HORIBA MIRA

ISO/SAE PAS 8475 and TR 8477

Update on assurance-related standards

Paul Wooderson

21 October 2026

© HORIBA MIRA Ltd. 2026

Introduction
ISO/SAE Cybersecurity Standards

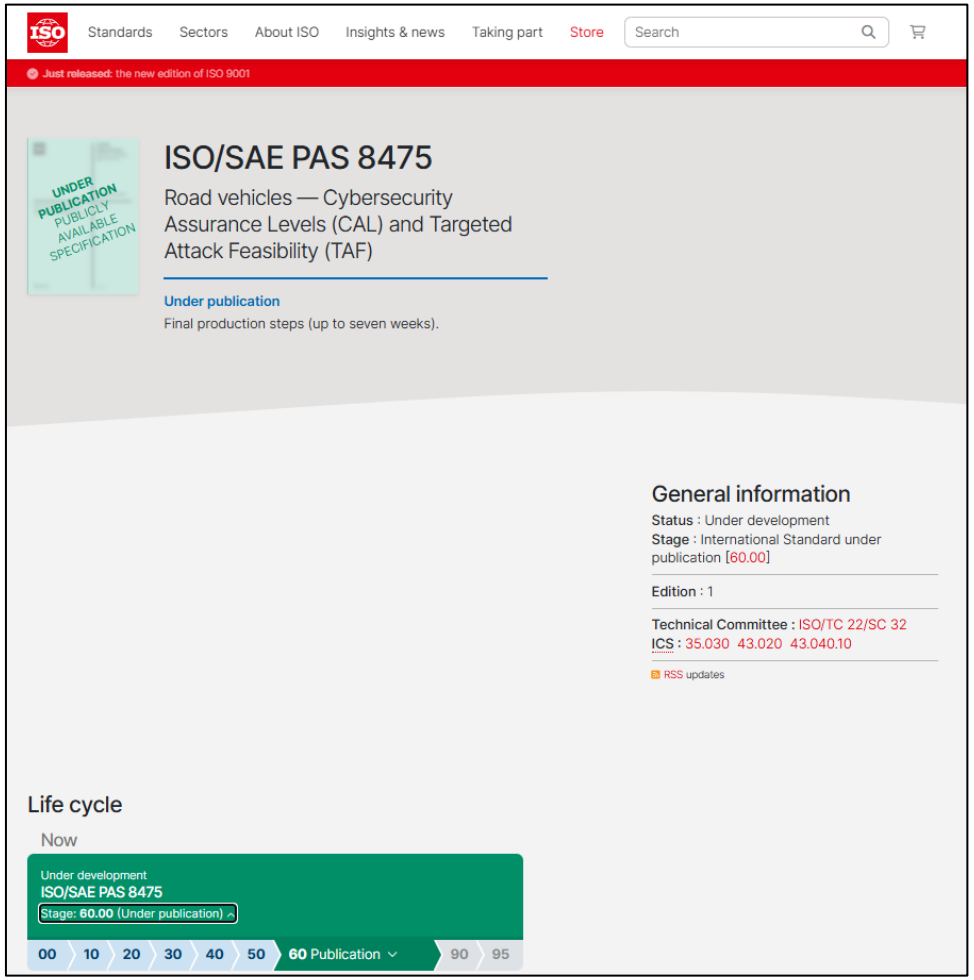
- Since the publication of ISO/SAE 21434 in 2021, the ISO/SAE joint working group has been working on several projects to develop additional guidance
- All of these documents are relevant to automotive cybersecurity assurance

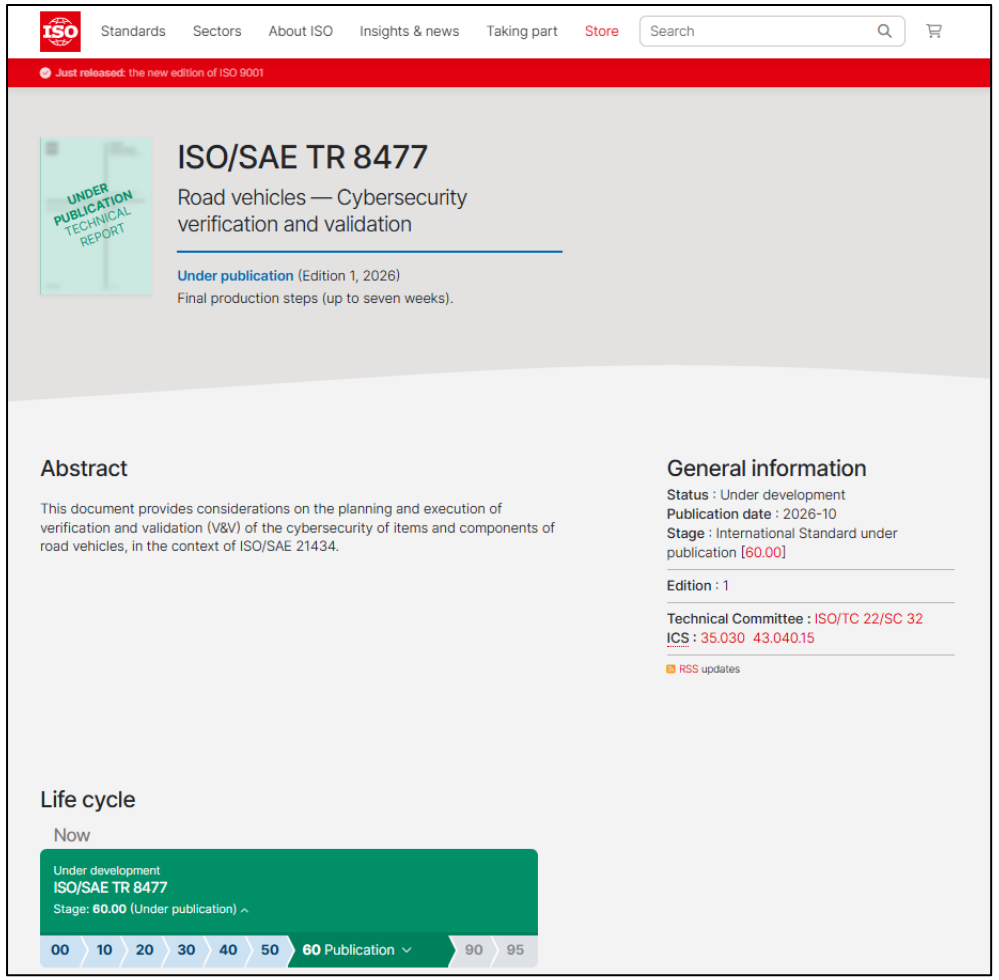
Working Group	Project Number	Project Name	Document Type	Status/Timeline
ISO TC22/SC32/WG11 ISO and SAE Joint Working Group for Cybersecurity	ISO/TS 5112	Guidelines for auditing cybersecurity engineering	Technical Specification (TS) – being converted from PAS	• Approval stage
	ISO/SAE PAS 8475	Cybersecurity Assurance Levels (CAL) & Targeted Attack Feasibility (TAF)	Publicly Available Specification (PAS)	• Approved by ISO and SAE • Under publication (expected within 2026)
	ISO/SAE TR 8477	Cybersecurity verification and validation	Technical Report (TR)	• Approved by ISO and SAE • Under publication (expected within 2026)
	ISO/SAE 21434 2nd edition	Cybersecurity engineering	International Standard	• Project started 1 Oct 2026

© HORIBA MIRA Ltd. 2026

Introduction
Current Status

- Both ISO/SAE PAS 8475 and ISO/SAE TR 8477 are under publication, expected within 2026





© HORIBA MIRA Ltd. 2026

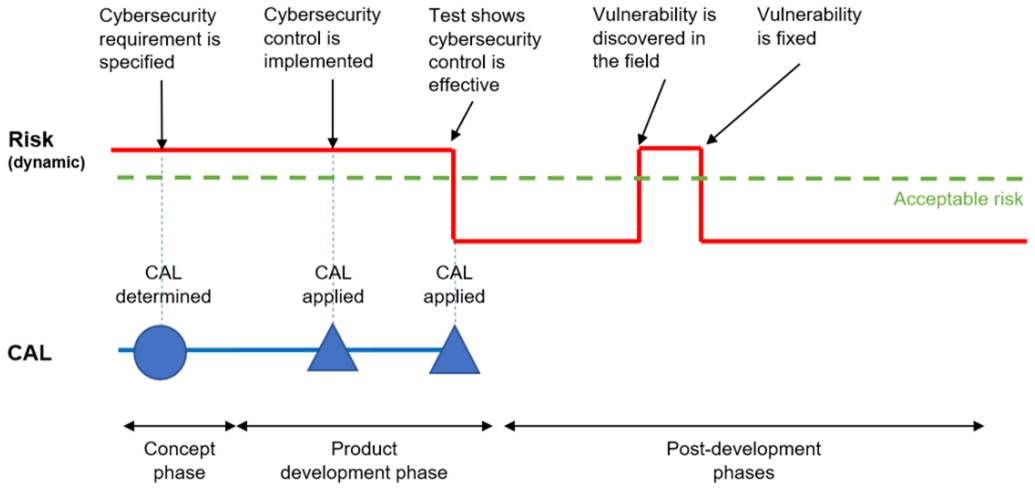
ISO/SAE PAS 8475
CAL and TAF

ISO/SAE PAS 8475 Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF)

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

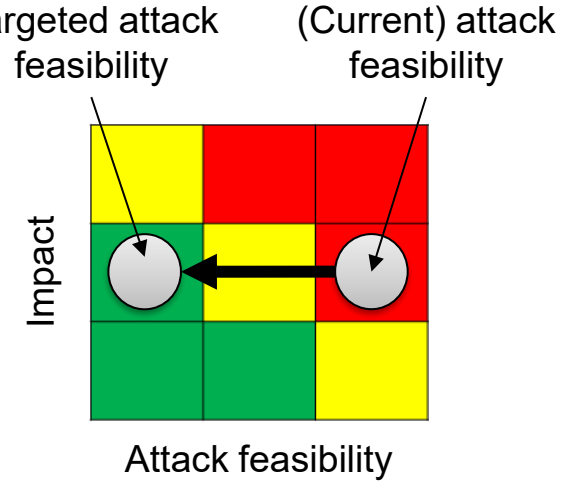
Cybersecurity Assurance Levels (CAL)

- 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



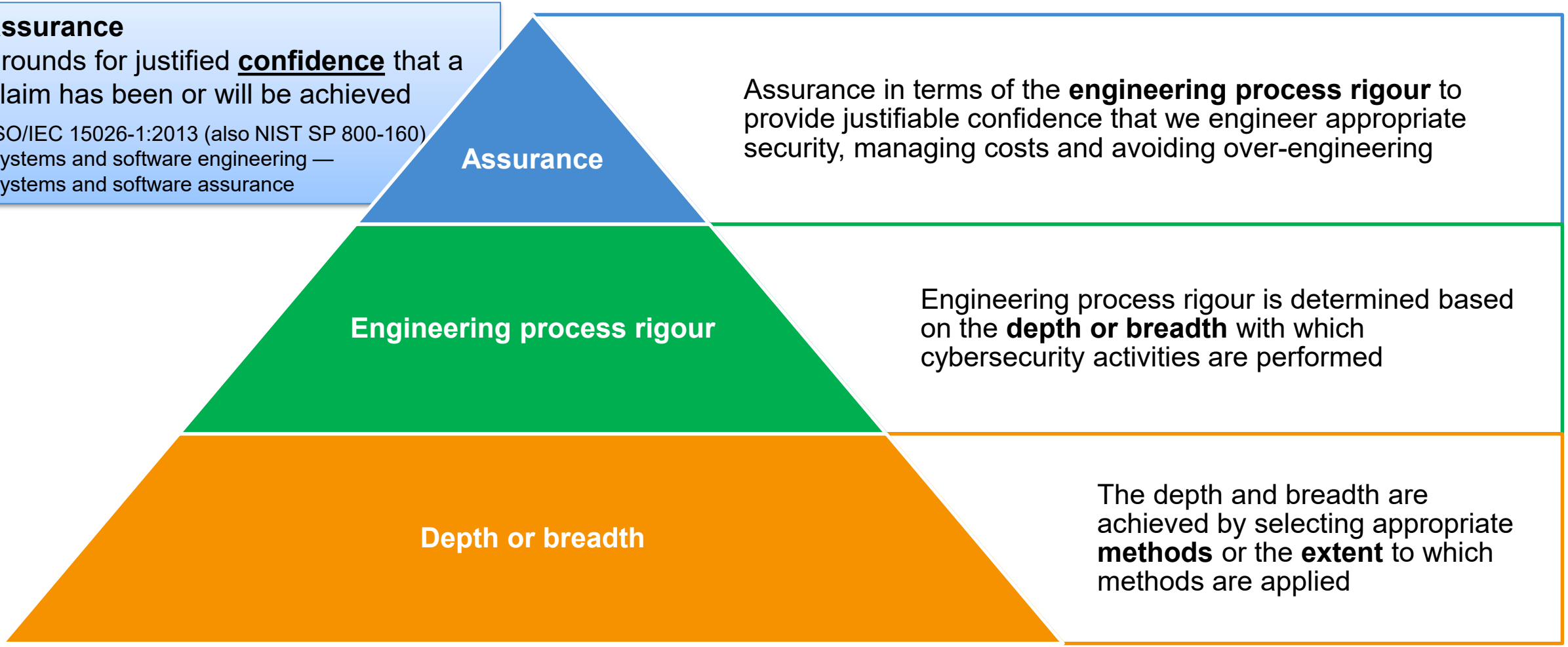
© HORIBA MIRA Ltd. 2026

ISO/SAE PAS 8475

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

© HORIBA MIRA Ltd. 2026

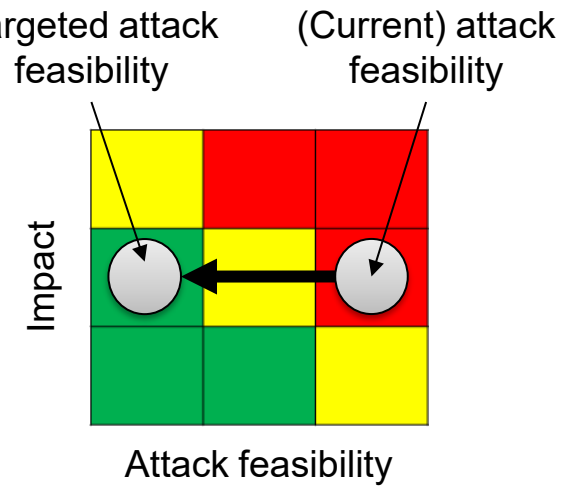
ISO/SAE PAS 8475
Targeted Attack Feasibility (TAF)

- Attack feasibility is defined in ISO/SAE 21434:

> **3.1.3**
> **attack feasibility**
> attribute of an *attack path* (3.1.4) describing the ease of successfully carrying out the corresponding set of actions

- Targeted attack feasibility is a new concept, not in ISO/SAE 21434, to specify the desired attack feasibility rating after applying cybersecurity controls
- Proposed definition in latest draft of ISO/SAE PAS 8475:

> **3.2**
> **targeted attack feasibility**
> **TAF**
> attack feasibility expected for an item or component after cybersecurity controls are applied



- TAF is currently expected to be an Informative Annex of ISO/SAE PAS 8475

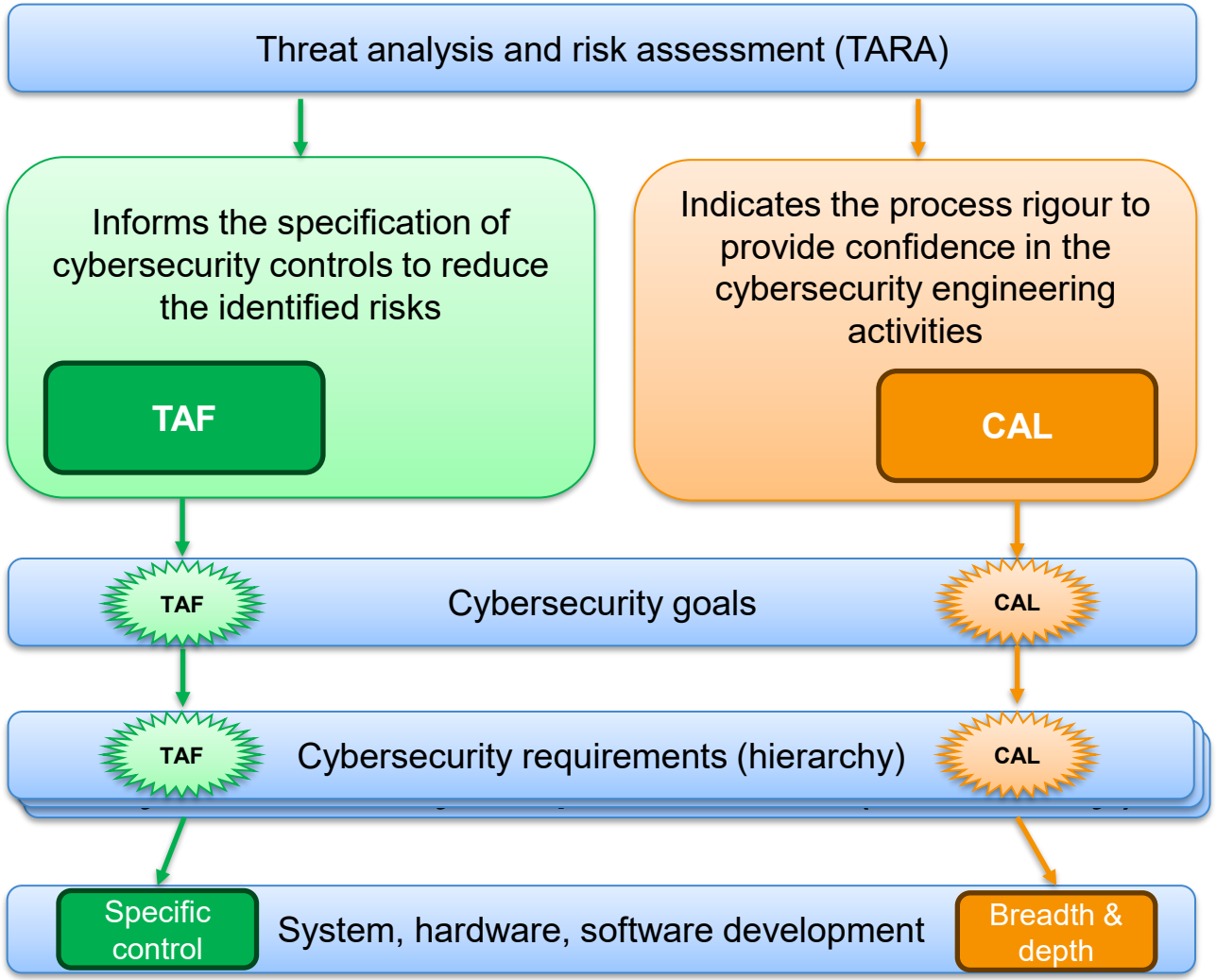
© HORIBA MIRA Ltd. 2026

ISO/SAE PAS 8475
Usage of CAL and TAF

HORIBA MIRA

- A CAL is **determined** for each cybersecurity goal by considering the related threat scenario(s)
- Cybersecurity requirements **inherit** the CAL from their parent cybersecurity goal
- A TAF rating is **determined** based on consideration of attack paths and **assigned** to a cybersecurity requirement
- Cybersecurity requirements including their associated CAL and TAF are **allocated** to components (e.g. ECUs)
- The CAL is used to scale the breadth and depth of the development methods for the component
- The TAF is used to specify appropriate controls for the component to achieve the TAF

Note: Conformance with the requirements of ISO/SAE 21434 is always mandatory, regardless of the CAL or TAF



© HORIBA MIRA Ltd. 2026

ISO/SAE TR 8477

Cybersecurity Verification and Validation

ISO/SAE TR 8477 Cybersecurity verification and validation

- ISO/SAE 21434 requirements on cybersecurity **verification** and **validation** are very high-level
- ISO/SAE TR 8477 aims to provide further guidance
- Document is a Technical Report (TR) – informative content only
- Scope is verification and validation for cybersecurity, objective-oriented, not solution-oriented
- A joint activity between ISO and SAE
- SAE have also recently published guidance on cybersecurity V&V **testing methods** (SAE J3322) which will be referenced from ISO/SAE TR 8477

© HORIBA MIRA Ltd. 2026

Open Challenges for Assurance

- 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 intended to be 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?
    - E.g. methods applicable to each specific supply chain tier
2. Is there value in linking the concept of **engineering assurance** (CAL) with the assurance provided by cybersecurity assessment or evaluation (e.g. SESIP)?

© HORIBA MIRA Ltd. 2026

CAL Usage at Different Integration Levels

HORIBA MIRA

ISO/SAE PAS 8475

Examples of methods for scaling rigour of ISO/SAE 21434 [RQ-10-10]

(Specification of integration and verification activities)

- 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

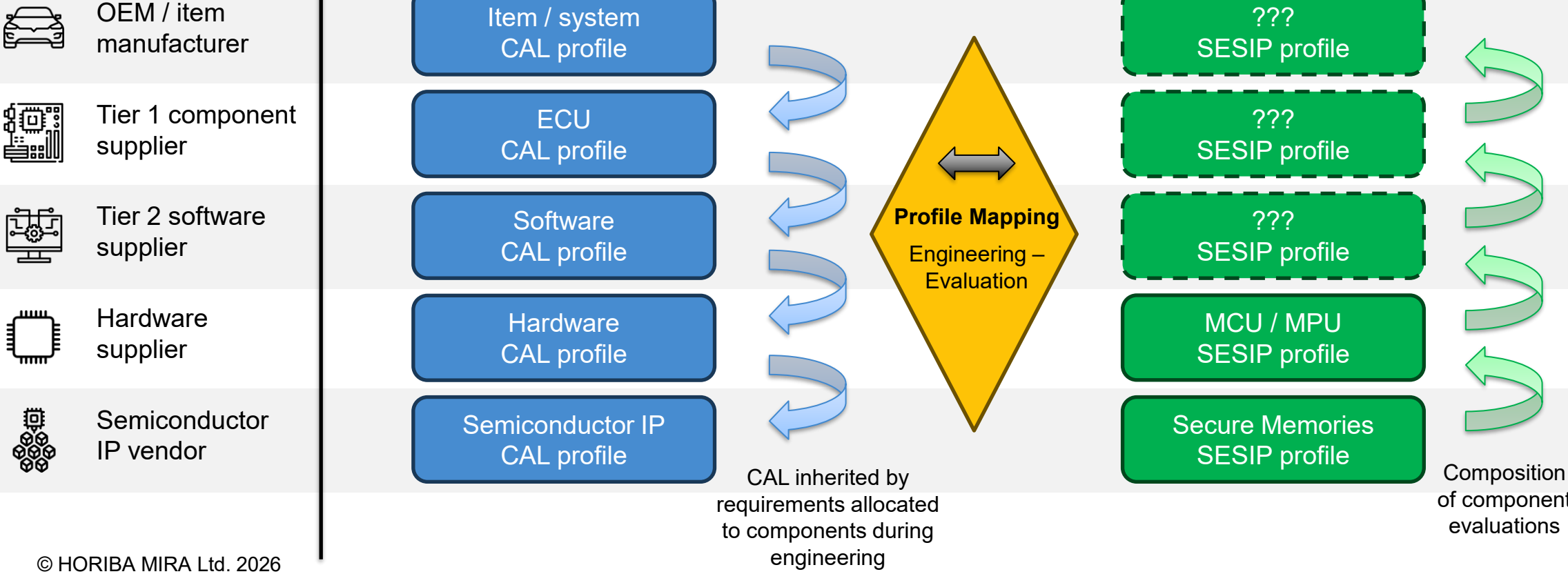
Factors affecting breadth and depth may differ at different integration levels, for example:

- **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

© HORIBA MIRA Ltd. 2026

Aligning Engineering and Assurance
Using Profiles

HORIBA MIRA



© HORIBA MIRA Ltd. 2026

Conclusion

- ISO/SAE PAS 8475 and ISO/SAE TR 8477 are approved by the respective ISO and SAE committees and are expected to be published by the end of 2026
- 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**
- TAF provides a means for customers to indicate the **expected capability of cybersecurity controls** to a supplier but allow flexibility for a supplier to specify the most appropriate cybersecurity control
- **Profiles defining CAL usage** for different integration levels might help increase usability of the CAL concept through the supply chain
- 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

Contributions to Assurance

© HORIBA MIRA Ltd. 2026