Welcome to Auto-ISAC!

Monthly Virtual Community Call

March 06, 2024

This Session will be recorded.

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Traffic Light Protocol (TLP)

Version 2.0 Definitions

Color		When Should It Be Used?	How May It Be Shared?
TLP:RED 🔴⚪⚪	**Not for disclosure, restricted to participants only.**	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	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.
TLP:AMBER+STRICT ⚪🟡⚪	**Limited disclosure, restricted to participants' and its organization.**	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER ⚪🟡⚪	**Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.**	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN ⚪⚪🟢	**Limited disclosure, restricted to the community.**	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR ○○○	**Disclosure is not limited.**	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Source: https://www.us-cert.gov/tlp

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We’re Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ Intelligence Highlights
11:15	***DHS CISA Community Update*** ➢ **Jeff Terra, Joint Cyber Defense Collaborative (JCDC)**
11:20	**Featured Speaker:** ➢ **Jay Schwartz, SAE G-32: S.A.E. Cyber-Physical Systems Committee’s Electric Vehicle Illustrative Example Subcommittee Chair** ➢ **Title: “The SAE Electric Vehicle Charging Station Illustrative Example: How to apply JA7496 standard to Electric Charging Scenarios”**
11:55	**Q&A & 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:. **Slides are at TLP:CLEAR and on our website. Discussions are TLP:GREEN & may be shared across Auto-ISAC Community, "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! *"Cybersecurity is a Team Sport!"*

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

28 *OEM Members*

48 *Supplier & Commercial Vehicle Members*

21 *Navigator Partners*

20 *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)*

AUTO-ISAC
Automotive Information Sharing and Analysis Center

2024 Board of Directors

Thank you for your Leadership!

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

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

Stephen Roberts
Secretary *of the*
Board of the Directors
Honda

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

Oliver Creighton
Chair *of the EuSC*
BMW

Andrew Hillery
Chair *of the CAG*
Cummins

Amine Taleb
Chair *of the SAG*
Harman

Maryann Combs
Polaris

Bob Kaster
Bosch

Brian Witten
Aptiv

Auto-ISAC Member Roster

As of March 1, 2024

77 Members + 2 Pending

- Aisin
- Allison Transmission
- Amazon
- American Axle & Manufacturing
- Aptiv
- AT&T
- AVL List GmbH
- Blackberry Limited
- BMW Group
- BorgWarner
- Bosch (ETAS-Affiliate)
- Bose Automotive
- ChargePoint
- CNH Industrial
- Continental
- Cummins (Meritor-Affiliate)
- Dana Inc.
- Daimler Truck
- Denso
- Deere & Company
- e:fs TechHub GmbH
- Faurecia
- Ferrari
- Flex
- Ford
- General Motors (Cruise-Affiliate)
- Geotab
- Harman
- Hitachi (Astemo- Affiliate)
- Honda
- Hyundai
- Infineon
- Intel
- JTEKT
- Kia America, Inc.
- Knorr Bremse
- KTM
- Lear
- LG Electronics
- Lucid Motors
- Luminar
- Magna
- MARELLI
- Mazda
- Mercedes-Benz
- Mitsubishi Electric
- Mitsubishi Motors
- Mobis
- Motional
- Navistar
- Nexteer Automotive Corp
- Nissan
- NXP
- Oshkosh Corp
- PACCAR
- Panasonic (Ficosa-Affiliate)
- Phinia
- Polaris
- Qualcomm
- Renesas Electronics
- Rivian
- Stellantis
- Stoneridge
- Subaru
- Sumitomo Electric
- thyssenkrupp
- Tokai Rika
- Toyota (Woven-Affiliate)
- Valeo
- Veoneer
- Vitesco
- Volkswagen (Cariad-Affiliate)
- Volvo Cars
- Volvo Group
- Waymo
- Yamaha Motors
- ZF

Pending: Jaguar Land Rover, Renault SAS

**All times are in ET

Auto-ISAC Business Updates and Events

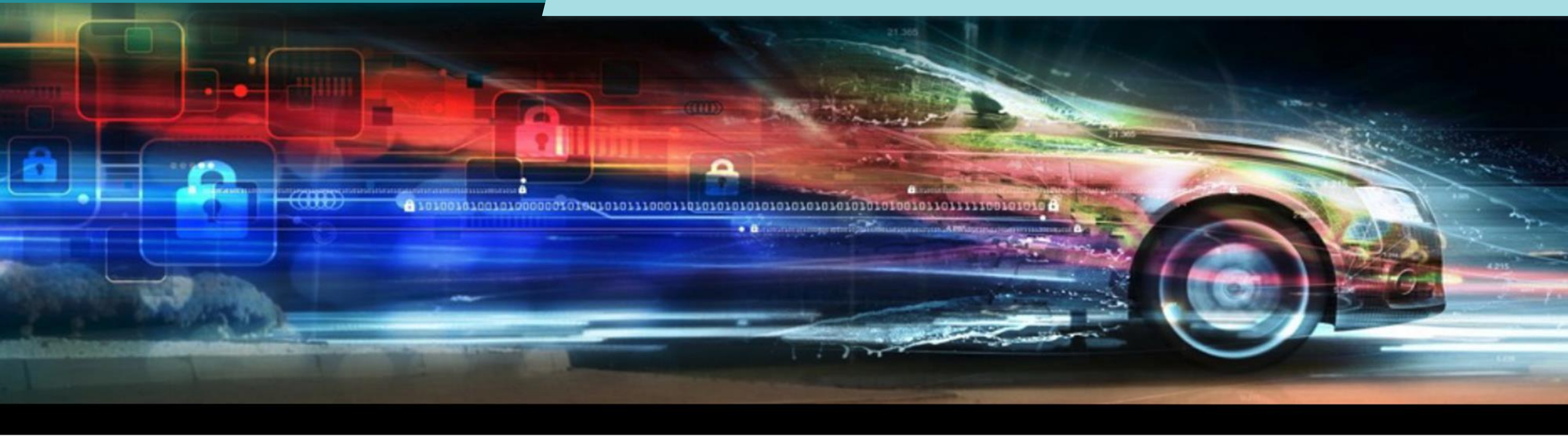
- **Community Call:** **Wednesday, April 3rd Time:** ***11:00am – 12:00 p.m.*** **Speaker: Brian Ramphal Comply.Law Title: Automotive Dealership Safeguard: Cybersecurity & Financial Compliance Guide**

- **Auto-ISAC 2nd European Summit - BMW Welt in Munich, Germany: June 12th – June 13th. The Titanium sponsor of the 2024 event will be BMW. Stay tuned for more details on our website.**

- **ACT Fundamental Course Block: Online, On-Demand, Anytime, Anywhere, and by Anyone $500/block**
  - **3 Blocks: Cybersecurity Basics (32 hrs.) | Security Engineering (28 hrs.) | Security Operations/Management (22.5 hrs.)**
  - **ACT Advanced Courses: *ACT Now!***

❑ **Cost per ADV Course: ***$2000 (Member Pricing), ($2250 Non-Member Pricing) with discount code.**

- **Advanced Engineering: January 22 - 26, 2024 FULL**
- **Wireless: February 5 - 9, 2024 FULL**
- **EV and EV Infrastructure: March 4 - 8, 2024 FULL**
- **Guided Attacks: April 29 - May 4, 2024 OPEN**
- **CAPEX to follow | Become CASE Certified!!**



Auto-ISAC Intelligence Highlight

Ricky Brooks, Intelligence Officer

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Intelligence

- Know what we track daily: subscribe to the DRIVEN; Auto-ISAC 2024 Threat Assessment for Members is complete; TLP:GREEN version will be released this month.
  - Send feedback, intelligence, or questions to analyst@automotiveisac.com

- Intelligence Notes
  - Geopolitical tensions involving Russia, China, North Korea, and Iran remain high with Russia-Ukraine and Israel-Hamas in crises (Russia-Ukraine [1] [2], Israel-Hamas [3], Iran, China [4] [5], North Korea [6]).
  - Ransomware [7] [8] Groups Targeting Automotive: 8Base, Akira, BianLian, Black Basta, Cactus, LockBit 3.0*, Mogilevich*, Alpha Locker/MyData
  - Notable Vehicle Research*: NDSS VehicleSec 2024 (NDSS); extracting SecOC keys (I CAN Hack); exploiting Unified Extensible Firmware Interface Vulnerabilities (Binarly); head unit hacking (Goncalo MB); exploiting China Edition Vulnerability Management tool (Cybellum, Delikley); 2024 Automotive Cybersecurity Report (Upstream); Automotive Cyberthreat Landscape Report (VicOne); Pwn2Own Automotive 2024 (VicOne).
  - Notable TTPs: Cloning GitHub repositories (arstechnica); living-off-the-land techniques (Interagency); integrating credential phishing and cloud account takeover (Proofpoint); exploiting Ivanti Connect Secure and Policy Secure Gateways (CISA, Mandiant); exploiting ConnecteWise ScreenConnect vulnerabilities (The Hacker News); using compromised credentials to access cloud service accounts (CISA); exploiting Cisco's Adaptive Security Appliance and Firepower Threat Defense products (Securityweek); Notable Tools: Glupteba (Unit 42); FudModule Rootkit (Avast); Bumblebee (Proofpoint).

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.
- 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*

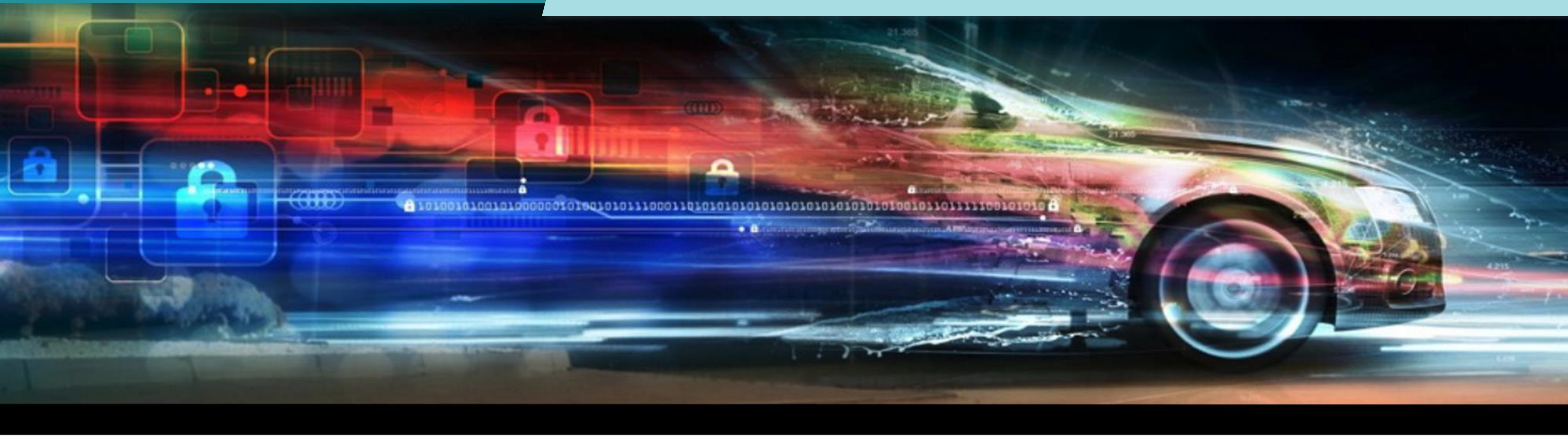
30+ *Featured Speakers to date*

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*



Featured Speaker

Meet the Speaker

Jay Schwartz, SAE G-32

Jay Schwartz has over 30 years of experience as an embedded software engineer in the automotive industry. He has worked on automated machine tools used in the assembly plant, diagnostic scan tools, and various onboard electronic control units. For the past 10 years, he has been involved with specifications and requirements for onboard cybersecurity for both his employers and SAE.

Jay was a Captain in the U.S. Air Force Auxiliary / Civil Air Patrol. He served as both a Squadron Communications Officer and Communications School Instructor.

He has been a licensed and active Amateur (Ham) Radio Operator since 1974 and has earned his Amateur Extra class (this highest possible class) license. His major Ham radio accomplishment was the privilege of being on the software team for the OSCAR 85 Amateur Radio cubestat communication satellite. (It was an orbiting FM repeater which did fly and has successfully completed its multi year mission.)

Jay has a B.S. Industrial Management, a B.S. Electrical Engineering, and B.S. Computer Science from Lawrence Technological University in Southfield, MI.

2024 Guest Speaker

Speaker AIM:

-Applying G-32 SAE JA7496 to an Electric Vehicle charging scenario

Electric vehicle charging stations are:

- **Proliferating**, and no end in sight for how many of them will ultimately exist.
- These stations are **highly dependent** on how they **interface** with both the vehicle and “the world”.
- **Electronic sophistication** requires them to be designed cybersafe and cybersecure.
- A **CPS Security Engineering Plan** is required (system context) that is agnostic to their hardware, software, electronic data, and functional purpose and properties.

Agenda for Presentation

TOPICS TO BE COVERED

1. What is the SAE G-32 Cyber Physical Systems Committee
   - Joint CPS Security committee
   - Bridging Pan-Industry standards and solutions

2. Electric Vehicle Illustrative Example subcommittee
   - Illustrate how to apply JA7496 standard to Electric Charging Scenario
   - Free videos available now

     a. Part 0 – Introduction – available for viewing at SAE – G-32

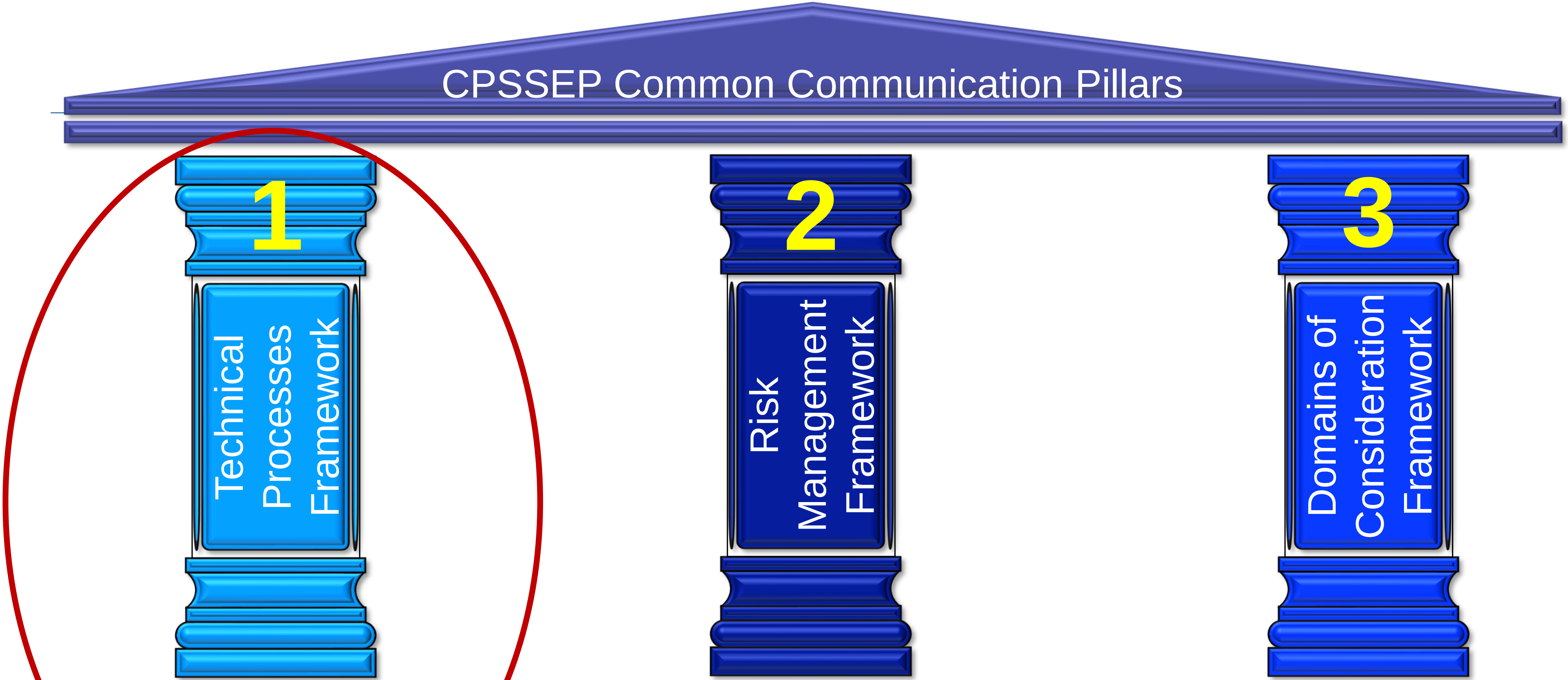
     b. Part 1 - video (17mins) – Adopting the CPSS technical process to incorporate secure product development

3. Q & A – save until end, note the slide number or email: jayschwartz200@yahoo.com

Links:

SAE G-32 Part 0 Introduction
SAE G-32 Part 1 CPSS vs Technical Processes

CPSSEP Common Communication Pillars



1 Technical Processes Framework

2 Risk Management Framework

3 Domains of Consideration Framework

…shall document in their CPSSEP their system and software engineering technical processes listed…

(JA7496, Section 3.3 as of 11/18/2022)

…shall develop and implement a risk based CPSSEP in accordance with the requirements specified…

(JA7496, Section 3 as of 11/18/2022)

… represent a set of areas to consider, when determining whether and how to manage CPSS risks …

(JA7496, Section 3.1 as of 11/08/2022)

PART 1

ADJUSTING OR ADOPTING THE CYBER-PHYSICAL SYSTEM SECURITY (CPSS) TECHNICAL PROCESSES TO INCORPORATE SECURE PRODUCT DEVELOPMENT

G-32 Cyber Physical Systems Committee General Information

- Today's presentation is only a small portion of what the team is working on.
- You are formally invited to participate in its ongoing work.
- All of these teams meet online and use Microsoft Teams, all times are U.S. Eastern, and all meetings are 1 hour long.
- The main team meets every Thursday at 11:00 hrs.
- The E.V. team meets every Monday at 13:00 hrs.
- The Software team meets every Tuesday at 13:00 hrs.
- The Hardware team meets every Tuesday at 16:00 hrs.
- The meeting announcements and links are at: G-32 Cyber Physical Systems Security Committee - SAE StandardsWorks
- To get on the mailing list send a request to: SAE G32 Staff Representative Ms. Dorothy Lloyd at dlloyd@sae.org and request to be put onto the G32 mailing list

Thank you for attending this presentation

Q & A

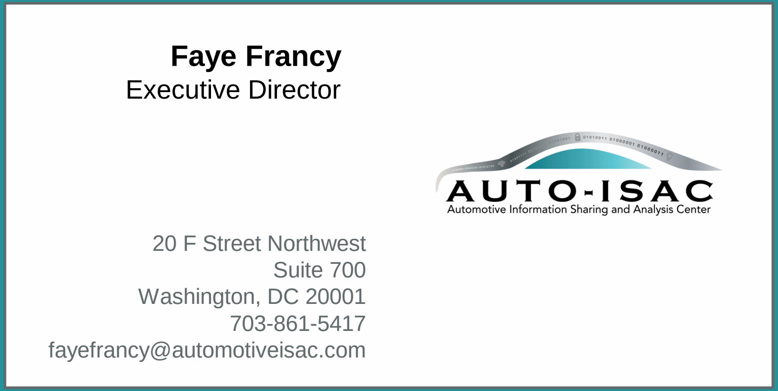
Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

Thank You

THANK
YOU
MAAKE
TERMA KASIH
RAIBH MAITH AGAT
GRAZIE
MULTUMESC
JUSPAXAR
OBRIGADO
MATONDO
SALAMAT
KIITOS
MOCHCHAKKERAM
MERCI
KIA ORA
MULTUMESC
CHOKRANE
SALAMAT
CAM ON BAN
RAIBH MAITH AGAT
MERCI
MERCI
MOCHCHAKKERAM
OBRIGADO
MOCHCHAKKERAM
GRAZIE
ASANTE
CHOKRANE
MATUR NUWUN
UA TSAUG RAU KOJ
MOCHCHAKKERAM
MATONDO
WELALIN
KIITOS
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
RAIBH MAITH AGAT
SPASIBO
SPASIBO
MAAKE
OBRIGADO
ARIGATO
KIITOS
DANKON
MOCHCHAKKERAM
NIRRINGRAZZJAK
MOCHCHAKKERAM
OBRIGADO
SPASIBO
MULTUMESC
VINAKA
NIRRINGRAZZJAK
MAMANA
OBRIGADO
DANK JE

Our Contact Info



Faye Francy
Executive Director

AUTO-ISAC
Automotive Information Sharing and Analysis Center

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

AUTO-ISAC
Automotive Information Sharing and Analysis Center

AUTOMOTIVEISAC.COM