CROSS-COLLABORATING TO SECURE AUTONOMOUS GROUND VEHICLES AND OTHER EMERGING TECHNOLOGIES AGAINST THE THREATS OF TOMORROW

Benjamin Gilbert
June 1, 2022

CISA – An Organizational Approach

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

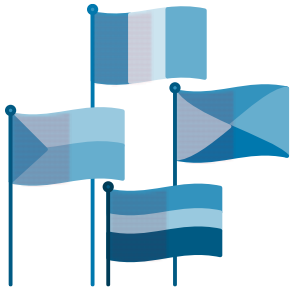
Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborates with industry to build more secure and resilient infrastructure for the future

CYBER THREAT LANDSCAPE

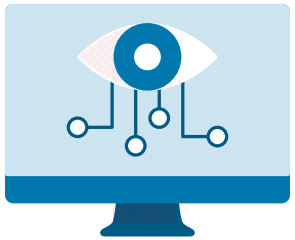
AV | CAT Threat Sources

CISA has identified five types of cyber threat sources that may be interested in AVs as a new target for cyber attacks

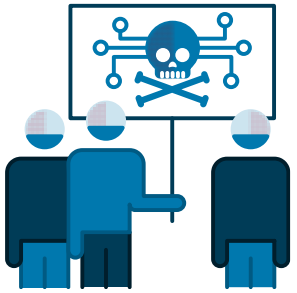


National Governments

Terrorists



Industrial Spies and Organized Crime



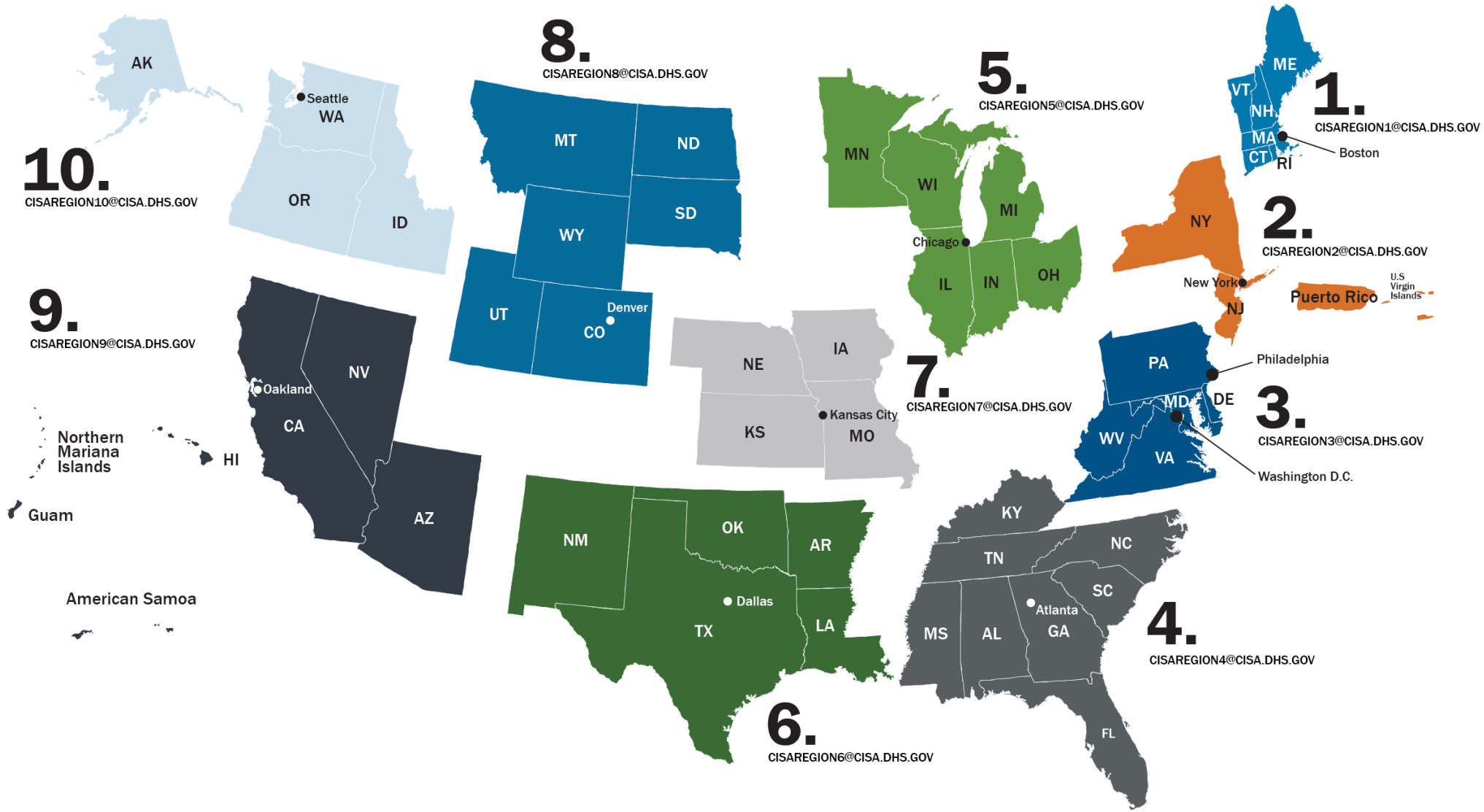
Hacktivists

Hackers

Source: https://us-cert.cisa.gov/ics/content/cyber-threat-source-descriptions

CISA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



CISA Operational Priorities

CYBER SUPPLY CHAIN AND 5G

CISA is focused on supply chain risk management in the context of national security. CISA is looking to reduce the risks of foreign adversary supply chain compromise in 5G and other technologies.

ELECTION SECURITY

CISA assists state and local governments and the private sector organizations that support them with efforts to enhance the security and resilience of election infrastructure. CISA's objective is to reduce the likelihood of compromises to election infrastructure confidentiality, integrity, and availability, essential to the conduct of free and fair democratic elections.

SOFT TARGET SECURITY

As the DHS lead for the soft targets and crowded places security effort, CISA supports partners to identify, develop, and implement innovative and scalable measures to mitigate risks to these venues; many of which serve an integral role in the country's economy.

FEDERAL CYBERSECURITY

CISA provides technology capabilities, services, and information necessary for agencies across the Federal civilian executive branch to manage sophisticated cybersecurity risks. CISA's authorities enable deployment of robust capabilities to protect Federal civilian unclassified systems, recognizing that continuous improvement is required to combat evolving threats. CISA also works to help State, Local, Tribal and Territorial governments improve cybersecurity and defend against cybersecurity risks.

INDUSTRIAL CONTROL SYSTEMS

CISA leads the Federal Government's unified effort to work with the Industrial control systems (ICS) community to reduce risk to our critical infrastructure by strengthening control systems' security and resilience.

Supply Chain Security

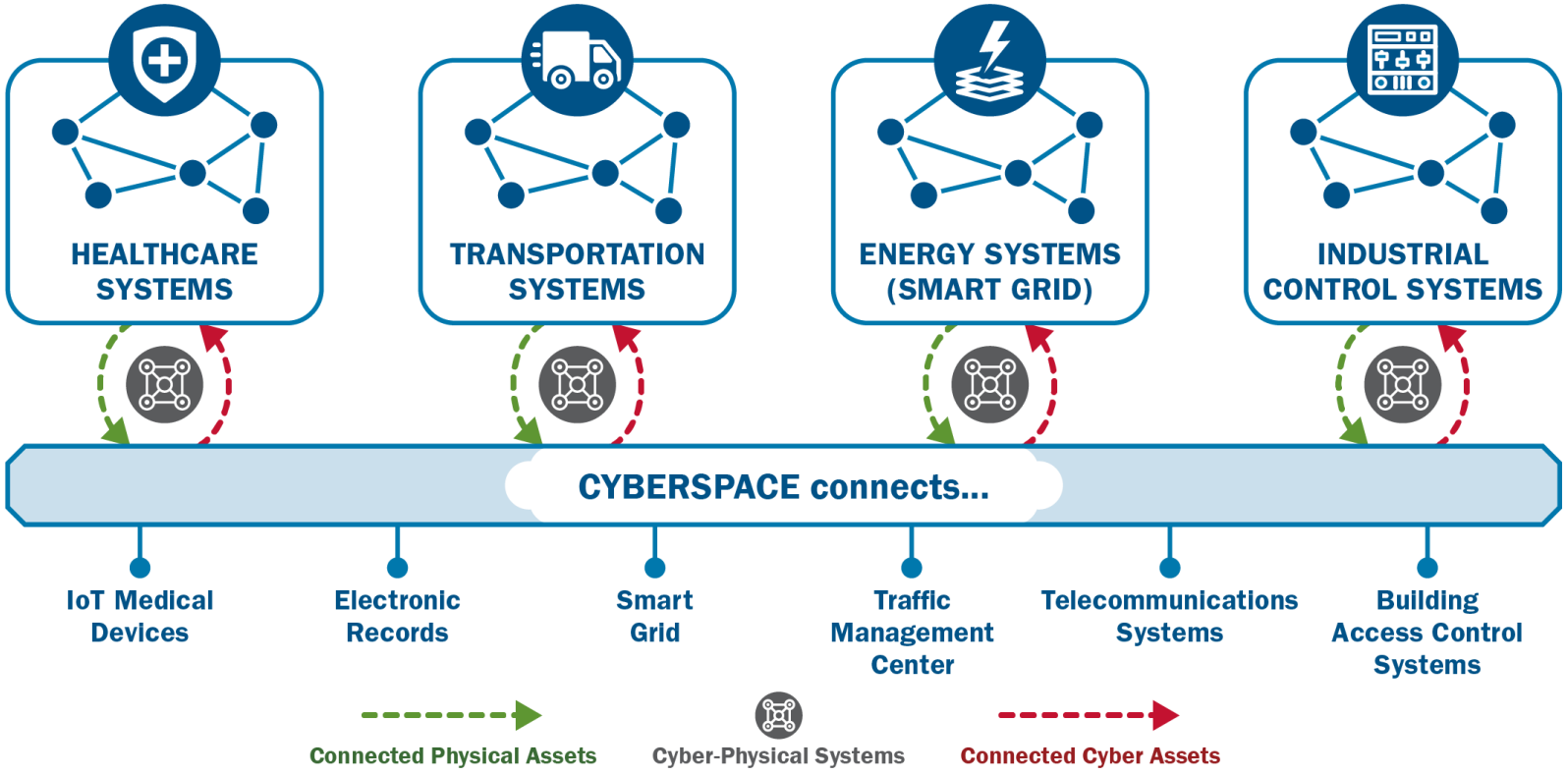
Cyber-Physical Convergence: IT vs. OT

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
ENDPOINT DETECTION	Common & widely used	**Can be difficult to deploy**
TECHNOLOGY LIFECYCLE	3 to 5 years	**Up to 30+ years**
APPLICATION OF PATCHES	Regular/ scheduled	**Slow; often unpatchable**
CHANGE MANAGEMENT	Regular/ scheduled	**Legacy based – unsuitable for modern security**

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
AVAILABILITY REQUIREMENTS	variable, depending on asset	**24 x 7 x 365 x forever (Integrity also critical)**
SECURITY AWARENESS	Good in both private and public sector	**Generally poor inside the control zone**
SECURITY TESTING/ AUDIT	Scheduled and mandated	**Occasional testing for outages / audit for event recreation**
PHYSICAL SECURITY	Secure	**Traditionally good**

A Connected Operating Environment

Today's threats are targeting **both physical and cyber assets** through sometimes sophisticated **hybrid attacks** with potentially disruptive impacts to data, property, and physical safety



SHIELDS UP

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
    - Cyber Hygiene Services
    - Risk and Resilience-based Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - Remote Assistance
  - Incident Coordination
  - Threat intelligence and information sharing
  - Malware Analysis
- **Cybersecurity Advisors**
  - Incident response coordination
  - Cyber assessments
  - Workshops
  - Working group collaboration
  - Advisory assistance
  - Public Private Partnership Development

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email report@cisa.dhs.gov | visit https://www.cisa.gov

Autonomous Ground Vehicle Security Guide

- **Goals:** Understand the risks associated with autonomous ground vehicles (AGVs) and implement mitigation strategies that reduce risk to people and property
- **Audience:** Chief Security Officers (CSOs) and Chief Information Security Officers (CISOs) of first adopters of autonomous vehicles such as trucking, last-mile delivery, and mass transit
- Autonomous Ground Vehicle Security Guide: Transportation Systems Sector

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.

Navigational uplink

Sync with command and operation center

Sync with smart systems like traffic coordination

Communicate and sync with other AVs

Sensors detect pedestrians, non-autonomous vehicles, traffic signals and signs, and road obstructions

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 towards full autonomy.

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

cisa.gov | Central@cisa.gov | LinkedIn.com/company/cisagov | @CISAgov | @cyber | @uscert_gov | Facebook.com/CISA | @cisagov

CISA Autonomous Vehicle Cyber-Attack Taxonomy (AV|CAT)

ATTACK VECTOR

Pathway a malicious actor takes to access a targeted system

TARGET

System a malicious actor seeks to exploit

CONSEQUENCE

Harm resulting from an attack; classifies overall intent

OUTCOME

Real-world result caused by the attack

SHIELDS UP

Call-to-Action: Recommended Steps to Take Today!

1. **Become familiar with CISA and the "Shields Up" webpage**
   - www.cisa.gov/shields-up
2. **Subscribe to the CISA Email Listing**
   - www.cisa.gov/subscribe-updates-cisa
3. **Engage with your local CSA and CSC**
   - https://www.cisa.gov/cisa-regions
4. **Sign-up for CISA's cyber hygiene services and resilience assessments**
   - Engage your local CSA
5. **Lower your reporting thresholds**

No-Cost CISA Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - Information / Threat Indicator Sharing
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - 24/7 Response assistance and malware analysis
  - Incident Coordination
  - Threat intelligence and information sharing

- **Cybersecurity Advisors –** Regionally deployed advisors
  - Incident response coordination
  - Public Private Partnership Development
  - Advisory assistance and cybersecurity assessments

CISA Contact Information

Benjamin Gilbert, CISA Region 3, CSA **General CISA Inquiries**	Benjamin.gilbert@cisa.dhs.gov central@cisa.gov
CISA URL	https://www.cisa.gov
To Report a Cyber Incident to CISA	***Call 1-888-282-0870*** ***Email*** *report@cisa.gov* ***visit*** *https://www.cisa.gov*

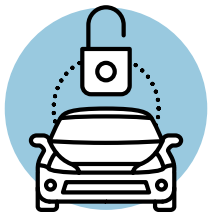

CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA

CISA Autonomous Vehicle Cyber-Attack Taxonomy (AV|CAT) Purpose and Development

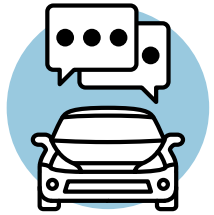
- The **Autonomous Vehicle Cyber-Attack Taxonomy (AV|CAT)** introduces a high-level and accessible language for studying and modeling potential cybersecurity threats with cyber-physical security outcomes.
- **Origins:**
  - Academic taxonomy and cyber attack framework review
  - Cyber attack analysis

Attack Vector

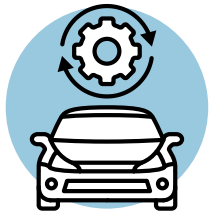
An ATTACK VECTOR is the path taken to a targeted system, which allows attackers to exploit that system's vulnerabilities



Physical Access



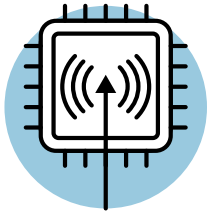
Communications



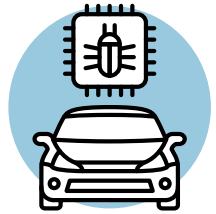
Software Updates

Connected Privileged System

Software Sensor Inputs



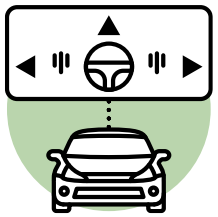
Hardware Sensor Inputs



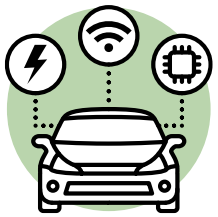
Malicious Hardware

Target

An attack vector is the pathway taken to the TARGET, the system a malicious actor seeks to exploit. These systems could be vectors to the target, or the end target themselves

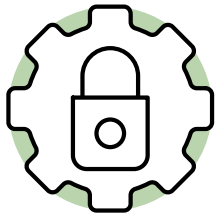


Driving Control Systems

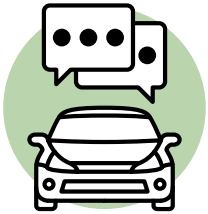


Auxiliary Control Systems

Autonomy Systems

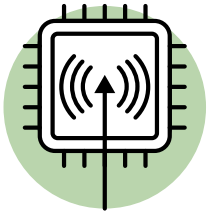


Security Systems



Communications

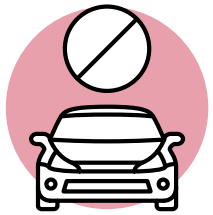
Software Sensor Inputs



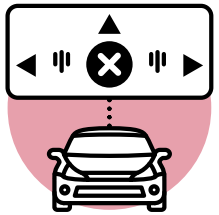
Hardware Sensor Inputs

Consequence

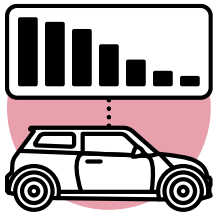
The CONSEQUENCE is the harm created by an attack and can be used to classify the overall intention of the exploit. Specifically, the harm to the vehicle system



Loss of Availability



Loss of Control

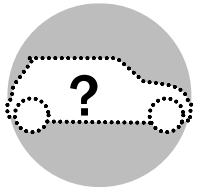


Performance Degradation

Information Disclosure

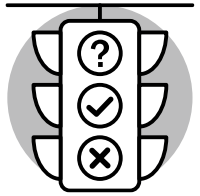
Outcome

The OUTCOME is the real-world result caused by an attack. The consequence may be considered the 'harm' to the vehicle system while the outcome is the real-world impact of that harm



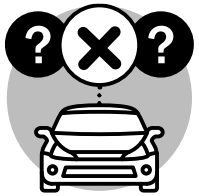
Theft

Malicious Cargo Delivery



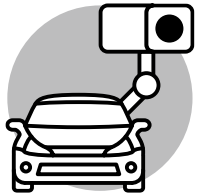
Disruption of Traffic Patterns

Vehicle Inaccessible

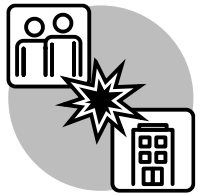


Vehicle Unable to Operate Properly

Spying



Surveillance

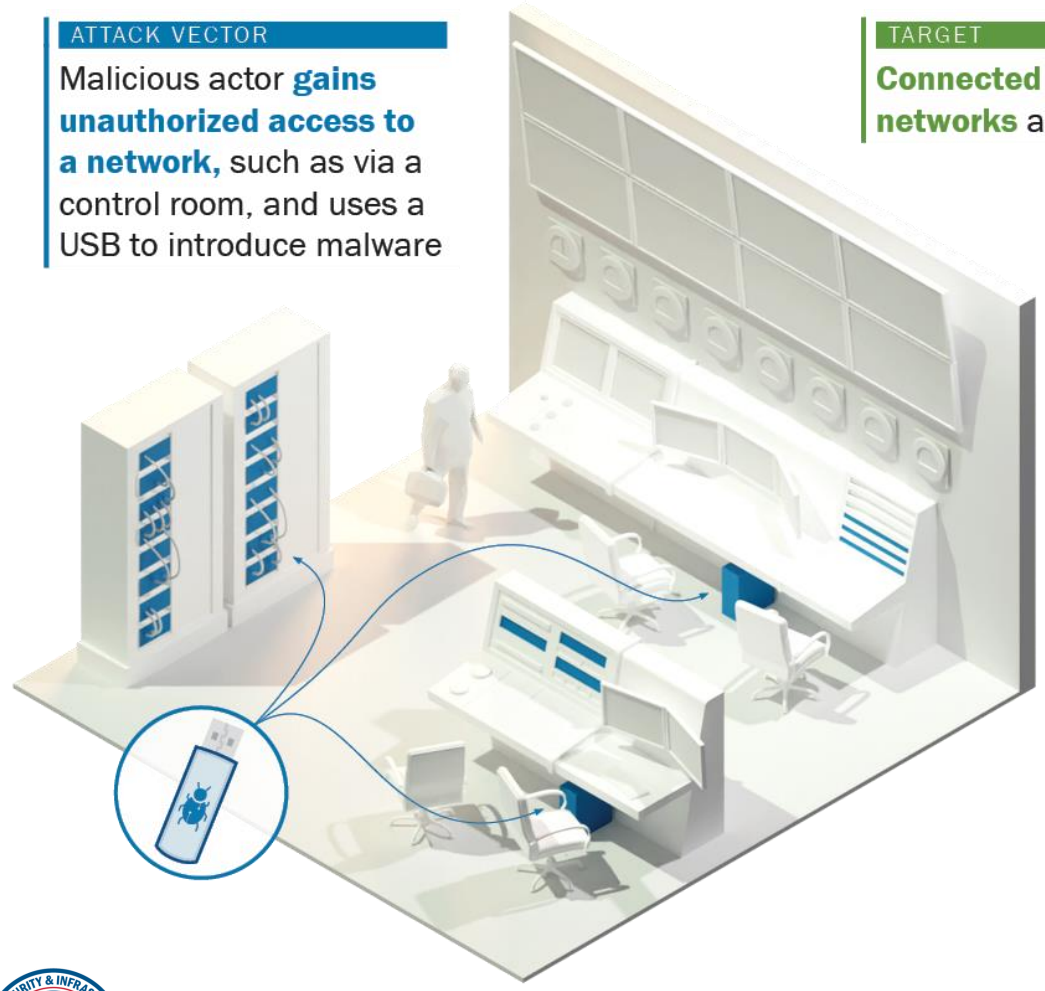


Harm to People or Property

AV | CAT Example – Enterprise: Compromising AV Network Security

ATTACK VECTOR

Malicious actor **gains unauthorized access to a network,** such as via a control room, and uses a USB to introduce malware

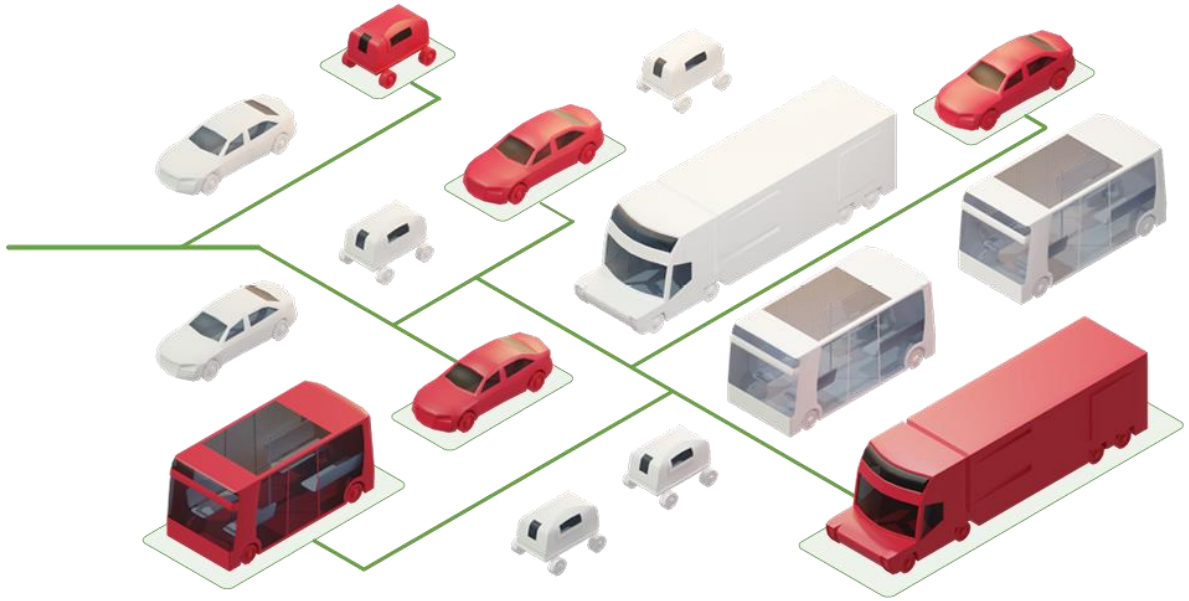


TARGET

Connected AVs and privileged networks are targeted

CONSEQUENCE

Proprietary and sensitive information could be disclosed and connected assets could become inaccessible



OUTCOME

Compromised company data and connected AV assets could result in **operational impacts and financial losses**

AV | CAT Example – Asset: Disrupting AV Sensors

ATTACK VECTOR

Malicious actor **uses paint and reflective stickers to alter information an AV relies on** to gauge its surroundings, such as a stop sign

TARGET

AV hardware sensors and hardware sensor inputs are targeted and could cease to function properly

CONSEQUENCE

AV could malfunction and performance could be degraded

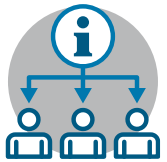
OUTCOME

AV malfunction could cause **a collision involving people or property, disrupt traffic patterns, or could cease to operate**

AV Risk Mitigation Strategies

Enterprise Security

Conduct vulnerability assessments; report vulnerabilities and cyber-physical incidents



Adopt and implement system security guidance, best practices, and design principles

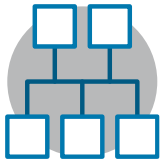
Formalize collaboration across organizational security functions

Asset Security

Conduct application, network, firmware, and hardware cybersecurity testing

Configure devices and services to the most secure default settings; implement recommended vehicle software updates regularly

Design, develop, and implement cybersecurity standards for connected vehicles and associated components



Design redundant and overlapping sensors to reduce single point failures

CISA.gov Resources

- **Autonomous Ground Vehicles Security Guide**
  cisa.gov/publication/autonomous-ground-vehicle-security-guide-transportation-systems-sector
- **Cybersecurity and Physical Security Convergence Action Guide**
  cisa.gov/publication/cybersecurity-and-physical-security-convergence
- **Insider Threat Mitigation**
  cisa.gov/insider-threat-mitigation
- **Cyber Resource Hub**
  cisa.gov/cyber-resource-hub
- **Cyber Hygiene Services**
  cisa.gov/cyber-hygiene-services
- **Cybersecurity Advisors**
  cisa.gov/csa
- **Protective Security Advisors**
  cisa.gov/protective-security-advisors
- **CISA Tabletop Exercises Packages**
  cisa.gov/cisa-tabletop-exercises-packages
- For more information or to seek additional help, contact us at Central@cisa.gov