IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

AUTONOMOUS GROUND VEHICLE SECURITY GUIDE: Transportation Systems Sector

AUTONOMOUS GROUND VEHICLES IN THE TRANSPORTATION SYSTEMS SECTOR

Autonomous vehicle (AV) technology will revolutionize how people and goods move within communities and across the country. Although fully autonomous vehicles are not common in the transportation landscape,[1] many companies and communities are carrying out pilots for supervised semi-autonomous trucks, shuttles, and delivery services. The U.S. Department of Transportation (USDOT) estimates that more than 80 companies are currently testing AVs across 40 U.S. states and Washington, D.C., and more than half of states have introduced legislation to allow testing on public roads.[2]

AVs represent a leading-edge technology in the evolution of 'Smart Cities,' where infrastructure relies on Internet of Things (IoT) devices to operate effectively. This includes AVs as a viable means for trucking, last-mile delivery, and mass transit—often referred to as mobility-as-a-service—which can benefit organizations and communities through improved mobility, access, and speed; decreased environmental impacts; enhanced safety; improved public transit options; reduced operating costs; and a shift from fixed-route, fixed-timetable services to dynamic, on-demand services.

But in addition to their benefits, these cyber-physical systems (CPS) can also increase vulnerability to physical and cyber attacks at the enterprise and asset level. The Cybersecurity and Infrastructure Security Agency (CISA) developed this product to help Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs) understand the risks associated with AVs and implement strategies that can greatly reduce risk to people and property.

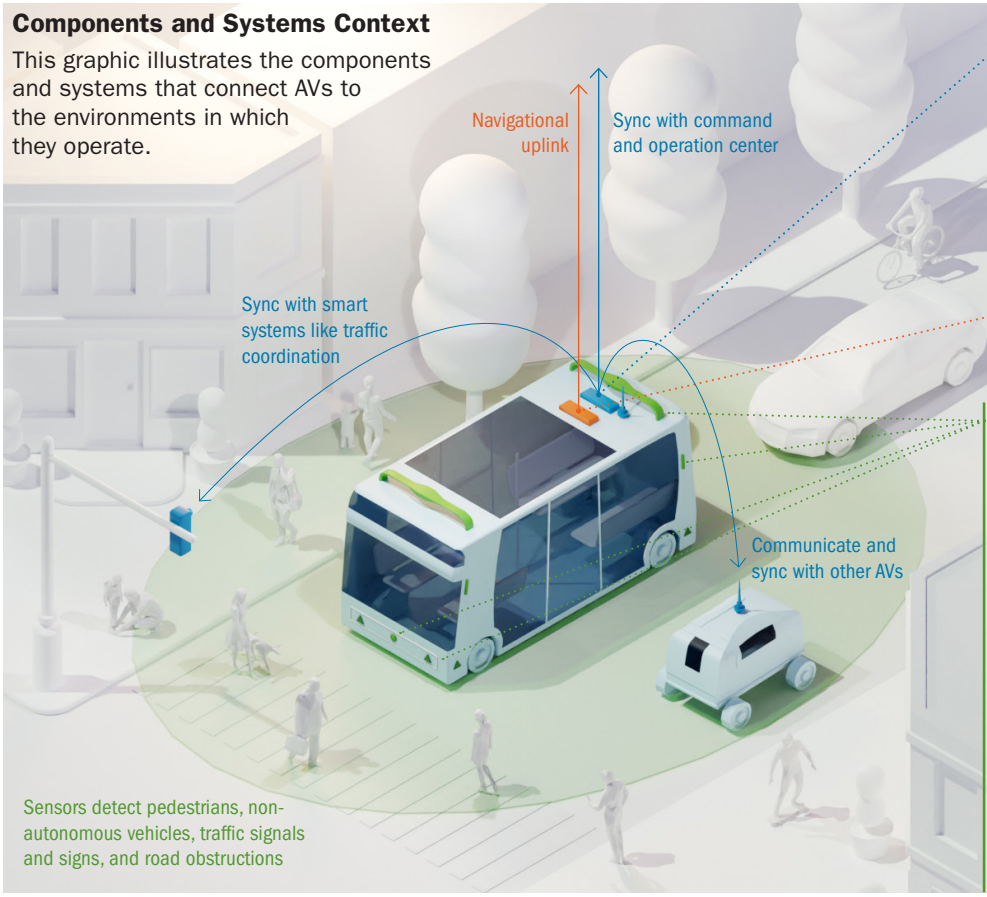
AV Technology in Action

In 2020, the NURO R2 became one of the first autonomous driving systems deployed on public roadways, making it a benchmark for AVs in the transportation landscape.

Source: nhtsa.gov/press-releases/nhtsa-grants-nuro-exemption-petition-low-speed-driverless-vehicle

Components and Systems Context

This graphic illustrates the components and systems that connect AVs to the environments in which they operate.



Operation and Communication Systems

Vehicle-to-everything (V2X) Technologies, such as 5G, enable communication to and from an AV system.

Parallel computing enables advanced information processing from vehicle sensors and operating systems.

Dedicated Short Range Communications (DSRC) communicate and sync capabilities with other AVs.

Global Navigation Satellite Systems / Inertial Navigational Systems (GNSS/INS) ensure accurate position, velocity, acceleration, and heading data for autonomous operation.

Sensor Systems

Light Detection and Ranging (LiDAR) uses light pulses to estimate distance and create high-resolution 3D images of the environment and road.

High-frequency acoustic sensors use audio waves to measure distance to an object.

Radio Detection and Ranging (RADAR) relies on radio waves to enable braking assistance applications and sensors that monitor blind spots for distance control.

Monocular cameras allow an AV to gather 3D images of its surroundings.

Stereo cameras capture images from two viewpoints to triangulate depth information.

Traffic-sign Recognition (TSR) uses forward-facing cameras to recognize and interpret traffic signs on roadways.

1 The Society of Automotive Engineers (SAE) classifies fully autonomous ground vehicles at levels 4 and 5 of SAE J3016. Many vehicles are SAE level 2 with connected capabilities and some degree of automation. They share technologies with higher level vehicles and pave the way toward full autonomy.

2 Department of Transportation, *Preliminary Analysis of Potential Workforce Impacts Report*, January 2021, transportation.gov/av/workforce/report.

UNDERSTANDING AV SECURITY RISKS AND UNIQUE CHALLENGES

As the CPS threat landscape continues to evolve, organizations will become increasingly vulnerable to attacks that can result in data breaches, supply chain disruptions, property damage, financial loss, injury, and loss of life. CSOs and CISOs should proactively monitor and manage AV technology risks using holistic security strategies that address both enterprise and asset vulnerabilities related to CPS integration with broader connected networks.

CISA's Autonomous Vehicle Cyber-Attack Taxonomy (AV|CAT) tool provides a framework for identifying AV risks based on the **attack vectors, targets, consequences,** and **outcomes** associated with a specific cyber-physical attack. Organizations can use the AV|CAT to understand risks related to AV technology integration, as well as risks to the AVs themselves and other physical assets. The tool offers a baseline for conceptualizing attack sequences and predicting an attack's ripple effects. Security teams can use the taxonomy to trace how a malicious actor can exploit a vulnerability, assess potential impacts, and identify associated risk mitigation strategies to enhance future resilience. The following scenarios use the CISA AV|CAT to illustrate examples of enterprise- and asset-level risks related to AVs:

ATTACK VECTOR	TARGET	CONSEQUENCE	OUTCOME
Pathway a malicious actor takes to access a targeted system	*System a malicious actor seeks to exploit*	*Harm resulting from an attack; classifies overall intent*	*Real-world result caused by the attack*

ENTERPRISE LEVEL RISK — COMPROMISING AV NETWORK SECURITY

ATTACK VECTOR	TARGET	CONSEQUENCE	OUTCOME
Malicious actor **gains unauthorized access to a network**, such as via a control room, and uses a USB to introduce malware	**Connected AVs and privileged networks** are targeted	**Proprietary and sensitive information could be disclosed** and connected assets could become inaccessible	Compromised company data and connected AV assets could result in **operational impacts and financial losses**

ENTERPRISE LEVEL RISK — EXPLOITING AV SUPPY CHAIN VULNERABILITIES

ATTACK VECTOR	TARGET	CONSEQUENCE	OUTCOME
Malicious actor **works with an insider at a third-party supplier** to nefariously modify data processing motherboards	External device could **remotely load malware** targeting networks and AV driving control, autonomy, and security systems	**Proprietary or sensitive information could be disclosed** and AVs could cease to function properly	Inoperable AVs could lead to **cascading supply chain impacts** and compromised data could result in **security/operational impacts and financial losses**

ENTERPRISE LEVEL RISK — REMOTELY DISABLING AV FLEETS

ATTACK VECTOR	TARGET	CONSEQUENCE	OUTCOME
Cyber criminal **creates privileged credentials to access an AV fleet's anti-theft system** and marks all vehicles as stolen	**Security systems** are targeted	Impacted AVs could become **inaccessible, stolen, or subject to tampering**	Compromised AVs cease to operate properly, causing **operational/supply chain disruptions and financial losses**

ASSET LEVEL RISK — DISRUPTING AV SENSORS

ATTACK VECTOR	TARGET	CONSEQUENCE	OUTCOME
Malicious actor **uses paint and reflective stickers to alter information an AV relies on** to gauge its surroundings, such as a stop sign	**AV hardware sensors and hardware sensor inputs** are targeted and could cease to function properly	**AV could malfunction** and performance could be degraded	AV malfunction could cause **a collision involving people or property, disrupt traffic patterns, or could cease to operate**

ASSET LEVEL RISK — KEYLESS RELAY THEFT

ATTACK VECTOR	TARGET	CONSEQUENCE	OUTCOME
Malicious actor near a corporate facility or AV fleet yard **intercepts the keyless entry signal to an AV** to gain access to the vehicle	**Driving control systems and security systems** are targeted	Impacted AVs could become **inaccessible, unreliable or inoperable due to tampering, or stolen**	Assets could be stolen, resulting in **financial losses**, or AVs could become **inaccessible or cease to operate properly**

ASSET LEVEL RISK — AV RAMMING ATTACK

ATTACK VECTOR	TARGET	CONSEQUENCE	OUTCOME
Malicious actor **gains access to an AV's On-Board Diagnostic (OBD-II) port**, uploads malware to bypass primary systems, and assumes remote control of the AV	**Driving control systems and security systems** are targeted	**Impacted AVs could become inaccessible** and the owner could be unable to regain control to prevent an attack	Compromised AVs could be **stolen, used to cause an accident, used to target public gathering spaces, or used for malicious cargo delivery**

ENTERPRISE AND ASSET RISK MITIGATION STRATEGIES

Securing AVs, like any other CPS, requires a multi-layered approach that evaluates threats to the *enterprise*, such as compromised proprietary data or operational disruptions, and to *assets*, such as an AV itself. Organizational resilience will increasingly rely on a converged approach to physical security and cybersecurity.

Prioritizing **communication, coordination, and collaboration** across security functions and the supply chain can enhance organizational operations and optimize strategies to reduce risk. In addition to CISA's recommended best practices, consider incorporating both enterprise- and asset-level risk mitigation strategies into security plans.

The Price of Inaction

Failing to manage cybersecurity risks related to AV systems could have significant impacts—**a single cyber incident today could cost an automaker up to $1.1 billion.**

Source: upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/

ENTERPRISE Risk Mitigation

Once CSOs and CISOs analyze risks using the AV|CAT framework, security teams can develop measures to minimize an enterprise-level attack. Consider the following enterprise risk mitigation strategies:

Develop and implement employee training and exercises to ensure on-the-ground personnel are aware of interconnected cyber-physical risks. Employees working with CPS devices should understand the potential impacts of a targeted attack and how best to respond.

Ensure physical access points to networks and systems are secure, including connected and non-connected building security systems. Maintain detailed access control logs and asset management lists.

Conduct vulnerability assessments to identify specific organizational vulnerabilities to inform an enterprise security strategy. Connect with CISA Protective Security Advisors (PSAs) and Cybersecurity Advisors (CSAs) for help with vulnerability assessments.

Report vulnerabilities and cyber-physical incidents immediately to the appropriate authorities. Maintain an open dialogue with federal, state, and local law enforcement, and CISA.

Analyze threats to cyber-physical AV systems on a recurring basis using CISA's AV|CAT framework, and update emergency response plans to anticipate future threats.

Leverage CISA's tools and resources to help identify vulnerabilities malicious actors could exploit. Subscribe to CISA Cybersecurity Alerts and CISA Insights to stay up-to-date on threat vectors.

Adopt and implement system security guidance, best practices, and design principles from the National Institute of Standards and Technology (NIST), the Automotive Information Sharing and Analysis Center (Auto-ISAC), and other established organizations.

Formalize collaboration across organizational security functions and integrate physical security and cybersecurity best practices into standard processes. Refer to the CISA *Cybersecurity and Physical Security Convergence Guide* for a convergence framework for developing a holistic security strategy.

Develop and implement an insider threat mitigation program to reinforce a culture of shared responsibility and asset protection. Refer to CISA's *Insider Threat Mitigation Guide* for more information on establishing an insider threat prevention and mitigation program.

ASSET Risk Mitigation

Enterprise risk mitigation strategies should extend to securing connected assets, including AVs. Consider the following asset risk mitigation strategies:

Conduct application, network, firmware, and hardware cybersecurity testing to identify vehicle cybersecurity vulnerabilities and attack vectors.

Implement recommended vehicle software updates regularly. Like a computer, AVs require frequent software updates to improve and maintain security and usability.

Avoid connecting non-manufacturer, unsecured, or unknown devices to vehicle systems, including connected devices outside of the AV ecosystem, which can contain malware.

Monitor vehicles for signs of physical access or tampering, such as unknown devices connected to OBD-II ports, spliced wires, or indications of a removed dashboard and report suspicious activity.

Prevent unauthorized physical access to vehicles by storing fleets in secure locations, locking doors, and safeguarding key fobs. Minimize unauthorized access to prevent tampering or accidental alterations.

Configure devices and services to the most secure default settings. Consult with manufacturers to learn how default settings could be modified to create vulnerabilities.

Ensure personnel understand advanced driver-assistance systems (ADAS) and how to disable and re-enable ADAS features to limit potential attack vectors and ensure proper functionality.

Design, develop, and implement cybersecurity standards for connected vehicles and associated components (e.g., infotainment systems, controller area networks, and sensors) through product and ecosystem reviews, remediation engineering, and supply chain security.

Safeguarding communities that rely on connected infrastructure requires a collaborative approach across the public and private sectors to address complex threats. Early adopters of this technology should leverage all available resources to understand and anticipate physical and cyber risks.

ADDITIONAL CISA RESOURCES:

Cybersecurity and Physical Security Convergence Guide:
cisa.gov/publication/cybersecurity-and-physical-security-convergence

Cyber Hygiene Services:
cisa.gov/cyber-hygiene-services

Cyber Resource Hub:
cisa.gov/cyber-resource-hub

Cyber Incident Response:
cisa.gov/cyber-incident-response

Cybersecurity Advisors:
cisa.gov/stakeholder-risk-assessment-and-mitigation

Cybersecurity Assessment:
cisa.gov/cybersecurity-assessments

Infrastructure Vulnerability Assessments:
cisa.gov/critical-infrastructure-vulnerability-assessments

Insider Threat Mitigation:
cisa.gov/insider-threat-mitigation

Protective Security Advisors:
cisa.gov/protective-security-advisors

Ransomware Guide:
cisa.gov/publication/ransomware-guide

Securing Public Gatherings:
cisa.gov/securing-public-gatherings

Vehicle Ramming Awareness:
cisa.gov/publication/active-assailant-security-resources

CISA Critical Infrastructure Exercises:
cisa.gov/critical-infrastructure-exercises

CISA 5G Security and Resilience:
cisa.gov/5g

For more information or to seek additional help, contact us at Central@cisa.gov