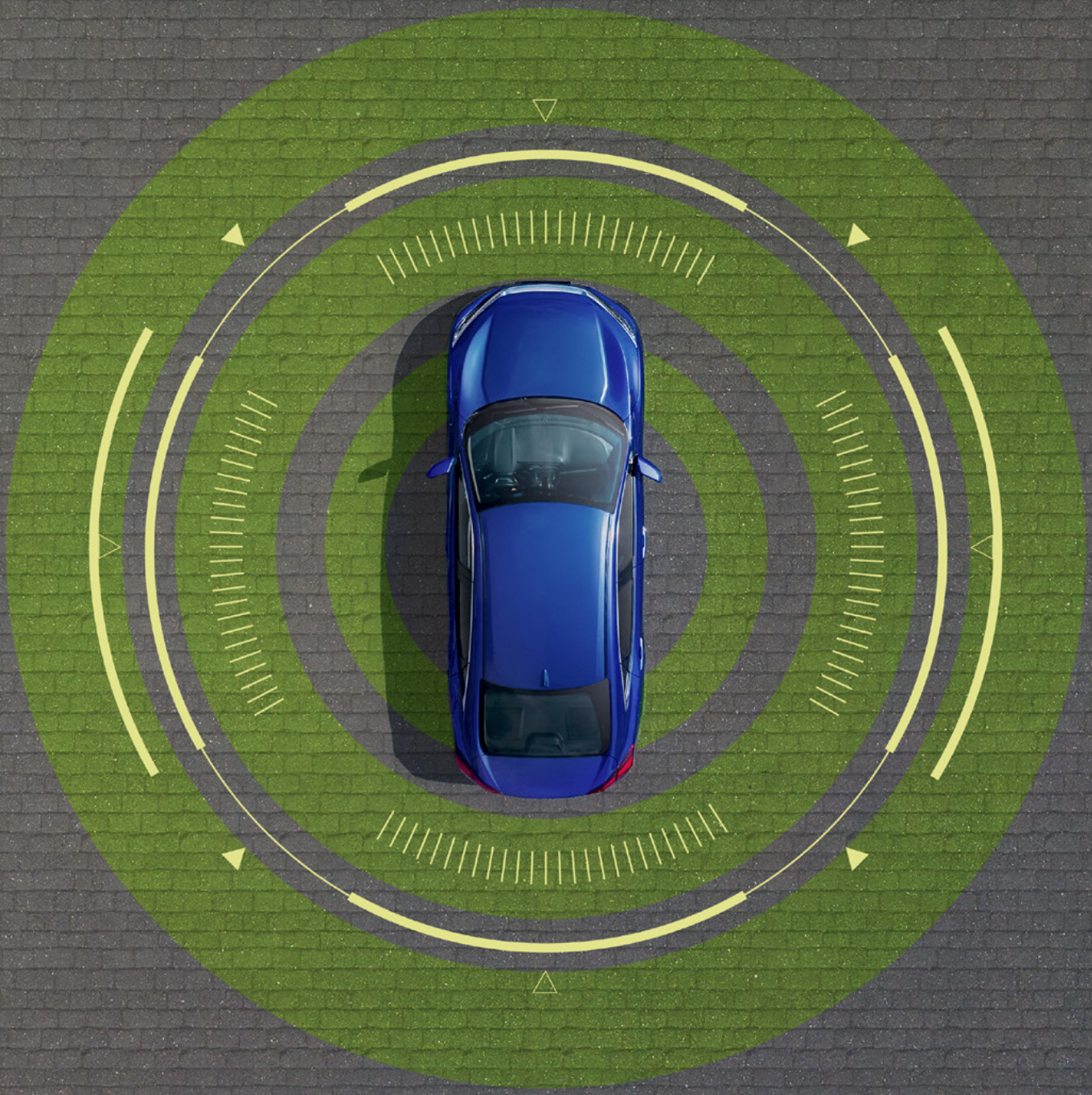
Deloitte.



Connecting Canada

Securing the vehicles of the future

Contents

Introduction

Ground transportation is undergoing a revolution. Hyperconnected vehicles, electrification, and increasing levels of autonomous technology are leading the charge.

Connected, autonomous, shared, and electric (CASE) vehicles have already penetrated the market. They're being tested and adopted around the world as taxi, shuttle transit, and short and long-haul delivery fleets within a variety of industries, from retail to public transit and parcel delivery.[1] Focusing on the rapid integration of hyperconnected vehicles and the strategic security posture that companies will now be adopting, we ask the question: what does this new opportunity mean for business?

Trust in this new world of CASE vehicles is a fresh challenge for manufacturers, suppliers, regulators, fleet owners, and governments as they seek to ensure safety and efficiency in connected ground transit. New levels of complexity, integration into current business architecture, increased attack surfaces, and the sheer volume and value of data will make CASE vehicles and infrastructure more vulnerable to cyberattacks. Given the high expectations and the potential for exploitation, ensuring that automotive cybersecurity technologies stay well ahead of the tactics of threat actors will no longer be a choice but an imperative for all businesses in the supply chain. These are challenges that should not be overlooked, but should also not become a barrier to entry for business. The drive to remain competitive, increase operational and energy efficiency, and create new customer value should offer sufficient motivation to overcome the challenges. In taking a strategic and integrated view, understanding the risks, and planning for the challenges, businesses can only benefit from engagement in CASE vehicles.

In this report, we'll explore the features of CASE technology, with particular attention on data connectivity in ground vehicular transit and the future of autonomous vehicles. We'll also highlight the current opportunities for businesses and how they can manage cybersecurity holistically to maximize engagement with the technology. We'll endeavour to help business to:

- Understand drivers for a strategic cybersecurity and risk approach in the CASE ecosystem.
- Identify how CASE-specific cybersecurity regulations and frameworks are being developed to support growth.
- Review how the development and implementation of cybersecurity and risk in CASE is a shared responsibility for all parties in the ecosystem.
- Review the importance of an inclusive cyber strategy across the entire life cycle for CASE-based fleets.

Driving the future of mobility

Interconnected devices, artificial intelligence (AI), edge computing, and data analytics are transforming the entire automotive value chain (Figure 1).[2] Adopting these technologies has without doubt given organizations many positive returns on their investments. However, the path to greater benefit means business must meet the strategic, cybersecurity, and risk challenges ahead. As the transportation industry continues its journey toward complete connectivity and automation, these emerging challenges will need to be considered. Cybersecurity principles should be built into the foundations of CASE integration, operation, and life cycle management to prevent disruptions to business operations, performance, and processes, while keeping people and products safe in the cyber and physical domains.

Figure 1. Key drivers and benefits of integrated cyber-enabled mobility

Life and safety

The World Health Organization estimates that road crashes cost **1.3 million lives each year, 3% of a country's GDP, and 20 to 50 million non-fatal injuries**.[3] This pushes safety and user experience to the forefront of industry leaders' agendas. Software-driven solutions such as lane change assistance, steering wheel correction, and blind spot checks **allocate decision-making to the vehicle, which reacts faster and more precisely than a human**.

Efficiency of transport

With 68% of the world's population projected to live in urban areas by 2050,[4] data-driven analytics for efficient route planning and reduced congestion will bring undisputed travel efficiency to **first-, middle-, and last-mile solutions**. Vehicle platooning will allow for **information sharing, improved road condition awareness, bolstered fuel economy, and cooperative strategies**.

Shortage of labour

The 20,000-person labour shortage in the Canadian trucking industry in **February 2020, expected to surge up to 50,000 by 2024** could be mitigated by **CASE trucks** that can theoretically **operate 24/7**.[5] Trucking, rail warehousing, and logistic companies could **employ flexibility during peak demand, take on cargo that is heavier, and pack products individually** by deploying CASE fleets and technologies to tap into much larger profit pools.

Environmental sustainability

Greener alternatives to transportation are on the rise because the **Canadian government requires all new vehicles to be zero-emission by 2035**.[6] Additionally, there will be more **alternative forms of mobility that reduce carbon emissions and overcrowding of roads which will provide greater accessibility, convenience and affordability**. Increased uptake of shared mobility means urban areas **(like parking lots) can be repurposed toward more green spaces and parks**.

Data-driven insights

Record e-commerce sales have driven companies to find innovative solutions to meet **rising customer expectations and proliferating needs.** Leveraging the **large volumes of data created by CASE vehicles allows for better supply-chain visibility, predictive analytics, and customization of services to each consumer**. Data-driven insights equip organizations to get their goods to customers faster.

Understanding cyber risk in the new ecosystem

Embedding complex Internet of Things (IoT) connectivity and software components (5G, Wi-Fi, cameras, LiDAR sensors, etc.) in CASE vehicles increase their attack surface as physical proximity is no longer needed for attacks to occur. In 2021, remote attacks largely exceeded physical attacks. From the attacks that were reported, 15.5% of them required physical access to the vehicle, and 84.5% of attacks were remote.[7] In addition to the increase in remote access attacks, the overall quantity of attacks are also increasing, since over 50% of the cybersecurity related automotive incidents ever reported have taken place in the last two years alone.[7]

Exponential rise in risk

The rise in automotive cyber incidents over the last decade is predicted to keep growing.[7] Last year, one industry leader in the CASE vehicle marketplace experienced the severity and danger of these attacks when 25 of the company's vehicles were remotely accessed.[8] The teenaged hacker was able to determine each vehicle's exact location, whether it was occupied by a driver, and, most significantly, run commands on it remotely.

The amalgamation of hardware and software components in a CASE vehicle leads to a complex distribution of responsibility in these kinds of attacks and breaches. In many instances, responsibility can fall on multiple stakeholders within the automotive supply chain.

Each stakeholder can help fortify against the rapidly evolving risk appetite, including governing bodies, Tier 1, 2, and 3 suppliers (including software provisioning companies), automobile manufacturers, communication service providers (CSPs), cloud provisioning companies, and smart transport business consumers (Figure 2). Strong partnerships, clear delegation of responsibilities, and identification of opportunities to mitigate cyber risk will be key to using the entire ecosystem safely, securely, and confidently.

Figure 2. Risk levels and attacks that CASE vehicles are susceptible to

Risk level	Threats to and attacks on CASE vehicles
Low	• Manipulation of vehicle diagnostic data • Unlawful vehicle tuning • Unauthorized access of back-end systems (manufacturing plants, cloud systems, etc.)
Medium	• Targeted malware • User account exploitation • Key spoofing
High	• GPS tracking/stalking • Manipulation of driver behaviour through misleading tactics • Remote control of vehicle or remote code execution in vehicle • Control of acceleration and braking

Source: Upstream Security Limited.

> The automotive and mobility sector is rapidly transforming through electric, connected, and autonomous vehicle technology. As a result, cybersecurity has become a fundamental consideration in the future movement of people and goods.
>
> —Raed Kadri, Head of the Ontario Vehicle Innovation Network (OVIN)

Figure 3. Automotive supply chain stakeholders and their responsibilities in securing CASE vehicles

GOVERNING BODIES	TIER 1, 2, AND 3 SUPPLIERS AND OEMS	CLOUD INFRASTRUCTURE PROVISIONING COMPANIES	COMMUNICATION SERVICE PROVIDERS	BUSINESS CONSUMERS
Federal, provincial, and municipal governments	Providers of CASE software applications, ADAS, operating systems, electronic modules, assembly warehouses, etc.	Cloud storage providers of GPS data, back-end applications, and communication enablers.	Telecommunication companies, 5G, 4G, LTE provisioning, etc.	Fleet operators, first-, middle-, and last-mile solution providers, logistics, etc.
• Enable safe, secure transportation and communication infrastructure • Uphold the shared responsibility model (publishing standards, best practices, and anticipating challenges) • Ensure attestation of compliance • Foster the relationship between government and industry by refining legislation, and supporting the economic development enabled by CASE vehicles while encouraging overall safety	• Integrate international cyber standards into hardware/software • Ensure end-to-end cybersecurity of all amalgamated vehicular components • Adhere to cross-border legislation (data protection and privacy) • Encrypt connected devices (fobs, phone applications, etc.) • Secure code of onboard units	• Assure cloud hardening, vulnerability management, and access control of stored data • Encrypt data-in-motion and data-at-rest • Prevent the exploitation of vulnerabilities due to manipulation of data or leaked code, and illicit backdoor entries • Protect sovereignty of data in cross-border vehicular data storage	• Assure availability of communication networks • Secure communication channels for different services (emergency and non-emergency communication, etc.) • Ensure connectivity coverage in non-urban areas, such as highways and cross-province/country • Provide reliable communication channels	• Monitor for insider threats • Secure integrations between on-premises and cloud infrastructure • Monitor vehicles as assets (through security operations and security event and incident management) • Protection of proprietary data and assets with appropriate SLAs • Conduct assurance and risk assessments of third-party software

Establishing secure-by-design protection

By weaving security into the design of systems and processes, organizations can bolster cyber resilience as they adapt to new ways of conducting business. This will require integrating secure-by-design—and privacy-by-design—principles in asset development and options such as a zero-trust-based, multi-layered approach to cyber defences. Zero-trust will be an important safeguard in this sector, as recognized in Deloitte's 2021 *Future of cyber survey*.[9]

Securing the CASE ecosystem—The road map to regulation

The transition to fully integrated mobility will be complex and challenging. The security of CASE vehicles begins with the vehicle itself and the associated hardware and software components. Automotive OEMs and Tier 1, 2, and 3 suppliers can follow best practices to ensure compliance with regulations, such as standards for hardware encryption and communication protocols for electronic control units (ECUs), supplemented with recurring risk and controls assessments. In Europe, the World Forum for Harmonization of Vehicle Regulations (WP.29) has begun developing a framework for globally harmonized regulations.[10] Transport Canada is following suit with its own guidelines, cybersecurity requirements, and compliance initiatives that will affect operational processes.[1] The United Nations' R155 is another regulation that will soon be mandatory in several countries, requiring auto manufacturers to integrate vehicle cybersecurity management systems that can protect against a specific list of cyberthreats.[11] To ensure holistic coverage, OEMs will need to provide attestation of compliance to regulations from both Tier 1 and 2 suppliers and software providers.

Software companies and Tier 1 suppliers that provide hardware with software should incorporate best practices and security-testing methodologies in their development processes. Hardware components such as chips, ECUs, and onboard units should be protected from illicit after-market modification by using tools to determine signs of tampering. Given the dispersed nature of the final product, companies should also consider securing cloud operations in order to confidently deploy software updates for components such as advanced driver-assistance systems (ADAS). Vehicle software will be patched and updated remotely over the internet or over the air (OTA), so encryption will be necessary to maintain the confidentiality, integrity, and availability of the delivered software.

With compliance secure for individual parts, putting adequate controls in place for the production life cycle of the vehicle will then ensure end-to-end compliance with cybersecurity standards for the entire CASE vehicle itself. This can be facilitated with standards such as International Standardization Organization (ISO) SAE 21434 ("Road Vehicles—Cybersecurity Engineering") and ISO SAE 24089 ("Road Vehicles—Software Update Engineering").[12,13] ISO SAE 21434 supplements the vehicle functional safety outlined in ISO SAE 26262 ("Road Vehicles—Functional Safety"), and includes facets such as security management, continuous cybersecurity activities, integrations, risk assessment methods, and product development cybersecurity considerations.

SAE also provides guides, best practices, and cybersecurity lessons from industry, government, and academia for securing vehicles.[14] It's here that governing bodies should look to mandate regulatory compliance and attestation. With regional requirements and mandates of these best practices and policies, stakeholders along the entire automotive supply chain will have a clear division of responsibility as well as a duty to uphold good cyber hygiene in automotive manufacturing processes.

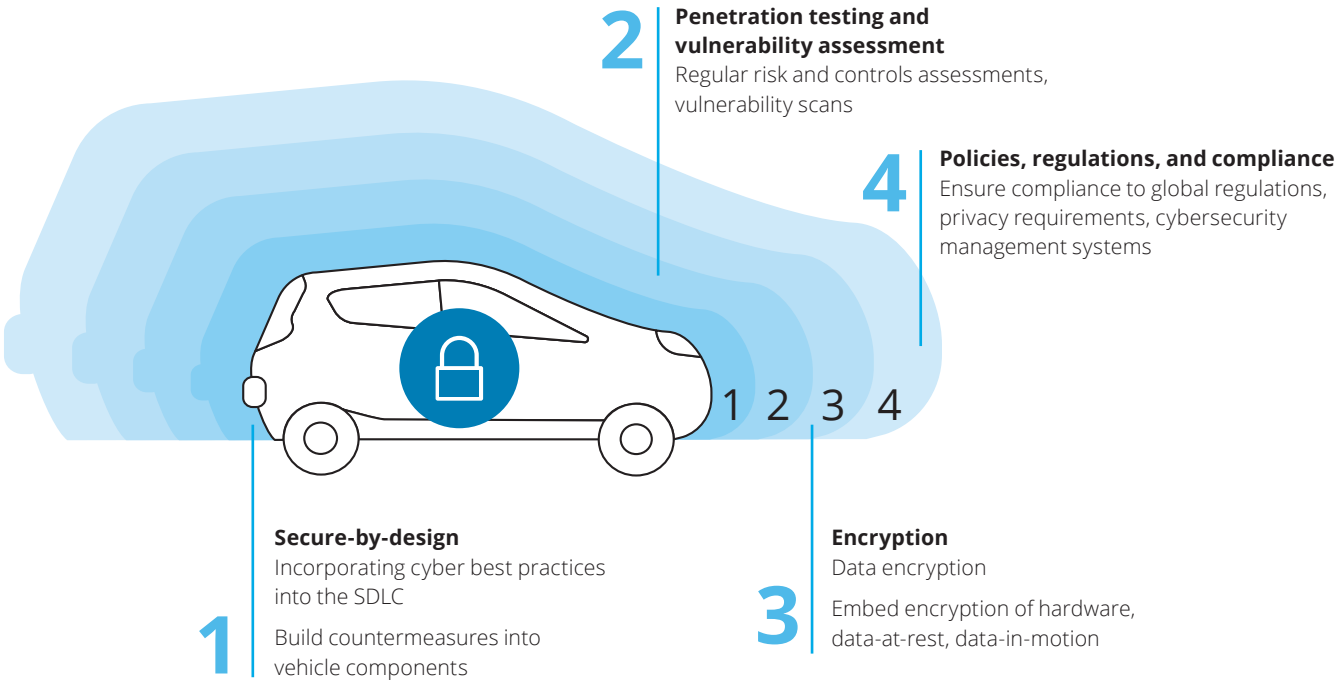
Each stakeholder has a critical role to play in securing the automotive value chain, and collaboration among stakeholders will result in reinforced cybersecurity capabilities. A shared responsibility model will enable a truly secure-by-design foundation for the adoption of CASE vehicles.

Figure 4. Shared responsibility matrix describing the responsibility of each stakeholder in the automotive production life cycle

	Tier 1, 2, and 3 suppliers and OEMs	Government and regulatory	Cloud infrastructure	Comms service providers (4/5G)	CASE business fleet operators
Secure OTA firmware management					
Cybersecurity operations centre					
Data privacy					
Communication infrastructure security					
V2X communications security					
Mobile application security					
Interface security (Wi-Fi/Bluetooth/5G)					
ADA systems security					
Embedded systems security					

Least responsible — **Most responsible**

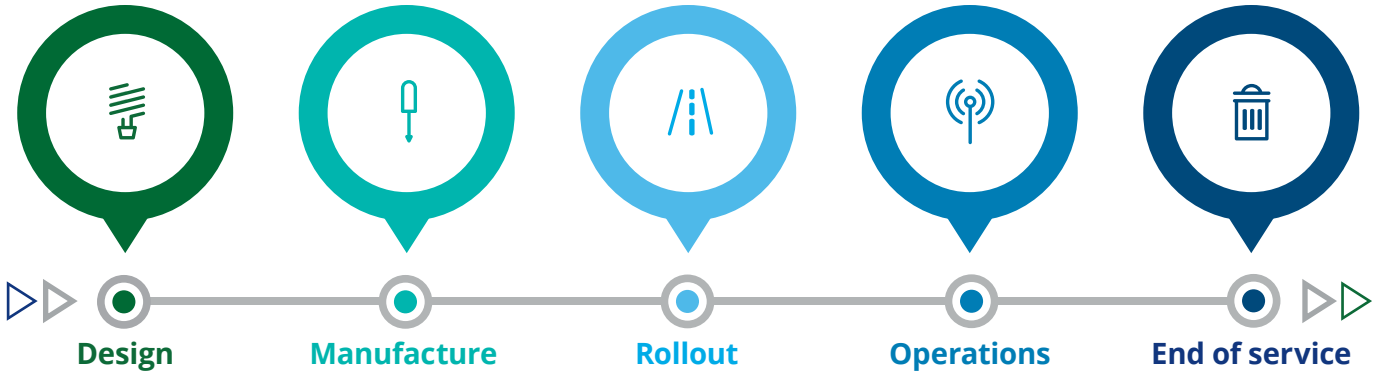
Figure 5. Defence-in-depth requires integration of cybersecurity within each layer of operation to ensure CASE vehicles and their users are protected and cyber-safe from the inside out



Shifting gears to accelerate cybersecurity

Stakeholders can effectively participate in a shared responsibility model by embedding various cybersecurity capabilities into their operations. From infrastructure protection and vulnerability assessments to privacy considerations and ongoing security monitoring, these capabilities will enable transportation organizations to confidently undergo the required digital transformation. For adopters of CASE technologies, we organize considerations for the life cycle of CASE vehicles into five stages: design, manufacture, rollout, operations, and end of service (Figure 6).

Figure 6. Cybersecurity considerations for CASE vehicle life cycle



	Design	Manufacture	Rollout	Operations	End of service
Stakeholders	• OEMs • Tier 1, 2, and 3 suppliers • Governing bodies and legislative agencies	• OEMs, Tier 1, 2, and 3 suppliers • Drone manufacturers • CASE vehicle retrofit/ installers • CASE software development companies	• CASE business consumers, logistics, and first/middle/last-mile solutions • Application security testing and telecommunication companies	• CASE business consumers, logistics, and first/middle/last-mile solutions • After-market software solution companies	• CASE business consumers • Logistics • First/middle/last-mile solutions
Cyber capabilities	• Data protection and privacy policies • Compliance assurance for data, testing, and integration • Maturity and readiness assessments for CASE vehicle integration • Governance structures, roles, and responsibilities for managing cyber risks • CASE vehicle cybersecurity training and awareness	• Third-party risk and controls assessments • Vulnerability reporting and tracking • Secure SDLC integration • Identity and access management • Endpoint protection • On-premises and cloud infrastructure security considerations	• In-vehicle intrusion detection and prevention • System configuration • Secure patching and OTA update provisioning • Cybersecurity contracts and SLA review • Threat intelligence and analysis • Application testing (SAST/DAST)	• Cyber risk dashboarding and reporting • Incidence response and management • Tabletop exercise training and simulation • DevSecOps • Post-incident analysis and forensics • Strategic growth for adoption of emerging technologies (5G, edge computing, blockchain, etc.)	• Secure deprovisioning of software and hardware • Data retention (in house and third party) • Compliance with regulations and policies at end of life cycle • Cyber risks of reselling CASE vehicles • Infrastructure and cloud considerations for termination of service • Device profiling and contract termination

Design

Throughout these stages, the various players can enable successful operations by embedding cybersecurity practices that ensure the safety, reliability, and privacy of people, processes, and technology across the board.

Governing bodies should lead the way by providing frameworks and regulations to guide all stakeholders along the entire production life cycle. These can include best practices for maturity and risk assessments and standards for safe CASE vehicle testing and deployment on public roads. It's important that they establish the allocation of responsibilities across the automotive production chain, fortified by methods for attestation to guidelines and best practices. Safe integrations within public infrastructure and guidelines on data privacy and testing requirements for CASE vehicles are also needed to ensure that cyber within transportation stimulates economic growth while protecting citizens.

Tier 1, 2, and 3 suppliers and OEMs can then use these standards to guide the cybersecurity-integrated design of CASE vehicles. Cyber risk management should be calibrated in existing governance structures, with roles and responsibilities clearly articulated. From there, the pre-set guidelines and regulatory requirements can guide the way for compliance assurance. This can include security considerations for the digitalization and procurement of core processes, maturity assessments for CASE vehicle production, strategizing post-production CASE testing, and CASE vehicle data storage and use. Stakeholders at this stage can benefit from the alignment of their cybersecurity strategy with organizational objectives. For example, a last-mile solution provider can identify its sustainability and customer satisfaction improvement goals over the next five to 10 years, and then leverage CASE technologies to address them simultaneously by implementing automated trucks that optimize routes, getting products to their destination faster and with fewer emissions.

Manufacture

As CASE vehicle designs move to the manufacturing phase, cybersecurity capabilities that consider the amalgamation of components in the various integrated systems (ADAS, infotainment, and real time operating systems (RTOS), etc.) will be crucial. For OEMs, this involves performing threat-risk assessments and identifying risks in third-party partnerships with software provisioning companies and Tier 1, 2, and 3 suppliers.

First, key security controls should be integrated into each stakeholder's own operations, from manufacturing to supply chain processes and everything in between. Improperly configured security on CASE vehicles can easily create points of entry to the entire process. Mobile applications, infotainment applications, OTA processes, and all integrations should also be secured.

At all stages, software providers, component manufacturers, cloud providers, and CSPs should simultaneously perform their own threat-risk assessments. Manufacturers must clearly set the standards for the supply chain and identify security requirements in the design. That way, their products can be assured for compliance prior to being integrated within the vehicle. Software, hardware, component hardening, encryption, storage, and the management of data are all key considerations that will be required for each integrated system.

Integrating these considerations into the manufacturing stage of the CASE vehicle production life cycle can protect stakeholders from a plethora of vulnerabilities as they create products that can be trusted by their consumers.

Rollout

Once manufactured, CASE vehicles will need to be tested before a full-scale rollout. Given the various requirements mandated by governing bodies on the testing of CASE vehicles, ensuring compliance should be a top priority. Reinforcement of security through penetration testing of CASE vehicles, risk-based scoping via threat vectors, and testing the functions and components of the overall platform are important considerations. OEMs should also work closely with CSPs to define ranges of connectivity and communication requirements, and to secure visibility over CASE vehicles once in the field.

For CASE vehicle business consumers, these technologies should be piloted to assess for any unforeseen vulnerabilities and risks prior to full ecosystem integration. A successful launch also requires a secure-by-design approach with protection of core infrastructure security and operations, such as micro network segmentation to restrict lateral movement, at its core. Organizations should ensure visibility over the entire infrastructure, supplemented with security controls addressing the present threat surfaces. This extends to integrating identity capabilities based on the principles of least privilege and zero-trust to delegate access of and to CASE vehicles (for endpoint protection). With identity analytics, organizations can facilitate swift change management and conveniently manage secure access.

Business consumers and fleet owners should work closely with the appropriate third-party cloud infrastructure and CSPs to understand where and how CASE vehicles will operate and to define any risks. These considerations will facilitate safe and secure integration on a smaller scale as well as at full scale, depending on requirements, to bolster the organization's capabilities.

Operations

A top consideration during the operational stage is fostering trust in CASE vehicles through visibility and oversight. As technologies evolve toward V2V communication, secure-by-design should be reinforced with secure-by-integration. Organizations should explore the unique requirements of patching and updating CASE vehicles and keep an eye on critical security risks like zero-day vulnerabilities. This includes the quick remediation of available patches and implementing trusted processes to verify and implement OTA software updates. For upgrades to CASE technology, organizations will require partnerships with third-party providers. Here, cloud infrastructure and CSPs play a key role in the facilitation of secure services.

Security incidents have proven to be a matter of "when they happen" rather than "if they happen," so these measures can be facilitated by planning for the inevitable. Incident response plans will be critical and can be strengthened with table-top exercises and simulations to ensure readiness and test communication channels. Business continuity plans should be updated for responsivity to CASE vehicles and returning to normal as soon as possible.

As new developments in 5G, AI, quantum computing, software-defined networks, and blockchain continue to unfold, new implications for cyber and CASE vehicles will emerge. Manufacturers, consumers, and governing bodies alike should perform continued risk assessments to identify opportunities to reduce vulnerabilities. Players that enable the backbones of communications (such as CSPs and cloud infrastructure providers) should consistently evolve and incorporate best practices and a well-communicated strategy. Organizations that remain flexible and up to date in their capabilities will enhance the benefits attained from CASE vehicles as well as increase public trust in their services.

End of service

There are unique cybersecurity considerations for CASE technologies at the end of the life cycle. Once a CASE vehicle reaches the end of its operational life, it cannot simply be disposed of or sold. Its connective components (both hardware and software) should ideally be securely deprovisioned to ensure the protection of organizational data and assets.

The successful and safe termination of service also requires consideration of the infrastructure and cloud environments. The vehicle's access to the organization's physical and digital locations should be removed. The data curated by the CASE vehicle should be evaluated for retention requirements. Any stored data should be handled in accordance with the privacy laws and regulations of the region of operation (where the CASE vehicle was employed) and organizations should ensure compliance to their timelines. Third-party retention of data is also included at the stage.

Finally, for organizations wishing to resell a CASE vehicle, holistic device profiling that exposes potential risk surfaces should be completed. That way, no accidental access to organizational data or assets is possible. The termination of CASE vehicle service should be considered by all members of the production life cycle, including dealerships, temporary owners, and manufacturers. At this stage, good digital hygiene will prove invaluable to the safe and secure use of CASE vehicles.

Final thoughts

All global business will be impacted by the introduction of CASE technology in the next five years. Connectivity for telematics, diagnostics, entertainment, and varying levels of available autonomy has become table stakes for manufacturers. Even if a fleet owner or individual consumer does not wish to proactively engage in the new features, the connected vehicle is here to stay and should therefore be considered when reviewing the cybersecurity strategy of any business.

The responsibility is a shared one. Governments, regulators, fleet owners, OEMs, and other organizations along the supply chain will all play a part in the new opportunities and threats that present themselves in CASE vehicles and infrastructure. If they do not, the risk to privacy, data, and physical security will become a serious challenge to the adoption, utilization, and realization of the great opportunity this new technology presents.

Some final considerations:

1. To accommodate the multitude of new and emerging risks, security by design should be the new mantra across the entire automotive supply chain. Only then will cybersecurity become an enabler rather than an impediment to the fast and widespread adoption of CASE vehicles.
2. The role of government and regulators will be critical to the future of transit supply and infrastructure security. The need for cybersecurity standards and enforcement throughout the ecosystem needs to be addressed by regulators and governing bodies; the market won't wait for regulations to catch up with technology.
3. Business and technology leaders should fully consider all the risks of a hyperconnected fleet. Cybersecurity strategy should be extended to include these fleet assets at all levels to ensure risk and threats are controlled.
4. The responsibility for security, privacy and risk throughout the CASE value chain is shared to minimize the threats to businesses and guarantee the safety of users.

New opportunities created by CASE vehicles and infrastructure will continue to be transformative. Innovative product and service models will enable greater efficiency, competitive advantage, environmental compliance, and cost savings. The promise of new customers and increased market share for those who fully engage, means that few organizations are ignoring how connectivity and autonomy can impact their business. Concerns about security, while increasingly important, can and should be managed through the inclusion of a clear, inclusive strategy throughout the life cycle of CASE vehicles, from procurement to end of life. Understanding the shared security responsibilities and controlling them with a clear, managed risk posture will pave the road to added value on our journey into the hyperconnected future.

Endnotes

1. Transport Canada, "Connected and automated vehicles," May 7, 2021.
2. B. De Muynck, "The 2020 Top Strategic Transportation Technology Trends," June 9, 2020.
3. WHO, "Road traffic injuries," June 21, 2021.
4. United Nations, "68% of the world population projected to live in urban areas by 2050, says UN," May 16, 2018.
5. M. Sconci and D. Buksner, "LABOUR SHORTAGE IN THE TRUCKING INDUSTRY: FURTHER IMPACTS OF COVID-19," July 2020.
6. Government of Canada, "Zero Emission Vehicle Infrastructure Program," December 21, 2021.
7. Upstream Security Limited, *2022 Global Automotive Cybersecurity Report*, Upstream Security Limited, 2022.
8. M. DeGeurin, *Teen Security Researcher Claims He Can Remotely Access 25 Teslas Around the Globe*, Gizmodo, 2022.
9. Deloitte, "Future of cyber survey," 2021.
10. UNECE, "WP29 World Forum for Harmonization of Vehicle Regulations (WP.29)," 2021. [Online].
11. Gartner, "How Automotive CIOs Can Lead a Successful Cybersecurity Implementation and Comply With WP.29 UN R155,".
12. ISO, "ISO/DIS 24089 Road vehicles — Software update engineering," 2021.
13. ISO, "ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering," August 2021.
14. SAE International, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," January 14, 2016.

Contact

Stephen Meagher
Director, Risk Advisory
416-202-2319
smeagher@deloitte.ca

Contributors

Damu Prabhu
Partner, Risk Advisory

Vaibhav Jani
Senior Manager, Risk Advisory

Noorullah Nouri
Senior Consultant, Risk Advisory

Aawista Chaudhry
Consultant, Risk Advisory

William Chinnery
Analyst, Risk Advisory

Leon Nash
Partner
Risk Advisory and CASE Vehicles Leader

Darren Plested
Partner
National Automotive Sector and
Transportation Innovation Leader

Yvonne Rene de Cotret
Partner
National Consumer Transport Sector and
Future of Mobility Leader

Andrew Pau
Partner
National GPS Transport Sector Leader and
BC Cluster Leader

Acknowledgements

The authors would like to thank the following Deloitte leaders who provided additional research and review support for this paper:

Amir Belkhelladi, Ashok Divakaran, Noemi Chanda, Don MacPherson, Marc MacKinnon, D'Arcy Moynaugh, Justin Fong, Kevvie Fowler, Ryan Robinson, Dejan Markovic, Ryan Ernst, Sima Gupta, Ian Davidson, and **Bear Zak.** The insights received from **Ian Todd, Bob Oates, Rita Barrios** and **Aditya Deshpande** from **BlackBerry Limited** as well as **Raed Kadri, Head of the Ontario Vehicle Innovation Network (OVIN)** also helped us shape this paper.

About Deloitte

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our Shared Values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.

To learn more about Deloitte's approximately 330,000 professionals, over 11,000 of whom are part of the Canadian firm, please connect with us on LinkedIn, Twitter, Instagram, or Facebook.

© Deloitte LLP and affiliated entities.
Designed and produced by the Agency | Deloitte Canada. 22-5608617