



WELCOME TO AUTO-ISAC!





MONTHLY VIRTUAL COMMUNITY CALL

November 3, 2021

TLP:WHITE



DHS TRAFFIC LIGHT PROTOCOL (TLP) CHART

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

From: <https://www.us-cert.gov/tlp>

AGENDA

Time (ET)	Topic
11:00	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ What's Trending
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speaker: <ul style="list-style-type: none">▪ Ms. Katherine McClaskey, <i>DHS Program Lead, U.S. Department of Homeland Security (DHS)</i>
11:45	Around the Room <ul style="list-style-type: none">➤ Sharing Around the Virtual Room
11:55	Closing Remarks

WELCOME - AUTO-ISAC COMMUNITY CALL!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

Classification Level: **TLP:GREEN** - May be shared within the Auto-ISAC Community and “off the record”

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!
(sharmilakhadka@automotiveisac.com)



ENGAGING IN THE AUTO-ISAC COMMUNITY

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren't eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *“Cybersecurity is everyone's responsibility!”*



❖ Participate

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

22
OEM Members

21
Navigator Partners

❖ Share – *“If you see something, say something!”*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

43 *Supplier & Commercial Vehicle Members*

15
Innovator Partners

*Membership represents **99%** of cars and trucks on the road in North America*

*Coordination with **26** critical infrastructure ISACs through the National Council of ISACs (NCI)*



2020 - 2021 BOARD OF DIRECTORS

EXECUTIVE COMMITTEE (EXCOM)

2022-2023 Leadership
Coming Soon



Kevin Tierney
*Chair of the
Board of the Directors*
GM



Josh Davis
*Vice Chair of the
Board of the Directors*
Toyota



Jenny Gilger
*Secretary of the
Board of the Directors*
Honda



Tim Geiger
*Treasurer of the
Board of the Directors*
Ford



Todd Lawless
*Chair of the
Advisory Board*
Continental

2020 - 2021 ADVISORY BOARD (AB) LEADERSHIP



Todd Lawless
*Chair of the
Advisory Board*
Continental



Michael Feiri
*Vice Chair of the
Advisory Board*
ZF



Chris Lupini
Chair of the SAG
Aptiv



Larry Hilkene
Chair of the CAG
Cummins

MEMBER ROSTER

AS OF NOVEMBER 1, 2021

63 Members

Aisin	Hyundai	NXP
Allison Transmission	Infineon	Oshkosh Corp
Aptiv	Intel	PACCAR
Argo AI, LLC	John Deere Electronic	Panasonic
AT&T	Kia	Polaris
Blackberry Limited	Knorr Bremse	Qualcomm
BMW Group	Lear	Renesas Electronics
BorgWarner	LGE	Stellantis
Bosch (Ecrypt-Affiliate)	Luminar	Subaru
Continental (Argus-Affiliate)	Magna	Sumitomo Electric
Cummins	MARELLI	Tokai Rika
Denso	Mazda	Toyota
Faurecia	Mercedes-Benz	TuSimple
Ford	Meritor	Valeo
Garrett	Mitsubishi Motors	Veoneer
General Motors (Cruise-Affiliate)	Mitsubishi Electric	Volkswagen
Geotab	Mobis	Volvo Cars
Google	Motional	Volvo Group
Harman	Navistar	Waymo
Hitachi	Nexteer Automotive Corp	Yamaha Motors
Honda	Nissan	ZF

BUSINESS ADMINISTRATION

➤ Upcoming Key Events:

- **Members Teaching Members – December 15** **Speaker:** Jenny Gilger, Honda **Title:** Corporate Impact and Lessons Learned from a Global Ransomware Attack **TLP:AMBER**

➤ Community Call:

- **Wednesday, December 3 -** **Speaker:** Michael Daniel, Cyber Threat Alliance **Title:** *Combating Ransomware: Creating a Ransomware Incident Response Network* **Time:** 11 – 12:00 p.m. **TLP:WHITE**

➤ Announcements:

- **Auto-ISAC and NHTSA Training Cooperative Agreement** was finalized on September 29th.
- All Members' CISOs/Deputy CISOs are invited to join the newly created **CISO Executive Working Group** to share best practices and for inner-industry collaboration on response and deterrence of ransomware. **Please share with your CISO!**
- **Call for CC Speakers** – Might you want to speak? Please send your ideas to **Andrea Schunn**. We are working to build a list of speakers in advance of presentations for MBSC approval.
- Successful **2021 Auto-ISAC Cybersecurity Summit**.
- **Auto-ISAC Year-end Community Call Survey**, will be sent after December Community Call. Please provide your thoughts and recommendations for improvement of this monthly engagement.
- Please welcome new staff member **Paul Hamburg** to the Auto-ISAC Team.

PAUL HAMBURG

CYBERSECURITY TECHNICAL LEADER (CTL)

We would like to welcome a new addition to our Auto-ISAC Staff Team, **Paul Hamburg**. Paul recently earned both a BSIT (summa cum laude) and MSIT from Walsh College with a concentration in Automotive Cybersecurity. He was offered a teaching position prior to graduation and currently works as an adjunct professor teaching a concentration in cybersecurity and automotive cybersecurity.

Prior to joining our organization, Paul began working in the auto industry as a technician after completing an education degree. Consistently recognized for his diagnostic skills, he moved into management positions as the shop foreman. He then moved on to a field engineering position with the Development and emissions teams with VWAG. This career brought Paul and his family to Michigan in 2016 to join the OBDII team for VWAG. After leaving Volkswagen, Paul worked for a J2534 tool manufacturer performing end of line and field testing. Paul is active in several SAE EE Diagnostics and Security committees and currently chairs J1930. Paul brings considerable experience in multiple facets of the automotive industry paired with current cybersecurity knowledge to Auto-ISAC.





AUTO-ISAC INTELLIGENCE

TLP:WHITE



AUTO-ISAC INTELLIGENCE

- Know what we track daily by subscribing to the DRIVEN
 - Send feedback, contributions or questions to analyst@automotiveisac.com
- Know our strategic perception of and outlook for the cyber threat environment by reading the 2020 Threat Assessment in the Auto-ISAC 2020 Annual Report. The 2021 Annual Report and Threat Assessment are in production.
 - Email us to request the report, provide feedback, or ask questions.
- **Intelligence Notes**
 - Study the “Trojan Source” vulnerabilities ([CVE-2021-42574](#), [CVE-2021-42694](#)) and assess the risk to your products, business networks, industrial systems, and their respective supply chains ([Trojan Source](#), [The Hacker News](#), [KrebsonSecurity](#)).
 - Cyber threat actors are increasingly conducting phishing attacks on smartphones. Monitor phishing tactics, techniques, and procedures threat actors use to attack smartphones and evolving malware capabilities, and assess risk implications for your products, business networks, industrial systems, and their respective supply chains ([ZDNet](#), [BleepingComputer](#)).
 - Like other industries, open-source reporting has noted a year-over-year increase in ransomware attacks on automotive organizations ([ThreatPost](#), [Fortinet](#), [Black Kite](#)).

CISA RESOURCE HIGHLIGHTS



TLP: WHITE – CISA Infrastructure Security Month 2021

- **2021 Theme- "Critical Infrastructure Security and Resilience: Build It In"**
- **Four (4) Weekly Themes:**
 - **Interconnected and Interdependent Critical Infrastructure: Shared risk means building in shared responsibility**
 - **Plan for Soft Target Security: Build in security for mass gatherings starting with your planning**
 - **Build Resilience into Critical Infrastructure**
 - **Secure our Elections: Build resilience into our democratic processes**
- **Website:**
 - **[https://www.\[.\]cisa\[.\]gov/infrastructure-security-month](https://www.[.]cisa[.]gov/infrastructure-security-month)**



TLP: WHITE – CISA Joint Cyber Defense Collaborative (JCDC) Webinar Recording

- CISA hosted a live webinar overview of the Joint Cyber Defense Collaborative (JCDC) on Tuesday, October 26, 2021
- A recording of the webinar will be posted to the JCDC website
- JCDC website: [https://www\[.\]cisa\[.\]gov/jcdc](https://www[.]cisa[.]gov/jcdc)
- Direct questions about JCDC to cisa.jcdc@cisa.dhs.gov



TLP: WHITE – CISA Current Activity Highlights

- **NSA-CISA Series on Securing 5G Cloud Infrastructures**

- [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/10/28/nsa-cisa-series-securing-5g-cloud-infrastructures](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/10/28/nsa-cisa-series-securing-5g-cloud-infrastructures)
- [https://www\[.\]nsa\[.\]gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2825412/nsa-and-cisa-provide-cybersecurity-guidance-for-5g-cloud-infrastructures/](https://www[.]nsa[.]gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2825412/nsa-and-cisa-provide-cybersecurity-guidance-for-5g-cloud-infrastructures/)

- **CISA, FBI, and NSA Release Joint Cybersecurity Advisory on BlackMatter Ransomware**

- [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/10/18/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-blackmatter](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/10/18/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-blackmatter)
- [https://us-cert\[.\]gov/ncas/alerts/aa21-291a](https://us-cert[.]gov/ncas/alerts/aa21-291a)



TLP: WHITE – CISA Current Activity Highlights

- **GPS Daemon (GPSD) Rollover Bug**

- [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/10/21/gps-daemon-gpsd-rollover-bug](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/10/21/gps-daemon-gpsd-rollover-bug)
- [https://gpsd\[.\]gitlab\[.\]io/gpsd/NEWS](https://gpsd[.]gitlab[.]io/gpsd/NEWS)

- **2021 CWE Most Important Hardware Weaknesses**

- [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/09/14/cert-nz-releases-ransomware-protection-guide-businesses](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/09/14/cert-nz-releases-ransomware-protection-guide-businesses)
- [https://cwe\[.\]mitre\[.\]org/scoring/lists/2021_CWE_MIHW.html](https://cwe[.]mitre[.]org/scoring/lists/2021_CWE_MIHW.html)



TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- CISA NCAS – <https://us-cert.cisa.gov/>
- CISA News Room - [https://www\[.\]cisa\[.\]gov/cisa/newsroom](https://www[.]cisa[.]gov/cisa/newsroom)
- CISA Blog - [https://www\[.\]cisa.gov/blog-list](https://www[.]cisa.gov/blog-list)
- CISA Publications Library - [https://www\[.\]cisa\[.\]gov/publications-library](https://www[.]cisa[.]gov/publications-library)
- CISA Cyber Resource Hub - [https://www\[.\]cisa\[.\]gov/cyber-resource-hub](https://www[.]cisa[.]gov/cyber-resource-hub)
- CISA Cybersecurity Directives - [https://cyber\[.\]dhs\[.\]gov/directives/](https://cyber[.]dhs[.]gov/directives/)
- CISA COVID-19 Response – [https://www\[.\]cisa\[.\]gov/coronavirus](https://www[.]cisa[.]gov/coronavirus)
- CISA Webinar Series on YouTube: [https://www\[.\]youtube\[.\]com/playlist?list=PL-BF3N9rHBLJN3HUIZnTnyZHex9gPk_Yy](https://www[.]youtube[.]com/playlist?list=PL-BF3N9rHBLJN3HUIZnTnyZHex9gPk_Yy)
- [https://us-cert\[.\]cisa\[.\]gov/ncas/current-activity/2021/11/03/cisa-issues-bod-22-01-reducing-significant-risk-known-exploited](https://us-cert[.]cisa[.]gov/ncas/current-activity/2021/11/03/cisa-issues-bod-22-01-reducing-significant-risk-known-exploited)
- [https://cyber\[.\]dhs\[.\]gov/bod/22-01/](https://cyber[.]dhs[.]gov/bod/22-01/)
- [https://www\[.\]cisa\[.\]gov/sites/default/files/publications/Reducing_the_Significant_Risk_of_Known_Exploited_Vulnerabilities_211103.pdf](https://www[.]cisa[.]gov/sites/default/files/publications/Reducing_the_Significant_Risk_of_Known_Exploited_Vulnerabilities_211103.pdf)
- [https://cisa\[.\]gov/known-exploited-vulnerabilities](https://cisa[.]gov/known-exploited-vulnerabilities)





For more information:
[cisa.gov](https://www.cisa.gov)

Questions?
CISAServiceDesk@cisa.dhs.gov
1-888-282-0870



AUTO-ISAC COMMUNITY MEETING

Why Do We Feature Speakers?

- ❖ These calls are an opportunity for information exchange & learning
- ❖ Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- ❖ Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- ❖ Goal is to showcase a rich & balanced variety of topics and viewpoints
- ❖ *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

How Can I Be Featured?

- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

30+
*Featured
Speakers to
date*

7 *Best
Practice
Guides
available on
website*

2000+
*Community
Participants*





FEATURED SPEAKER

TLP:WHITE



KATE MCCLASKEY, DHS-CISA

DHS PROGRAM LEAD



Kate McClaskey is an award-winning U.S. Department of Homeland Security (DHS) Program Lead. She has managed several policy and domestic security programs and campaigns, including the development of the Congressionally mandated Strategy for Vehicular Terrorism Prevention, strategic national action plans for international partners, and CISA's advanced technology autonomous ground vehicle security program.

Ms. McClaskey also has experience providing executive advice and communication for a Presidential Council; leading initiatives to identify statutory, legislative, and regulatory authority security needs; and working within the U.S. Senate.

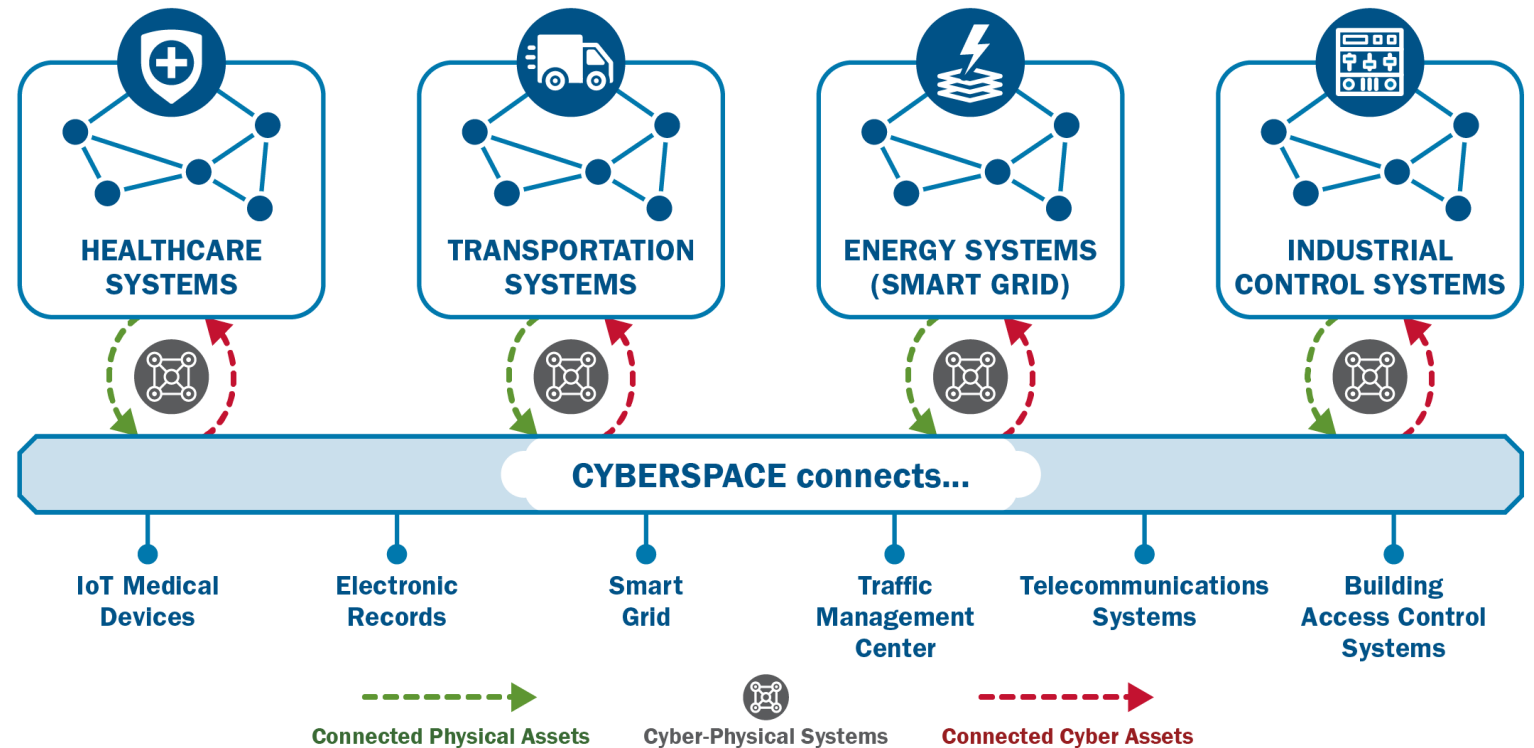
She has a J.D. from George Mason University School of Law and a B.S. in Communications from the University of Tennessee.

AUTONOMOUS GROUND VEHICLE SECURITY GUIDE: TRANSPORTATION SYSTEMS SECTOR



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.

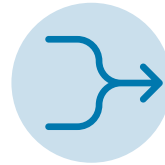


Cyber-Physical Convergence Components



Component 1

Cyber-physical **threats and vulnerabilities converging** to cause disruption to critical infrastructure service delivery, essential supply and operating chains, and national critical functions



Component 2

Integration of cyber and physical security management in planning, operations, incident, and contingency response



Component 3

Cyber-physical systems – complex IT/OT, technology-enabled, digitally transformed environments supporting or delivering infrastructure services



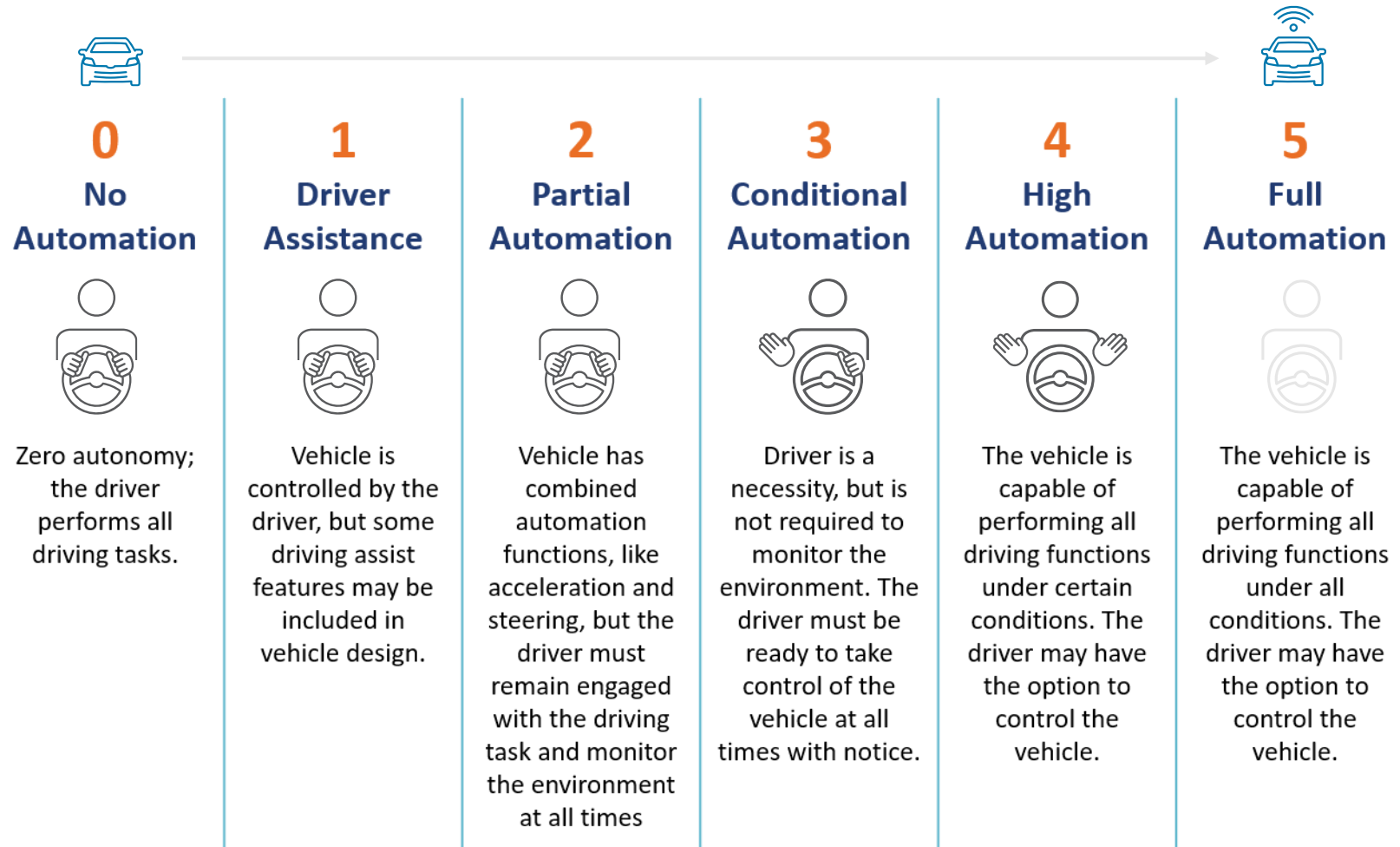
Current State of Autonomous Ground Vehicles

Autonomous vehicles:

A vehicle that can execute and decide when it is appropriate to use safety-critical functions without direct input from a human operator. This system can adapt to unforeseen conditions and environments in real-time.

Early adopters:

- NURO R2
- Tesla
- Waymo



Source: NHTSA <https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety#topic-road-self-driving>



Kate McClaskey
November 3, 2021

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 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: <https://www.cisa.gov/press-releases/2020/11/18/cisa-grants-exemption-petition-to-speed-driverless-vehicle>

Components and Systems Context

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

Operations 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 Navigation 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 tracking 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.

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

Communicate and sync with other AVs.

Sync with smart systems like traffic coordination.

Sync with command and operation center.

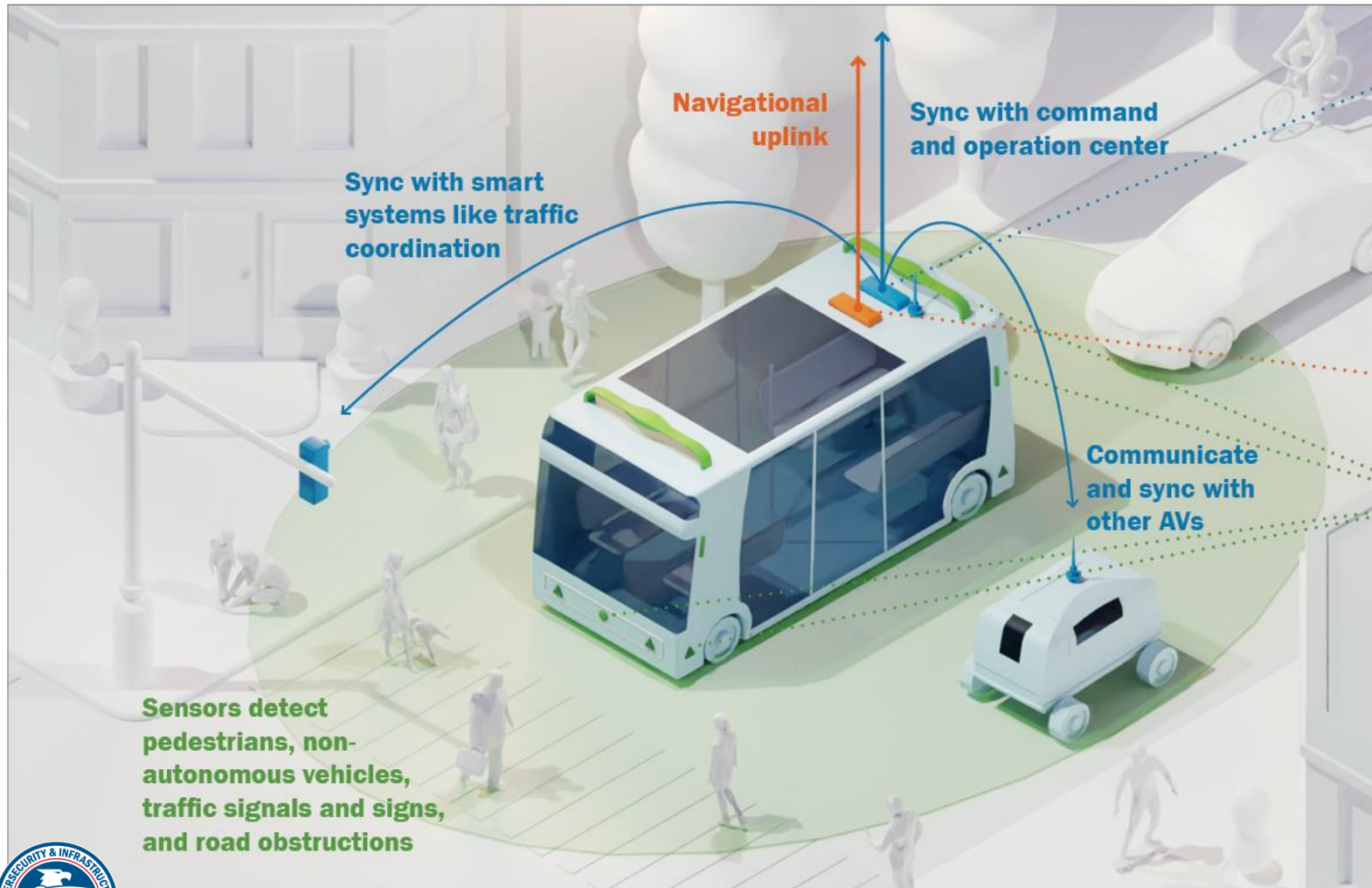
Navigation splunk.

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/avi/workforce/report](https://www.transportation.gov/avi/workforce/report).

[cisa.gov](https://www.cisa.gov) Central@cisa.gov [LinkedIn.com/company/cisagov](https://www.linkedin.com/company/cisagov) [@CISAgov](https://twitter.com/CISAgov) [Facebook.com/CISA](https://www.facebook.com/CISA) [@cisagov](https://www.instagram.com/cisagov)

Autonomous Cyber-Physical Systems



Operation and Communication Systems
Vehicle-to-everything (V2X) Technologies
Parallel computing
Dedicated Short Range Communications (DSRC)

Global Navigation Satellite Systems / Inertial Navigational Systems (GNSS/INS)

Sensor Systems
Light Detection and Ranging (LiDAR)
High-frequency acoustic sensors
Radio Detection and Ranging (RADAR)
Monocular cameras
Stereo cameras
Traffic-sign Recognition (TSR)



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



ATTACK VECTOR

Pathway a malicious actor takes to access a targeted system



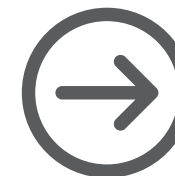
TARGET

System a malicious actor seeks to exploit



CONSEQUENCE

Harm resulting from an attack; classifies overall intent



OUTCOME

Real-world result caused by the attack



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>

AV Cyber Attacks

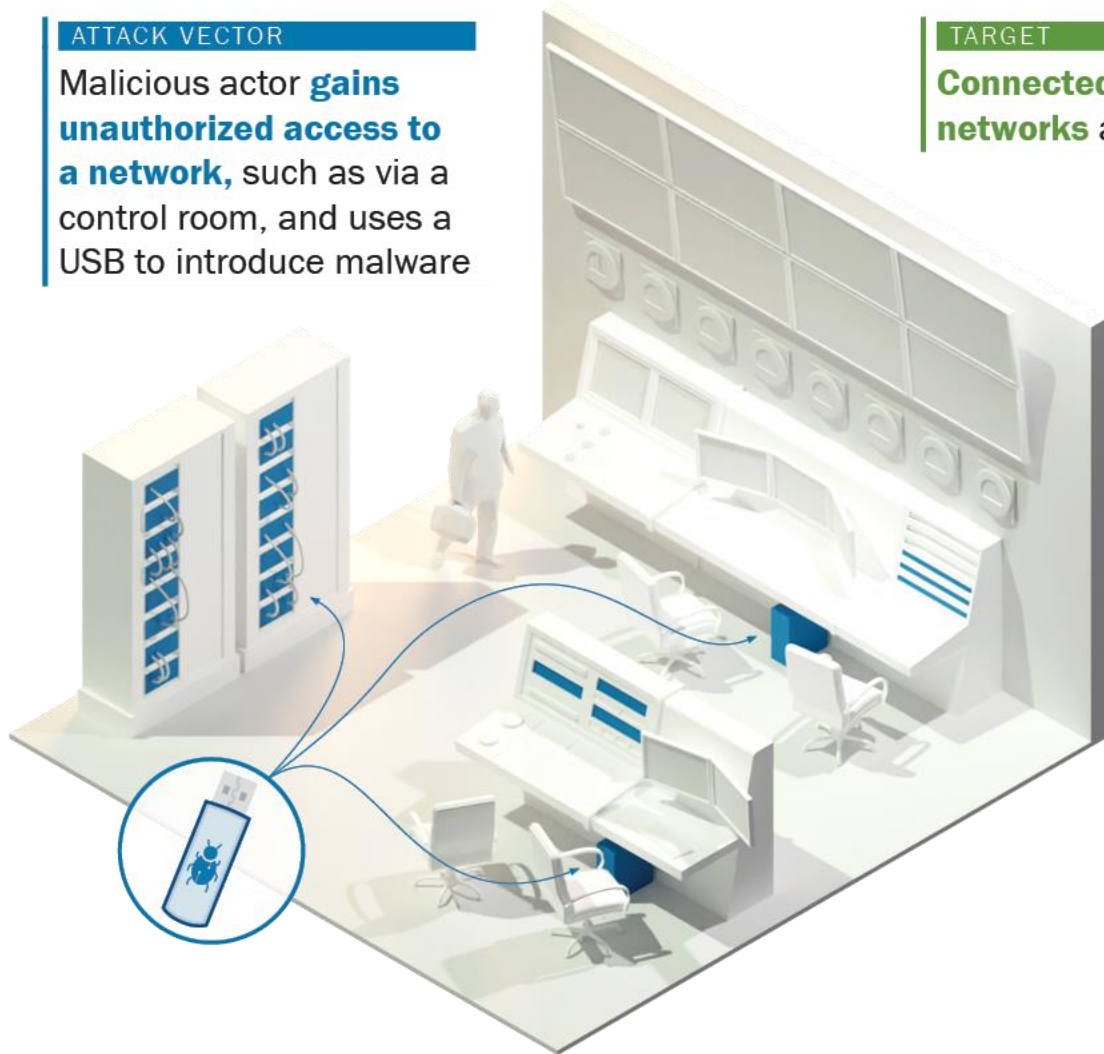
Attack Vector	Target	Consequence	Outcome
Physical Access	Driving control systems	Loss of control	Harm to people or property
Communications	Auxillary control systems	Loss of availability	Theft
Software Updates	Autonomy systems	Performance degradation	Malicious cargo delivery
Connected privileged systems	Security systems	Information disclosure	Disruption of traffic patterns
Software sensor inputs	Communications		Vehicle inaccessible
Hardware sensors inputs	Software sensors		Vehicle unable to operate properly
Malicious Hardware	Hardware sensors inputs		Spying
	Hardware sensors		Surveillance
	Information		



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

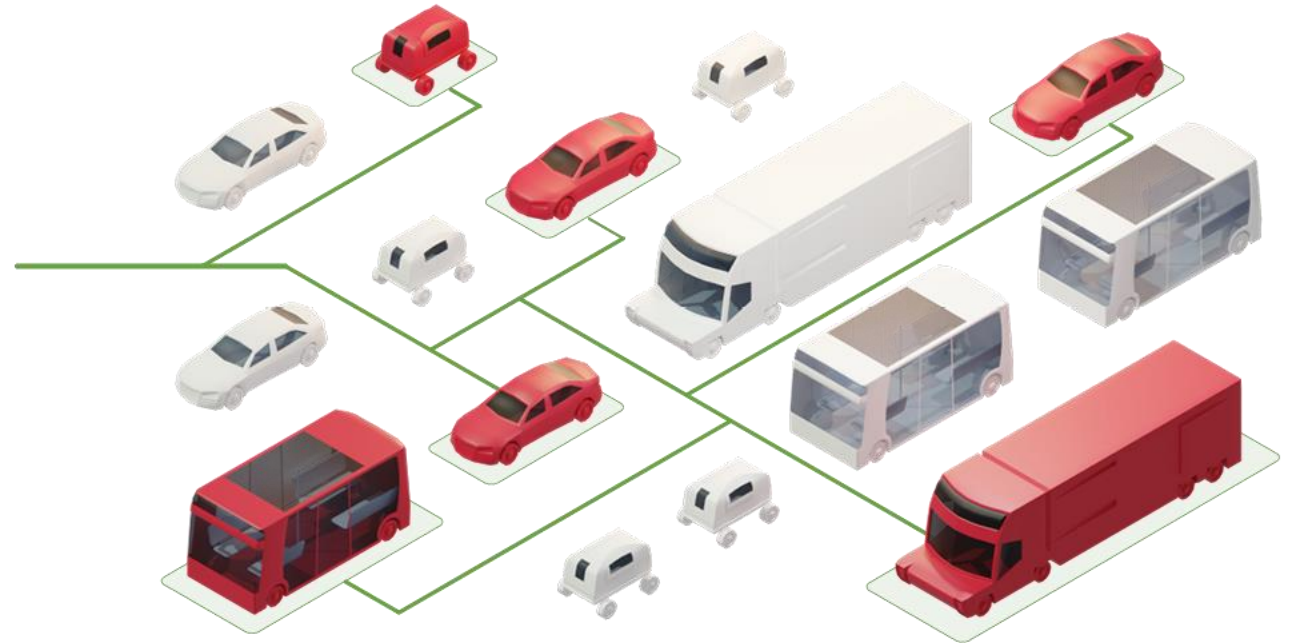


TARGET

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

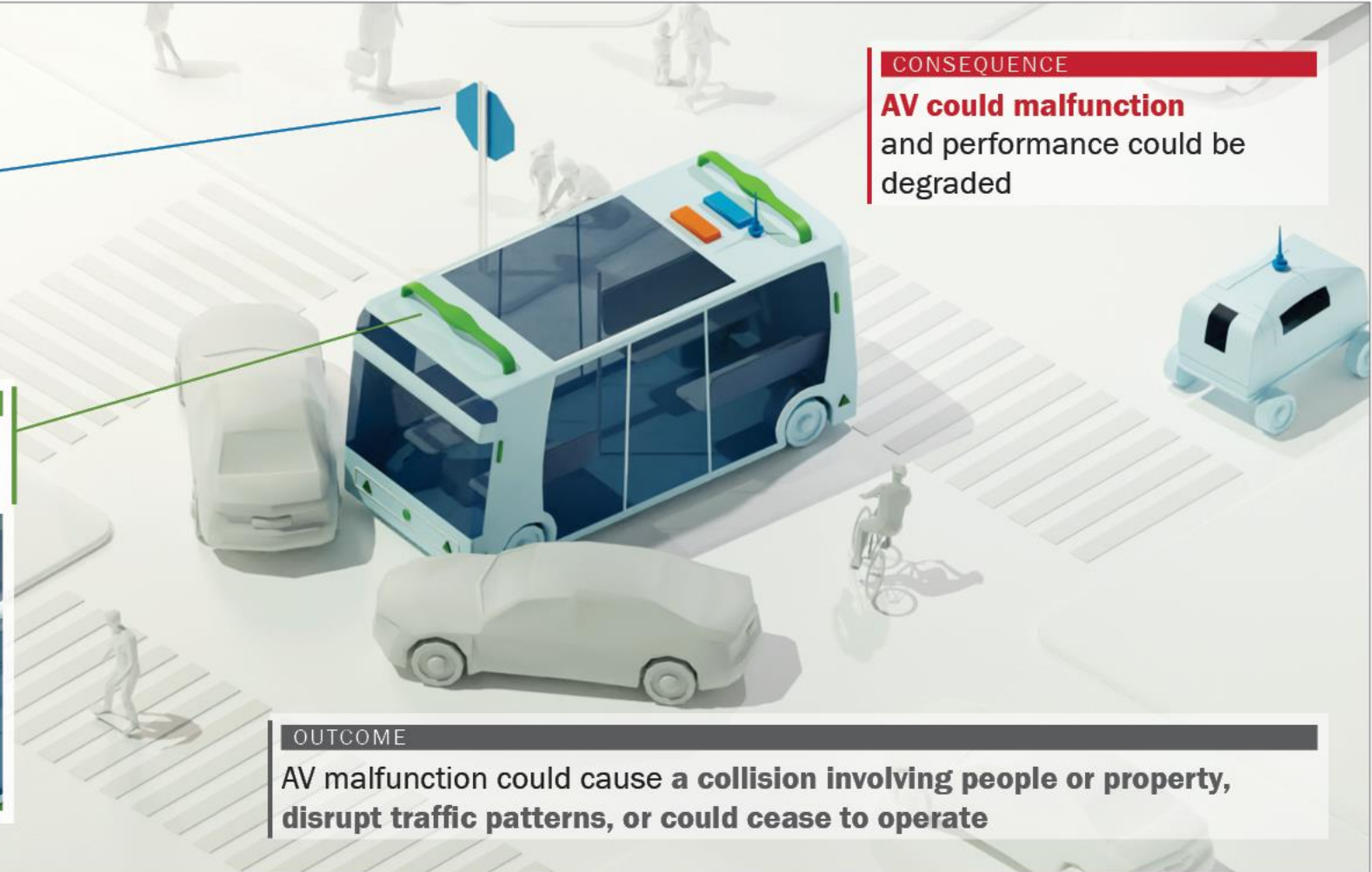


CONSEQUENCE

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

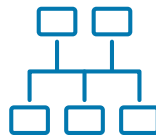
Conduct application, network, firmware, and hardware cybersecurity testing



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](https://www.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](https://www.cisa.gov/publication/cybersecurity-and-physical-security-convergence)
- **Insider Threat Mitigation**
[cisa.gov/insider-threat-mitigation](https://www.cisa.gov/insider-threat-mitigation)
- **Cyber Resource Hub**
[cisa.gov/cyber-resource-hub](https://www.cisa.gov/cyber-resource-hub)
- **Cyber Hygiene Services**
[cisa.gov/cyber-hygiene-services](https://www.cisa.gov/cyber-hygiene-services)
- **Cybersecurity Advisors**
[cisa.gov/csa](https://www.cisa.gov/csa)
- **Protective Security Advisors**
[cisa.gov/protective-security-advisors](https://www.cisa.gov/protective-security-advisors)
- **CISA Tabletop Exercises Packages**
[cisa.gov/cisa-tabletop-exercises-packages](https://www.cisa.gov/cisa-tabletop-exercises-packages)
- For more information or to seek additional help, contact us at Central@cisa.gov





For more information,
please contact:

Kate McClaskey

katherine.mcclaskey@cisa.dhs.gov



OPEN DISCUSSION

*ANY QUESTIONS ABOUT THE AUTO-ISAC OR FUTURE
TOPICS FOR DISCUSSION?*

HOW TO GET INVOLVED: MEMBERSHIP

**IF YOU ARE AN OEM, SUPPLIER OR COMMERCIAL VEHICLE,
CARRIER OR FLEET, PLEASE JOIN THE AUTO-ISAC!**

- *REAL-TIME INTELLIGENCE SHARING*
- *INTELLIGENCE SUMMARIES*
- *REGULAR INTELLIGENCE MEETINGS*
- *CRISIS NOTIFICATIONS*
- *MEMBER CONTACT DIRECTORY*
- *DEVELOPMENT OF BEST PRACTICE GUIDES*
- *EXCHANGES AND WORKSHOPS*
- *TABLETOP EXERCISES*
- *WEBINARS AND PRESENTATIONS*
- *ANNUAL AUTO-ISAC SUMMIT EVENT*

**To learn more about Auto-ISAC Membership, please contact andreaschunn@automotiveisac.com.
For Partnership, please contact sharmilakhadka@automotiveisac.com.**

AUTO-ISAC PARTNERSHIP PROGRAMS

Strategic Partner

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, IOActive, Karamba, Grimm

INNOVATOR
Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed
- Must be educational provide awareness

Community Partners

Associations

Industry associations and others that want to support and invest in the Auto-ISAC activities.

Examples: Auto Alliance, ATA, ACEA, JAMA

NAVIGATOR
Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities
- Supports Auto-ISAC

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: NCI, DHS, NHTSA, Colorado State

COLLABORATOR
Coordination Partnership

- “See something, say something”
- May not require a formal agreement
- Information exchanges-coordination activities
- Information Sharing / research & development

Community

Companies or individuals interested in engaging the automotive ecosystem and supporting & educating the community.

Examples: Sponsors for key events, technical experts, etc.

BENEFACTOR
Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

CURRENT PARTNERSHIPS

MANY ORGANIZATIONS ENGAGING

INNOVATOR

Strategic Partnership

(15)

ArmorText
Celerium
Cybellum
Ernst and Young
FEV
GRIMM
HackerOne
Karamba Security
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trillium Secure
Upstream

NAVIGATOR

Support Partnership

AAA
ACEA
ACM
American Trucking
Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR

*Coordination
Partnership*

AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVI
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence
Center (NCRIC)
NTIA - DoCommerce
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsch College

BENEFACTOR

*Sponsorship
Partnership*

2020 Summit Sponsors-

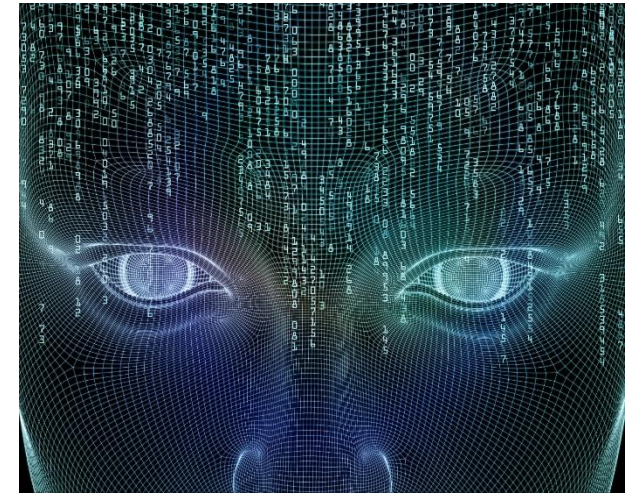
Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
ValiMail

2019 Summit Sponsors-

Argus
Arxan
Blackberry
Booz Allen Hamilton
Bugcrowd
Celerium
Cyber Future Foundation
Deloitte
GM
HackerOne
Harman
IOActive
Karamba Security
Keysight
Micron
NXP
PACCAR
Recorded Future
Red Balloon Security
Saferide
Symantec
Toyota
Transmit Security
Upstream
Valimail

AUTO-ISAC BENEFITS

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency



Building Resiliency Across the Auto Industry

OUR CONTACT INFO

Faye Francy
Executive Director



20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Sharmila Khadka
Information Technology Executive
Coordinator



20 F Street NW, Suite 700
Washington, DC 20001
443-962-5663
sharmilakhadka@automotiveisac.com



www.automotiveisac.com
[@auto-ISAC](#)