Suzanne Lightman

Co-Chair

CAL/TAF Project Group

Overview of PAS 8475: Cybersecurity Assurance Levels (CAL) and TAF

Process overview

- JWG began work on a Publicly Available Specification In late 2022
  - A temporary document
    - Good for two years
    - Can be renewed for up to four years

Purpose of PAS 8475

- Extend the information on CAL
- Provide requirements
  - CAL determination
  - CAL usage
- Introduce the TAF concept

CAL

- Introduced in Annex E of 21434
- Represented the level of rigor to provide confidence that protection of the assets of an item or component is adequately developed
- Certain base concepts were set forth
  - The CAL should be based on stable factors as opposed to being directly related to risk (which can change over time)
  - CAL is assigned in the concept phase of the lifecycle
  - CAL is about the rigor associated with cybersecurity activities
  - CAL is assigned to cybersecurity goals

CAL in PAS 8475 (STILL IN DRAFT)

- Definition of CAL levels
  - Reduced to 3 levels (Basic, Intermediate, Advanced)
  - 4 factors
    - Activities (include the unique cybersecurity activities from ISO/SAE 21434)
    - Depth of performance
    - Formality
    - Independence
- Examples of scaling rigor with different CALs
- Clarification on the assignment of CAL to cybersecurity goas
  - When there are multiple CALs for a goal
  - When there are multiple CALs for a cybersecurity requirement

CAL in PAS 8475 (still in draft)

- Examples
  - CAL assignment
  - CAL allocation
- Currently the document is in comment resolution
- Target publication of early 2026

TAF

- New concept introduced
  - Informative only
  - In Annex
- The expected attack feasibility rating for an item or component **after** cybersecurity controls are applied
- Designed to
  - Allow flexibility to suppliers
  - Allow customers to reduce detail
- PAS provides examples

Example of TAF

- Customer is developing an item which contains a secure gateway protecting component A
- They contract with supplier for component A
- They give the supplier a TAF rating of TAF 1 for the communication pathway for the component
  - TAF 1 = the attack feasibility for a given attack path is reduced to Medium when cybersecurity measures are applied
  - Customer does not supply their item architecture to supplier