SYNOPSYS®

ISO 21434: Best Practices on Development and Testing and Alignment with SESIP

Dennis Kengo Oka
Senior Principal Automotive Security Strategist and Executive Advisor
dennis.kengo.oka@synopsys.com

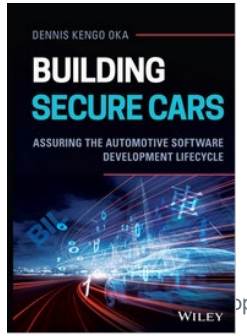
GlobalPlatform Cybersecurity Vehicle Forum, Tokyo, Japan
2023/9/14

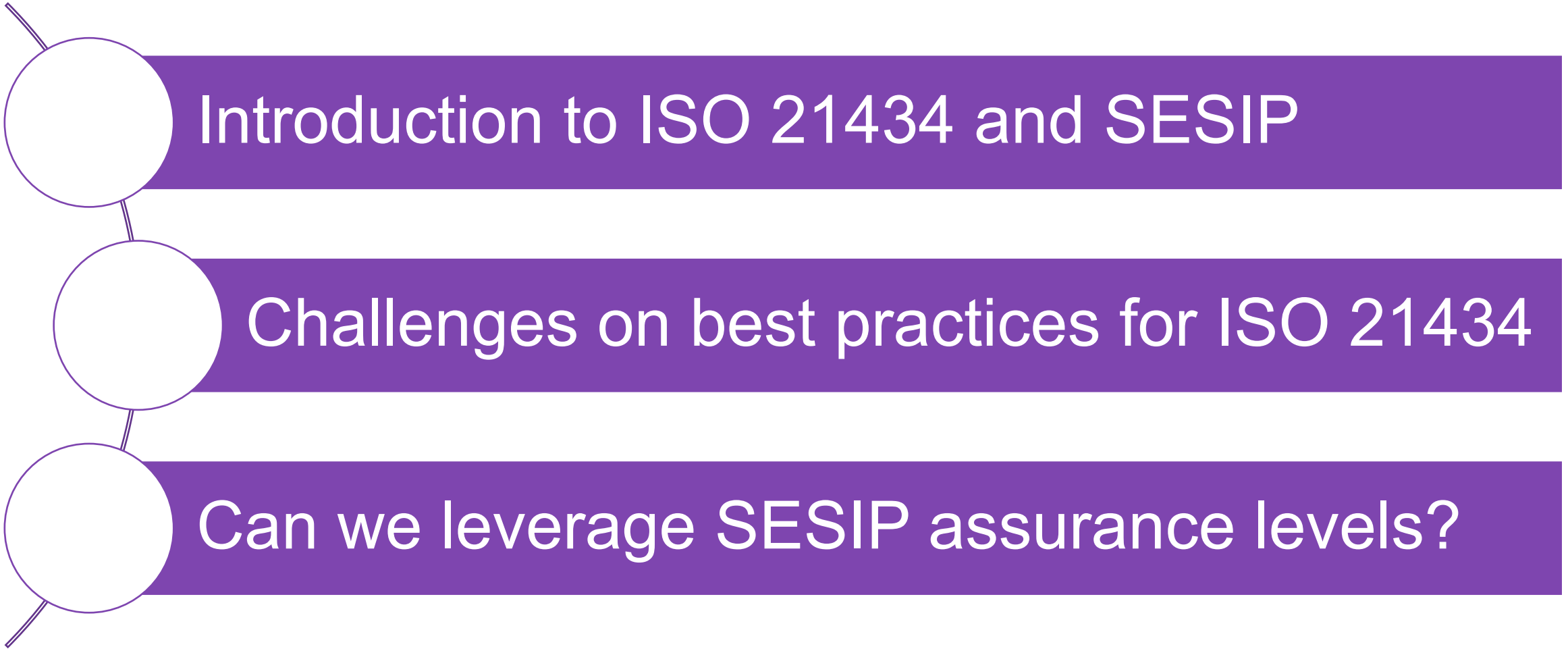
Dennis Kengo Oka

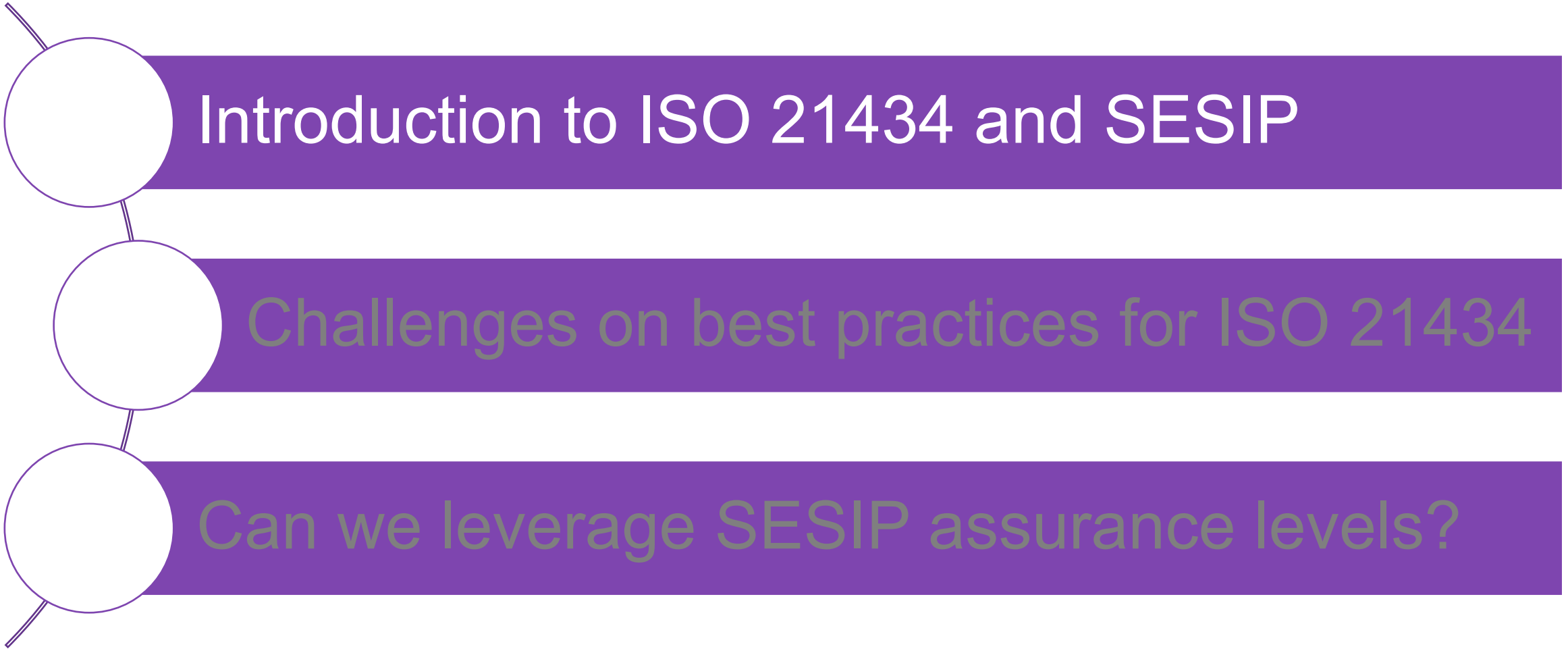
Senior Principal Automotive Security Strategist and Executive Advisor

- Ph.D. in Automotive Security from Chalmers University of Technology, Sweden
- Started working on automotive security in 2006
- Contributed to improving security at multiple OEMs and suppliers
- Standardization and best practices activities: JASPAR, LTA TR-68, OpenChain Automotive WG, Uptane, …
- 70+ publications and presentations at, e.g., SAE World Congress, JSAE, escar, Embedded World, Code Blue, …

Author of the book: "*Building Secure Cars: Assuring the Automotive Software Development Lifecycle*"







ISO/SAE 21434

- **ISO/SAE 21434** Road Vehicles — Cybersecurity Engineering

- Jointly published standard by ISO and SAE in August 2021

- Contents:
  - Organizational cybersecurity management
  - Continual cybersecurity activities
  - Concept
  - Product development
  - Cybersecurity validation
  - Production, Operations & Maintenance
  - Threat analysis and risk assessment methods

ICS › 43 › 43.040 › 43.040.15

ISO/SAE 21434:2021

Road vehicles — Cybersecurity engineering

ABSTRACT PREVIEW

This document specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

This document is applicable to series production road vehicle E/E systems, including their components and interfaces, whose development or modification began after the publication of this document.

This document does not prescribe specific technology or solutions related to cybersecurity.

GENERAL INFORMATION

Status : Published | Publication date : 2021-08

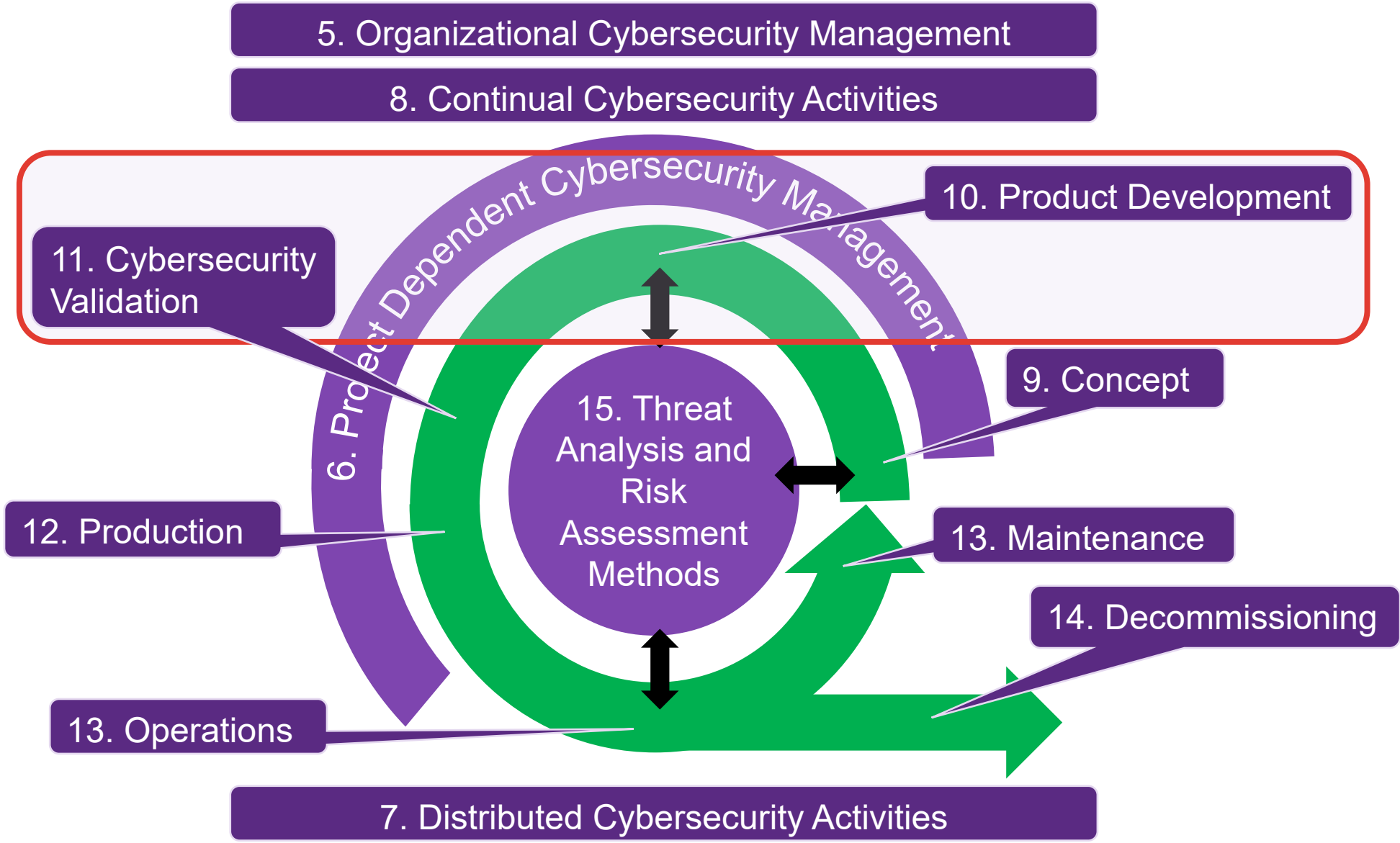
Edition : 1 | Number of pages : 81

Technical Committee : ISO/TC 22/SC 32 Electrical and electronic components and general system aspects

ICS : 43.040.15 Car informatics. On board computer systems

Overview of ISO 21434

1. Scope
2. Normative references
3. Terms and abbreviations
4. General considerations



Activities

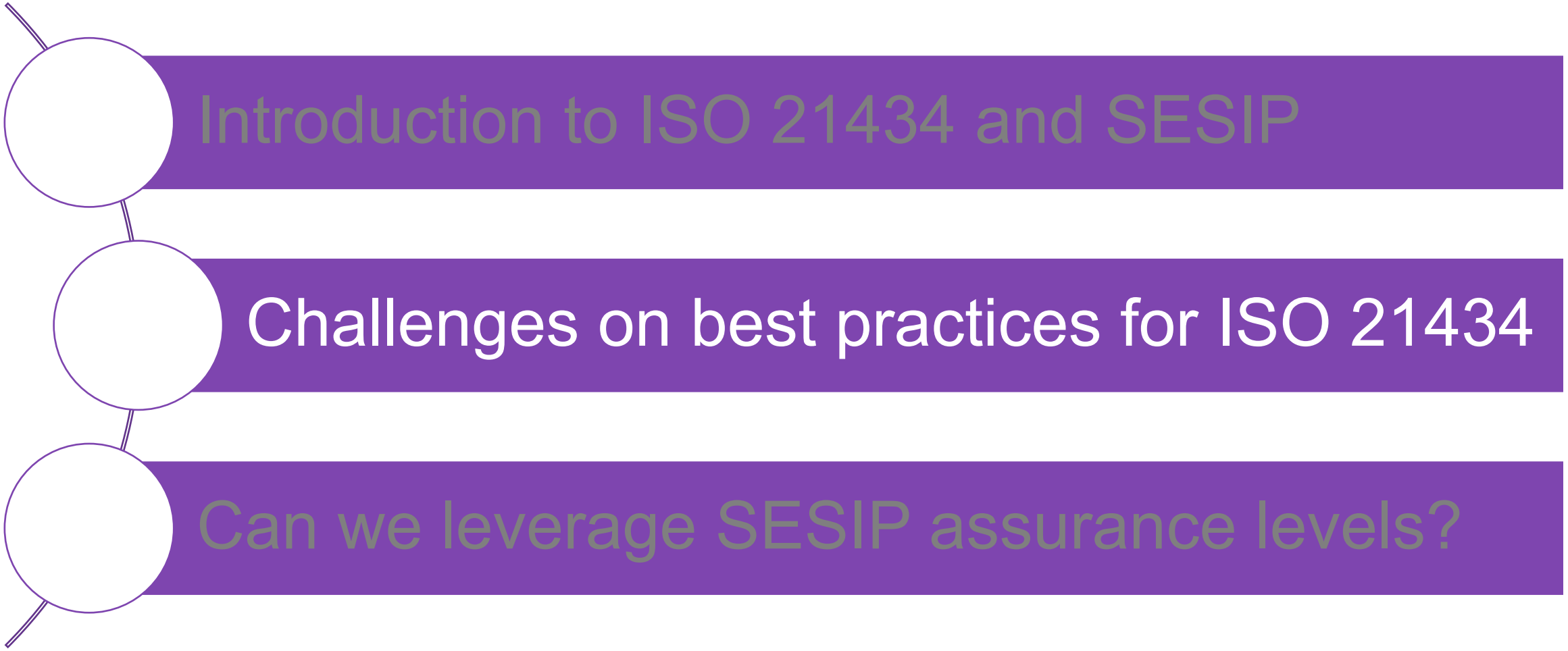
Product lifecycle

SESIP (EN 17927)

- Security Evaluation Standard for IoT Platforms (SESIP) is a security evaluation methodology introduced by GlobalPlatform

- Assists IoT device manufacturers and certification bodies in adopting a standardized approach for evaluating the security of IoT devices

- Additionally, by mapping to other security requirements like NIST, ISA/IEC 62443 and ETSI/EN 303 645, (ISO 21434?), SESIP allows to define assurance levels that are mutually recognizable across multiple various schemes, achieving scalability



ISO 21434 Project-Level Artifacts (Development and Testing Phases)

Activities	Artifacts
[RQ-10-09][RQ-10-10] Integration and verification activities	[WP-10-06] Integration and verification specification [WP-10-07] Integration and verification report
[RQ-10-11] Test coverage evaluation using metrics	[WP-10-07] Integration and verification report
[RC-10-12] Test to confirm unidentified weaknesses and vulnerabilities remaining are minimized	[WP-10-07] Integration and verification report
[RQ-10-05] Coding guidelines criteria	[WP-10-03] Documentation on coding guidelines
[RQ-10-07] Analyze to identify weaknesses and vulnerabilities	[WP-10-05] Weaknesses found during product development
[RQ-11-01][RQ-11-02] Validation activities	WP-11-01 Validation report

Level of effort, coverage, type of test methods etc. may vary depending on the risk level… but what is the best practice?

Challenges

- How to define the best practice to fulfill the requirements for cybersecurity activities during development and testing?
- How to achieve a certain level of assurance?
- If focus only on compliance, the risk is that only the minimum is done to fulfill requirements (check-box approach)
- How can we improve product quality (security) using best practices?

CAL - Cybersecurity Assurance Levels (Annex E in ISO 21434)

- CAL can be used to specify and communicate a set of assurance requirements, in terms of levels of rigor to provide confidence that the protection of the assets of an item or component is adequately developed
- CAL can be used to determine:
  - Methods used for development and verification
  - Methods to identify weaknesses and analyze vulnerabilities
  - Approaches for cyber security assessment

Example of CAL determination based on impact and attack vector

	Attack Vector:	Physical	Local	Adjacent	Network
Impact:	Severe	CAL 2	CAL 3	CAL 4	CAL 4
	Major	CAL 1	CAL 2	CAL 3	CAL 4
	Moderate	CAL 1	CAL 1	CAL 2	CAL 3
	Negligible	--	--	--	--

Each increasing CAL corresponds to an increase in the level of assurance based on cyber security engineering methods used

CAL – Example of testing parameters

Example usage of CAL in product development and validation

Method	Requirements	CAL 1	CAL 2	CAL 3	CAL 4
Static code analysis	[RQ-10-10], [RQ-10-05]	T1	T1	T2	T2
Functional testing	[RC-10-12], [RQ-11-01]	T1	T1	T2	T2
Vulnerability scanning	[RC-10-12], [RQ-11-01]	T1	T1	T1	T1
Fuzz testing	[RC-10-12], [RQ-11-01]	-	T1	T2	T2
Penetration testing	[RC-10-12], [RQ-11-01]	-	-	T1	T2
…	…				

T1: Limited test time/test cases

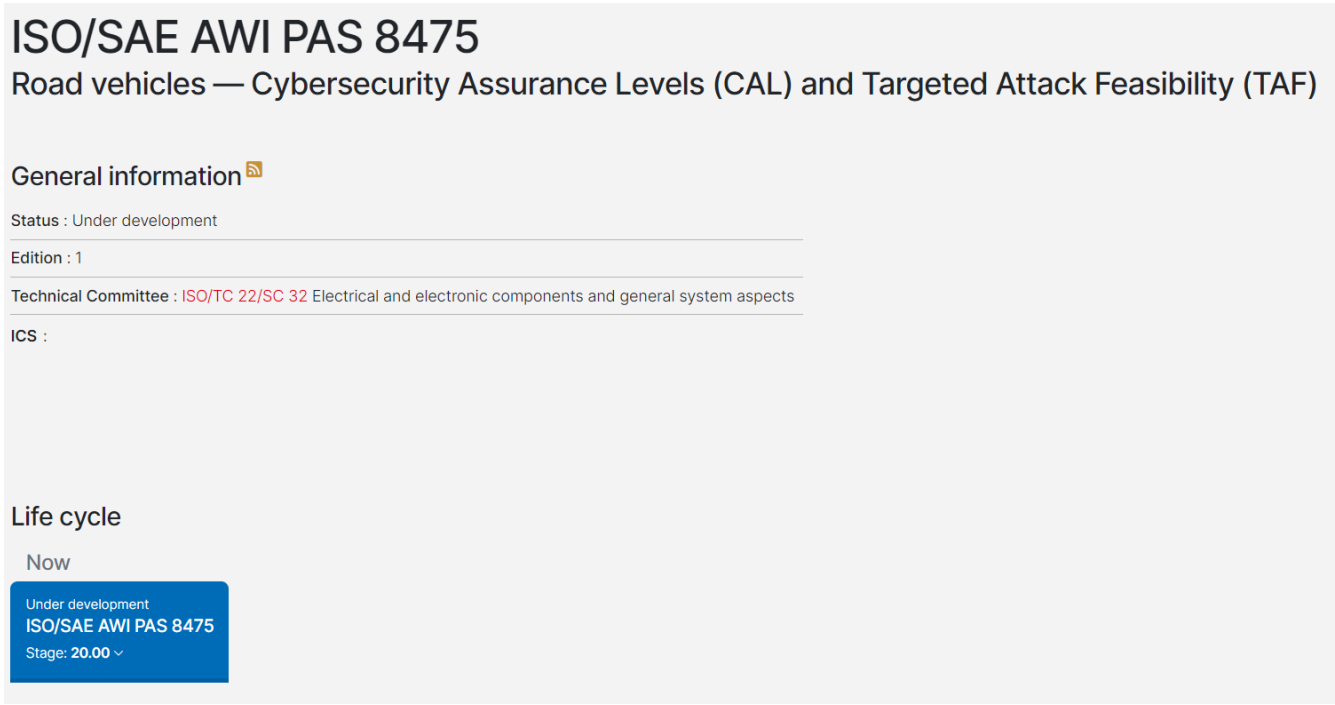
T2: Increased test time/test cases

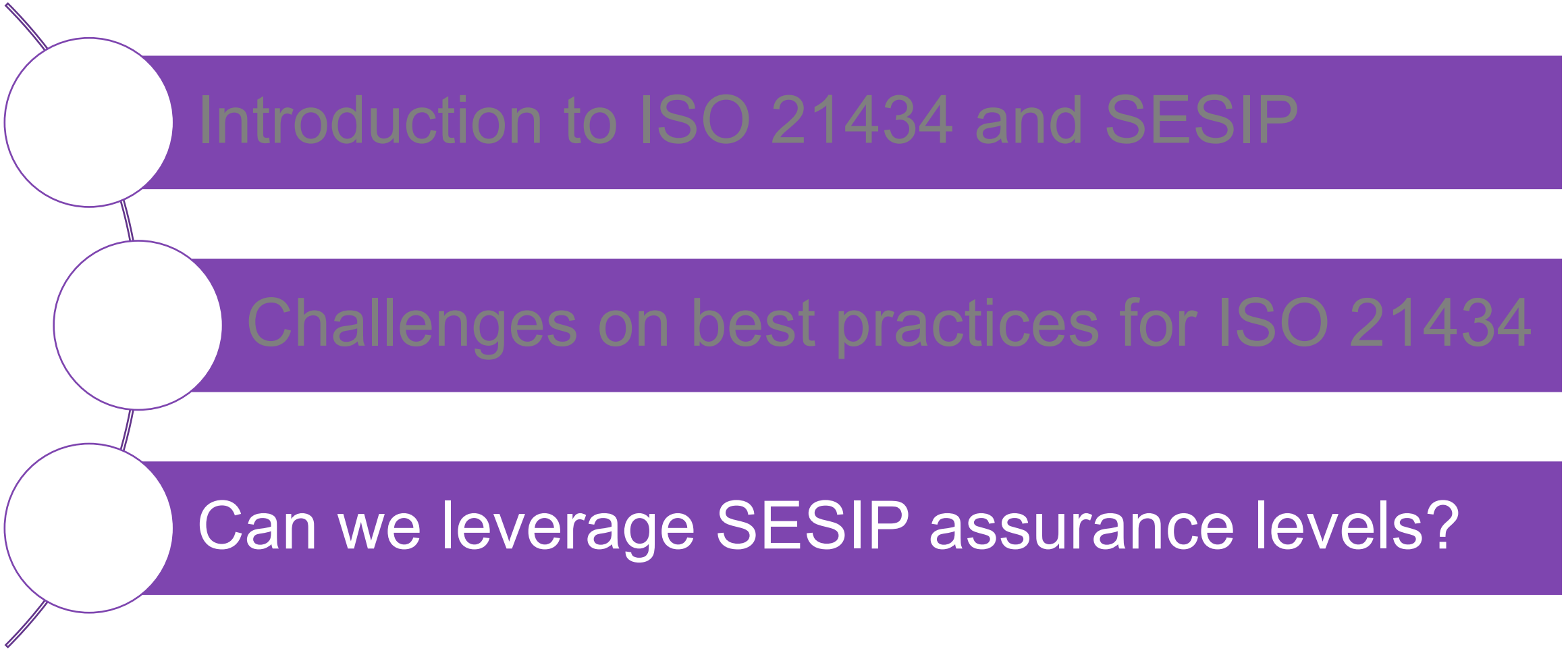
CAL: Cybersecurity Assurance Level
TAF: Targeted Attack Feasibility

ISO/SAE AWI PAS 8475 – CAL and TAF

- Joint ISO/SAE working group
- Under development
- Committee draft: July 2024
- Public release: ~Nov 2024

- Expand on CAL concept from ISO 21434 (only described as informative section in Annex E)





Can We Leverage SESIP Assurance Levels?

SESIP Assurance Levels

- 5 levels: SESIP1-5 to evaluate IoT platforms

- Covers various topics including
  - Security Target evaluation (requirements)
  - Development (specification)
  - Guidance documents
  - Lifecycle support (procedures, tools)
  - Tests (coverage, testing)
  - Vulnerability assessment

- Can we map SESIP to CALs and help define best practices?
  - Vulnerability assessment (AVA) as an example

Table 4-5: SESIP5 Assurance Requirements

Assurance Class	Assurance Families	
ASE: Security Target evaluation	*ASE_INT.1*	*ST Introduction*
	ASE_OBJ.1	*Security requirements for the operational environment*
	ASE_REQ.3	**Listed security requirements**
	ASE_TSS.1	*TOE summary specification*
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_TDS.3	Basic modular design
	ADV_IMP.2	Complete mapping of the implementation representation of the TSF
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_TAT.1	Well-defined development tools
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.1	Independent testing: conformance
AVA: Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

CAL: Cybersecurity Assurance Level
TOE: Target of Evaluation

SESIP2: CAL1

Evaluation activity – Vulnerability analysis

AVA_VAN .2	Evaluation activity	Test approach	Rigor (example)
AVA_VAN. 2.1E	Confirm that information provided meets all requirements for content and presentation of evidence	Manual review	N/A
AVA_VAN. 2.2E	Search public domain sources to identify potential vulnerabilities in the TOE, components in list of 3rd party components, IT products in the env. TOE depends on	Vulnerability scanning	Vulnerable software versions
AVA_VAN. 2.3E	Independent vulnerability analysis using guidance doc., functional spec., TOE design, and security arch. description to identify potential vulnerabilities in the TOE	Manual review	
AVA_VAN. 2.4E	Penetration testing based on identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by attacker possessing **Basic** attack potential	Penetration testing Identify potential vulnerabilities	Basic attack potential

CAL: Cybersecurity Assurance Level
TOE: Target of Evaluation

SESIP3: CAL2

Evaluation activity – **Focused** vulnerability analysis

AVA_VAN .3	Evaluation activity	Test approach	Rigor (example)
AVA_VAN. 3.1E	Confirm that information provided meets all requirements for content and presentation of evidence	Manual review	N/A
AVA_VAN. 3.2E	Search public domain sources to identify potential vulnerabilities in the TOE, components in list of 3rd party components, IT products in the env. TOE depends on	Vulnerability scanning	Vulnerable software versions
AVA_VAN. 3.3E	Independent, **focused** vulnerability analysis using guidance doc., functional spec., TOE design, security arch. description and **implementation representation** to identify potential vulnerabilities in the TOE	• Manual review • Static analysis • Fuzz testing • Dynamic analysis	• SANS Top 25 CWE • 16 hours, in-band instrumentation • Known vuln.
AVA_VAN. 3.4E	Penetration testing based on identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by attacker possessing **Enhanced-Basic** attack potential	Penetration testing	Enhanced-Basic attack potential

CAL: Cybersecurity Assurance Level
TOE: Target of Evaluation

SESIP4: CAL3

Evaluation activity – **Methodical** vulnerability analysis

AVA_VAN .4	Evaluation activity	Test approach	Rigor (example)
AVA_VAN. 4.1E	Confirm that information provided meets all requirements for content and presentation of evidence	Manual review	N/A
AVA_VAN. 4.2E	Search public domain sources to identify potential vulnerabilities in the TOE, components in list of 3rd party components, IT products in the env. TOE depends on	Vulnerability scanning	Vulnerable software versions
AVA_VAN. 4.3E	Independent, **methodical** vulnerability analysis using guidance doc., functional spec., TOE design, security arch. description and **implementation representation** to identify potential vulnerabilities in the TOE	• Manual review • Static analysis • Fuzz testing • Dynamic analysis	• SANS Top 25 CWE, CISQ CWE • 40 hours, external instrumentation • Unknown vuln. using known attack patterns
AVA_VAN. 4.4E	Penetration testing based on identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by attacker possessing **Moderate** attack potential	Penetration testing	Moderate attack potential

CAL: Cybersecurity Assurance Level
TOE: Target of Evaluation

SESIP5: CAL4

Evaluation activity – **Advanced methodical** vulnerability analysis

AVA_VAN .5	Evaluation activity	Test approach	Rigor (example)
AVA_VAN. 5.1E	Confirm that information provided meets all requirements for content and presentation of evidence	Manual review	N/A
AVA_VAN. 5.2E	Search public domain sources to identify potential vulnerabilities in the TOE, components in list of 3rd party components, IT products in the env. TOE depends on	Vulnerability scanning	Vulnerable software versions
AVA_VAN. 5.3E	Independent, **methodical** vulnerability analysis using guidance doc., functional spec., TOE design, security arch. description and **implementation representation** to identify potential vulnerabilities in the TOE	• Manual review • Static analysis • Fuzz testing • Dynamic analysis	• SANS Top 25 CWE, CISQ CWE • 160 hours, external instrumentation • Verify exploitability
AVA_VAN. 5.4E	Penetration testing based on identified potential vulnerabilities to determine that the TOE is resistant to attacks performed by attacker possessing **High** attack potential	Penetration testing	High attack potential

Discussion

- If mappings are appropriate and we can leverage SESIP, it is possible to state that if a product meets a certain CAL, it also meets the corresponding SESIP
- There may be requirements defined in SESIP that are not in ISO 21434 as well as requirements in ISO 21434 that are not covered in SESIP ⇒ Therefore, it may not be possible to do a one-to-one mapping between SESIP and CAL
- Instead, we could use SESIP as a base and fill the gaps with additional ISO 21434 specific requirements

Call to Action

Mapping between ISO 21434 and SESIP

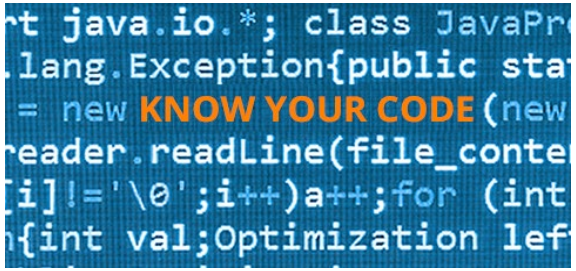
- Continue mapping requirements between SESIP and ISO 21434
- Use SESIP as a base

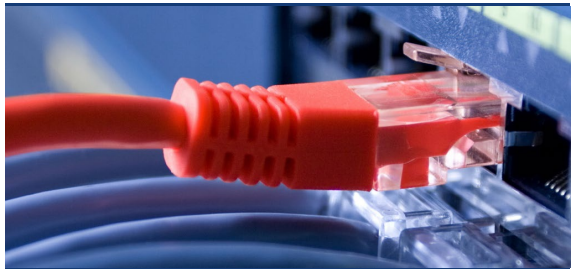
Consider how use ISO/SAE 8475 (CAL)

- Realign mapping between SESIP and ISO 21434 using ISO 8475
- Consider how to leverage SESIP (and ISO 8475) for improving best practice for ISO 21434

Thank You

Synopsys Automotive Software Cybersecurity & Quality





Coverity Static Analysis	Defensics Fuzz Testing	Black Duck OSS Management	Security Services
Find critical defects and vulnerabilities in code	Find vulnerabilities before hackers	Find known vulnerabilities in OSS	Best practices consulting
Automotive compliance (MISRA, ISO26262)	Fuzzing for automotive protocols	Generate SBOM for supply chain management	Security testing services
Security: CERT-C and CWE Top 25	CAN, Ethernet, WiFi, Bluetooth, IPv4, mp3, mp4	Alerts for newly detected vulnerabilities	Gap analysis/remediation planning