


Update on ISO/SAE PAS 8475 and TR 8477

Paul Wooderson

9 December 2025

- 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)	<ul style="list-style-type: none">• Preparing for DPAS ballot• Publication expected Q1 2026
	ISO/SAE TR 8477	Cybersecurity Verification and Validation	Technical Report (TR)	<ul style="list-style-type: none">• Preparing for DTR ballot• Publication expected Q12026

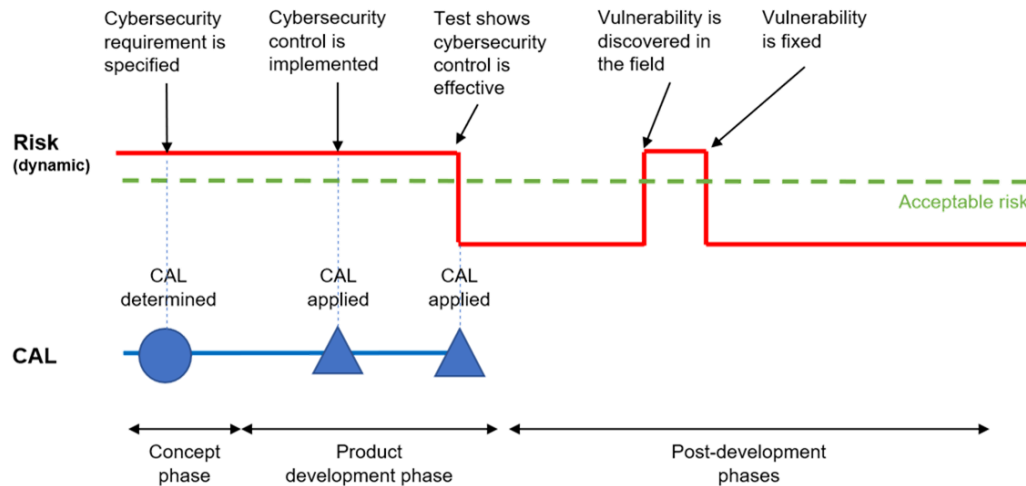


ISO/SAE PAS 8475 project started in November 2022 to develop further guidance on two concepts

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

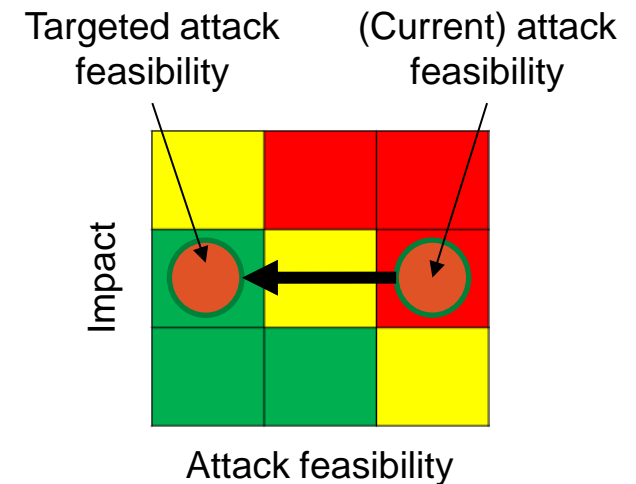
Cybersecurity Assurance Levels (CAL)

- 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



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 /
confidence**

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

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

Depth or breadth

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

- **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:

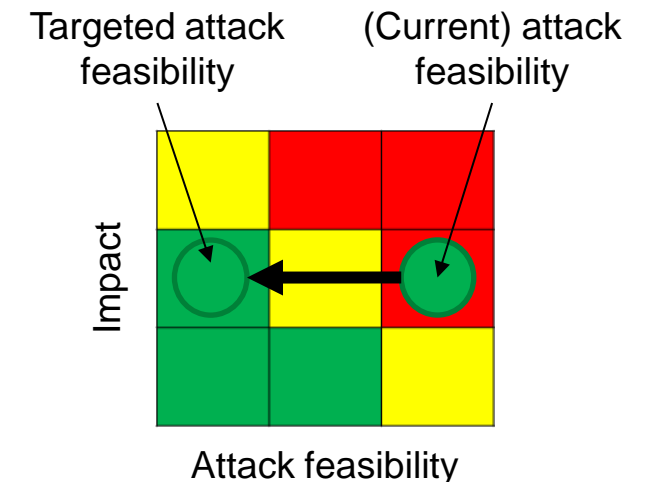
3.2

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



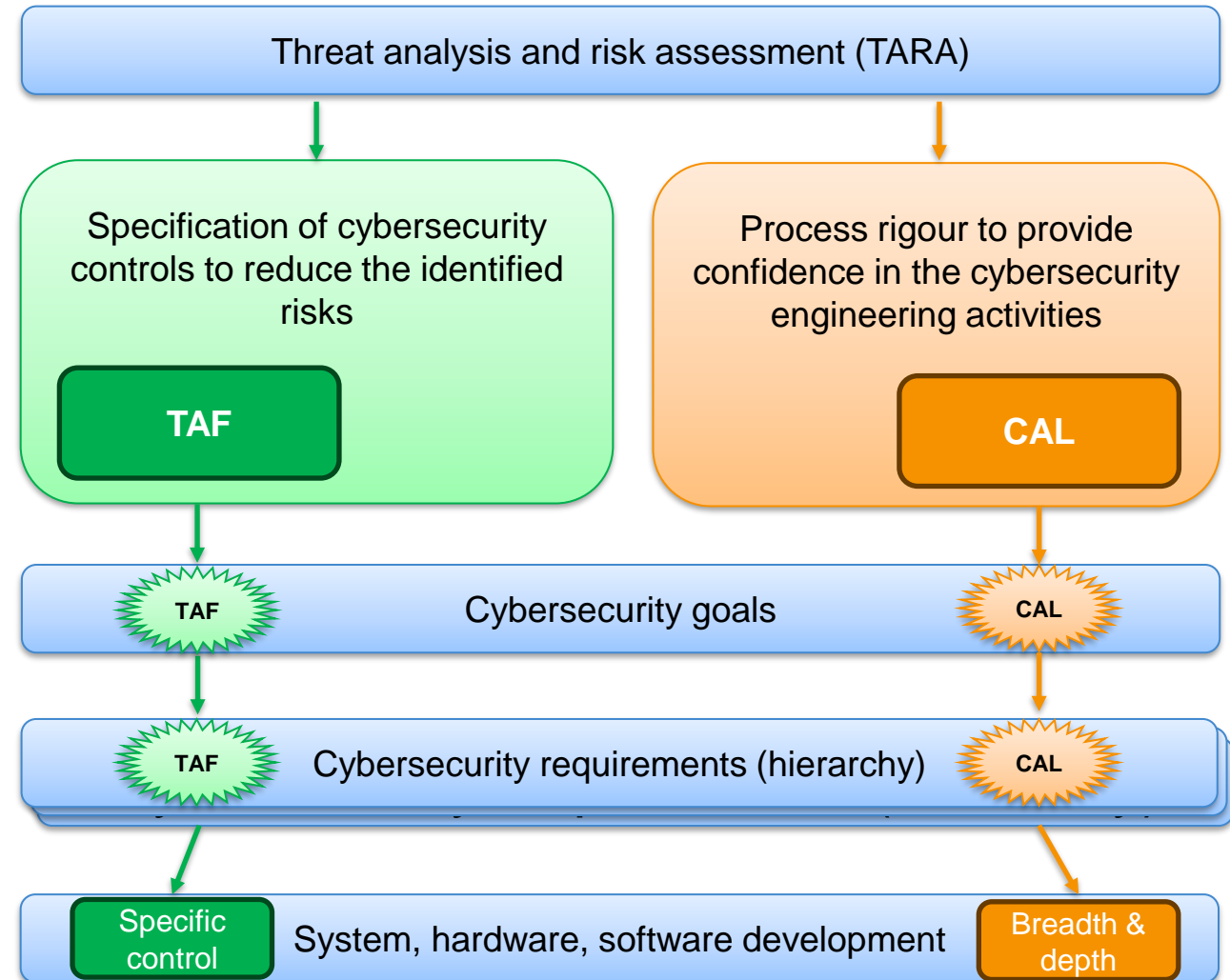
Cybersecurity Assurance Levels (CAL)

Usage of CAL and TAF

- 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
 - The CAL provides a means to justify the breadth and depth applied to the development activities





ISO/SAE TR 8477 project started in October 2023 to develop further guidance on cybersecurity V&V

- ISO/SAE 21434 requirements on cybersecurity **verification** and **validation** are very high-level
- ISO/SAE TR 8477 aims to provide further guidance
- Target 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 recently published guidance on cybersecurity V&V **testing methods** (SAE J3322) which will be referenced from ISO/SAE TR 8477

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