Global Platform®

CSVF Detroit– June 4th Novi 2024

Tom.Viswat@SGS.com
SGS Brightsight
SESIP accredited Cyber Security Labs

Automotive Taskforce

Global Platform®

JUNE 2024

How to utilize SESIP from a pragmatic or practical perspective in Automotive?

SGS brightsight

SESIP™

Agenda

1. Problems in the Automotive Supply Chain
   - Current Landscape
2. Drivers for Cyber Security Certification in Automotive
   - Risk Management
   - Cost Savings
3. Solution
   - SESIP + SGS Brightsight
4. Summary
5. Next steps

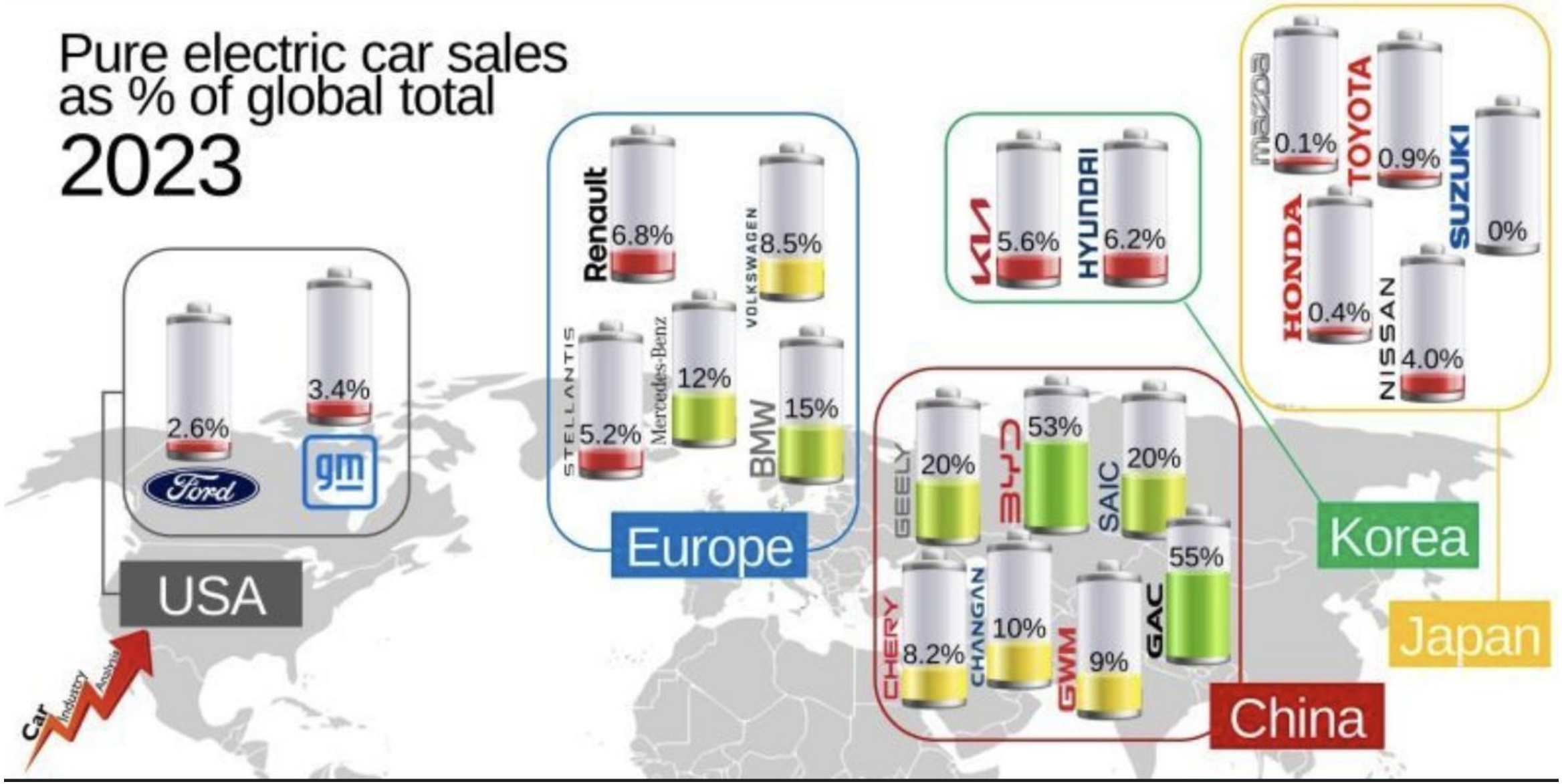
1. Problems in Automotive Supply Chain

Here are some of the primary problems faced by the automotive supply chain:

1. Supply Chain Disruptions
2. Semiconductor Shortages
3. Raw Material Price Volatility
4. Complexity and Interdependence
5. Quality Control:
6. Regulatory Compliance:
7. Technological Advancements
8. Inventory Management
9. Cybersecurity Risks
10. Etc….it is a long list

To address these challenges, the OEMs strategy focuses on:

- **Diversifying Suppliers**
- **Increasing Transparency**
- **Strengthening Relationships**
- **Investing in Technology**


Pure electric car sales
as % of global total
2023
2.6%
3.4%
Ford
gm
USA
Renault
6.8%
VOLKSWAGEN
8.5%
STELLANTIS
5.2%
Mercedes-Benz
12%
BMW
15%
Europe
KIA
5.6%
HYUNDAI
6.2%
Korea
mazda
0.1%
TOYOTA
0.9%
HONDA
0.4%
SUZUKI
0%
NISSAN
4.0%
Japan
GEELY
20%
53%
SAIC
20%
CHERY
8.2%
CHANGAN
10%
GWM
9%
GAC
55%
China
Car Industry Analysis

1. Problem in Automotive Supply Chain - dynamics

- SDV (any power source), AD, ADAS, V2X, battery tech, Chinese EV competition, legacy OEMs vs new BEV entrants, AI, etc.
- Technology is very fast + market reaction slower: average car development takes 72 months
- New Tech drives up price and risk, hence the bigger SLAs + time spend (1,000s hours?)
- Sales volumes not there yet, tax incentives ending/prolonged for EVs, charging infrastructure issues for EVs, warranty for batteries, …
- TARAs: Different cybersecurity threats and risks per project. The TARA approach is very much based on the end Vehicle. HW/SW component attacks maybe excluded or not taken into account
- New tech with the threat of Tier2s becoming Tier1s
  - Tier2 getting direct JV with OEMs incl. Cloud SP
- Strategic re-orientation, Tier1s buying IP and getting SoC via foundries, leading to more fragmentation in volume

How to:

- Connecting/bridging (legacy) automotive environment towards world of component cyber security
- How to demonstrate proper cyber sec to governments, consumers, stakeholders?

Current Automotive Landscape

- **UNR 155/156**
- **ISO/SAE 21434**

What OEMs told me:

- ISO/SAE 21434 great starting point and discussion document, but this is just the start / basic level cybersecurity
- Structure for automotive safety is used now for cyber requirements on top following same approach
- What about HW/SW components/full platform certification beyond ISO/SAE 21434? Knowing the many E/E architectures.

SGS Brightsight – market requests in automotive:

- **Pentesting** – various HW components
- **ISO/SAE 21434 compliance testing** - various HW components
- **Common Criteria/SESIP** – SoC, OS, Hypervisor, V2X, ADAS, AD components
- **PSA Certified** – sensors, IVI related components
- **SESIP** – sensors, IVI related components

Also:

- **CCC** – keyfobs
- **GSMA**: eSIM/iSIM/SIM for automotive

Why do OEM/Tier1/2 want and need certification? Drivers?

2.Certification Drivers in Automotive

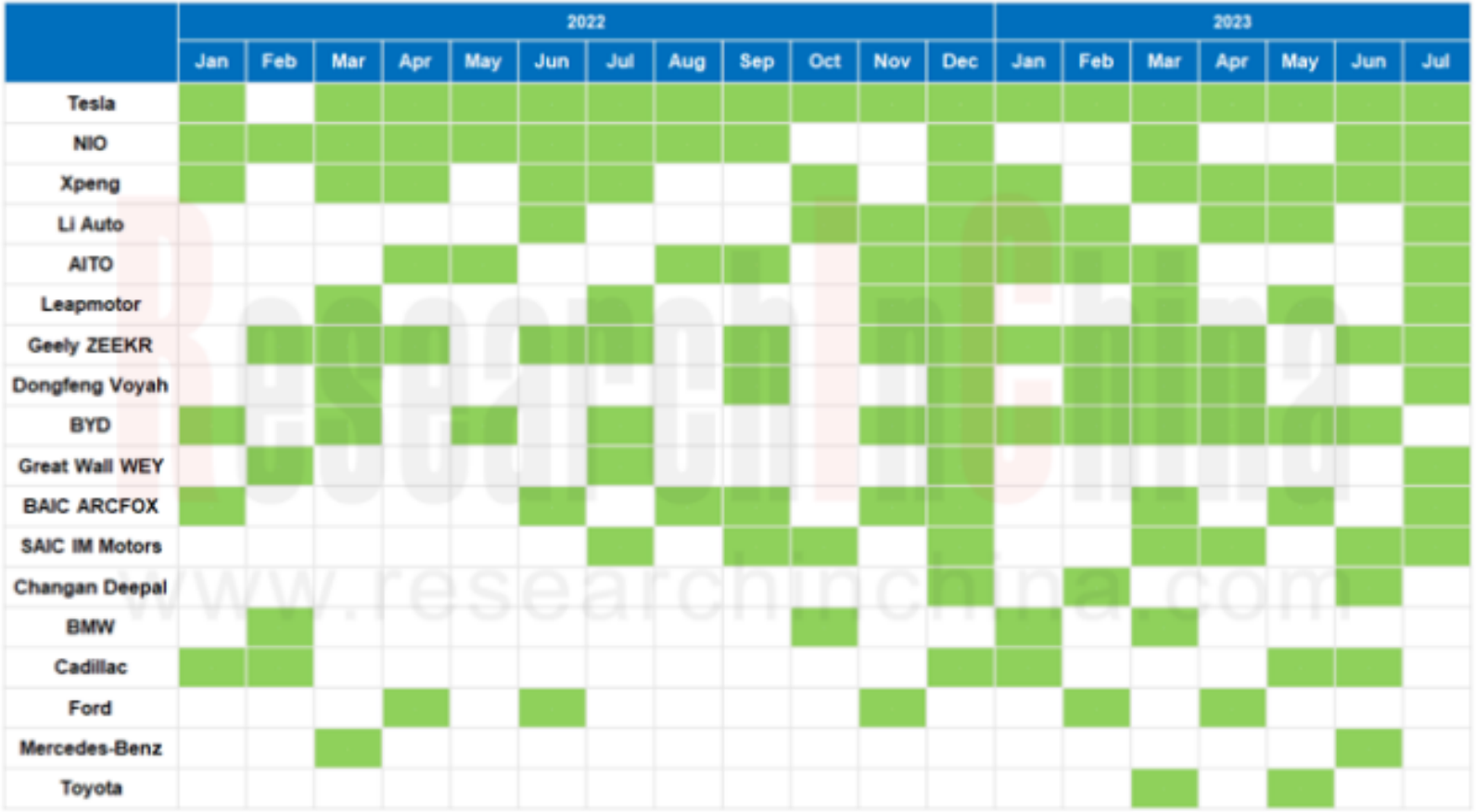
- Compliance: ISO/SAE 21434 took about 5 years and the bare minimum the automotive industry could agree upon
  - Basically, it is good discussion document/starting point especially for component certification
- Risk management: This makes more sense.
  - What are the downsides if things really go wrong, who takes the hit?
  - Recalls, brand damage, end user annoyance
  - Role of insurance companies?
- Marketing differentiator
  - Could be, but not leading
- Cost Savings
  - We all like this

- **Time? If ever.**
- **Ongoing exercise**
- **Smaller companies**
- **Large Service Level Agreements**

Stick (risk management) and Carrot (cost savings)

2.Driver: Risk Management

OTA Update Frequency of Major Auto Brands, Jan 2022-Jul 2023



Source: ResearchInChina

SDV Platforms vs Mobile Oss evolution:

- IOS
- Symbian
- Java
- Android,
- BB
- Harmony OS
- Etc.

Frequent Updates…
Looks familiar?

2.Driver: Risk Management

- But what about HW/SW components/full platforms? Critical infrastructure of the SDVs?
- Critical infrastructure managing the patches, updates, new services, managing all sorts of sensors, etc?
- At the core of the domain/zonal/new E/E architectures allowing for Software Defined Vehicle platforms to function?

Risk management considerations leading to certification:

- Acceptable Risk vs Investment/ Cost trade off?
- How much composition / re-use is expected?
- OEM/Tier1- risk managements criteria/variables? How do they deal with risk/identify risk?
- Enterprise/Integrated Risk Management system? Who decides? Role Insurance companies? Big data + ReInsurers (Swiss Re)
- What are considered Core Components per OEM (high assurance/mid assurance levels)
- Tier 2 Selection Criteria - does a certificate provide a quick check box/acceptance in an RFP?
- And more…..?

2. Driver: Cost Saving

How about a 4th driver for cyber security certification?

Cost Saving (no force, no fear, no marketing). Easy to accept for all? How?

- Supply chain automotive is massive and complex, risk is delegated to the next level where possible
- OEMs do not necessarily understand cyber security risks for HW/SW components
- We need to get clarity along the supply chain of what it is means, and if certification or a PP simplifies their processes
- No need for same amount of massive paperwork cycles and hours spend?
  - Legal, procurement, engineers, CISO/PISO/CIO, ….at each part of the supply chain
  - Cost saving? How much?
  - Other benefits: time to market, just a simpler transparent process for government/consumer i.e. standardization

2.Driver: Cost Saving

Cost Savings considerations/info needs:

- OEM SLA examples with requirements, Tier 1 SLA requirements, Tier 2, etc.
- Insight and fair estimates into time+effort+overhead+repeats for a project
- What if SESIP L2 or any other standardized approach would be a proper translation of all these SLA requirements going through the supply chain?
- Would it help in Tier2 supplier selection process?
  - Would it lower the cost and efforts?
  - Would it be a cost saving? Break-even?
  - Cost if the wrong Core Components are chosen (Risk Management again)
  - Increased transparency benefits
  - Time to market benefits
  - And more ….

3.Solution

SESIP (EN 17927) since 2019 developed by Global Platform

- Security Evaluation Standard for IoT Platforms EN 17927: SESIP is a certification standard developed to allow composition / re-use of security testing across complex connected products.
- It provides a technology agnostic approach (Lego™-box) to allow technology to define a set of security requirements and common security vulnerability assessment and testing approach.
- It is built around the security services provided by all layers of a system from sub-component to final product.
- It is written in easy-to-understand language and provides a cost/time effective approach to security validation and testing.
- Security Evaluation Standard for IoT Platforms (SESIP) methodology has been adopted as the basis for a European Standard (EN) by the European Committee for Standardization, CEN and CENELEC.
- Benefits: Proven, efficient, time-to-market, support leading Tier2, promotes re-use / composition in automotive.

SESIP™

3.Solution: Tier 2/3 – already SESIP certified

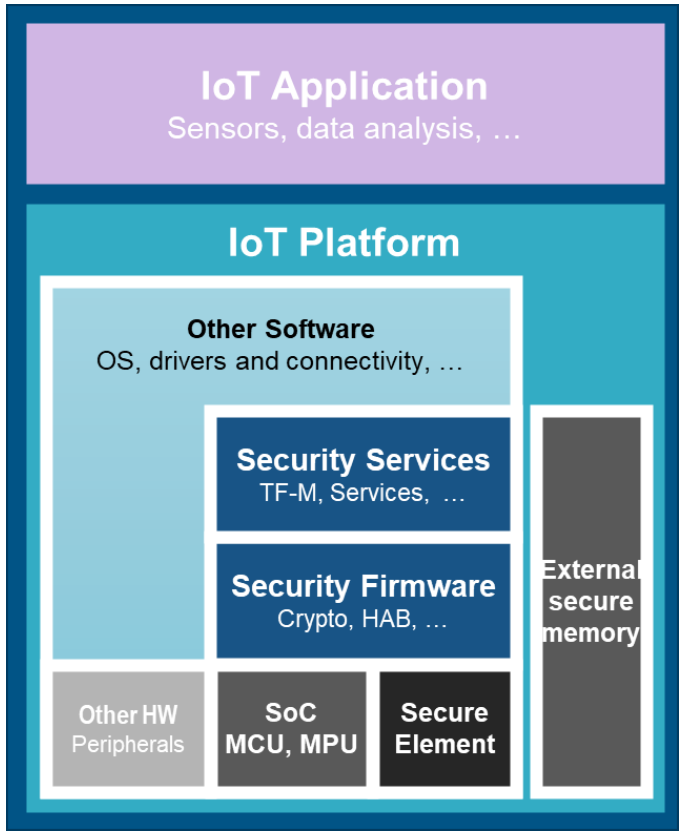
3.Solution: Re-using certified components

Device-level certification

Bottom-up certification

SESIP

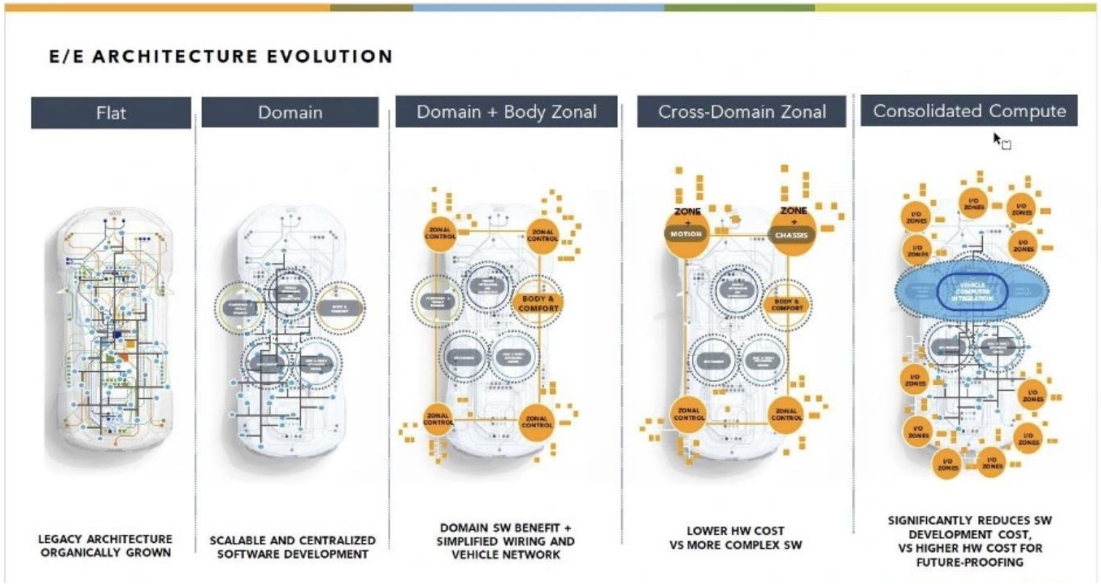
IoT Application	**Using the platform's services** • Reducing the risk of doing security wrong
IoT Platform	**Offering low level security services** • Secure connectivity, secure interfaces • Application SW separation
Root of Trust	**Protecting most sensitive assets** • Keys, FW integrity, Secure boot, Crypto primitives, …



An evaluation framework for IoT components like SoC, Root of Trust, OS, Hypervisors, etc. – i.e. Central Compute component of the SDV platforms

4.Summary

- Beyond UNR155+ ISO/SAE 21434 there is an open space for HW/SW component certification
- HW/SW component certification likely driven by risk management considerations and potential cost savings
- Need for data validation with help from OEM/Tier1/2 to fully understand these drivers
- SESIP standard is ideal for Automotive IoT especially for the new E/E- architectures
- Benefits: re-use in automotive globally, existing Tier2 support, time to market, efficiency, transparency, CEN Cenelec standard, why reinvent the wheel/no need for more cost/complexity?
- Leading to lower risk + cost savings across the supply chain (?)



5.Next steps

Call for:

- participation from GP Network members ATF, OEMS, Tier1s and Tier2s to share cyber security risk management and SLA data and to help validate the cyber security evaluation/certification drivers:
  - Risk Management: How SESIP can help lower risk?
  - Cost Savings in the supply chain: How SESIP can be a driver of savings?

Objective:

- Benefits through SESIP Certification - document
  - Includes shared cyber security approach / framework / guidance on how to manage HW/SW components/full platform cyber security certification and how to get these benefits
- Ideally resulting in pilot / PoC with OEM/Tier1+2 to prove the benefits of SESIP

Questions?

Global Platform®

The standard for secure digital services and devices

→globalplatform.org