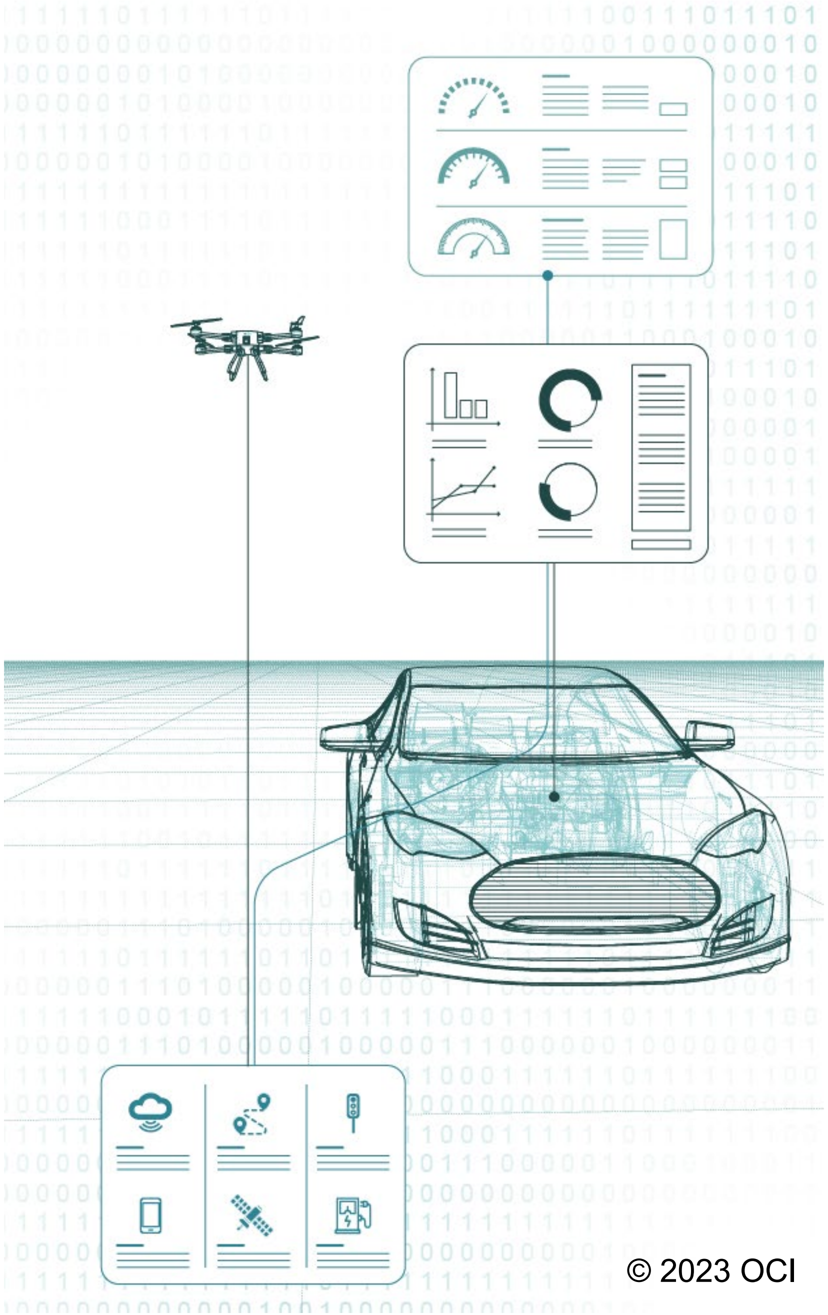
Moving forward, research institutions in Ontario can continue to play a vital role in ensuring safe and secure software and hardware for new mobility technologies. As predictions for trends in automotive cyber security foresee increased numbers of attacks against EV charging infrastructure and increased adoption of emerging technologies in smart cities,[66] these areas represent key avenues of research. 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.[67]

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. For example, Area X.O, the Ottawa RTDS, is a technology-rich, secure research and development (R&D) complex that helps to address challenges and opportunities in a range of sectors, including cyber security.

At the Waterloo RTDS, researchers are advancing Vehicle Safety System technology in support of fully autonomous vehicles. The technologies—which include collision avoidance systems, lane departure warnings, and driver alertness monitoring—are enabled by a range of technologies that require protection through cyber security solutions.

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.



© 2023 OCI

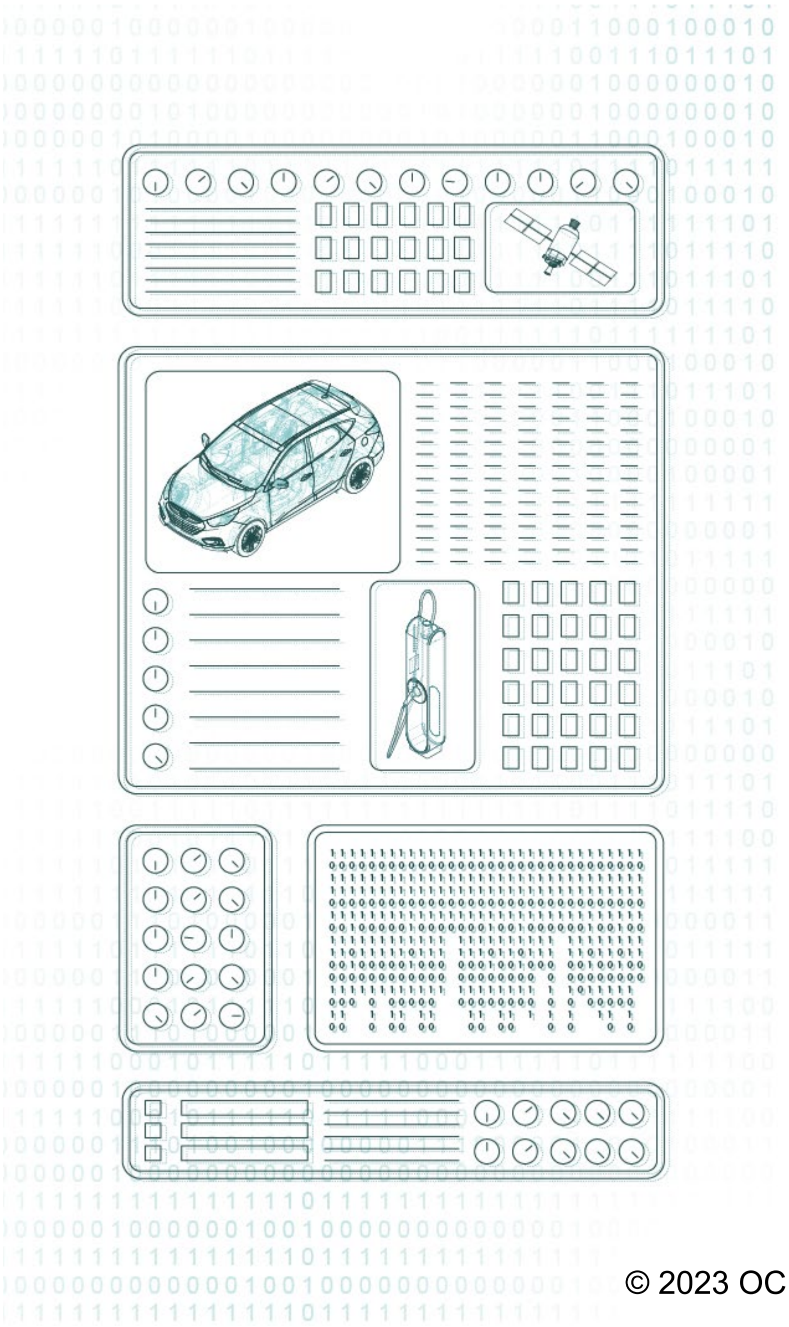
Ensuring quick recovery

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.[68] In some cases, an organization may need to consult their Incident Response Plan or Disaster Recovery Plan, which help to ensure continuity during unplanned service disruptions and protect sensitive information.[69]

Organizations can also work with specialized incident response teams to ensure that the appropriate steps are taken following an attack. Companies such as Toronto-based CYPFER provide cyber security consulting services to help clients navigate their response to cyber security incidents.[70]

Canada's Vehicle Cyber Security Guidance also notes the importance of partnership building and information sharing for the development of adequate cyber security defences.[71] 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.



© 2023 OCI

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.

References

[1] Statistics Canada. (2022, October 18). Impact of cybercrime on Canadian businesses, 2021. https://www150.statcan.gc.ca/n1/daily-quotidien/221018/dq221018b-eng.htm

[2] Statista. (2022, December 7). Average cost of a data breach in Canada from 2019 to 2022. https://www.statista.com/statistics/1346934/canada-average-cost-incurred-by-a-data-breach/

[3] Statistics Canada. (2022, October 18). Impact of cybercrime on Canadian businesses, 2021. https://www150.statcan.gc.ca/n1/daily-quotidien/221018/dq221018b-eng.htm

[4] Invest Ontario. (2023, January 25). University of Windsor’s SHIELD Automotive Cybersecurity Centre of Excellence is innovating to protect connected and autonomous vehicles. https://www.investontario.ca/success-stories/north-americas-first-automotive-cybersecurity-organization-ontario

[5] Deloitte. (n.d.). Connecting Canada: Securing the vehicles of the future. https://www2.deloitte.com/ca/en/pages/risk/articles/securing-the-vehicles-of-the-future.html

[6] Transport Canada. (2020). Canada’s Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

[7] Upstream Security. (2022). 2022 Global Automotive Cybersecurity Report: Automotive Cyber Threat Landscape in Light of New Regulations. https://upstream.auto/2022report/

[8] Transport Canada. (2022, December). Road Infrastructure Operational Technology Cyber Security Primer. https://tc.canada.ca/sites/default/files/2022-12/Road_Infrastructure_Operational_Technology_Cyber_Security_Primer-ENG.pdf

[9] Transport Canada. (2020). Canada’s Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

[10] Ibid.

[11] Deloitte. (n.d.). Connecting Canada: Securing the vehicles of the future. https://www2.deloitte.com/ca/en/pages/risk/articles/securing-the-vehicles-of-the-future.html

[12] Transport Canada. (2020). Canada's Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

[13] Public Sector Consultants and Center for Automotive Research. (2017, March). Planning for Connected and Automated Vehicles. Greater Ann Arbor Region Prosperity Initiative. https://www.cargroup.org/wp-content/uploads/2017/03/Planning-for-Connected-and-Automated-Vehicles-Report.pdf

[14] ITS Canada. (n.d.). ITS In Society - An Integration of Technologies. https://www.itscanada.ca/it/society/index.html

[15] RGBSI. (n.d.). 7 Types of Vehicle Connectivity. https://blog.rgbsi.com/7-types-of-vehicle-connectivity

[16] Heineke, K., Kampshoff, P., Mkrtchyan, A., & Shao, E. (2017, May 22). Self-driving car technology: When will the robots hit the road?. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/self-driving-car-technology-when-will-the-robots-hit-the-road

[17] Public Sector Consultants and Center for Automotive Research. (2017, March). Planning for Connected and Automated Vehicles. Greater Ann Arbor Region Prosperity Initiative. https://www.cargroup.org/wp-content/uploads/2017/03/Planning-for-Connected-and-Automated-Vehicles-Report.pdf

[18] Upstream Security. (2022). 2022 Global Automotive Cybersecurity Report: Automotive Cyber Threat Landscape in Light of New Regulations. https://upstream.auto/2022report/

[19] Transport Canada. (2022, December). Road Infrastructure Operational Technology Cyber Security Primer. https://tc.canada.ca/sites/default/files/2022-12/Road_Infrastructure_Operational_Technology_Cyber_Security_Primer-ENG.pdf

[20] Transport Canada. (2020). Canada's Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

[21] Hodge, C., Hauck, K., Gupta, S. & Bennett, J. (2019, August). Vehicle Cybersecurity Threats and Mitigation Approaches. National Renewable Energy Lab. https://www.nrel.gov/docs/fy19osti/74247.pdf

[22] Ibid.

[23] Ibid.

[24] CBC News. (2021, October 29). Toronto transit system hit by ransomware attack, TTC says no significant disruptions. https://www.cbc.ca/news/canada/toronto/ttc-ransomware-attack-1.6231349

[25] Toronto Transit Commission. (2021, November 8). TTC provides update on cyber security incident. https://www.ttc.ca/news/2021/November/TTC-provides-update-on-cyber-security-incident

[26] Spurr, B. (2021, November 10). TTC hires ‘breach counsel’ to respond to ransomware attack. Toronto Star. https://www.thestar.com/news/gta/2021/11/10/ttc-hires-breach-counsel-to-respond-to-personal-data-attack.html

[27] Toronto Transit Commission. (2021, November 8). TTC provides update on cyber security incident. https://www.ttc.ca/news/2021/November/TTC-provides-update-on-cyber-security-incident

[28] LIFARS. (2021, December 16). Ransomware Attack on Toronto Transit Commission. https://www.lifars.com/2021/12/ransomware-attack-on-toronto-transit-commission/

[29] Toronto Transit Commission. (2021, November 8). TTC provides update on cyber security incident. https://www.ttc.ca/news/2021/November/TTC-provides-update-on-cyber-security-incident

[30] Transport Canada. (2020). Canada’s Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

[31] Hodge, C., Hauck, K., Gupta, S. & Bennett, J. (2019, August). Vehicle Cybersecurity Threats and Mitigation Approaches. National Renewable Energy Lab. https://www.nrel.gov/docs/fy19osti/74247.pdf

[32] European Union Agency for Cybersecurity. (2019, November). ENISA Good Practices for Security of Smart Cars. https://www.enisa.europa.eu/publications/smart-cars

[33] Kovacs, E. (2022, November 4). Cyberattack Cause Trains to Stop in Denmark. Security Week. https://www.securityweek.com/cyberattack-causes-trains-stop-denmark/

[34] Skydsgaard, N. (2022, November 3). Danish train standstill on Saturday caused by cyber attack. https://www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/

[35] Transport Canada. (2020). Canada’s Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

[36] Government of Canada. (2023, February 6). CyberSecure Canada. https://ised-isde.canada.ca/site/cybersecure-canada/en

[37] Government of Canada. (2023, February 7). Alerts and advisories. https://www.cyber.gc.ca/en/alerts-advisories

[38] Government of Ontario. (2020, September 30). Cyber Security Centre of Excellence. https://www.ontario.ca/page/cyber-security-centre-excellence

[39] Transport Canada. (2020). Canada’s Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

[40] Ibid.

[41] Cybeats Technologies Inc. (2023). Software Bill of Materials: SBOM Studio. https://www.cybeats.com/sbom-studio

[42] Vehiqilla. (2023). Witness the Automotive Industry Transformation. https://vehiqilla.com/

[43] QA Consultants Inc. (2023). Automotive. https://qaconsultants.com/industries/automotive/

[44] ISO. (2021, August). ISO/SAE 21434:2021 Road vehicles – cybersecurity engineering. https://www.iso.org/standard/70918.html

[45] United Nations Economic Commission for Europe. (2021, April 4). UN Regulation No. 156 - Software update and software update management system. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

[46] United Nations Economic Commission for Europe. (2021, April 3). UN Regulation No. 155 – Cyber security and cyber security management system. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

[47] Transport Canada. (2021, August 10). Canada's Vehicle Cyber Security Assessment Tool (VCAT). https://tc.canada.ca/en/road-transportation/innovative-technologies/connected-automated-vehicles/canada-s-vehicle-cyber-security-assessment-tool-vcat

[48] Transport Canada. (2020). Canada's Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

[49] Transport Canada. (2021, November 1). Transport Canada's Vehicle Cyber Security Strategy. https://tc.canada.ca/en/road-transportation/innovative-technologies/connected-automated-vehicles/transport-canada-s-vehicle-cyber-security-strategy

[50] Transport Canada. (2019, February). Canada's Safety Framework for Automated and Connected Vehicles. https://tc.canada.ca/sites/default/files/2020-05/tc_safety_framework_for_acv-s.pdf

[51] University of Windsor. (n.d.). Certificate in Cybersecurity. https://www.uwindsor.ca/continuingeducation/524/cybersecurity

[52] Academica Group. (2022, February 1). St Clair approves cybersecurity, greenhouse operator/technician programs. https://www.academica.ca/top-ten/st-clair-approves-cybersecurity-greenhouse-operatortechnician-programs

[53] St. Clair College. (2023). Cybersecurity – Automobility. https://www.stclaircollege.ca/programs/cybersecurity-automobility

[54] St. Clair College. (2023). Cybersecurity Analytics – Automobility. https://www.stclaircollege.ca/programs/cybersecurity-analytics-automobility

[55] Rogers Cybersecure Catalyst at Toronto Metropolitan University. (2023, February 28). Rogers Cybersecure Catalyst at Toronto Metropolitan University launches new dual-certification program designed to launch or elevate cybersecurity careers. https://www.newswire.ca/news-releases/rogers-

cybersecure-catalyst-at-toronto-metropolitan-university-launches-new-dual-certification-program-designed-to-launch-or-elevate-cybersecurity-careers-888983804.html

[56] Government of Ontario. (2020, September 30). Cyber Security Centre of Excellence. https://www.ontario.ca/page/cyber-security-centre-excellence

[57] Ontario Smart Mobility Readiness Forum. (2022). Regional Future Workforce Program. https://www.ovinhub.ca/ecosystem/regional-future-workforce-program/

[58] Ontario Smart Mobility Readiness Forum. (2022). Talent Development – TalentEdge Fellowship Program (TFP). https://www.ovinhub.ca/programs/talent-development-fellowships/

[59] Ontario Smart Mobility Readiness Forum. (2022). Talent Development – TalentEdge Internship Program (TIP). https://www.ovinhub.ca/programs/talent-development-internships/

[60] Invest Ontario. (2023, January 25). University of Windsor’s SHIELD Automotive Cybersecurity Centre of Excellence is innovating to protect connected and autonomous vehicles. https://www.investontario.ca/success-stories/north-americas-first-automotive-cybersecurity-organization-ontario

[61] Automotive Cybersecurity Centre of Excellence. (n.d.). SHIELD. https://www.shieldautocybersecurity.com/

[62] Automotive Cybersecurity Centre of Excellence. (n.d.). Collaborators. https://www.shieldautocybersecurity.com/collaborators

[63] Automotive Cybersecurity Centre of Excellence. (n.d.). Projects. https://www.shieldautocybersecurity.com/projects

[64] Mehanaz Yakub. (2021, October 4). Cybersecurity for AVs is focus of a new UWaterloo-Magna research project. https://electricautonomy.ca/2021/10/04/magna-uwaterloo-av-cybersecurity/

[65] TELUS Communications Inc. (2023, January 25). UWindsor secures $5M partnership with TELUS to propel 5G research and innovation in agriculture, advanced manufacturing and connected and autonomous vehicles. https://www.globenewswire.com/news-release/2023/01/25/2595118/0/en/UWindsor-secures-5M-partnership-with-TELUS-to-propel-5G-

research-and-innovation-in-agriculture-advanced-manufacturing-and-connected-and-autonomous-vehicles.html

[66] Upstream Security. (2022). 2022 Global Automotive Cybersecurity Report: Automotive Cyber Threat Landscape in Light of New Regulations. https://upstream.auto/2022report/

[67] Ontario Smart Mobility Readiness Forum. (2022). R&D Partnership Fund – Connected and Autonomous Vehicle (C/AV) and Smart Mobility: Stream 1. https://www.ovinhub.ca/rd-partnership-fund-connected-and-autonomous-vehicle-c-av-smart-mobility-stream-1/

[68] Transport Canada. (2020). Canada's Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf

[69] Canadian Centre for Cyber Security. (2021, January). Developing your IT recovery plan. https://www.cyber.gc.ca/en/guidance/developing-your-it-recovery-plan-itsap40004

[70] CYPFER. (n.d.). Incident Response. https://cypfer.com/incident-response/cyber-security-incident-reponse-retainer-services/

[71] Transport Canada. (2020). Canada's Vehicle Cyber Security Guidance. https://publications.gc.ca/collections/collection_2020/tc/T46-61-2020-eng.pdf