Welcome to Auto-ISAC!

Monthly Virtual Community Call

October 7, 2020

AGENDA

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities – *the Summit* ➢ Heard Around the Community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker: Dr. Amine TALEB, Valeo; Director - Innovation & Marketing and Monica Nogueira, Director of Content Acquisition/Multimedia, SAE International**
11:45	**Around the Room** ➢ 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! (lisascheffenacker@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!"*

19 *Navigator Partners*

12 *Innovator Partners*

❖ Participate

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

20 *OEM Members*

❖ 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

36 *Supplier & Commercial Vehicle Members*

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

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

2020 Board of Directors

Executive Committee (ExCom)

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 Advisory Board (AB) Leadership

Todd Lawless
Chair of the Advisory Board
Continental

Brian Murray
Vice Chair of the Advisory Board
ZF

Chris Lupini (New)
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

Member Roster

As of October 7, 2020

Highlighted = Change

Aisin	Honda	Oshkosh Corp
Allison Transmission	Hyundai	PACCAR
Aptiv	Infineon	Panasonic
AT&T	Intel	Qualcomm
Blackberry Limited	Kia	Renesas Electronics
BMW Group	Knorr Bremse	Subaru
Bosch	Lear	Sumitomo Electric
Continental	LGE	Tokai Rika
Cummins	Magna	Toyota
Delphi Technologies	MARELLI	TuSimple
Denso	Mazda	Valeo
FCA	Mercedes-Benz	Veoneer
Ford	Mitsubishi Motors	Volkswagen
Garrett	Mitsubishi Electric	Volvo Cars
General Motors	Mobis	Volvo Group
Geotab	Navistar	Waymo
Google	Nexteer Automotive Corp	Yamaha Motors
Harman	Nissan	ZF
Hitachi	NXP	TOTAL: 56

Auto-ISAC Activities

- **Auto-ISAC Europe 2020 Meeting Members & Potential Members only – Completed – very positive feedback for this event.**

- **Other Key Auto-ISAC Member Events -**
  - **Education & Training Series Series: Sept 16th Completed**
  - **All Member's Meeting: Sept 23rd Completed**
  - **Advisory and Board of Director Meetings: Sept 24th Completed**
  - **Commercial Vehicle All Member's Presentation – Oct 9th**

- **Auto-ISAC Summit October 14-15th – registration until OCT 7th, sponsorships on website – www.automotiveisac.com. *VIRTUAL***
  - **REGISTER TODAY!!! Closes October 7th, 6 virtual passes for price of 1.**
  - **Final Agenda https://www.prodevmedia.com/Auto-ISAC/2020/Auto-ISAC-Agenda.pdf**
    - **More info on website - automotiveisac.com**

AUTO-ISAC SUMMIT | OCT 14-15TH | VIRTUAL

AUTO-ISAC SUMMIT

Oct. 14-15, 2020

Virtual

2 days

400 attendees

ABOUT THE AUTO-ISAC SUMMIT:
The 2020 Auto-ISAC Summit connects global automotive industry insiders during two days of transformative conversations around cyber attack resilience and response.

Registration Open Until OCT 7th || Sponsorships CLOSED

Final AGENDA For Review

BUILDING 'A' TEAM – Kevin Tierney, GM Emcee

Session 1 – October 14th 10:00 AM – 12:45 PM ET

10:00 - 10:05	Welcome & Introduction of Kevin Tierney	Faye Francy, Auto-ISAC Executive Director
10:05 - 10:25	**Building an Automotive Collaborative Platform for Industry Resilience**	**Kevin Tierney, GM, Vice President and Auto-ISAC Chair**
10:25 - 10:45	**Building the Partnership for Best Practices Across the Automotive Industry**	**James Owens, Deputy Administrator, NHTSA**
10:45 - 11:00	Q&A | Break	
11:00 - 11:20	**Building a Community to Secure Automotive Mobility**	**Christopher Church, Senior Mobile Forensic Specialist, INTERPOL**
11:20 - 11:50	**Building Understanding Across Industry: Auto-ISAC Members Teaching Members**	**Todd Lawless, Continental Moderator** Kristie Pfosi, Aptiv; Tobias Gaertner, BMW; Matt MacKay, GM; Mike Westra, Ford
11:50 - 12:00	Q&A | Break	
12:00- 12:20	**Building ONE Global Auto-ISAC**	**Faye Francy, Auto-ISAC, Moderator** Bob Kaster, Bosch; Tobias Gaertner, BMW; Mike Cesarz, Mitsubishi Motors; David Pyun, Sumitomo Electric.
12:20-12:30	Q&A	
12:30 - 12:50	**National Initiative for Cybersecurity Education (NICE) Overview Building Knowledge and the Future Workforce**	**Matt MacKay, Moderator** Marian Merritt, Deputy Director NICE; Tamara Shoemaker, Director, Detroit Mercy Center for Cyber Security & Intel Studies
12:50	Wrap-up of Session 1 Building A Team – Summary	Kevin Tierney, GM, Vice President and Auto-ISAC Chair
12:50 - 13:15	LUNCH & Exhibit Hall	

Final AGENDA For Review

VULNERABILITIES & MITIGATING RISK – Josh Davis , Toyota

Session 2 – October 14th 1:15 pm – 5:00 pm ET

13:15 - 13:30	**What is Your Actionable Plan to Discover Vulnerabilities and Mitigate Risk?**	**Josh Davis, Toyota, CISO**
13:30 - 13:50	**Public-Private Partnerships in Reducing Risk**	**Brandon Wales, Executive Director**, Cybersecurity and Infrastructure Security Agency (CISA), DHS
13:50 - 14:00	Q&A | Break	
14:00 - 14:20	**United Nations Economic Commission for Europe (UNECE) Harmonization of Vehicle Regulations (WP.29)**	**Dr. Moritz Minzlaff, Escrypt**
14:20 - 14:45	**ISO/SAE 21434 Road Vehicle - Cybersecurity Engineering & Managing Vulnerabilities from Sourcing to Post-Production**	**Lisa Boran, Vehicle Cybersecurity Leader, Ford**
14:45 - 15:00	Q&A | Break	
15:00 - 15:20	**The Auto ATT&CK Framework - Adversarial Tactics, Techniques, and Common Knowledge**	**Karl LeBeouf, GM**
15:20 - 15:45	**Automotive Cybersecurity Risk Assessment in light of SAE/ISO 21434 and WP.29**	**Lisa Boran, Ford, Moderator,** Bill Mazzara, FCA, David Mor Ofek, Harman, Yonatan Appel, Upstream, Suzanne Lightman, NIST
15:45 - 16:00	Q&A | Break	
16:00 - 16:45	**Putting it Together to Manage Policy & Risk Against the 21434, WP.29, Cyber Type Approval, Privacy**	**Daniel Warsh, Bosch, Moderator,** Auto-ISAC Legal Working Group Panel Mike King, Continental, Linda Rhodes, Mayer Brown, John Ohly, Auto's Innovate!
16:45 - 17:00	Q&A	
17:00	Wrap-up of Session 2 Vulnerabilities & Mitigating Risk	Josh Davis, Toyota, CISO
17:00 - 1830	HAPPY HOUR & Exhibit Hall	

Final AGENDA For Review

COMMUNICATIONS IN AN INFORMATION SHARING ENVIRONMENT – Jenny Gilger, Honda

Session 3 – October 15th 10:00 AM – 12:40 PM ET

10:00 - 10:15	**Communications Across the Global Automotive Sector is Key To Mitigating Risk**	**Jenny Gilger, Vice President, Product Regulatory Office, Honda**
10:15 - 10:40	**The Importance of Communications Across the Automotive Ecosystem**	**Congresswoman Debbie Dingell**
10:40 - 11:00	**Harmonizing Cybersecurity Across the Automotive Ecosystem**	**Nathaniel Meron, Chief Product Officer, C2A Security**
11:00 - 11:10	Break	
11:10 - 11:30	**Communications During an Incident & Sharing Threat Intelligence**	**Brian Murray, ZF; Moderator,** Sandra Hosler, FCA; Ricky Brooks
11:30 - 11:50	**Communicating 2020 CyberStorm Lessons Learned For Auto-ISAC**	**Matt MacKay, GM, Moderator** Nick Reddig, GM; Delia Zdrojewski; Ford; Kate Horanburg, BAH; Josh Poster, Auto-ISAC
11:50 - 12:00	Q&A | Break	
12:00 - 12:20	**How the Automotive Industry is Collaborating on Automotive Ethernet Security Research- The ACIC Consortium & Mcity**	**David Balenson, SRI International, Moderator**, Andre Weimerskirch, Lear; Mike Westra, Ford; Ryan Elder, Southwest Research Institute; Simon Halford, SBD Automotive
12:20 - 12:40	**Threat Intelligence for Automotive Security**	**Sapir Rotenberg & Romy Moav**, Mercedes-Benz Research & Development
12:40	Wrap-up of Session 3 Communications	Jenny Gilger, Vice President, Product Regulatory Office, Honda
12:40 - 13:15	LUNCH & Exhibit Hall	

Final AGENDA For Review

DISINFORMATION ABOUNDS – Tim Geiger, Ford

Session 4 – October 15th 1:15 pm – 5:20 pm ET

13:15 - 13:35	**How to Determine What is Actionable in an Era of Disinformation** **Intro of FBI Johnny Starrunner**	**Tim Geiger, Manager, Vehicle and Mobility Cyber Security, Ford**
13:35 - 13:55	**FBI Partnership Program for the Transportation Sector** **How to Mitigate Disinformation**	**Johnny Starrunner, FBI Partnership Program**
13:55 - 14:15	**Building Resiliency against Disinformation: how data privacy legislation lessons can help you cope with ISO21434 and WP.29**	**Ian Todd, BlackBerry**
14:15 - 14:30	Q&A | Break	
14:30 - 14:50	**The Power of a Vehicle Test Bench**	**Brandon Barry, Block Harbor**
14:50 - 15:05	Q&A | Break	
15:05 - 16:00	**Commercial Vehicle Affinity Group Panel and Lightning Talks**	**Jake Walker, Auto-ISAC, Moderator** Chris Lupini, Aptiv, Jose Valerdi, Cummins;
	Commercial Vehicle Cybersecurity Working Group	**Urban Jonson, NMFTA**
	Open Telematics API: Ensuring Portability Across Telematics Service Providers	**Sean Bumgarner, Old Dominion Freight Line**
16:00 - 16:10	Q&A | Break	
16:10 - 16:30	**Identifying the Why, What and How of In-Vehicle Attacks**	**Liron Kaneti, Argus**
16:30 - 16:50	**Enhancing Penetration Testing for Automotive Embedded Systems**	**Carlos Mora-Golding, Denso**
16:50 - 16:55	Wrap-up of Session 4 Disinformation	**Tim Geiger, Manager,** Vehicle and Mobility Cyber Security, Ford
16:55 - 17:00	Kevin Tierney Closing Remarks, 2021 Summit Announcement	**Kevin Tierney, GM**, Vice President and Auto-ISAC Chair
17:30 - 1900	Happy Hour & Exhibit Hall	

The Auto-ISAC recommends that automakers review the below Bluetooth vulnerabilities and patch any affected components

Billions of Devices Vulnerable to New 'BLESA' Bluetooth Security Flaw

In a research project at Purdue University, a team of seven academics set out to investigate a section of the BLE protocol that plays a crucial role in day-to-day BLE operations but has rarely been analyzed for security issues. Their work focused on the "reconnection" process. As a result, two systemic issues have made their way into BLE software implementations, down the software supply-chain:

- The authentication during the device reconnection is optional instead of mandatory.
- The authentication can potentially be circumvented if the user's device fails to enforce the IoT device to authenticate the communicated data.

These two issues leave the door open for a BLESA attack — during which a nearby attacker bypasses reconnection verifications and sends spoofed data to a BLE device with incorrect information and induce human operators and automated processes into making erroneous decisions.

BLURtooth Vulnerability Lets Attackers Defeat Bluetooth Encryption

A vulnerability exists in certain implementations of Bluetooth 4.0 through 5.0 which allows an attacker to overwrite or lower the strength of the pairing key, giving them access to authenticated services. The bug was discovered independently by two teams of academic researchers and received the name BLURtooth. It affects “dual-mode” Bluetooth devices, like modern smartphones. An attacker can exploit BLURtooth on devices that support both Bluetooth Classic and Low Energy (LE) data transport methods and use Cross-Transport Key Derivation (CTKD) for pairing with each other.

For more information or questions please contact analyst@automotiveisac.com

CISA RESOURCE HIGHLIGHTS

3rd Annual National Cybersecurity Summit

- **The last of four CISA 2020 National Cybersecurity Summit sessions will be held today Wednesday October 7th, 2020.**
- **October 7th theme is "Defending our Democracy"**
- **No-cost event but pre-registration is required at https://cisacybersummit2020[.]Eventbrite[.]com/**
- **More information at https://www[.]cisa[.]gov/cybersummit2020**

October 2020 – National Cybersecurity Awareness Month (NCSAM)

- **NCSAM 2020 theme is "Do Your Part. #BeCyberSmart."**
- **NCSAM events:**
  - If You Connect It, Protect It
  - Securing Devices at Home and Work
  - Securing Internet-Connected Devices in Healthcare
  - The Future of Connected Devices
- **More information at:**
  - **https://www[.]cisa[.]gov/national-cyber-security-awareness-month**
  - **https://staysafeonline[.]org/cybersecurity-awareness-month/**

CISA Telework Essentials Toolkit

- **Designed to assist business leaders, IT staff, and end users in their transition to a secure, permanent telework environment through simple, actionable recommendations**
- **Provides three personalized modules for executive leaders, IT professionals, and teleworkers**
- **More information at**
  - **https://www[.]cisa[.]gov/publication/telework-essentials-toolkit**
  - **https://www[.]cisa[.]gov/sites/default/files/publications/20-02019b%20-%20Telework_Essentials-08272020-508v2.pdf**

Joint Ransomware Guide

- Released on September 30, 2020 as a joint product from CISA and the Multi-State ISAC
- Released as a customer centered, one-stop resource with best practices and ways to prevent, protect and/or respond to a ransomware
- The Ransomware Guide includes two sections:
  - Part 1: Ransomware Prevention Best Practices
  - Part 2: Ransomware Response Checklist
- Available at:
  - https://www[.]cisa[.]gov/publication/ransomware-guide
  - https://www[.]cisa[.]gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

TLP: WHITE – CISA Emergency Directive ED20-04 Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday

- **Action directed at US Federal Departments and Agencies (D/As), directive made publicly available for deployment consideration**
- **ED20-04 required the following actions be taken by D/As:**
  - **Update all Windows Servers with the domain controller role**
  - **Apply the August 2020 security update and ensure technical and/or management controls are in place**
- **See:**
  - https://cyber[.]dhs[.]gov/ed/20-04/
  - https://us-cert[.]cisa[.]gov/ncas/current-activity/2020/09/24/unpatched-domain-controllers-remain-vulnerable-netlogon
  - https://us-cert[.]cisa[.]gov/ncas/current-activity/2020/09/14/exploit-netlogon-remote-protocol-vulnerability-cve-2020-1472
  - https://portal[.]msrc[.]microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

TLP: WHITE – CISA Analysis Report AR20-275A/Malware Analysis Report (MAR) – 10303705-1.v1 – Remote Access Trojan – SLOTHFULMEDIA

- Result of result of analytic efforts between the Cybersecurity and Infrastructure Security Agency (CISA) and the Cyber National Mission Force (CNMF)
- New malware variant SLOTHFULMEDIA used by what is considered to be a sophisticated cyber actor
- Resources:
  - https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar20-275a
  - STIX-format IOCs at https://us-cert[.]cisa[.]gov/sites/default/files/publications/MAR-10303705-1.v1.stix.xml
  - https://www[.]virustotal[.]com/en/user/CYBERCOM_Malware_Alert/

TLP: WHITE – Alert (AA20-259A) - Iran-Based Threat Actor Exploits VPN Vulnerabilities

- Joint advisory released by CISA and the FBI regarding an Iran-based malicious cyber actor targeting several U.S. federal agencies and other U.S.-based networks
- The advisory analyzes the threat actor's indicators of compromise (IOCs); and tactics, techniques, and procedures (TTPs); and exploited Common Vulnerabilities and Exposures (CVEs)
- IOCs are included in Malware Analysis Report AR20-259A/MAR-10297887-1.v1 – "Iranian Web Shells"
- **See:**
  - https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-259a
  - https://us-cert[.]cisa[.]gov/ncas/analysis-reports/ar20-259a
  - CISA summary at https://us-cert[.]cisa[.]gov/ncas/current-activity/2020/09/15/iran-based-threat-actor-exploits-vpn-vulnerabilities

TLP: WHITE – CISA Alert (AA20-258A) - Chinese MSS-Affiliated Cyber Threat Actor Activity

- Released on September 14, 2020 as a joint effort between CISA and FBI
- Chinese Ministry of State Security (MSS)-affiliated cyber threat actors consistently observed to use publicly available information sources and common, well-known TTPs to target U.S. Government agencies
- Leverages the MITRE ATT@CK Framework to characterize the observed TTPs. References additional CISA, MITRE, and FBI resources.
- **See:**
  - https://us-cert.cisa.gov/ncas/alerts/aa20-258a
  - https://us-cert.cisa.gov/china

TLP: WHITE – Additional Resources From CISA

- CISA Homepage - https://www[.]cisa[.]gov/
- CISA News Room - https://www[.]cisa[.]gov/cisa/newsroom
- CISA Blog - https://www[.]cisa.gov/blog-list
- CISA Publications Library - https://www[.]cisa[.]gov/publications-library
- CISA Cyber Resource Hub - https://www[.]cisa[.]gov/cyber-resource-hub
- CISA Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) - https://www[.]us-cert[.]gov/resources/ncats/
- CISA Cybersecurity Directives - https://cyber[.]dhs[.]gov/directives/
- CISA COVID-19 Response – https://www[.]cisa[.]gov/coronavirus

For more information:
cisa.gov

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


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

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

30+
Featured Speakers to date

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!

7 ***Best Practice Guides available on website***

2000+
Community Participants

Slides available on our website – www.automotiveisac.com

Featured Speaker
Amine TALEB, Valeo
Monica Nogueira, SAE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Dr. Amine TALEB, Valeo

Director - Innovation & Marketing

Dr. Amine Taleb is the Innovation & Marketing Director for Valeo's Comfort and Driving Assistance (CDA) Business Group in North America. In this role, he leads the organization in the innovation strategy and advancement of driving assistance technologies in three focus areas of Valeo's intuitive driving: ADAS/Automated Driving (AD)/Automated Parking (AP), Connected Car, and Intuitive Controls. Prior to this position, Amine held several technical leadership positions at Valeo and prior to that at other automotive innovation suppliers in the areas of driving assistance, advanced lighting, smart sensing devices, LED and Laser products. Prior to automotive, he worked in start-up and government research lab institutions. He builds on more than 25 years experience in cutting-edge technologies.

Dr. Taleb is a 21-year member of SAE and Valeo's representative to the Auto-ISAC advisory board. He has participated as invited speaker and panelist on automated driving and user-experience, and contributed as SAE technical paper reviewer around ADAS, HMI, and smart sensing topics

Monica Nogueira, SAE International

Director of Content Acquisition and Development

Monica Nogueira is the Director for Content Acquisition and Development for SAE International's EDGE Research Reports. Originally from Sao Paulo, Brazil, Ms. Nogueira has been working on technical fields such as Finite Element Analysis software and Engineering Publishing in different capacities such as business development, sales management, content acquisition and partnerships. Fluent in four languages (English, Portuguese, French and Spanish), she has been with SAE International for over 10 years. Ms. Nogueira holds three Masters' degrees in General Business Administration, International Business Management and Environmental Sciences.

SAE INTERNATIONAL

EDGE RESEARCH REPORTS

PUBLICATIONS FOCUSED ON THE UNSETTLED TOPICS IMPACTING THE AEROSPACE, AUTOMOTIVE AND COMMERCIAL VEHICLE SECTORS.

THE SAE EDGE RESEARCH REPORTS OFFER A STRUCTURED AND METHODICAL APPROACH TO ADDRESSING RAPIDLY SHIFTING TECHNOLOGIES.

A SUBJECT MATTER EXPERT REACHES OUT TO INDUSTRY AND ACADEMIA TO GATHER THE BEST INSIGHTS ON A SPECIFIC UNSETTLED TOPIC. THE COALESCENCE OF THESE TECHNICAL CONVERSATIONS BECOMES THE EDGE RESEARCH REPORT TOGETHER WITH MEANINGFUL RECOMMENDATIONS.

ALL TOPICS CARRYING MORE QUESTIONS THAN ANSWERS ARE POSSIBILITIES TO BE DISCUSSED.

CONTACT: MONICA.NOGUEIRA@SAE.ORG

Current Customers

American Honda
SAIC Motor Co.
Toyota
Volvo Cars

Siemens Ind. Software
Rivian Automotive
California Digital Library

U.Michigan- Ann Arbor
U. Toronto
U. Nevada- Reno
U. Nevada- Las Vegas

Stanford University
Cummins Inc.
Allison Transmission
Columbia University

Amazon
BP Corp. NA
Daimler AG
Ford Motor Co.

Rolls Royce Corp.
Volvo Technology AB

User Experience and Acceptance of Automated Vehicles

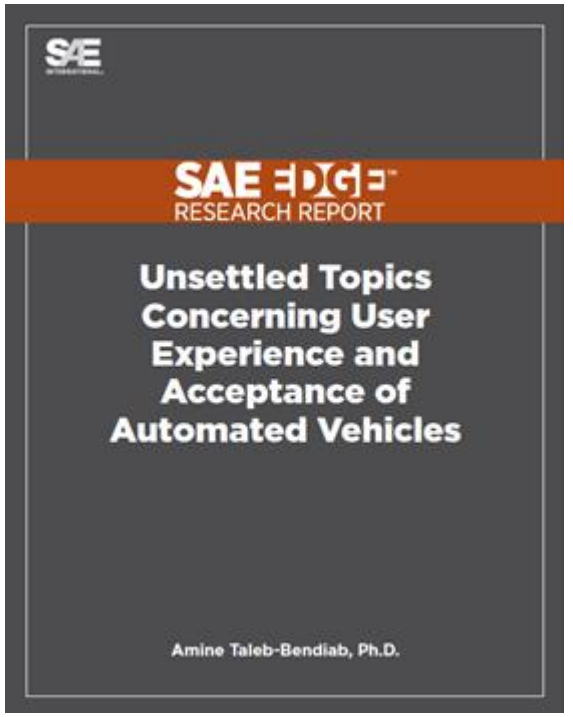
SAE EDGE Research Report - EPR 2020012

Dr. Amine Taleb
Director - Innovation & Marketing

SMART TECHNOLOGY FOR SMARTER MOBILITY

SAE EDGE UNSETTLED TOPIC: Trust in Automated Vehicles

"Driver assistance and low-level automation are creating a pathway of experience and projected acceptance toward higher automation levels when there is a positive experience and consumers see value in the technology…"



Enablers for User Acceptance & Intuitive Experience

- Need for safer driver/user engagement with driving
- Consumer voice on ADAS - Does it echo the AV needs?
- Consumer sentiment - AV likes and dislikes !
- Driver expectation for intuitive AV user experience

"...However, the basics must still be met - safety and reliability, along with comfort and convenience - in order to gain consumer trust."

AV: Automated Vehicle

CONTRIBUTORS

Courtesy: SAE

Greg Brannon
Dir., Automotive Engineering

Nicolas De Cremiers
Dir., Marketing

Alex Epstein
Dir., Transportation Safety

Rachel Forestier
Mgr., Product Marketing

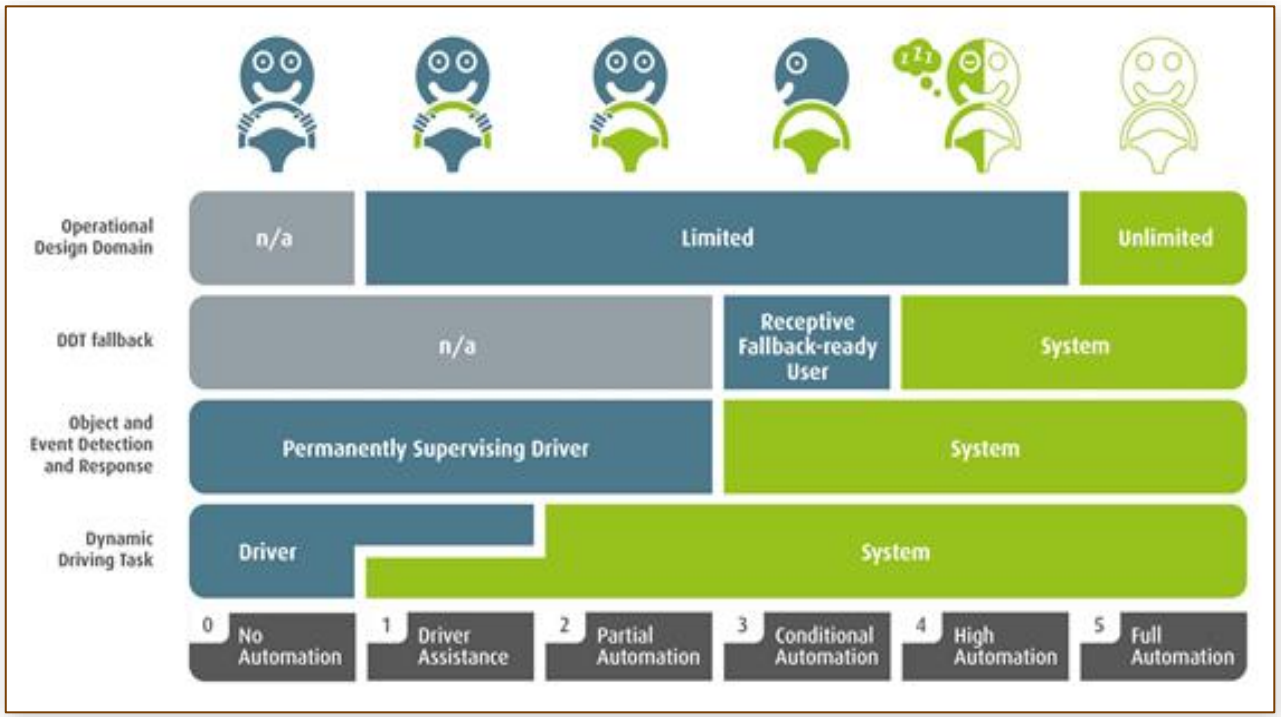
David Hofert
CMO / VP Sales

Katharina Hottelart
Mgr., UX Research & Marketing

Kristin Kolodge
Exec. Dir., Driver Interaction & HMI

Dr. Sheldon Russell
Sr. Research Associate

SAE AUTOMATION LEVELS: Driver Perspective



Ref: SAE J3016 (Jun. 2018)

Driver Engagement
vs.
Automation Level

- **Driver** in control: **L0 - L2**
- **Driver** or **System** in control: **L3**
- **System** in control: **L4 - L5**

SAFE DRIVER ENGAGEMENT AND EXPECTATIONS: L0-L2 & L3

“Hands-on-Wheel” & “Eyes-on-Road”: L0-L3

- Activities placing **visual** and **manual** demands on the driver lead increased **crash risk**
- In **L2** NDS, **26.2%** hands not on wheel and **4.2%** in glances off road greater than 2 seconds

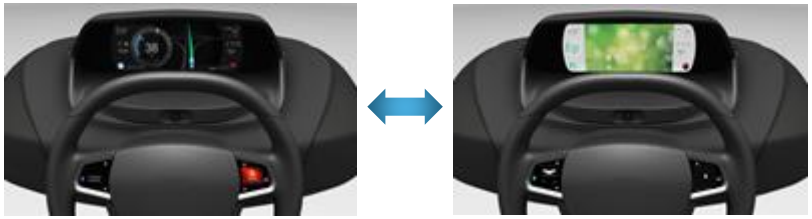
---

- In **L3** AV to Manual transition, ability to confirm a **timely engagement by driver**

Minimum Risk Maneuver: L3, only

Ref: Thatcham Research & ABI Report (Sept. 2019)

HMI: L3



Manual Automated

- **Faster** take-over control **time**
- Situational **awareness HMI** during AV

NDS: Naturalistic Driving Studies

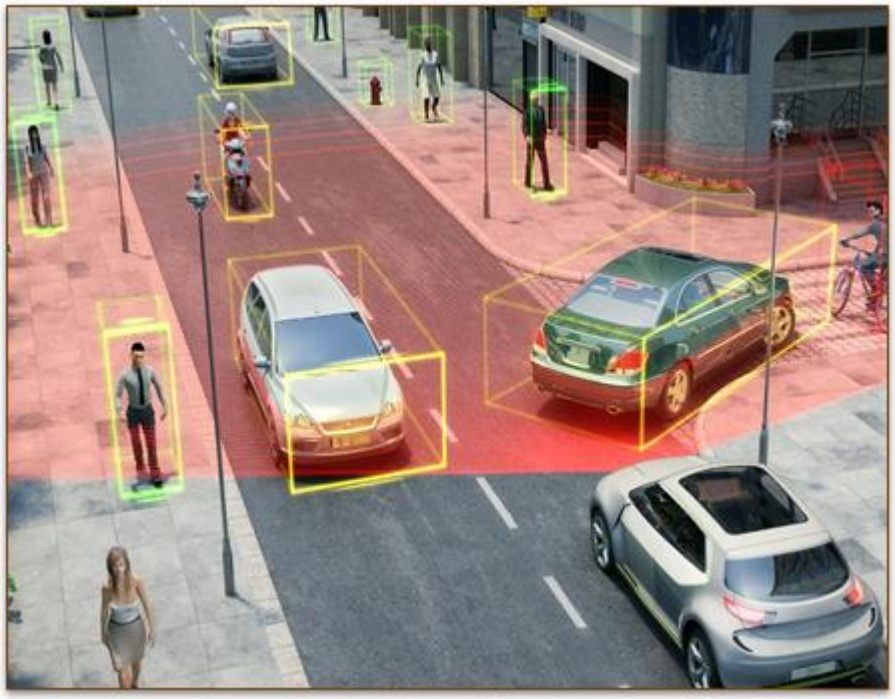
SAFE DRIVING AND EXPECTATIONS: L4-L5

- In **L4/L5**, “hands-on-wheel” and “eyes-on-road” not required since the **driving** is done by the **ADS**
- Other monitoring use-cases:
  - Well-being of occupants and safety operator
  - Passenger count, seating position, type of passenger, safety, etc.
- Mcity driverless shuttle (L4) - Understanding **rider’s behavior** and **experience**

Courtesy: Mcity

ADS: Automated Driving System

LEARNING FROM ADAS



Reaction to ADAS **alerts**:

- **Lane Departure Warning:** up to **40%** of respondents disable the feature
- **Blind Spot Warning:** only **4%** who disable it.

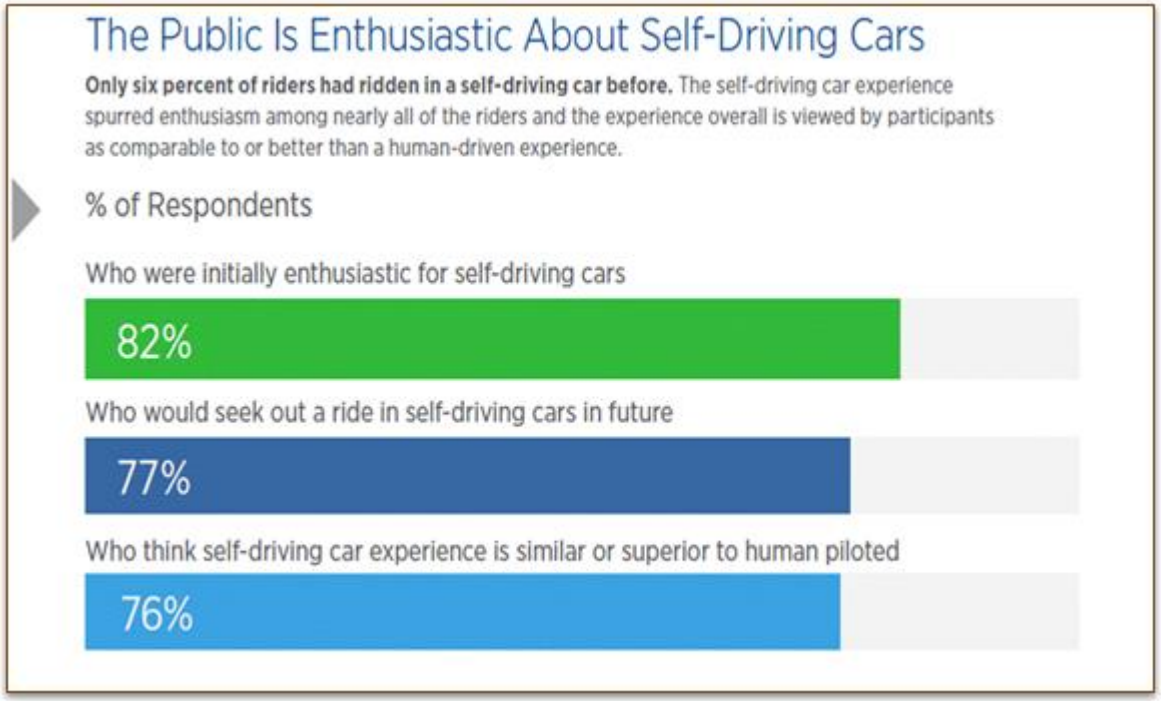
Misunderstanding of ADAS **limits**:

- **80%** of drivers not knowing the limits of the blind spot warning function.

Standardized ADAS tech. **naming**:

- Initiative taken to **standardize naming** of ADAS functions - Bring **clarity** and **market acceptance**

CONSUMER VOICE OF AUTOMATED VEHICLES - SAE Demo Event

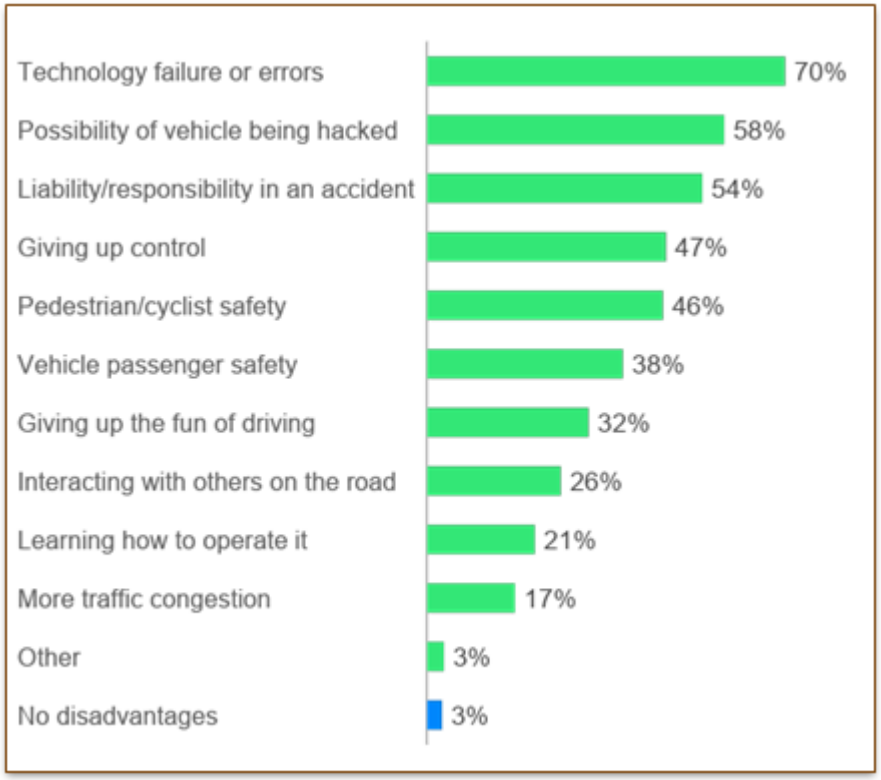


Source: SAE Demo Report (Oct. 2019)

- Up **10%**: **pre** to **post**-rides
- **Sharing control** with AV: **73%**
  - **Possible reasons:** Missing the joy of driving and loss of driving skills, or concern with AV capabilities
- **Car brand preference for** AV:
  - **Split** between established OEMs and new market entrant

Courtesy: SAE

CONSUMER VOICE OF AUTOMATED VEHICLES - J. D. Power Survey



Source: J.D. Power Q4/2019 MCI Survey (Jan. 2020)

J. D. Power Mobility Consumer Index (MCI) Survey: Perceived Disadvantages

Technology failure and security at the top of consumer concerns about automated vehicles

- View of AV possibly getting **hacked** at **58%** - 2nd highest

"The Auto-ISAC is positioned to build a global strategy in an effort to thwart the global cybersecurity threat that may impede the progress of automated vehicle development."

Faye Francy
Executive Director, Automotive ISAC

USER EXPERIENCE ANALYSIS IN AUTOMATED VEHICLES - Valeo Study

Immersive cockpit concept with **L3-like simulated driving scenarios**:

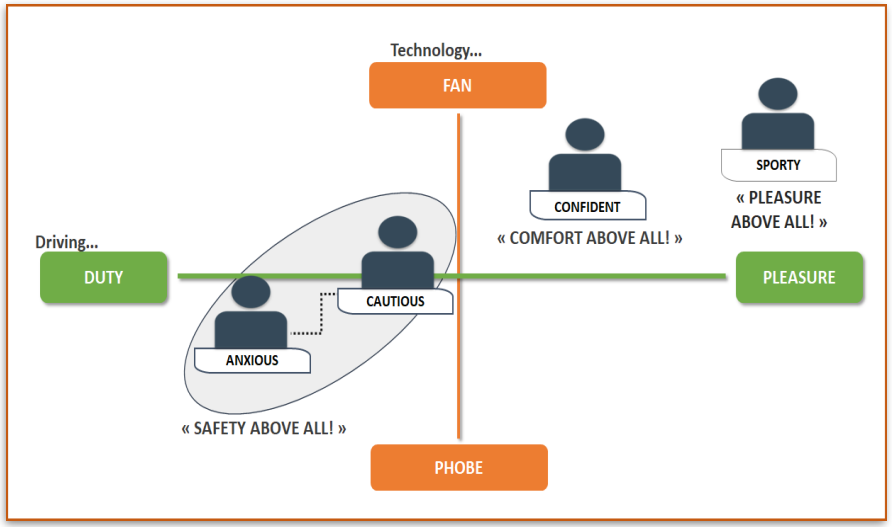
- Traffic jam
- Highway pilot
- Automated parking (in/out)
- L3 Automated-to-Manual transition capability

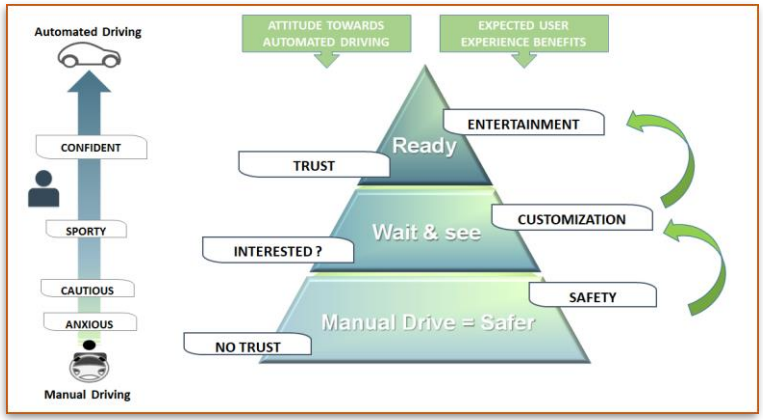
Advanced HMI and reconfigurable cockpit for the user-centric analysis:

Use-Centric Clinic:

- 100 participants
- USA, France, Germany, Japan.
- Mix of age and gender
- Mix of experience with ACC and/or HUD

USER EXPERIENCE ANALYSIS IN AUTOMATED VEHICLES - Findings





- **Limited experience** with **ADAS** and **new technology**: Simple/intuitive ADAS HMI to bring safety benefits
- **Extensive experience** with **ADAS** and **new technology**: Clear safety benefits and ready to enjoy their freed up time, toward other tasks, in an AV

TAKEAWAYS

- Apparent enthusiasm for automated vehicles through awareness events
- Proper ADAS execution is key confidence builder for automated vehicles
- Key criteria defined for safe driving when human driver is behind the wheel for an L3 automated vehicle or lower
- Initiatives across various agencies in developing standards/best practices/policies in safety, cybersecurity and data privacy to aid toward system design robustness of vehicles at all levels of automation
- User experience in automated vehicle must be tailored based on consumer knowledge and experience with the ADAS/AV technology

SMART TECHNOLOGY
FOR SMARTER MOBILITY

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 or Partnership, please contact Auto-ISAC! fayefrancy@automotiveisac.com

Auto-ISAC Partnership Programs

Strategic Partners

Strategic Partner

Community Partners

Solutions Providers

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

Examples: Hacker ONE, IOActive, Karamba, Grimm

Associations

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

Examples: Auto Alliance, ATA, ACEA, JAMA

Affiliations

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

Examples: NCI, DHS, NHTSA, Colorado State

Community

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

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

INNOVATOR
Paid Partnership

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

NAVIGATOR
Support Partnership

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

COLLABORATOR
Coordination Partnership

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

BENEFACTOR
Sponsorship Partnership

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

Current Partnerships

Many organizations engaging

INNOVATOR
Strategic Partnership (12)

ArmorText

Celerium

Cybellum

Ernst and Young

FEV

GRIMM

HackerOne

Karamba Security

Pen Testing Partners

Red Balloon Security

Regulus Cyber

Saferide

Trillium Secure

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

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

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

Thank you!

рахмат
danke
謝謝
ngiyabonga
شكراً جزيلاً
Баярлалаа
spas
mersi
kia ora
barka
welalin
tack
teşekkür ederim
mahalo
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
tapadh leat
kiitos
dankie
nanni
nandri
dhanyavad
thank you
gracias
хвала
asante
manana
bedankt
bayarlalaa
gràcie
hvala
maururu
köszönöm
akun
dankon
aciu
obrigada
tenki
murakoze
enkosi
djiere dieuf
tau
mochchakkeram
дякую
mamnun
chokrane
dziękuję
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
sobodi
dēkuji
sagolun
sukriya
kop khun krap
taiku
arigatô
takk
dakujem
trugarez
obrigado
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
grazie
kam sah hamnida
rahmat
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercé
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci

Our contact info

Faye Francy
Executive Director

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

Sharmila Khadka
Executive Organizational Secretary

20 F Street NW, Suite 700
Washington, DC 20001
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC