



WELCOME TO AUTO-ISAC!

MONTHLY VIRTUAL COMMUNITY CALL

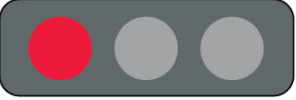



June 1, 2022

This Session will be recorded.

TLP:WHITE



DHS TRAFFIC LIGHT PROTOCOL (TLP) CHART

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

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

AGENDA

Time (ET)	Topic
11:00	Welcome <ul style="list-style-type: none">➤ Why We're Here➤ Expectations for This Community
11:05	Auto-ISAC Update <ul style="list-style-type: none">➤ Auto-ISAC Activities➤ Heard Around the Community➤ What's Trending
11:15	<i>DHS CISA Community Update</i>
11:20	Featured Speaker: <ul style="list-style-type: none">▪ François-Frédéric Ozog, Director, Business Development, Linaro
11:45	Around the Room <ul style="list-style-type: none">➤ Sharing Around the Virtual Room
11:55	Closing Remarks

WELCOME - AUTO-ISAC COMMUNITY CALL!

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

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

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

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

How to Connect: For further info, questions or to add other POCs to the invite, please contact us!

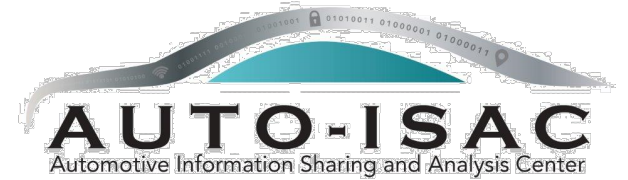
(sharmilakhadka@automotiveisac.com)



ENGAGING IN THE AUTO-ISAC COMMUNITY

❖ Join

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



❖ Participate

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

22
OEM Members

21
Navigator Partners

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

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

43 *Supplier & Commercial Vehicle Members*

13
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)*



2022 - 2023 BOARD OF DIRECTORS

EXECUTIVE COMMITTEE (EXCOM)



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



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



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

2022-2023 ADVISORY BOARD (AB) LEADERSHIP



Todd Lawless
*Chair of the
Advisory Board*
Continental



Bob Kaster
*Vice Chair of the
Advisory Board*
Bosch



Allen Houck
Chair of the SAG
NXP



Larry Hilken
Chair of the CAG
Cummins

MEMBER ROSTER

AS OF JUNE 1, 2022

Highlight = Change

68 Members, 2 in Progress

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

UPCOMING EVENTS

➤ Upcoming Meetings

➤ Q2 European Workshop:

- Wednesday, June 22 **Theme:** Streamlining Information Sharing **Time:** 1-5 pm CET (7-11 am ET)
[Register here.](#) **TLP:AMBER**

➤ IT/OTWG Quarterly Workshop (Virtual) Thursday June 30 **Time:** 9 a.m. – 12 p.m. **TLP:AMBER**

➤ Members Teaching Members:

- Wednesday, July 20 **Speaker:** Larry Hilkene, Cummins et al. **Title:** TBD (J1939 Topic) **Time:** 10 – 11:30 a.m. **TLP:AMBER**

➤ Announcements

- **Auto-ISAC Cybersecurity Summit – *Registration is Open!*** Both in-person and virtual venue. Dates: September 7-8, 2022 in Dearborn, MI at The Henry Hotel. Your Company PoC has the “free passes” please check with them!
- **TLP:GREEN** version of the **Annual Report** has been approved and was released May 4.

2022 AUTO-ISAC CYBERSECURITY SUMMIT

DRIVING A SECURE FUTURE

Hybrid Event • Dearborn, MI and Virtual • September 7-8, 2022



[More information here](#)

EVENT HOST & TITANIUM SPONSOR





AUTO-ISAC INTELLIGENCE

TLP:WHITE



AUTO-ISAC INTELLIGENCE

- Know what we track daily: [subscribe](#) to the DRIVEN; know our strategic view of the cyber threat environment: read the **TLP:GREEN** Threat Assessment in our 2021 Annual Report
 - **Send feedback**, contributions, or questions to analyst@automotiveisac.com
- Intelligence Notes
 - We continue to advise the automotive community to maintain heightened vigilance for indications of malicious activity or compromise within their business networks and industrial systems. We expect the Russia threat to persist after hostilities end ([CISA-Known Exploited Vulnerabilities Catalog](#), [CISA Shields Up](#), [CISA-Technical Approaches to Uncovering and Remediating Malicious Activity](#)).
 - We continue to see threat actors targeting automotive companies' business networks with ransomware (including [Hive](#), [Lockbit 2.0](#), [Black Basta](#), [Vice Society](#)) and other cyberattacks. Impacts include theft of sensitive proprietary information and customer data, and disruption of business operations.
 - Other than vehicle theft, we are not seeing malicious cyberattacks on vehicles. We continue to consume and internally discuss the latest vehicle cybersecurity research.
 - Notable Tactics Techniques and Procedures: Credential Stuffing ([MITRE](#)); Zero-Click ([SecurityWeek](#)); Exploitation of Vulnerabilities in Enterprise Resource Planning Solution ([Cybereason](#)); Spoofing Software-as-a-Service Vanity Uniform Resource Locators ([Varonis](#)); Exploitation of Known vs. zero-day Vulnerabilities ([ThreatPost](#)).

CISA RESOURCE HIGHLIGHTS



TLP: WHITE – Corporate Security Symposium (CSS)

- Events coordinated between DHS Intelligence & Analysis (I&A) Private Sector Engagement, Domestic Security Alliance Council, state and local governments, and private sector partners
- Provides a forum for public and private sector partners to discuss current and emerging security threats relevant to their regions
- Provides opportunities to forge new relationships and strengthen existing relationships
- See <https://www.dhs.gov/private-sector-engagement>, <https://www.dhs.gov/publication/css-one-pager>, and <https://www.dsac.gov>
- Contact email for more information at I&APrivateSector@hq.dhs.gov



TLP: WHITE – CISA Current Activities – Joint Products

- **5G Security Evaluation Process Investigation Study – CISA, DoD**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/26/cisa-and-dod-release-5g-security-evaluation-process-investigation](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/26/cisa-and-dod-release-5g-security-evaluation-process-investigation)
 - [https://www\[.\]cisa\[.\]gov/blog/2022/05/26/cisa-dhs-st-dod-introduce-results-assessment-5g-security-evaluation-process](https://www[.]cisa[.]gov/blog/2022/05/26/cisa-dhs-st-dod-introduce-results-assessment-5g-security-evaluation-process)
- **Weak Security Controls and Practices Routinely Exploited for Initial Access – Cybersecurity authorities of US, Canada, New Zealand, Netherlands, UK**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/17/weak-security-controls-and-practices-routinely-exploited-initial](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/17/weak-security-controls-and-practices-routinely-exploited-initial)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-137a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-137a)



TLP: WHITE – CISA Current Activities – Joint Products - continued

- **Advisory on Protecting MSPs and their Customers – Cybersecurity authorities of US, UK, Australia, New Zealand**

- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/11/cisa-joins-partners-release-advisory-protecting-msps-and-their](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/11/cisa-joins-partners-release-advisory-protecting-msps-and-their)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-131a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-131a)

- **U.S. Government Attributes Cyberattacks on SATCOM Networks to Russian State-Sponsored Malicious Cyber Actors – CISA, FBI**

- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/10/us-government-attributes-cyberattacks-satcom-networks-russian](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/10/us-government-attributes-cyberattacks-satcom-networks-russian)
- [https://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-076a](https://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-076a)



TLP: WHITE – CISA Current Activities

- **CISA Issues Emergency Directive and Releases Advisory Related to VMware Vulnerabilities**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/18/cisa-issues-emergency-directive-and-releases-advisory-related](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/18/cisa-issues-emergency-directive-and-releases-advisory-related)
 - [https://www\[.\]cisa\[.\]gov/emergency-directive-22-03](https://www[.]cisa[.]gov/emergency-directive-22-03)
 - [http://www\[.\]cisa\[.\]gov/uscert/ncas/alerts/aa22-138b](http://www[.]cisa[.]gov/uscert/ncas/alerts/aa22-138b)

- **CISA Releases Analysis of FY21 Risk and Vulnerability Assessments**
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/19/cisa-releases-analysis-fy21-risk-and-vulnerability-assessments](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/19/cisa-releases-analysis-fy21-risk-and-vulnerability-assessments)
 - [https://www\[.\]cisa\[.\]gov/cyber-assessments](https://www[.]cisa[.]gov/cyber-assessments)



TLP: WHITE – Eighty-four (84) Known Exploited Vulnerabilities (KEV) added to the catalog in April 2022:

- [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/25/cisa-adds-34-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/25/cisa-adds-34-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/24/cisa-adds-20-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/24/cisa-adds-20-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/23/cisa-adds-21-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/23/cisa-adds-21-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/16/cisa-adds-two-known-exploited-vulnerability-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/16/cisa-adds-two-known-exploited-vulnerability-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/11/cisa-adds-one-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/11/cisa-adds-one-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/10/cisa-adds-one-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/10/cisa-adds-one-known-exploited-vulnerabilities-catalog)
 - [https://www\[.\]cisa\[.\]gov/uscert/ncas/current-activity/2022/05/04/cisa-adds-five-known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/uscert/ncas/current-activity/2022/05/04/cisa-adds-five-known-exploited-vulnerabilities-catalog)
- **KEV Catalog:**
- [https://www\[.\]cisa\[.\]gov/known-exploited-vulnerabilities-catalog](https://www[.]cisa[.]gov/known-exploited-vulnerabilities-catalog)



TLP: WHITE – Additional Resources From CISA

- CISA Homepage - [https://www\[.\]cisa\[.\]gov/](https://www[.]cisa[.]gov/)
- CISA NCAS – [https://us-cert\[.\]cisa\[.\]gov/](https://us-cert[.]cisa[.]gov/)
- CISA Shields Up - [https://www\[.\]cisa\[.\]gov/shields-up](https://www[.]cisa[.]gov/shields-up)
- Free Cybersecurity Services and Tools - [https://www\[.\]cisa\[.\]gov/free-cybersecurity-services-and-tools](https://www[.]cisa[.]gov/free-cybersecurity-services-and-tools)
- CISA News Room - [https://www\[.\]cisa\[.\]gov/cisa/newsroom](https://www[.]cisa[.]gov/cisa/newsroom)
- CISA Blog - [https://www\[.\]cisa\[.\]gov/blog-list](https://www[.]cisa[.]gov/blog-list)
- CISA Publications Library - [https://www\[.\]cisa\[.\]gov/publications-library](https://www[.]cisa[.]gov/publications-library)
- CISA Cyber Resource Hub - [https://www\[.\]cisa\[.\]gov/cyber-resource-hub](https://www[.]cisa[.]gov/cyber-resource-hub)
- CISA Cybersecurity Directives - [https://cyber\[.\]dhs\[.\]gov/directives/](https://cyber[.]dhs[.]gov/directives/)





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

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



AUTO-ISAC COMMUNITY MEETING

Why Do We Feature Speakers?

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

What Does it Mean to Be Featured?

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

How Can I Be Featured?

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

30+
*Featured
Speakers to
date*

7 *Best
Practice
Guides
available on
website*

2000+
*Community
Participants*





FEATURED SPEAKER

TLP:WHITE



FRANÇOIS-FRÉDÉRIC OZOG, LINARO

DIRECTOR OF BUSINESS DEVELOPMENT



François-Frédéric is an entrepreneur with almost 40 years of experience in technical, sales and marketing positions. He is director of business development at Linaro which is a collaborative engineering organization working for its members such as Arm, Google, Qualcomm, Huawei.

In addition to his business role, François-Frédéric chairs Linaro industrial edge segment group and leads the automotive initiative. François-Frédéric holds a degree in computing science from Université de Paris VII.

He is the author of seven patents and was recognized by ETSI NFV for contributions in acceleration interfaces.

Cybersecurity

Made simpler for firmware, hypervisor and OS



Member companies Linaro collaborates with



In My Humble Opinion

The Good

ISO 21434

UN-R155, UN-R156 / ISO 24089

Not an afterthought

Builders/Breakers

Auto-ISAC

The Bad

Richer authorization schemes missing
(key duplicates, P2P, insurance...)

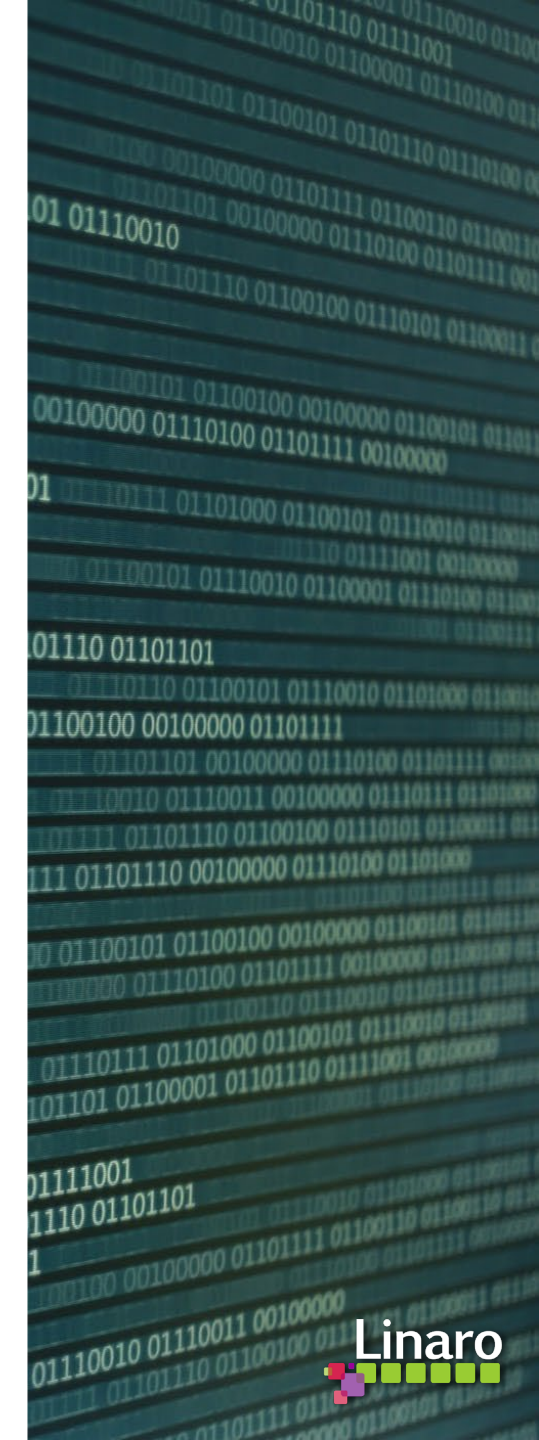
Standardized dependable cybersecurity

Virtualization and Confidential Computing

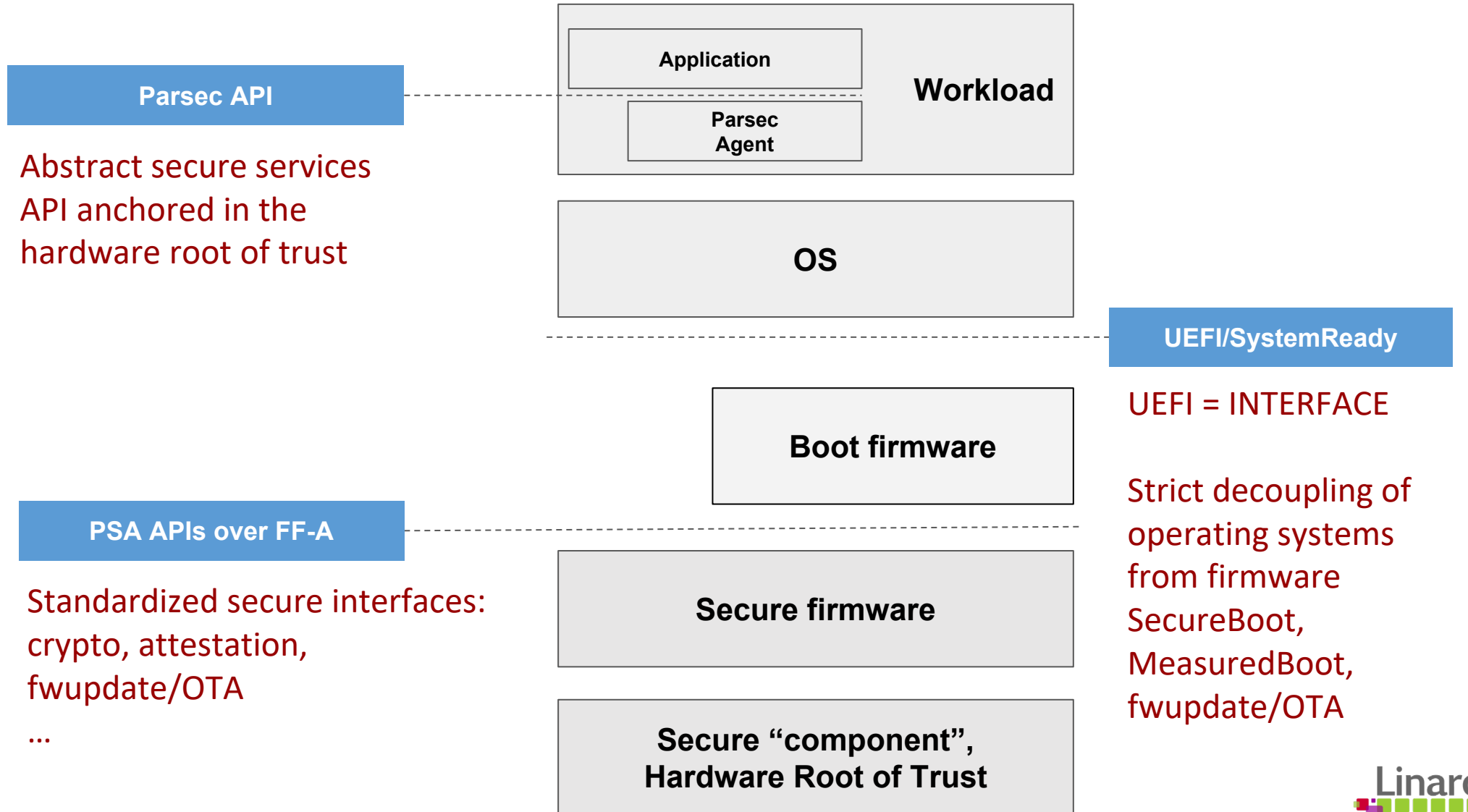
The ugly

Do you know your hardware and firmware?

Arm new standards



Arm Cassini



SystemReady flavors / generalized UEFI interface

SystemReady-IR

- U-Boot and device tree (DT) based
 - UEFI interface implementation (SecureBoot, MeasuredBoot...)
 - Backward and forward compatibility through certification of DT
 - Firmware provided authenticated DT preferred method
- System Device Tree work in progress

SystemReady-ES

- Embedded servers, EDK2 and ACPI based
 - Currently more targeted at telecom edge
 - Safety hurdles: EDK2 cyclomatic complexity > 10 times U-Boot, ACPI byte code engine

SystemReady-LS

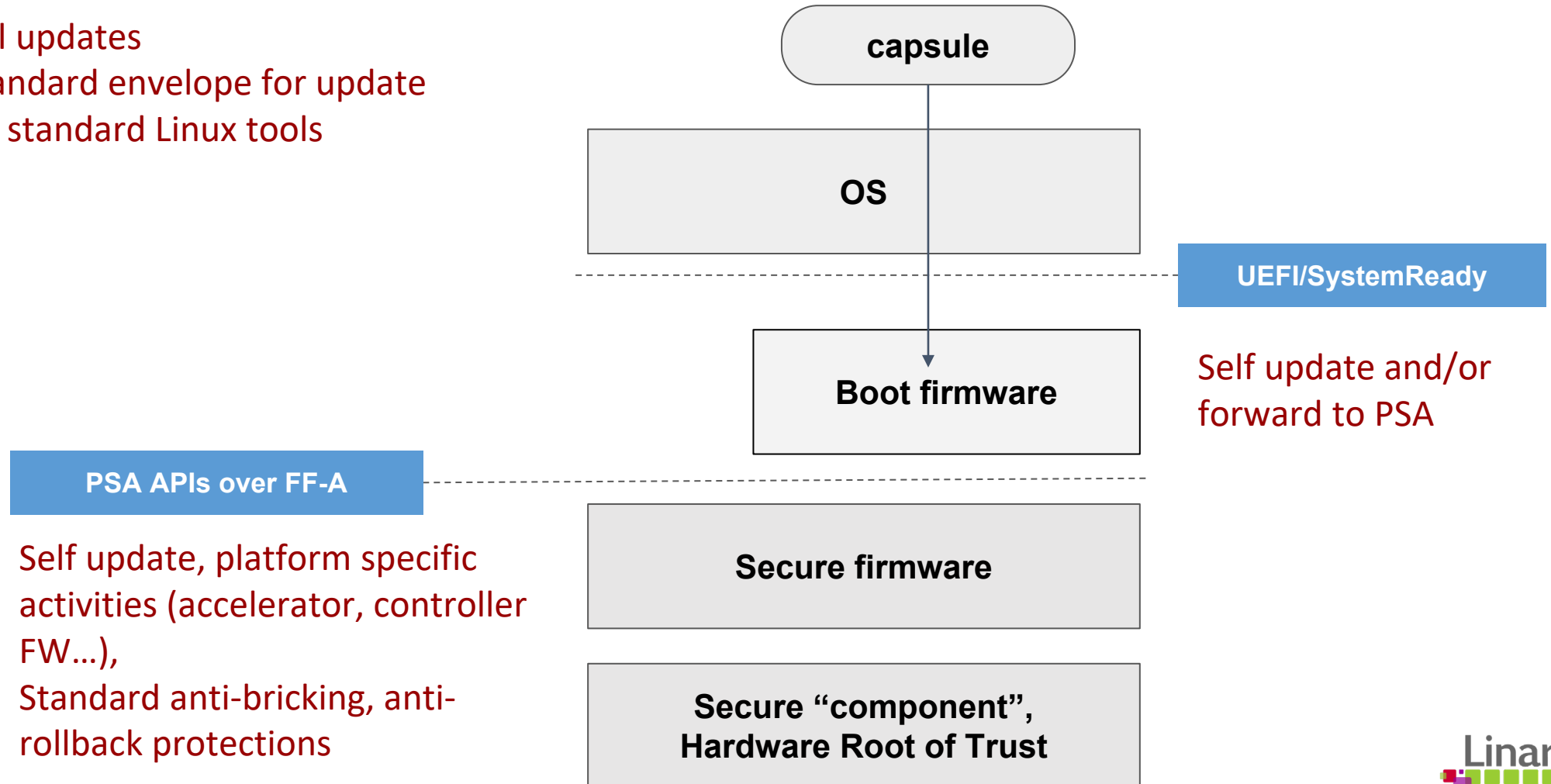
- LinuxBoot + minimal UEFI (possibly ACPI or DT, probably DT for embedded)

SystemReady-SR

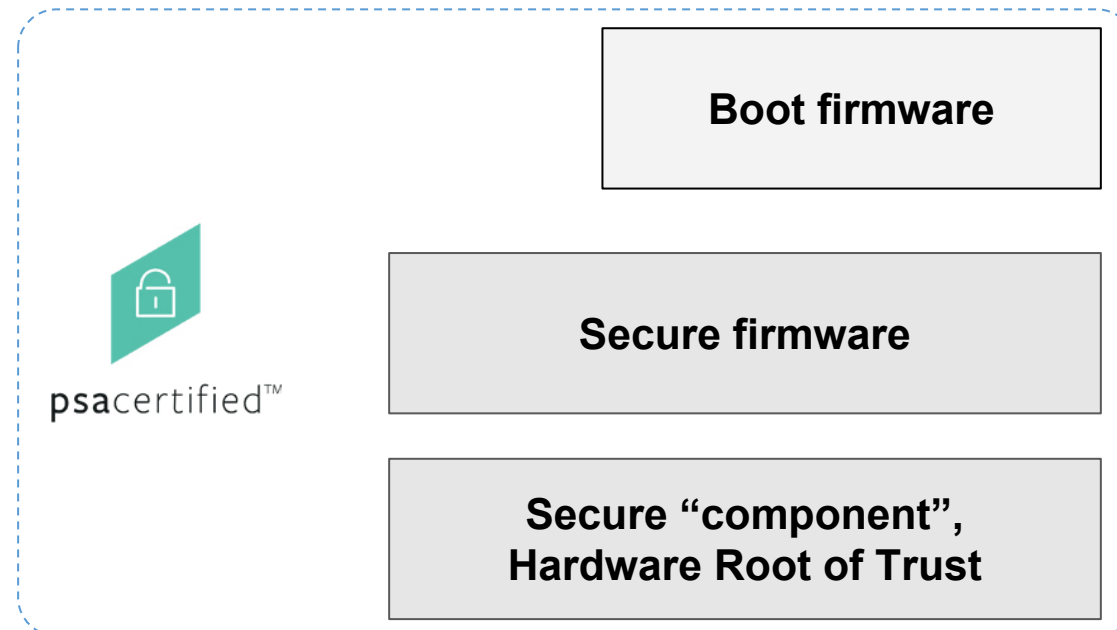
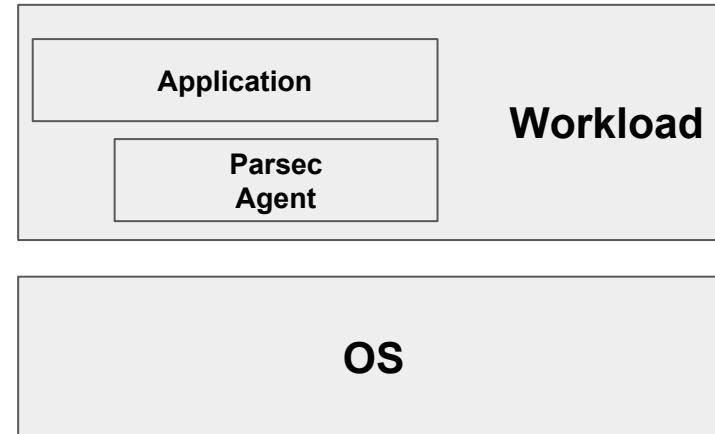
- Servers, EDK2 and ACPI based

Standardized firmware update: capsules

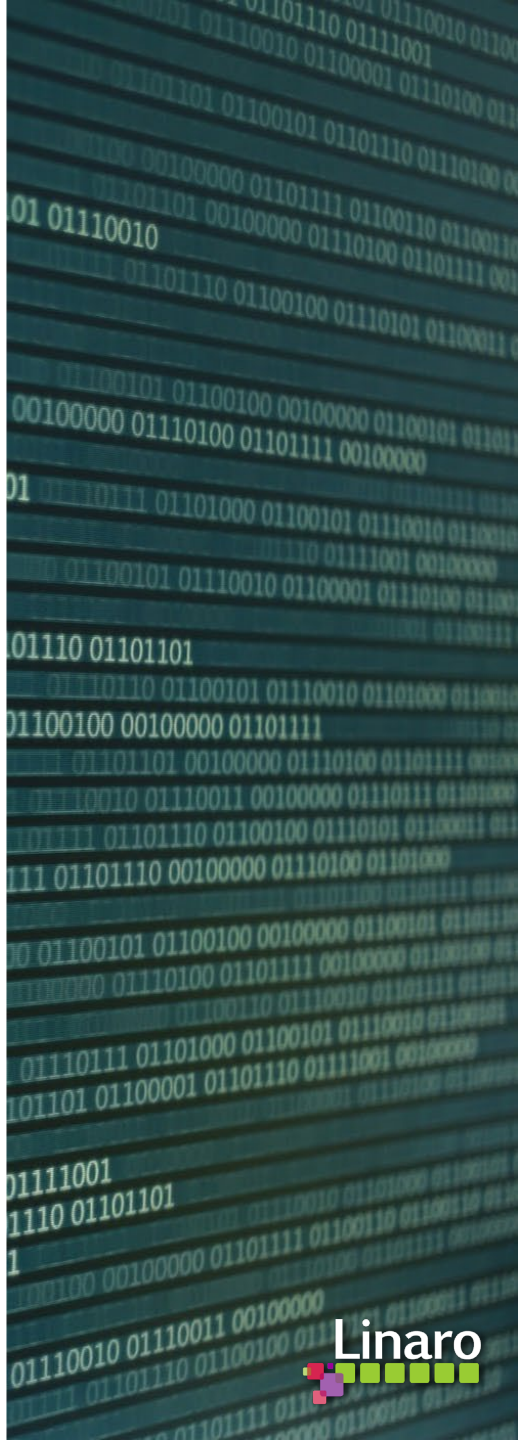
- Transactional updates
- Capsule is standard envelope for update
- Integrated in standard Linux tools



Arm PSA certified

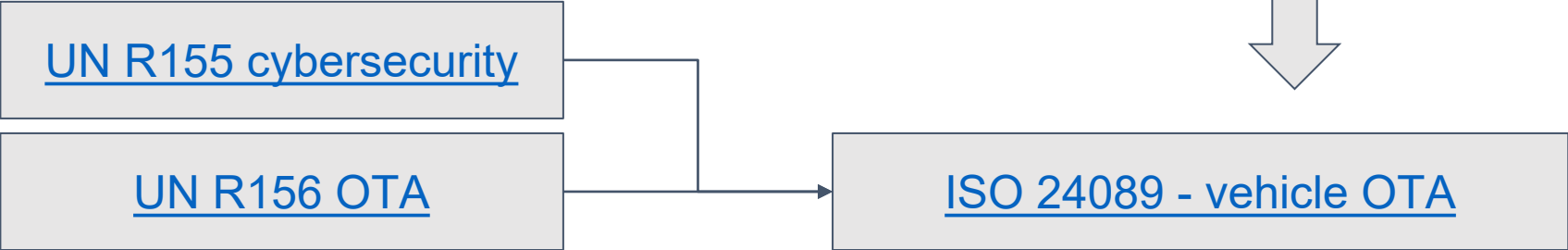


Firmware



Regulations, standards & recommendations

UN WP.29:



NIST 800 series

UN-R155 Annex 5 - threat analysis done

4	High level and sub-level descriptions of vulnerability/ threat	Example of vulnerability or attack method	Ref	Mitigation	GAP	
62	4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened	26 Cryptographic technologies can be compromised or are insufficiently applied	26.1	Combination of short encryption keys and long period of validity enables attacker to break encryption	M23 Cybersecurity best practices for software and hardware development shall be followed	- security policy based on the best practice
63			26.2	Insufficient use of cryptographic algorithms to protect sensitive systems		
64			26.3	Using already or soon to be deprecated cryptographic algorithms		
65		27 Parts or supplies could be compromised to permit vehicles to be attacked	27.1	Hardware or software, engineered to enable an attack or fails to meet design criteria to stop an attack	M23 Cybersecurity best practices for software and hardware development shall be followed	- security fault tree analysis
66	Software or hardware development permits vulnerabilities		28.1	Software bugs. The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present	M23 Cybersecurity best practices for software and hardware development shall be followed Cybersecurity testing with adequate coverage	- Security test automation? - LAVA Lab extension to support JTAG/debug ports ,etc.
67			28.2	Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) can permit access to ECUs or permit attackers to gain higher privileges		
68	Network design introduces vulnerabilities		29.1	Superfluous internet ports left open, providing access to network systems	M23 Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity best practices for system design and system integration shall be followed	Network segmentation/isolation
69			29.2	Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages		
70	Physical loss of data loss		30.1	Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft	M24 Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. Example Security Controls can be found in ISO/SC27/WG5	sentitive data must be cloned in cloud
71			30.2	Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues		DRM must not remove the data
72			30.3	The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example)		sentitive data must be cloned in cloud
73	Unintended transfer of data can occur	31.1	Information breach. Personal data may be leaked when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)	M24 Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data.	- Secure storage cleanup? - activation/decryption system for personal data	
	Physical manipulation of systems can enable an attack	32.1	Manipulation of electronic hardware, e.g. unauthorized electronic hardware added to a vehicle to enable "man-in-the-middle" attack	M9 Measures to prevent and detect unauthorized access shall be employed	N/A (Hardware electrical anti-temper hardening is required.)	

UN-R155 impact on firmware

Taxonomy of firmware

- xCU
 - Application processor boot, runtime and confidential compute services
 - Controllers (Arm System Control Processor, Intel Management Engine)
 - Devices (GPU, 5G modem...)
- Key FOB

Basics

- Secure Boot + Measured Boot + Full disk encryption
- Standard OTA with anti-bricking, anti-rollback protections

Less obvious

- Device Identifier Composition Engine (DICE)
- Fault injection resilience (Secure Boot evasion for instance)
- Detection of abnormal behavior
- Firmware re-encryption (*image attacks do not leak to all instances of the same model*)

UN-R156 impact on firmware

UN-R156 / 7.1.2.3

“For every RXSWIN, there shall be an auditable register describing all the software relevant to the RXSWIN of the vehicle type before and after an update. This shall include information of the software versions and their integrity validation data for all relevant software for each RXSWIN.”

ISO24089 / 9.3.2.7

“The integrity and authenticity of the software update package shall be verified before activation in a recipient of the software update operation.”

- Non repudiable audit trails (not just for OTA)
- Collect vehicle IDs (unique or not) interface (to prepare for OTA campaigns)
- Software IDs and versions across all aspects (accelerator firmware...)
- Transactional multi-xCU OTA

Additional firmware needs for automotive

Dependable boot (A/B and per OS vouching)

Boot time

Freedom of interference for safety workloads

System Control and Management Interface (SCMI) and virtualized SCMI

firmwareTPM (per tenant instances)

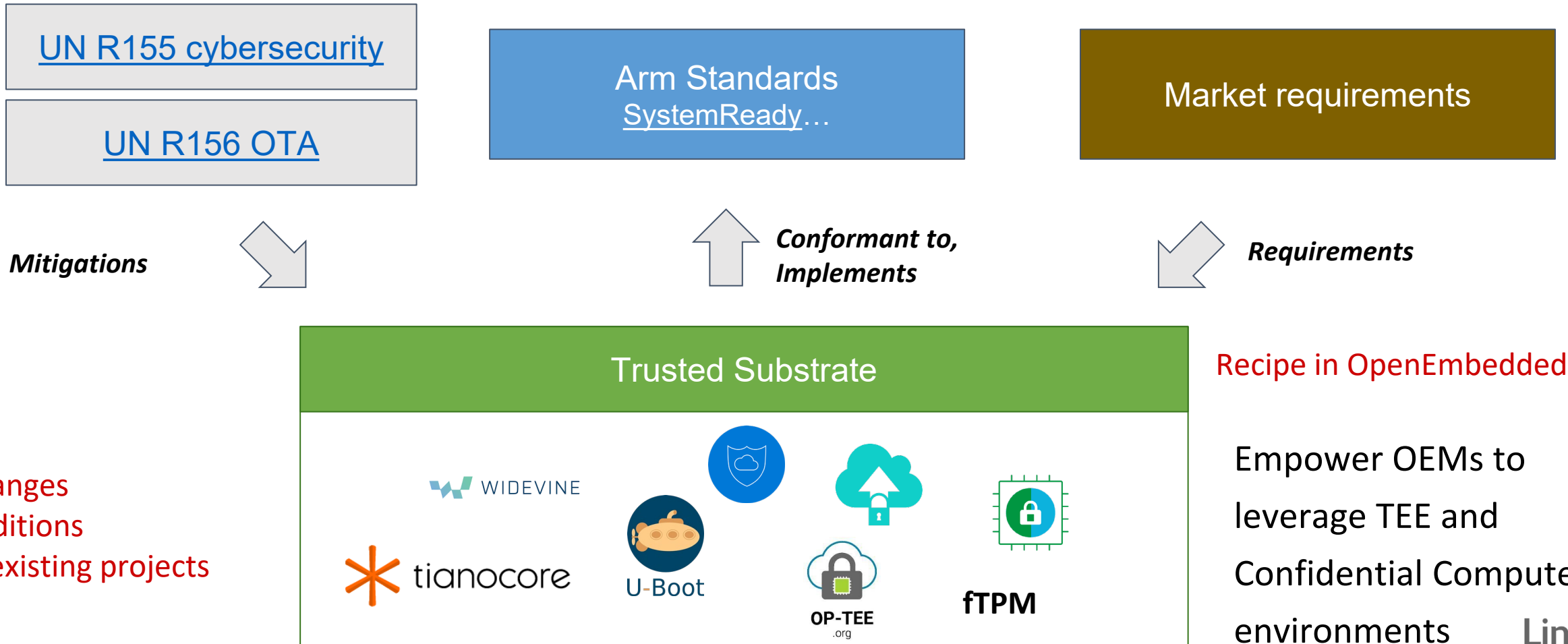
TEE support

- SoC generic: Crypto services, secure storage, attestation services
- 3rd Party: DRM, non repudiable logging
- TEE access with hypervisor, virtualized TEE

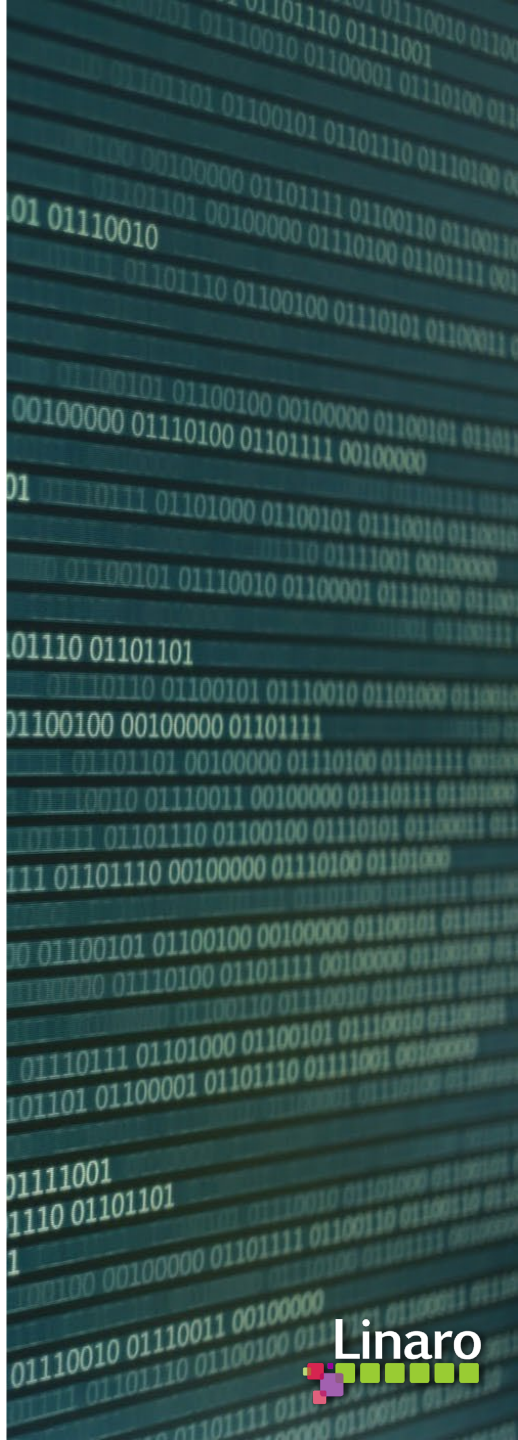
Confidential Compute support

- V8 in TrustZone, v9 in Realms and TrustZone (Open Enclave SDK)
- In-vehicle with cloud extensions multi-tenancy

Implementing SystemReady for automotive



Hypervisor



Embedded hypervisor cybersecurity

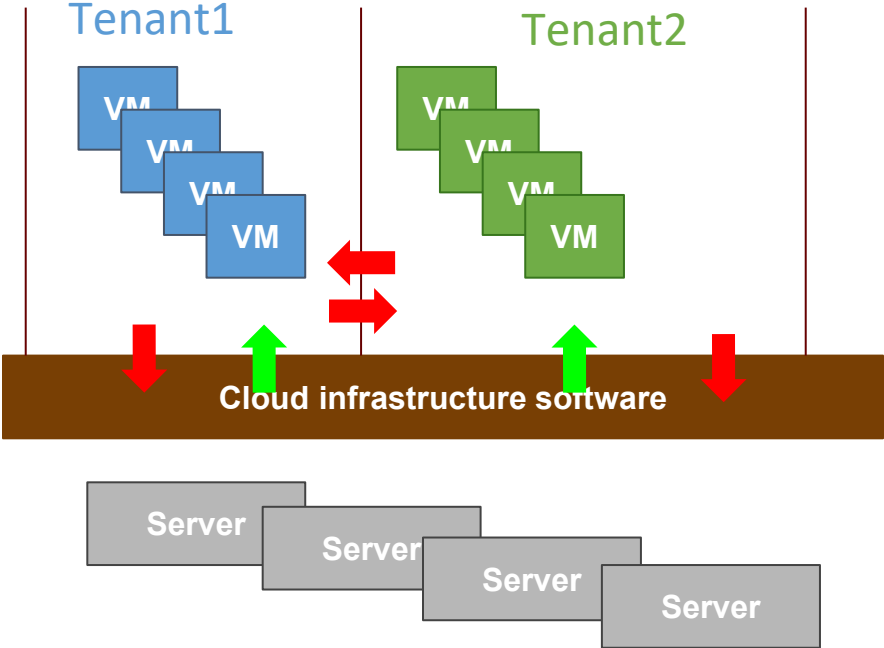
Hypervisor robustness

- UN-R155/156 requirements translation yet to be done
- Cybersecurity domains are still to be formalized/accepted:
 - core, VMM and overall orchestration, devices, updates (firmware, hypervisor, images, applications/models)

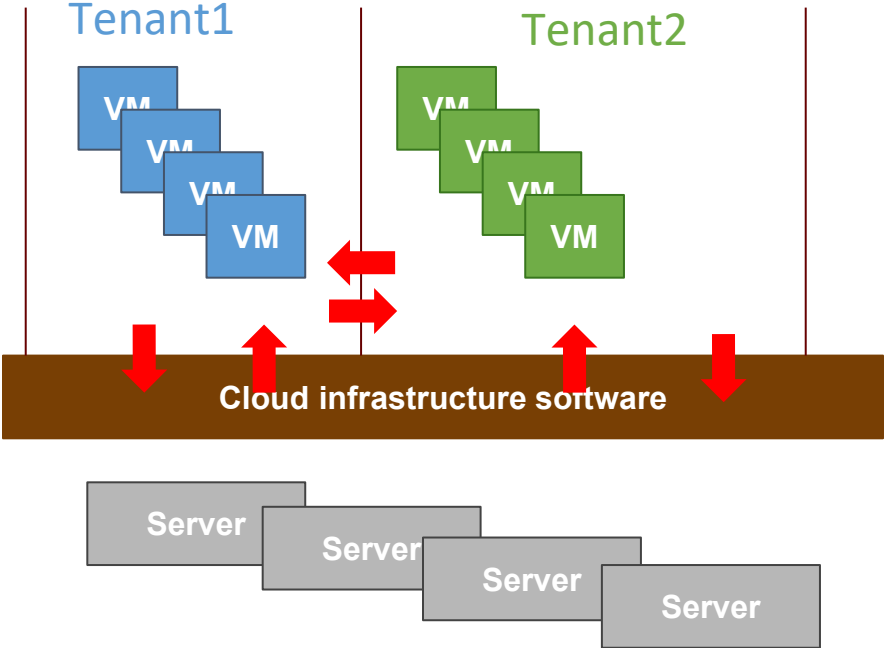
Operations

- Paravirtualized Trusted Substrate
- TEE access from VMs
 - Expected to be fully available this October (we are today at 50% of work)
- SoC independent hardware anchored attestations (TrustZone or discrete chip)
- Device assignment challenges
 - Shared devices initialization and control challenges / virtio-SCMI
 - Network specific: pause frames handling, TSN authorization
- Heterogeneous computing (Cortex R providing network access to Cortex A)
- Confidential Computing

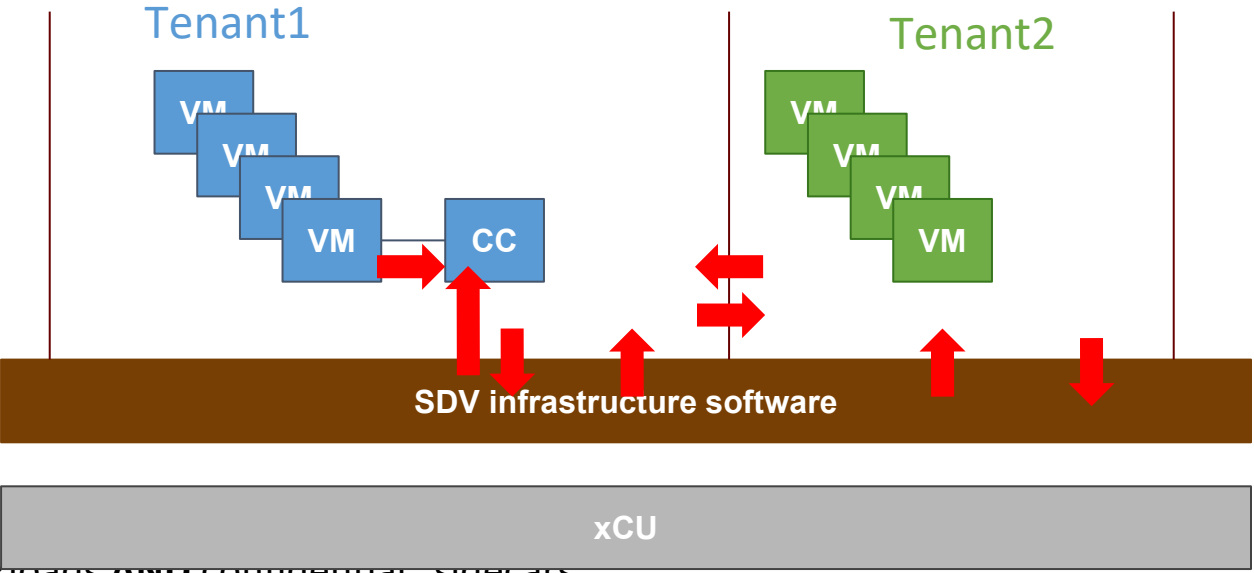
Confidential compute - the problem



Confidential compute - in the cloud



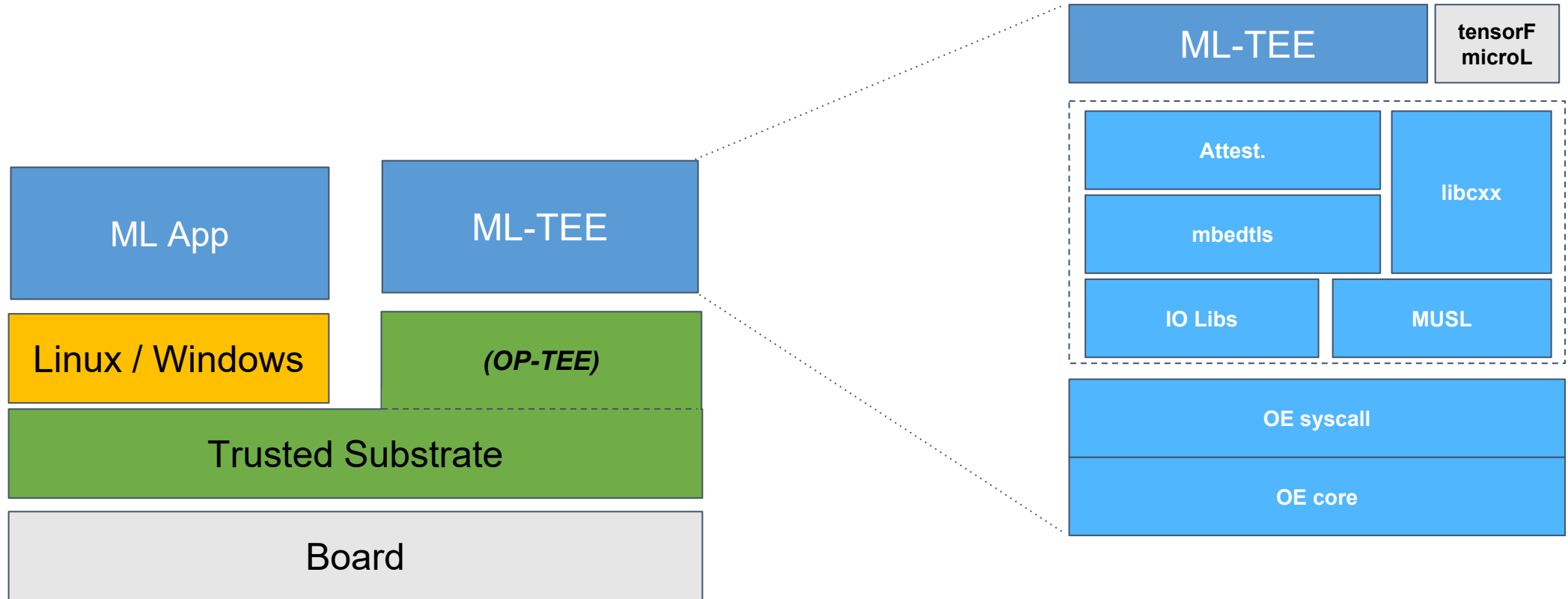
Confidential Compute - automotive



- OEM (feature subscription...)
- Insurance company
- Rental, fleet
- Digital Content provider
- Car owner (P2P rentals)

Confidential workloads **AND** confidential sidecars
High level use case being studied at Global Semiconductor Alliance TIES/Automotive

Confidential AI with OpenEnclave SDK (OESDK)



- Available on Intel (SGX) and Arm (currently TrustZone later Arm v9 Realms)
- Linux and Windows support on the normal world side
- Builds on Global Platform APIs for TrustZone but greatly extends its capabilities

Operating system & container



meta-“ledge”-security (Arm Cassini program)

Direct secure booting from UEFI now possible (no grub)

Kernel constant verification from TEE PoC

Full disk encryption with TPM unsealing (firmwareTPM in some cases)

Base SELinux configuration

IMA with multiple signers almost finished (Red Hat effort)

Parsec

Container attestations based on hardware root of trust

- Pushing PSA APIs through FF-A to allow SoC independent hardware anchored attestations (TrustZone or discrete chip)
- Need to be integrated with container frameworks that actually do attestation

Call to actions

**Assess whether you want to have
Arm Cassini standard (SystemReady-IR, PSA, Parsec)
in your RFPs**

**Revisit all embedded best practices
as many things are rapidly changing**

francois.ozog@linaro.org

Thank you



OPEN DISCUSSION

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

HOW TO GET INVOLVED: MEMBERSHIP

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

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

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

AUTO-ISAC PARTNERSHIP PROGRAMS

Strategic Partnership

- **For-profit** companies such as “Solutions Providers” that sell connected vehicle cybersecurity products & services.
 - **Examples:** *Hacker ONE, Upstream, IOActive, Karamba, Grimm*
1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
 2. Formal agreements: **NDA, SPA, SoW, CoC** required.
 3. **In-kind contributions** allowed. Currently no fee.
 4. **Does not** overtly sell or promote product or service.
 5. Commits to **support the Auto-ISAC’s mission**.
 6. Engages with the automotive ecosystem, **supporting & educating Auto-ISAC Members and its Community**.
 7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
 8. **Summit Sponsorship** allowed for promotion. Summit Booth **priority**.
 9. Engagement **must provide Member awareness, education, training, and information sharing**
 10. **Builds relationships, shares, and participates** in information sharing Auto-ISAC activities.
 11. Supports our mission through **educational webinars and sharing of information**.

Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
 - Includes **Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non-Profit, Technical Experts, Auto-ISAC Sponsors**.
 - **Examples:** *Autos Innovate, ATA, ACEA, JAMA, MEMA, CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.*
1. **No formal agreement** required.
 2. **No approval** required.
 3. Added to **Auto-ISAC Community Distro** List to stay engaged in Community events and activities.
 4. Participate in **Auto-ISAC Monthly Community Calls**.
 5. Learn **what is trending** in the ISACs and hear from key leaders during the **special topic of interest** presentation.
 6. Added to **Auto-ISAC DRIVEN** list to receive our **daily cyber automotive newsletter**.
 7. Part of the Network with **Automotive Community and the extended automotive ecosystem**.
 8. Invitation to **attend and support** our yearly Summit.

CURRENT PARTNERSHIPS

MANY ORGANIZATIONS ENGAGING

Thanks for your Support to our Many Partners

COMMUNITY PARTNERS

INNOVATOR

**Strategic Partnership
(13)**

Cybellum
Deloitte
FEV
GRIMM
HackerOne
Karamba Security
KELA
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Upstream

NAVIGATOR

Support Partnership

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

COLLABORATOR

**Coordination
Partnership**

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

BENEFACTOR

**Sponsorship
Partnership**

2021 Summit Sponsors-

Celerium
Cyware
Denso
NDIAS
IOActive
Claroty
Deloitte
Finite State
Tanium
Recorded Future
PaloAlto Networks
Upstream
Securonix
Zimperium
Micron
Block Harbor
SecurityScorecard
Booz Allen
CybelAngel
ATT
Ford
Cybellum

2020 Summit Sponsors-

Claroty
Upstream
Escrypt
Blackberry
Cybellum
Blockharbor
C2A
Synopsis
Intsignts
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!



OUR CONTACT INFO

Faye Francy
Executive Director



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

Sharmila Khadka
Information Technology Executive
Coordinator



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



www.automotiveisac.com
[@auto-ISAC](https://twitter.com/auto-ISAC)