



DRIVING A SECURE FUTURE

2022 ANNUAL REPORT



TABLE OF CONTENTS

Chairperson’s Welcome Letter	1
Executive Director’s Letter	2
Our Mission	3
Major Accomplishments	4
Membership	5
The Auto-ISAC Member Advantage	6
Cybersecurity Awareness Month	7
Partnership Program	9
Standing Committees	10
Affinity and Working Groups	11
Programs	12
Members Teaching Members	13
Community Calls	14
Events	15
6th Annual Auto-ISAC Cybersecurity Summit	16
Cyber Storm / Cyber Challenges	17
ACT—Automotive Cybersecurity Training	18
Auto-ISAC Europe	20
Euro Workshop	21
European Steering Committee	22
2022 Threat Assessment Summary	23
Auto-ISAC Member Roster	24
Auto-ISAC Strategic Partners	25





CHAIRPERSON'S LETTER

JOSH DAVIS

GROUP VICE PRESIDENT, CHIEF CYBERSECURITY OFFICER AT TMNA
AUTO-ISAC CHAIR, AUTO-ISAC CISO XWG CHAIR

2022 culminated in a cascade of growth and accomplishments that not only supports Auto-ISAC membership and the whole of the automotive industry, but also prepares the organization for progress beyond its seventh year.

As the automotive ecosystem continues to expand, so do efforts needed to protect against cybersecurity threats. During this year, many initiatives were launched or expanded to increase information sharing between members, which is key to providing cybersecurity protections and capabilities.

We are pleased to see our membership continue to grow, with 12 members added in 2022, five of them in Europe. I look forward to the continued collaboration of all Auto-ISAC Members. When members come together to Trust, Share, Teach, Learn, and Act—no matter what corporate brand they hail from—we work toward ensuring zero safety-related cyber events. With the support of membership, we will continue to advance our mission.

Josh Davis

JOSH DAVIS

SOME KEY AREAS ADDRESSED IN 2022:

- Approval of new streamlined governance structure
- Launched Threat Indicator Report Exchange (TIRE)—STIX/TAXII automation
- Automotive Cybersecurity Best Practice Guides update started
- Approval of new membership tier for smaller prospective members
- Continued development and progress of the Automotive Cybersecurity Training (ACT) program



EXECUTIVE DIRECTOR'S LETTER

FAYE FRANCY EXECUTIVE DIRECTOR, AUTO-ISAC, INC.

2022 was a year where we experienced growth in both membership and staff and a maturing of our Auto-ISAC operations. Our Chairman continues to lead not only our Board but also our CISO Executive Working Group. One of the biggest accomplishments in 2022 was the approval of a new streamlined Board. I wish to give a hearty thank you to our twenty-four Board members who served for so many years and voted in these recent changes. Thanks to the 10 Board members who have volunteered their time to serve our organization as we enter into 2023. And a very special thank you goes to our Executive Committee who served this organization well and supported me in the daily operations of our ISAC over the past six years. These executives worked tirelessly to make a difference in building our organization and were instrumental in designing our future steps.

We hit a very important milestone with the registration and stand-up of our European office in Stuttgart. Dr. Martin Emele signed our Memorandum of Understanding (MoU) in October with the two key Trade Associations in Europe, ACEA and CLEPA, representing the European OEMs and Suppliers. This MoU solidifies our trajectory for a vibrant and engaged European operations. Our Japan Working Group has ramped up increased collaboration with the Japan Auto-ISAC and is working on a MoU to strengthen that relationship and enhance the sharing of information.

Each of our four Standing Committees and two Affinity Groups continue to provide exceptional leadership and guidance for progressing our organization. We held a very successful and well attended summit in 2022 and made many other significant strides you'll read about in our report. Of note is our **commitment-to-share** across the ISAC, which was formalized and our Board endorsed in order to enhance member information sharing. Our Legal Working Group (LWG) provided needed support in the upgrade of our legal documents and in producing a "release document" for supporting members sharing earlier and more often, even amid the challenge of existing contracts.

And lastly, I am so pleased with our progress in education and awareness thanks to our NHTSA Cooperative Agreement. The Automotive Cybersecurity Training (ACT) program development has been stellar. We are updating the courses based upon our last pilots and working towards a sustainment program that will allow the training to be made available to the whole of industry. I am looking forward to a fabulous 2023 and I hope to see you in the new year!

Faye Francy

FAYE FRANCY



WE'RE ALL CONNECTED

OUR MISSION

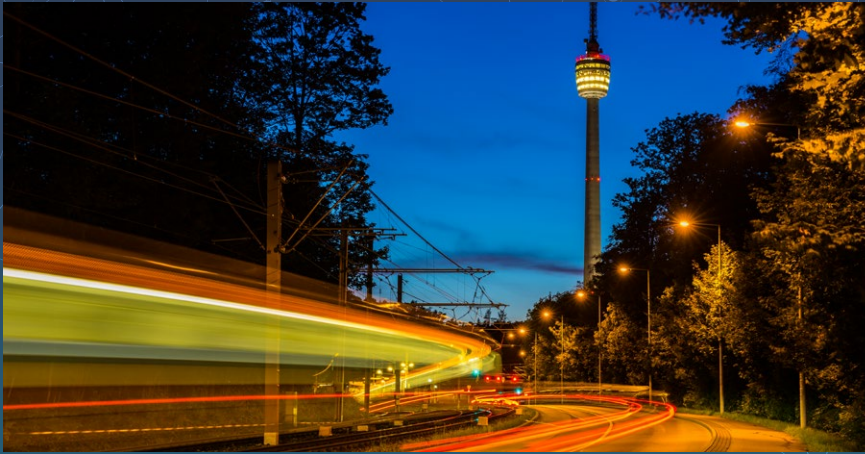
The Auto-ISAC collaborates with global partners to identify and assess cybersecurity threats, provide best practices for auto manufacturers, and ensure a safe user experience for consumers.

The early 21st century has seen a transformative movement in digitization and technological innovation. Connected vehicles are now the norm. In this modern vehicle ecosystem, cybersecurity is a collective responsibility.

To combat ongoing risks and forecast future ones, Auto-ISAC facilitates discussion and analysis of issues facing vehicles during the entire life cycle. Manufacturing is now considered critical infrastructure and has become a target for cyber criminals. To build a secure environment in manufacturing, we need to keep our systems up to date, secure our devices, and be aware of social engineering scams. As threats continually evolve, automotive over the air (OTA) updates and vehicle security operations centers (VSOC) will help protect the vehicles of today and tomorrow, driving towards a safe and secure future for all.

With membership and partnerships growing each year, we are able to collectively enhance vehicle cybersecurity capabilities across the globe. Currently, Auto-ISAC Members account for more than 99% of light-duty vehicles in North America, with over 75 global OEM and supplier members that include the commercial vehicle sector including fleets and carriers.

MAJOR ACCOMPLISHMENTS



CONTINUED PROGRESS IN EUROPE

Last year was pivotal for Auto-ISAC in Europe. In October 2022, the Auto-ISAC announced a formal collaboration with the European Automobile Manufacturers' Association (ACEA) and the European Association of Automotive Suppliers (CLEPA) to create a central European hub for information sharing on motor vehicle cybersecurity.

Since then, the European Working Group (EuWG) has gained more members and is focused on establishing a network among European members. Two task forces were established with formal Board approval in 2023: the EuWG Sharing Task Force, which is planning two studies in 2023 on Information Sharing & Vulnerability Scoring to address concrete needs identified by European members and to help them meet new regulations and standards; and the European Event and Summit Task Force, which is getting into full swing and planning the first ISAC Europe Summit. The European Steering Committee (EuSC) is working hard to define the strategic direction for Europe. The EuSC Chair is also on our Board of Directors providing an invaluable global view.

NEW AUTO-ISAC BOARD OF DIRECTORS GOVERNANCE STRUCTURE APPROVED

In 2022, the approval of this new structure allowed for the consolidation of the Board of Directors, Advisory Board, and Executive Committee into one Board consisting of 10 members.

In addition, a Member Advisory Forum was created to facilitate open discussion on progress-to-plan against organizational goals and objectives and to allow for Member ideas, questions, and concerns.



AUTOMOTIVE CYBERSECURITY TRAINING

The Automotive Cybersecurity Training (ACT) project, with support from the National Highway Traffic and Safety Administration (NHTSA), has developed an unprecedented training program that utilizes globally sourced expert instructors to provide training to the automotive industry. Auto-ISAC Members in 2022 participated in two pilots to support the design of this first of its kind training.

The training culminates in a Capability Exercise (CAPEX), which is a scenario-based exam to test the participants learning and capabilities. By passing this exam, the individual will receive a Certified Automotive Cybersecurity Engineer certification (CASE). In 2023, the Auto-ISAC team will work to build a sustainment plan and provide this training to the greater automotive industry.

MEMBERSHIP



THE AUTO-ISAC MEMBER ADVANTAGE

Auto-ISAC provides a unique confidential community of industry leaders and cybersecurity experts with access to a secure portal that enables anonymous information sharing, houses real-time cybersecurity intelligence reports and analysis, and facilitates live interaction among members.

In addition, members can participate in standing committees, affinity groups, working groups and workshops. The more we remain immersed and invested in cybersecurity, the better we're able to protect the technology we need in a connected world.

Being an active Member of the Auto-ISAC has benefited Polaris tremendously. The Auto-ISAC has helped us gather intel on potential and emerging threats, educate employees through training and awareness, and in general, move our corporate Cybersecurity program maturity forward. It is invaluable participating in this group of seasoned professionals, learning from each other and making this industry better as a whole. I am excited to see how the Auto-ISAC tackles this industry and potential future threats.

MONICA MITCHELL
CHIEF ENGINEER, POLARIS INDUSTRIES
AUTO-ISAC BOARD MEMBER

12 NEW MEMBERS



—chargepoint+®

flex®

LUCID

nuro

nuspire

5 IN EUROPE

Ferrari S.p.A.



e:fs
TechHub GmbH



thyssenkrupp

vttesco
TECHNOLOGIES

CYBERSECURITY AWARENESS MONTH

Cybersecurity Awareness Month is every October and has existed since 2014 when the President of the United States and Congress established it to educate individuals on how to protect themselves online as threats to technology and confidential data became commonplace. The Education and Training Standing Committee (ETSC) came together to produce awareness videos for members' use in 2021. These awareness videos help all of us to be "cyber aware" and address specific automotive issues the industry faces.

In 2022, ETSC produced four videos with corresponding posters incorporating different cybersecurity themes. A video and poster were released each week which included these themes:

Living Cyber Secure for a Sustainable Future

AUTO-ISAC
LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

WE ARE ALL CONNECTED

- To ensure that **safety is maintained** as top priority, it is imperative that **signal integrity is maintained**, which means that the data is confirmed to be accurate and complete, **not manipulated** by an adversary.
- Cybersecurity** is not a bolt-on solution. Like safety and quality, it needs to be designed in from the concept phase, and **supported** through the end of life of the product.
- In this modern vehicle ecosystem, cybersecurity is everyone's responsibility. We are all in this together. **We are all connected.**

AUTO-ISAC
LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

PURPOSE DRIVEN SECURITY

- Advanced connectivity** across the variety of smart devices requires application of a **purpose-driven security** approach to ensure that our customers and their data are **safe**.
- Application of key security principles such as **security-by-design** and **defense-in-depth** are vital for a robust, secure system.

Incorporating key defense principles in security products and then ensuring **successful implementation through verification** and validation demonstrates a product with purpose-driven security is delivered to the customer.

- Security-by-design** ensures security controls and tools are built into devices from initial design phases and are incorporated in critical architecture.
- Defense-in-Depth** ensures multi-layered security mechanisms are utilized for a holistic cybersecurity strategy.

AUTO-ISAC
LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

BUILD & DELIVER SECURELY

TO BUILD A SECURE ENVIRONMENT IN MANUFACTURING, WE NEED TO:

- Keep our system **up-to-date**. Cyber criminals use vulnerabilities within systems, applications and devices. This is why it is important to **update or patch** them to ensure they are secure.
- Secure our **devices and accounts**, protect your devices with a lock screen, use **strong passphrases** for your online accounts and use **multi-factor authentication** for an extra layer of protection.
- Be aware** of social engineering scams like phishing emails and malicious text messages. Watch for suspicious emails and text messages and **don't become a victim.**

AUTO-ISAC
LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

CONTINUOUS SECURITY

- As threats continually evolve, it is critical that we consider risk during the **entire vehicle lifecycle**. With vehicles becoming more connected and software driven, attack vectors and vulnerabilities increase.
- Over-the-air** updates will help to enable **cost effective** and **continuous** software and security maintenance. Vehicle Security Operations Center will continuously monitor, assess and correct these threats to help protect the vehicles of today and tomorrow, driving toward a safe and secure **future for all.**

CLICK POSTER TO ENLARGE

INTELLIGENCE / INFORMATION SHARING

- Analysts deliver pre-filtered, focused and curated information
- Member-only Reporting Exchange and Discussion (RED) Platform enables secure sharing of intelligence and vulnerabilities
- Requests for Information (RFIs) enabling member-requested and member-driven intelligence on events or best practices
- Conference calls on selected topics
- Daily Research, Incident, Vulnerability & Executive News (DRIVEN) Report provides open source intelligence and analysis to members and community
- Weekly Cyber & Automotive Report CAR provides highlights of open-source and member-only intelligence and analysis curated throughout the week
- Receive threat intelligence from members and external sources
- Share intel and incident information within a secure environment
- Assist in identifying and mitigating industry vulnerabilities
- Aggregate data to identify and discuss emerging trends



Information sharing is not a competitive endeavor—it's critical when navigating the evolving threat landscape facing the automotive industry. The Auto-ISAC cultivates a collaborative environment that prioritizes shared situational awareness and threat analysis, from which GM and all members continue to benefit."

CHAD LAIDLAW
PRODUCT CYBERSECURITY INTELLIGENCE
COORDINATOR, GM

MEMBER COLLABORATION

- Best Practice Collaboration
- Monthly Community Calls
- Standing Committees, Affinity Groups, Working Groups, and Task Forces
- Cyber event response exercise programs that enhance collective and individual member readiness
- Implementing Cybersecurity Best Practices
- Exchanging experiences with cybersecurity program development
- Participating in exercises and workshops to test readiness
- **Member Teaching Members** and **Partner Teaching Members** forums

CYBERSECURITY CULTURE

- Building a collaborative environment around cybersecurity
- Creating trusted relationships within vehicle cybersecurity industry
- External outreach and networking
- Non-prescriptive, aspirational best practice guides that do not limit technological innovation
- Helping grow the future work force
- Offering a good opportunity for members to reflect on and build internal processes
- Working together to build resiliency for the whole of the automotive industry



PARTNERSHIP PROGRAM

Enriching Our Membership

Through partnership with Auto-ISAC, a diverse set of organizations and individuals can support our mission—because **an attack on one is an attack on all**. Strategic partners have a vested interest in helping build industry resiliency. Community partners raise awareness with consumers and local organizations.

STRATEGIC PARTNERS

Are for-profit companies such as “solutions providers” that sell connected vehicle cybersecurity products and services.

COMMUNITY PARTNERS

Are companies, individuals, or organizations interested in engaging with the automotive ecosystem and educating members and the community.

5 NEW PARTNERS



PARTNER WEEK

Our first Partner Week was held May 23–27. Two hundred and six members registered with an average of 35 attendees per each 30-minute session. As the event was held virtually, participants were able to opt in and out of their preferred sessions and also be able to visit the partners’ virtual booths for additional resources and conversations. The sessions, which were divided into four blocks, included three Partners and one supplier member.

Partners and members provided highly positive feedback for continuing the event every year:

100%

Responded they will attend partner week event next year and 60% preferred virtual format that allowed them to send different designees on different days with an ability to go in and out of the presentations.

70%+

Of respondents advised they will review slides and recordings from Partner Week on our internal Member Access Platform (MAP) as well as advise their colleagues to do the same.

70%

Of attendees said the solutions and services they learned about were very relevant to their company.

TOPICS COVERED INCLUDED:

Cybellum: Securing Your Vehicles from Development to the Driveway — A Live Demo

Cymotive: Lessons learned from IT and OT ICS/SCADA cybersecurity applied to automotive

Upstream: Make connected vehicles safe and secure

STANDING COMMITTEES

EDUCATION AND TRAINING STANDING COMMITTEE (ETSC)

The ETSC's mission is to enhance Member capabilities and elevate overall resilience through training and education based on the Auto-ISAC's Best Practices, Member experiences, and lessons learned.



The task of updating the Auto-ISAC Best Practice Guides began in 2022 to provide better alignment with the current state of automotive cybersecurity by leveraging the membership's pool of industry experts to demonstrate true "best practices."

INFORMATION SHARING STANDING COMMITTEE (ISSC)

The ISSC is the organization within the ISAC focused on driving effective and efficient methods of proactive information sharing to and between members to enhance the awareness of security intelligence.

The ISSC finalized, gained Board endorsement, and promoted the "Auto-ISAC Commitment to Share" that outlines our Member-focused pledge to share security related information and threat intelligence. Additionally, the ISSC launched an Intelligence Needs Tiger Team to identify, outline and fulfill Member intelligence needs.



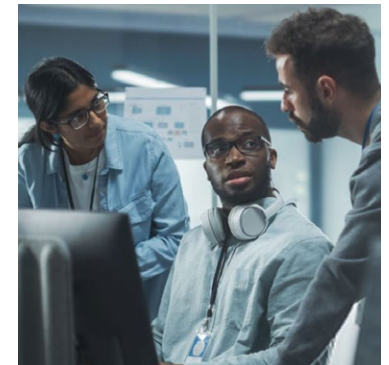
FINANCE & AUDIT STANDING COMMITTEE (FASC)

The FASC is an advisory body to the Board of Directors and Executive Director in overseeing and planning the budget to ensure the organization's financial stability.

In 2022, the FASC established a format for committees and working groups to request funds to support the undertaking of activities that provide value to the Auto-ISAC membership.

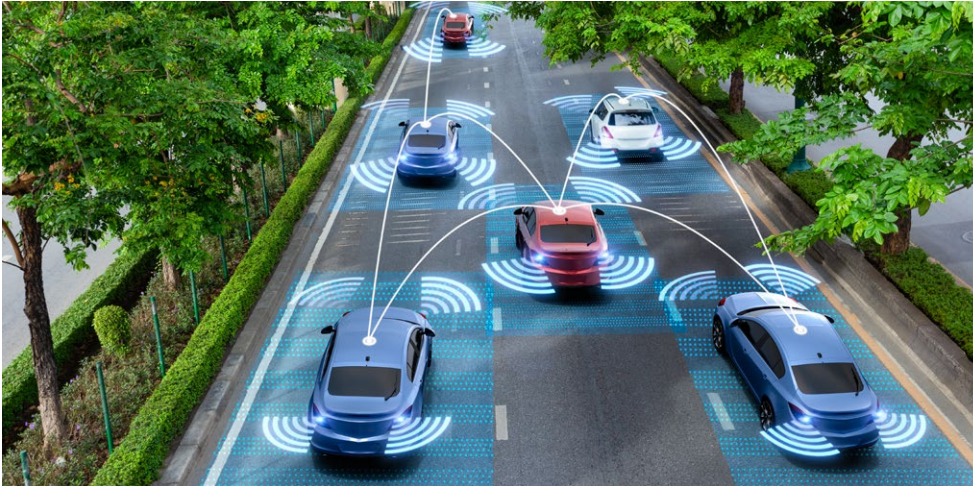
MEMBERSHIP AND BENEFITS STANDING COMMITTEE (MBSC)

The MBSC strives to ensure an active pipeline of connected vehicle companies that should be members or strategic partners of the Auto-ISAC. It drives to sustain Member satisfaction by obtaining regular feedback and by implementing continuous improvement actions.



Recently onboarded members are paired with a seasoned Auto-ISAC Member to share tips and tricks for success during the first year of membership.

AFFINITY AND WORKING GROUPS



CISO EXECUTIVE WORKING GROUP (CISO XWG)

The Chief Information Security Officer (CISO) Executive Working Group (CISO XWG) provides a forum for Auto-ISAC Member CISOs, deputy CISOs, and executive personnel supporting the security of the automotive ecosystem to deliberate on sensitive cybersecurity topics facing their organizations and the automotive industry. The purpose of the CISO XWG is to discuss threats and attacks experienced within Member company environments and across the automotive ecosystem. Additionally, the group examines security concerns as the automotive industry expands vehicle connectivity, autonomy, and electrification.

In 2022, we had 27 member companies which identified their respective CISO Executives to actively participate in the monthly discussions. A monthly ransomware product was produced for CISO consumption, and several Member companies shared their experience in a Ransomware CISO Roundtable shared across the organization. The group discusses what is topical to include topics such as Cybersecurity & Risk Management, Cyber Resiliency in the Supply Chain, Zero Trust Strategy, and Current Threat Observation.

COMMERCIAL VEHICLE AFFINITY GROUP (CAG)

The purpose of the Commercial Vehicle Affinity Group is to collaborate across the industry to understand the commercial vehicle threat landscape and proactively work together to mitigate cyber risks.



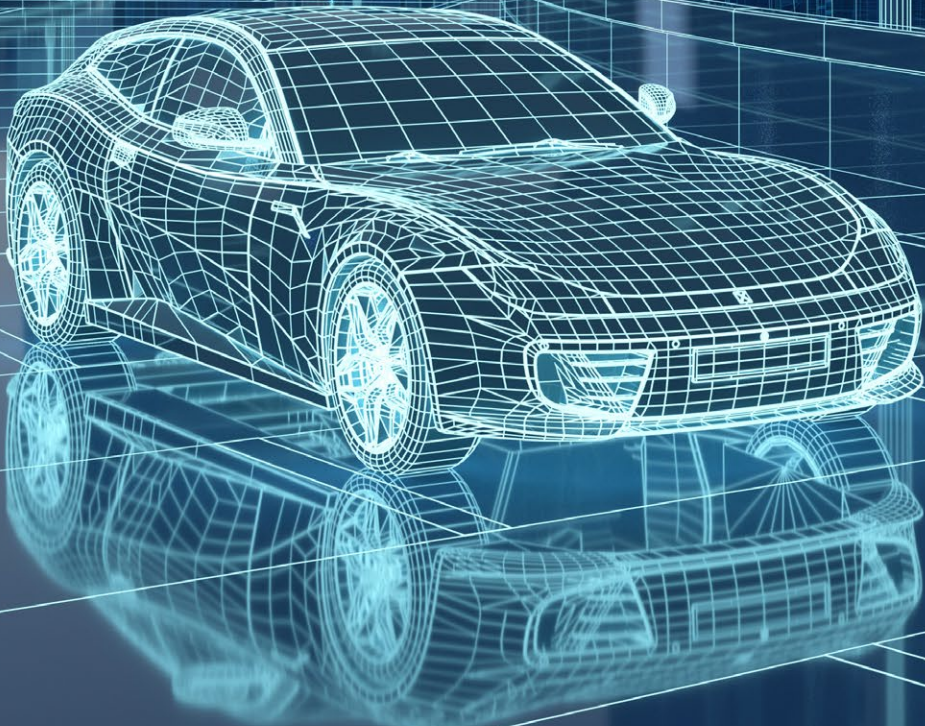
2022 was a good year for the CAG. The group has held monthly discussions on topics ranging from assisted steering to UNECE R155 and is engaging with both global members and Partners in the commercial vehicle sector.

SUPPLIER AFFINITY GROUP (SAG)

Automotive suppliers play an integral role in supporting automotive security, but suppliers have different challenges than original equipment manufacturers. The SAG provides a venue for automotive suppliers to voice concerns applicable to suppliers to the Auto-ISAC and to work on topics that are different from OEM-level issues.

Finalized development of an informational report on implementing Software Bill of Materials (SBOM) within the automotive industry. This work led to the establishment of the Auto-ISAC SBOM Working Group.

PROGRAMS



MEMBERS TEACHING MEMBERS

The Auto-ISAC's Members Teaching Members program is founded upon the power of information exchange, or what we call "sharing lessons." We tap into the experience and expertise of both members and partners for innovative solutions to complex cybersecurity issues. Through this sharing of lessons, members can take advantage of industry-wide best practices, in turn building resilience and helping achieve our goal of zero safety impacts from vulnerabilities.

PARTNERS TEACHING MEMBERS

In addition, our Strategic Partners are encouraged to participate in Partners Teaching Members by providing value-added presentations specific to automotive cybersecurity that provides value to our members and the industry.

6

MEMBERS TEACHING MEMBERS

1

PARTNERS TEACHING MEMBERS

126

AVERAGE MTM ATTENDANCE

7

TOTAL SESSIONS IN 2022

2022 TOPICS



Auto-ISAC Best Practice Guides Overview & Plan Forward



Panel on IT Product Cybersecurity Working Relationships

• APTIV •

Compare & Contrast Automotive Product Security with Aerospace, Medical, Industrial Controls & More

NIST

NIST Cybersecurity Framework



SAE J1939 Heavy-Duty Vehicle Standard Update Panel

ETAS

Benefits of an Automotive Security Maturity Model



Cybersecurity: Not Just an Annual Check-Up

COMMUNITY CALLS

The Auto-ISAC holds monthly virtual community meetings for members and connected vehicle ecosystem stakeholders to stay informed of Auto-ISAC activities and share information on key vehicle cybersecurity topics, technologies, and regulation.

Participants include Auto-ISAC Members, Strategic and Community Partners, government partners, academia and research institutions, and key automotive stakeholders that are globally located. During the session, Auto-ISAC Executive Director provides key business operation updates, the Intelligence Officer provides an update, CISA's Joint

Cyber Defense Collaborative (JCDC) partner provides topics of the last month, and a featured speaker makes up the last portion of the call. These speakers are subject-matter experts in a variety of public and private sectors presenting key topics of interest, providing learning experiences and Q&A opportunities for participants.

Participants are encouraged to submit recommendations on various speakers or topics of interest for future Community Calls. The presentations are made available on the Auto-ISAC website.

In 2022, our calls covered a diverse range of topics reflecting the state of the industry and best practices as well as opportunities for growth and development:

JAN

Multi-stakeholder
Cyber Crisis Response

FEB

Research into Defending
Automobiles Via Intrusion
Detection Systems (IDS)

MAR

Become A CyberPatriot
Youth Mentor: Validate
your Leadership Skills

APR

Public Policy Affecting
Automotive Cybersecurity

MAY

Protecting and Enabling
Global Revenue Streams

JUN

Automotive Firmware,
Hypervisor and OS
Cybersecurity
Made Simpler

JUL

The FBI's InfraGard
Program

AUG

Continuous Automated
Vulnerability Manage-
ment for Safer Cars and
Regulatory Compliance

SEP

Program SAE EV Charging
Public Key Infrastructure
Program

OCT

Auto-ISAC Education and
Training Standing
Committee (ETSC) 2022
Cybersecurity Awareness
Project

NOV

A Global Grassroots
Community of 10,000+
Automotive Security
Folks: The ASRG

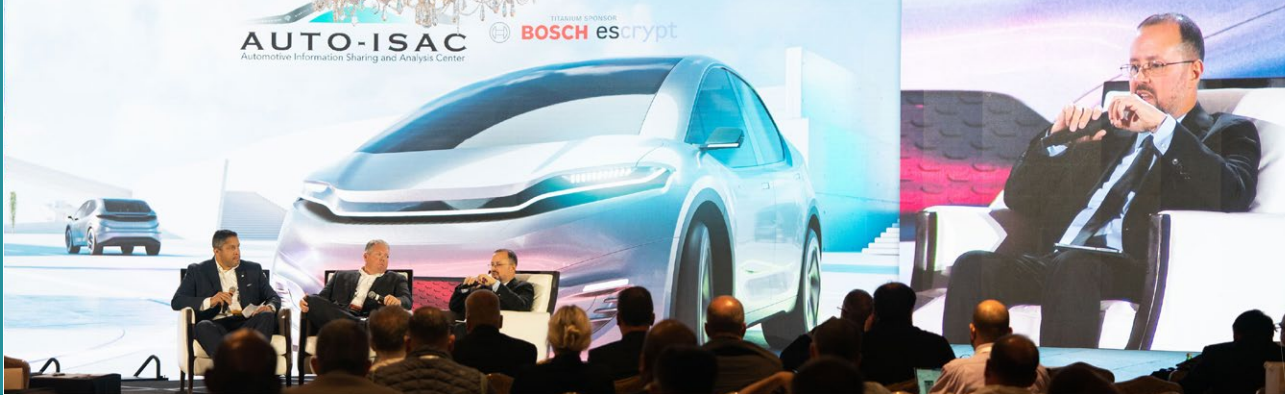
DEC

CISCP to JCDC Transition



EVENTS





The Auto-ISAC provides an invaluable arena to share appropriate levels of security communication within the industry to benefit our customers, other members, and partners. Through additional activities in areas such as the annual Summit, we are able to build organizational maturity, not only to lead discussions, but to benefit other members and customers alike. We learn from others, help others and can openly communicate about security topics in a well-organized and managed fashion which the Auto-ISAC enables.

ANTHONY FREILACH
PRODUCT & CYBER SECURITY
BOSCH USA

- Robust Automotive Security Culture
- Aligning perspectives of product security and data privacy
- Global security initiatives
- Securing tomorrow's automotive software

6TH ANNUAL AUTO-ISAC CYBERSECURITY SUMMIT

The 2022 Auto-ISAC Cybersecurity Summit was a hybrid event that took place September 7–8 in Dearborn, MI as well as virtually. Focusing on “Driving a Secure Future,” this year’s summit highlighted the automotive industry’s position at the nexus of emerging societal, cultural, and technological trends that herald a new era of mobility.

As was done every year since its inception, this year’s conference showcased insights from manufacturers, suppliers, thought leaders, lawmakers, practitioners and other stakeholders. Collaborative events such as our Cybersecurity summits encourage a collective commitment to Trust, Share, Teach, Learn, and Act.

546
TOTAL
REGISTRANTS

424
IN PERSON

122
VIRTUAL

281
INDIVIDUAL
MEMBERS

26
SPONSORS

83%
FOUND THE
CONTENT VALUABLE

KEYNOTE SPEAKERS

Steve D’Antuono, FBI

Congresswoman Debbie Dingell

Dan Strachan, CISA

Cordell Schachter, DOT

Ann Carlson, NHTSA Acting Administrator

Cem Hatipoglu, NHTSA Associate Administrator



CYBER STORM

In March 2022, Auto-ISAC Members participated in three days of live play in the **Cyber Storm VIII National Cyber Exercise**. This functional exercise allowed Auto-ISAC Members the opportunity to test their incident response plans and identify opportunities for coordination and information sharing. Members joined over 2,000 players who uncovered lessons learned related to common vulnerabilities and the policies, processes, and procedures for recovery from a major cyber incident. Participants improved their understanding of current cyber risks, awareness of incident response resources, strengthened relationships with counterparts, and refined communications strategies.

CYBER CHALLENGES

At the request of members, the Auto-ISAC sponsored the **CYBERAUTO** and **CYBERTRUCK CHALLENGES** in 2022.

These exciting events combine professional development and practicum-based training in a high-energy format that captures the imagination and raises awareness of participating students from around the globe.

The goal of Cyber Challenges is to reach across disciplines, companies, and organizations in the automotive and heavy-vehicle domain to establish a community of interest for automotive cybersecurity and help create a more universal and experienced base of engineers and managers.

Having a neutral playing ground for these groups to meet, collaborate, and learn from each other has been an invaluable resource for Ford. Not only does it build bridges between OEMs, but it is also providing a unique team building experience and is an excellent recruiting ground to find the Cyberauto engineers of tomorrow.

TIM GEIGER

MANAGER, VEHICLE AND MOBILITY CYBER SECURITY AT FORD MOTOR COMPANY AND AUTO-ISAC TREASURER





134

TRAINEES

Attended the Fundamentals Alpha and Beta Courses

224

INDIVIDUALS

From 53 member companies signed up for courses



ACT

AUTOMOTIVE CYBERSECURITY TRAINING

105

TRAINEES

Attended Advanced Alpha and Beta Courses

62

MEMBERS

Are scheduled to sit for the Capability Exercise (CAPEX) to qualify for the first Certified Automotive cyberSecurity Engineer (CASE) designation

ACT

In a world where connectivity is embedded in daily life, cybersecurity is critical. Proactive, effective security means protecting the entire lifecycle of vehicles, from design to manufacturing to daily operation.



Addressing the challenges specific to motor vehicles requires specialized skills and training. To close a gap in security education, the Auto-ISAC established the Automotive Cybersecurity Training (ACT) program. ACT is a comprehensive curriculum that supports workforce development and continuous education as crucial steps to improve motor vehicle cybersecurity.

DESIGN AND DEVELOPMENT OF THE ACT PROGRAM

The Automotive Cybersecurity Training (ACT) Team conducted research on existing vehicle cybersecurity training and education from across the globe. In the pilot program, the ACT team and Auto-ISAC membership work separately and in concert. By way of in-depth research and careful review, all stakeholders ensure the curriculum aligns with overarching auto industry needs. The surveys from the Alpha and Beta pilot will be used to determine any necessary course corrections for the training. Surveys will be implemented on a regular basis to ensure the ACT remains current in the changing landscape of cybersecurity.

ACT CLOSES THE EDUCATIONAL GAP BY:

Defining a comprehensive training program for vehicle cybersecurity training to improve safety and security.

Bridging the skill gap between cybersecurity enterprise and vehicle embedded systems training.

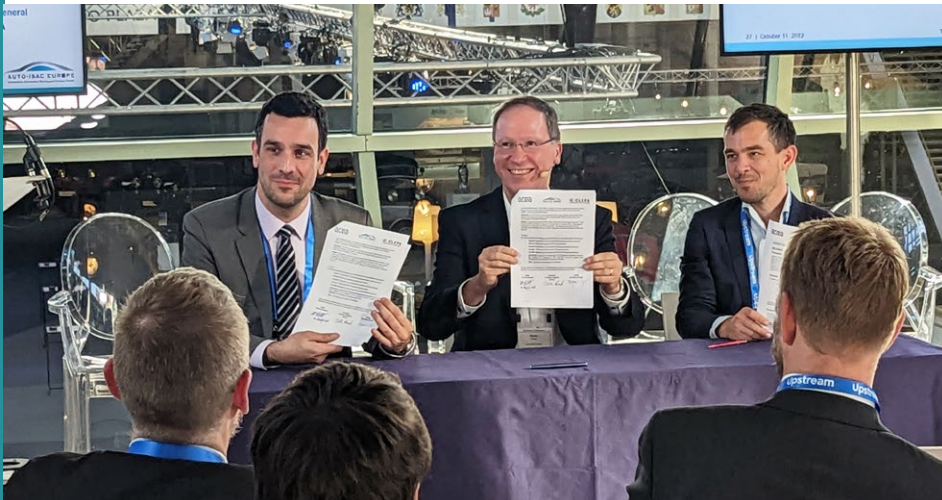
Providing guidance to academia to align with government/industry priorities in automotive cybersecurity.

AUTO-ISAC EUROPE



AUTO-ISAC EUROPE

Through global collaboration, we maximize our mission. In 2022, we solidified our presence in Europe through a formal collaboration with the European Automobile Manufacturers' Association (ACEA) and the European Association of Automotive Suppliers (CLEPA).



The automobile industry is one of the primary cutting-edge industries in Europe, with automakers leading the way towards a new generation of mobility that is ever more sustainable, safe, and smart. Through the European Auto-ISAC, we will push ahead with our digital transformation while working to protect the security of connected vehicles.

SIGRID DE VRIES ACEA DIRECTOR GENERAL

EURO WORKSHOP

Held in Brussels, Belgium, the two-day Q3 workshop had 72 participants including 55 members and 17 external partners. Our strategic partner Deloitte presented the outcome of our joint study on "How to set up a European ISAC" and together, we invited speakers from the European Commission, ENISA, and ACEA and CLEPA, and similar organizations.

The theme for day one was "Collaboration with Partners" and the second day was a members-only event for discussing topics of special interest to our European participants, including "Automotive Scoring of Vulnerabilities" and "Challenges for Setting Up a VSOC."

As a special highlight at the workshop, Auto-ISAC announced a formal collaboration with the ACEA and the CLEPA to create a central European hub for information sharing on motor vehicle cybersecurity. To make it official, the European ISAC Memorandum of Understanding with ACEA and CLEPA was signed at the event.

In the post-workshop survey, we gained valuable insights and highly positive feedback regarding content, location, and organization of the event which was supported by three external sponsors.

AUTO-ISAC EUROPE

EUROPEAN STEERING COMMITTEE

The European Office will be supported by the newly defined European Steering Committee (EuSC) which is composed of five designated representatives from our European members, the European Director, and the EuSC Chair who will also have a seat on the Auto-ISAC Board of Directors. The EuSC defines the strategic goals and general policy for Europe, and its main deliverable will be the creation of a manifesto for Europe based on the Auto-ISAC Europe Memorandum of Understanding with ACEA and CLEPA.

EUROPEAN STEERING MEMBERS 2022

VOLKSWAGEN
AKTIENGESELLSCHAFT

Continental 

BMW
GROUP

STELLANTIS 



2022 THREAT ASSESSMENT SUMMARY

The Auto-ISAC completed its third annual Automotive Threat Report which outlined the current automotive cyber threat landscape. It provided key outlooks regarding threats to automotive products (vehicles), business networks, and manufacturing systems in 2023. This annual Threat Assessment is collaboratively developed and produced by the members of the Auto-ISAC Product Working Group, IT/OT Working Group, and Intelligence & Analysis Staff. A **TLP:GREEN** version is available to all Auto-ISAC community partners by requesting access through the Auto-ISAC website.

Threats to Automotive Business (IT) and Manufacturing (OT) Operations

- Ransomware groups and other cybercriminals will attack some automotive OEMs', suppliers', and service providers' business infrastructure via internal or supply chain-based vulnerabilities, social engineering, or insiders.
- State-sponsored APT groups may attack some automotive OEMs', suppliers', and service providers' business and manufacturing infrastructure via internal or supply chain-based vulnerabilities, social engineering, or insiders.

Threats to Automotive Products (Vehicles)

- Technology-enabled vehicle theft activity will persist and its adverse impacts on customers' personal property and privacy will continue to attract negative attention to affected brands and the broader automotive industry.
- It is possible though unlikely that cyber threat actors will attack automotive products via internal or supply chain-based vulnerabilities to achieve outcomes other than vehicle theft.
- Compromised mobile devices that are connected to in-vehicle systems may cause the infotainment system to function in an unexpected or uncontrollable manner which could distract the vehicle operator.



AUTO-ISAC MEMBER ROSTER

(AS OF DECEMBER 31, 2022)

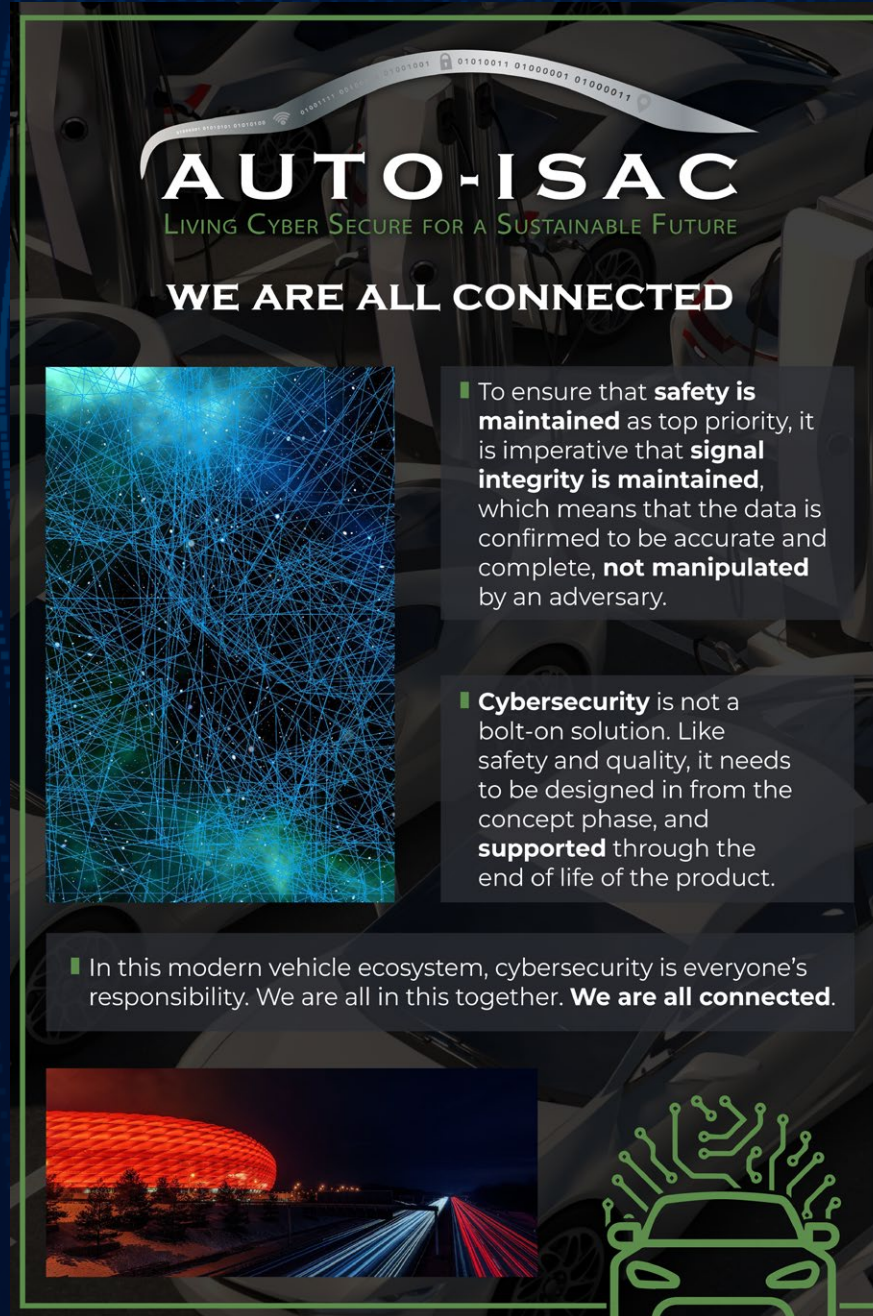
Aisin	Faurecia	Luminar Qualcomm	Qualcomm
Allison Transmission	Ferrari	Magna	Renesas Electronics
American Axle & Manufacturing	Flex	MARELLI	Stellantis
Aptiv	Ford	Mazda	Subaru
Argo AI	Garrett	Mercedes-Benz	Sumitomo Electric
AT&T	General Motors (Cruise-Affiliate)	Meritor	thyssenKrupp
AVL List GmbH	Geotab	Mitsubishi Electric	Tokai Rika
Blackberry Limited	Harman	Mitsubishi Motors	Toyota (Woven Planet-Affiliate)
BMW Group	Hitachi	Mobis	Tusimple
BorgWarner	Honda	Motional	Valeo
Bosch (ETAS-Affiliate)	Hyundai	Navistar	Veoneer
Canoo	Infineon	Nexteer Automotive Corp	Vitesco
ChargePoint	Intel	Nissan	Volkswagen
Continental (Argus-Affiliate)	John Deere Electronic	Nuro	Volvo Cars
Cummins	Kia America, Inc.	Nuspire	Volvo Group
Cymotive	Knorr-Bremse	NXP	Waymo
Denso	KTM	Oshkosh Corp	Yamaha Motors
e:fs TechHub GmbH	Lear	PACCAR	ZF
	LG Electronics	Panasonic	
	Lucid Motors	Polaris	

AUTO-ISAC STRATEGIC PARTNERS

(AS OF DECEMBER 31, 2022)

ArmorText	Cybellum	Deloitte	FEV
GRIMM	HackerOne	Irdeto	Itemis
Karamba Security	KELA	Pen Testing Partners	Red Balloon Security
Regulus Cyber	Saferide	Security Scorecard	Trustonic
Upstream	Vultara		

CYBERSECURITY AWARENESS MONTH


The graphic features a dark background with a car's engine and mechanical parts. At the top, a curved banner contains binary code (0s and 1s). The main title 'AUTO-ISAC' is in large white letters, with the tagline 'LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE' below it. The central theme 'WE ARE ALL CONNECTED' is written in white. A blue network diagram of interconnected nodes is on the left. Three text boxes on the right contain key messages. At the bottom, there are two images: a night view of a large, illuminated stadium and a stylized car icon with circuitry on top.

AUTO-ISAC

LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

WE ARE ALL CONNECTED

- To ensure that **safety is maintained** as top priority, it is imperative that **signal integrity is maintained**, which means that the data is confirmed to be accurate and complete, **not manipulated** by an adversary.
- **Cybersecurity** is not a bolt-on solution. Like safety and quality, it needs to be designed in from the concept phase, and **supported** through the end of life of the product.
- In this modern vehicle ecosystem, cybersecurity is everyone's responsibility. We are all in this together. **We are all connected.**



◀ BACK TO CYBERSECURITY AWARENESS MONTH

CYBERSECURITY AWARENESS MONTH

AUTO-ISAC
LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

PURPOSE DRIVEN SECURITY

- 
Advanced connectivity across the variety of smart devices requires application of a **purpose-driven security** approach to ensure that our customers and their data **are safe**.
- Application of key security principles such as **security-by-design** and **defense-in depth** are vital for a robust, secure system.

Incorporating key defense principles in security products and then ensuring **successful implementation through verification** and validation demonstrates a product with purpose-driven security is delivered to the customer.

- Security-by-design** ensures security controls and tools are built into devices from initial design phases and are incorporated in critical architecture.
- Defense-In-Depth** ensures multi-layered security mechanisms are utilized for a holistic cybersecurity strategy.

◀ [BACK TO CYBERSECURITY AWARENESS MONTH](#)

CYBERSECURITY AWARENESS MONTH



AUTO-ISAC

LIVING CYBER SECURE FOR A SUSTAINABLE FUTURE

BUILD & DELIVER SECURELY



TO BUILD A SECURE ENVIRONMENT IN MANUFACTURING, WE NEED TO:

- Keep our system **up-to-date**, Cyber criminals use vulnerabilities within systems, applications and devices. This is why it is important to **update or patch** them to ensure they are secure.
- Secure our **devices and accounts**, protect your devices with a lock screen, use **strong passphrases** for your online accounts and use **multi-factor authentication** for an extra layer of protection.
- **Be aware** of social engineering scams like phishing emails and malicious text messages. Watch for suspicious emails and text messages and **don't become a victim.**

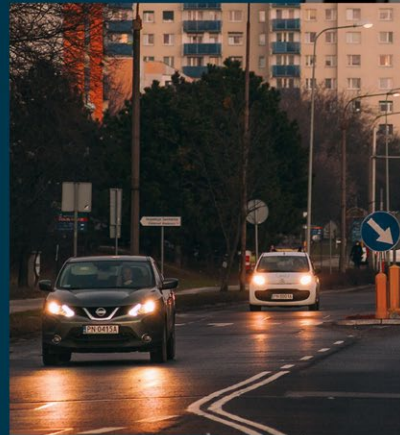


◀ BACK TO CYBERSECURITY
AWARENESS MONTH

CYBERSECURITY AWARENESS MONTH



CONTINUOUS SECURITY



■ As threats continually evolve, it is critical that we consider risk during the **entire vehicle lifecycle**. With vehicles becoming more connected and software driven, attack vectors and vulnerabilities increase.

■ **Over-the-air** updates will help to enable **cost effective** and **continuous** software and security maintenance. Vehicle Security Operations Center will continuously monitor, assess and correct these threats to help protect the vehicles of today and tomorrow, driving toward a safe and secure **future for all**.



◀ BACK TO CYBERSECURITY AWARENESS MONTH