HORIBA MIRA

Cybersecurity Assurance Levels Supporting ISO/SAE 21434 Objectives

Paul Wooderson

26 May 2025

Introduction

- Since the publication of ISO/SAE 21434 in 2021, the ISO/SAE joint working group started two further projects to develop additional guidance

Working Group	Project Number	Project Name	Document Type	Status/Timeline
ISO TC22/SC32/WG11 Joint Working Group between ISO and SAE for Cybersecurity	ISO/SAE PAS 8475	Cybersecurity Assurance Levels (CAL) & Targeted Attack Feasibility (TAF)	Publicly Available Specification (PAS)	• Preparing for DPAS ballot • Publication expected Q1 2026
	ISO/SAE TR 8477	Cybersecurity Verification and Validation	Technical Report (TR)	• Preparing for DTR ballot • Publication expected Q12026

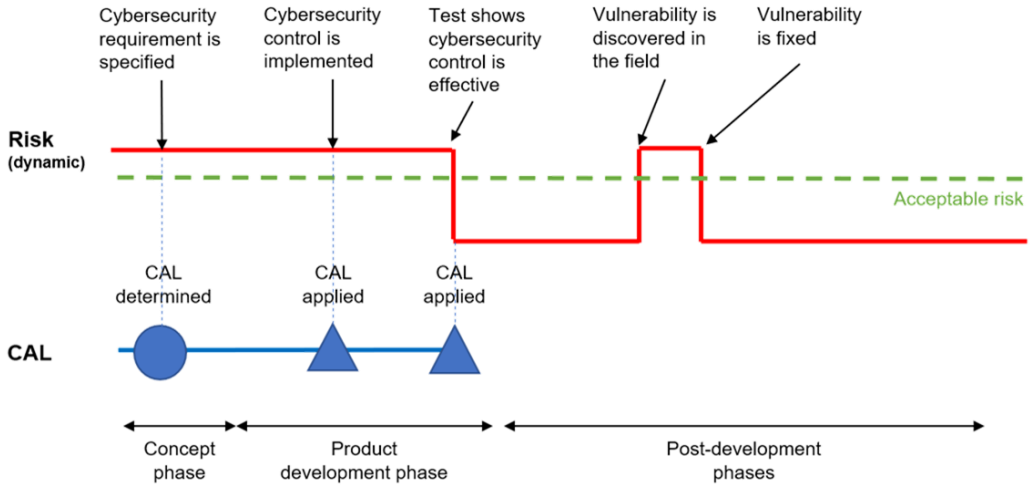
ISO/SAE PAS 8475

ISO/SAE PAS 8475 project started in November 2022 to develop further guidance on two concepts

- A Publicly Available Specification (PAS) which remains valid for 3 years and can be extended once for a further 3 years

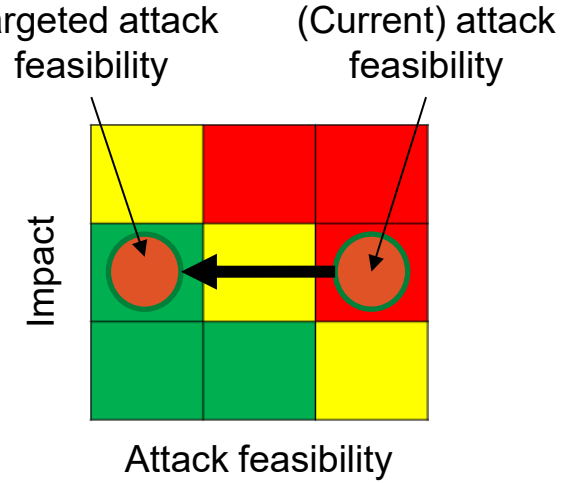
Cybersecurity Assurance Levels (CAL)

- To scale the rigour of cybersecurity engineering activities
- Based on breadth and depth with which activities are performed
- Appear already in ISO/SAE 21434 Annex E



Targeted Attack Feasibility (TAF)

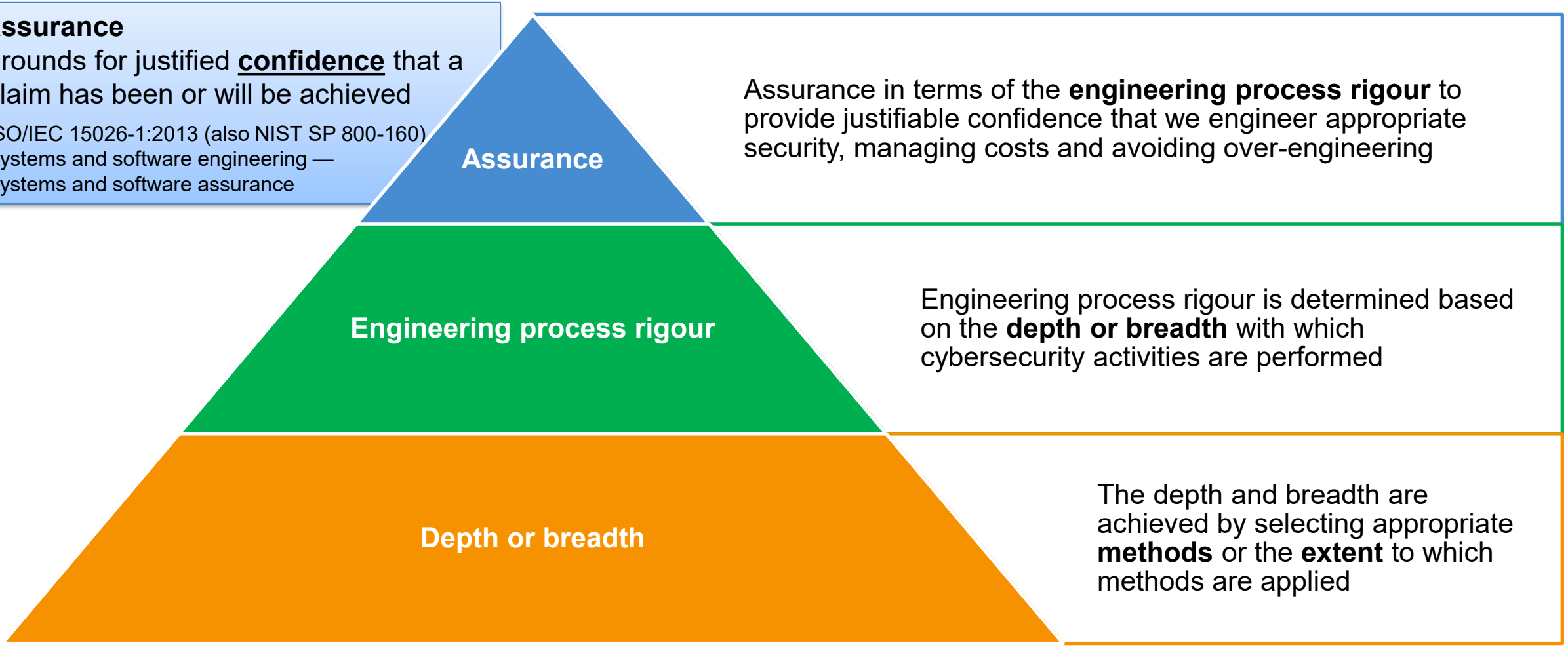
- Not currently part of ISO/SAE 21434
- A way to specify the expected “strength” of cybersecurity controls
- Intended to facilitate communication between customer and supplier



Cybersecurity Assurance Levels (CAL)

assurance
grounds for justified **confidence** that a claim has been or will be achieved

ISO/IEC 15026-1:2013 (also NIST SP 800-160) Systems and software engineering — Systems and software assurance



Assurance in terms of the **engineering process rigour** to provide justifiable confidence that we engineer appropriate security, managing costs and avoiding over-engineering

Engineering process rigour is determined based on the **depth or breadth** with which cybersecurity activities are performed

The depth and breadth are achieved by selecting appropriate **methods** or the **extent** to which methods are applied

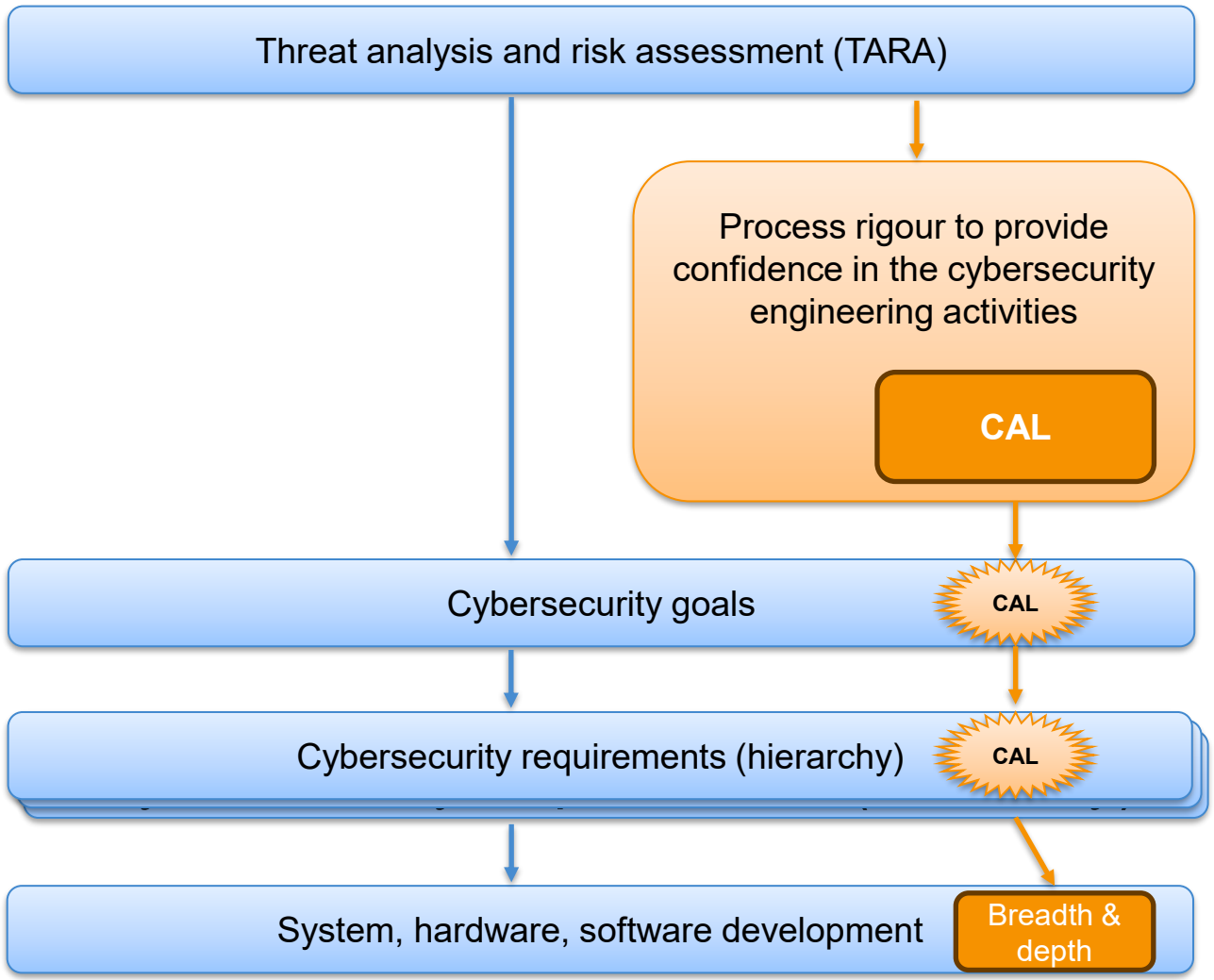
Cybersecurity Assurance Levels (CAL)

Usage of CAL

- A CAL is **determined** for each cybersecurity goal by considering the related threat scenario(s)
  - Impact rating
  - Attack vector
- Cybersecurity requirements **inherit** the CAL from their parent cybersecurity goal
- Cybersecurity requirements including CAL are **allocated** to architectural elements (e.g. ECUs)
- Each element is developed to the highest CAL of its allocated cybersecurity requirements

Note

- Conformance with the requirements of ISO/SAE 21434 is **always mandatory**



Cybersecurity assessment

Example use of CAL for cybersecurity assessment

- ISO/SAE DPAS 8475 provides an example of using CAL to determine:
  - The independence with which to review the decision to perform a cybersecurity assessment [RQ-06-25]
  - The contents of the cybersecurity assessment [RQ-06-26]
- This could be extended to also define the independence with which the cybersecurity assessment itself is performed [RQ-06-27]

I0: If a cybersecurity assessment is performed, it shall be performed by a different person in relation to the person(s) responsible for the creation of the considered work product(s).

I1: The cybersecurity assessment is performed by a different person in relation to the person(s) responsible for the creation of the considered work product(s);

I2: The cybersecurity assessment is performed by a person who is independent from the team that is responsible for the creation of the considered work product(s), i.e. by a person not reporting to the same direct superior.

I3: The cybersecurity assessment is performed by a person who is independent, regarding management, resources and release authority, from the department responsible for the creation of the considered work product(s).

ISO 26262 approach for functional safety assessment

Items with safety goals with ASIL	Functional safety assessment	Independence
ASIL A	Not required	N/A
ASIL B	Recommended	I0
ASIL C	Required	I2
ASIL D	Required	I3

Proposed approach for cybersecurity assessment

Items with cybersecurity goals with CAL	Cybersecurity assessment	Independence
CAL1	Not required	N/A
CAL2	Required	I2
CAL3	Required	I3

Open Challenges

- The CAL concept has been under development since the start of ISO/SAE 21434 first edition in 2016
- Based on an identified industry need to scale the **rigour applied to cybersecurity engineering** to provide sufficient confidence while avoiding under- or over-engineering
- ISO/SAE PAS 8475 is built on and used with ISO/SAE 21434, which is inherently flexible and **applicable to the whole supply chain**
- This makes it challenging to standardise a single definition of how CAL scales cybersecurity activities that can be used by each supply chain tier
- Some questions:

1. How can the usage of CAL to scale activities be more precisely specified?
2. Is there value in linking the concept of **engineering assurance** (CAL) with the assurance provided by cybersecurity assessment or evaluation (e.g. SESIP)?

CAL Usage at Different Integration Levels

ISO/SAE DPAS 8475
Examples of breadth and depth for scaling rigour of ISO/SAE 21434 [RQ-10-10]
(Specification of integration and verification activities)

Breadth	Depth
Verification activities are specified that are appropriate for the component (e.g. hardware, software or both): • requirements-based test • interface test • resource usage evaluation • verification of the control flow and data flow • hardware emulation • penetration testing • fuzz testing • hardware formal methods • mutation testing • dynamic analysis • static analysis	Methods for deriving test cases, as listed in ISO/SAE 21434:2021 • analysis of requirements • generation and analysis of equivalence classes • boundary value analysis • error guessing based on knowledge or experience

Factors affecting breadth and depth may differ at different integration levels, for example:

- Hardware formal methods would not be applicable at vehicle level
- Resource usage evaluation might not apply at hardware level
- Some methods for deriving test cases are software oriented

CAL Profiles for CAL Usage

HORIBA MIRA

Integration Level	Engineering Assurance CAL profiles Based on ISO/SAE PAS 8475 tailored to each layer
OEM / item manufacturer	Item / system CAL profile
Tier 1 component supplier	ECU CAL profile
Tier 2 software supplier	Software CAL profile
Hardware supplier	Hardware CAL profile
Semiconductor IP vendor	Semiconductor IP CAL profile

CAL inherited by requirements allocated to components during engineering

Each profile could define more specific examples of breadth and depth relevant for a single integration level or supply chain tier

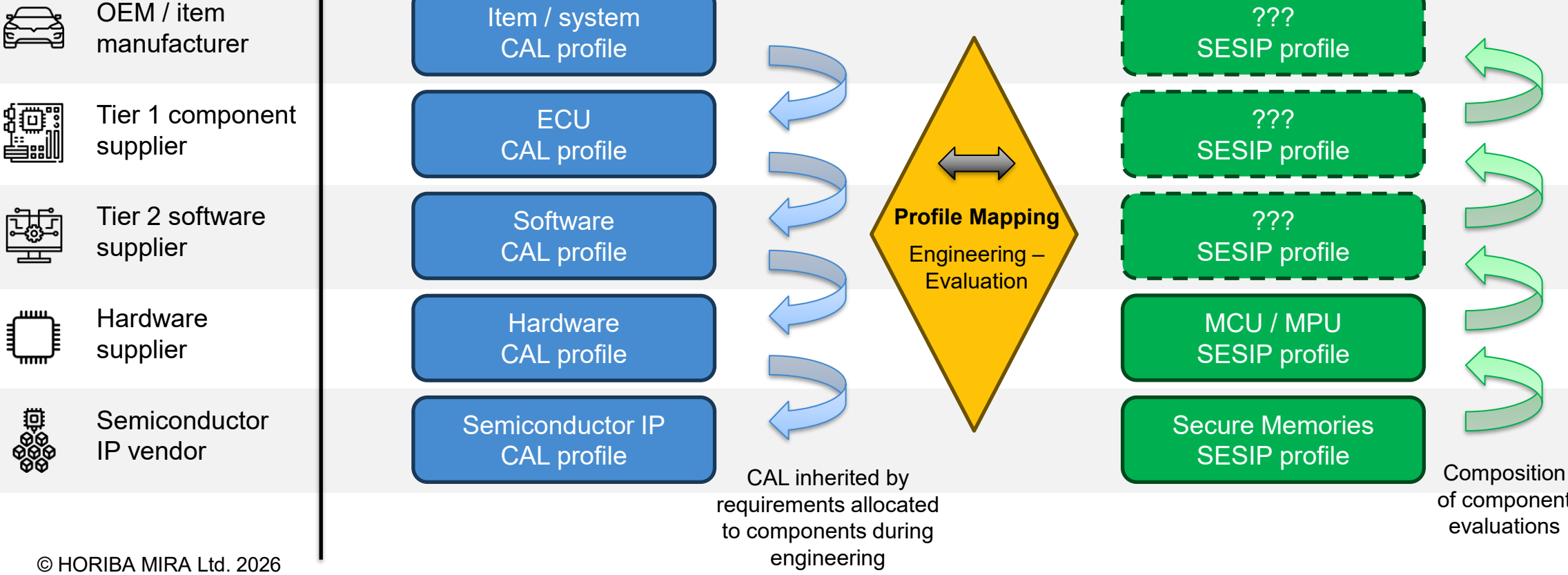
Profiles could be agreed between organisations within each tier

Benefits of Security Evaluation

- Other industries have adopted independent security evaluation as a means of demonstrating assurance
  - Common Criteria evaluation of smartcards, digital tachographs, smart meters
  - SESIP evaluation of secure microcontrollers and external memories
- **Commonly cited disadvantages of evaluation**
  - Slow and expensive
  - Difficult to scale to diversity of automotive systems and components
  - Need to control disclosure of intellectual property
- **Potential benefits**
  - International mutual recognition
  - Comparable evaluations through accredited test laboratories
  - Composite evaluation allows costs to be shared through the supply chain

Aligning Engineering and Assurance
Using Profiles

HORIBA MIRA



Conclusion

- The Cybersecurity Assurance Levels (CAL) concept initially defined in ISO/SAE 21434 is being elaborated in a new document ISO/SAE PAS 8475
- CAL provides a means of scaling the rigour (breadth and depth) with which cybersecurity activities of ISO/SAE 21434 are performed to achieve **engineering assurance**
- CALs are assigned to cybersecurity goals and requirements, inherited as cybersecurity requirements are refined, enabling the necessary rigour to be **communicated through the supply chain**
- **Profiles defining CAL usage** for different integration levels might help increase usability of the CAL concept
- Aligning CAL with security evaluation (e.g. SESIP) via profiles could help provide joined-up assurance through both **engineering and evaluation**, composable through the supply chain