Roadmap and development status of joint ISO-SAE automotive cybersecurity publications and standards

John T. Krzeszewski

May 21, 2025

Powering Business Worldwide

There is no better time than now to be an **intelligent power management company.**

Powering Business Worldwide

Speaker Introduction

- Member and co-convener of ISO/SAE Joint-Working-Group
- Chair of ISO/SAE 21434 (TARA)
- Chair, SAE Vehicle Cybersecurity Systems Engineering Committee
- Eaton Functional Excellence, Cybersecurity & Functional Safety lead

Today's Discussion

Ongoing joint activities

Enhance existing concepts, introduce new concept, additional guidance

Timing

Release of specification and technical report

ISO/SAE 21434

Current activities as a precursor to version 2

A G E N D A

ISO/SAE PWI 8475 CAL/TAF

- *History/motivation*
- *Current state & open items*
- *Timing*

ISO/SAE PWI 8477 V&V

- *History/motivation*
- *Current state & open items*
- *Timing*

ISO/SAE 21434 2nd Edition

- *Current state*
- *Timing*

Opportunities in development

Powering Business Worldwide

ISO/SAE PWI 8475 project

Cybersecurity Assurance Level (CAL)
&
Targeted Attack Feasibility (TAF)

Cybersecurity Assurance Level

Concept origin & motivation

History

- ***Concept development started in 2017***
- ***Initial version released as annex in 21434 in 2021***

Motivation

- ***Introduced to scale process rigor according to criticality in supply chain***
- ***Desire to leverage other static risk factors in CAL determination***
- ***Desire to expand application to all applicable 21434 requirements***
- ***Ensure consistent application to facilitate efficient communications and provide justifiable confidence***

Powering Business Worldwide

PWI 8475 CAL/TAF group members[1]

- ISO/SAE PWI 8475 CAL-TAF member countries
  - Austria
  - Belgium
  - Canada
  - France
  - Germany
  - India
  - Japan
  - Republic of Korea
  - Sweden
  - United Kingdom
  - United States (SAE)
  - Czechia

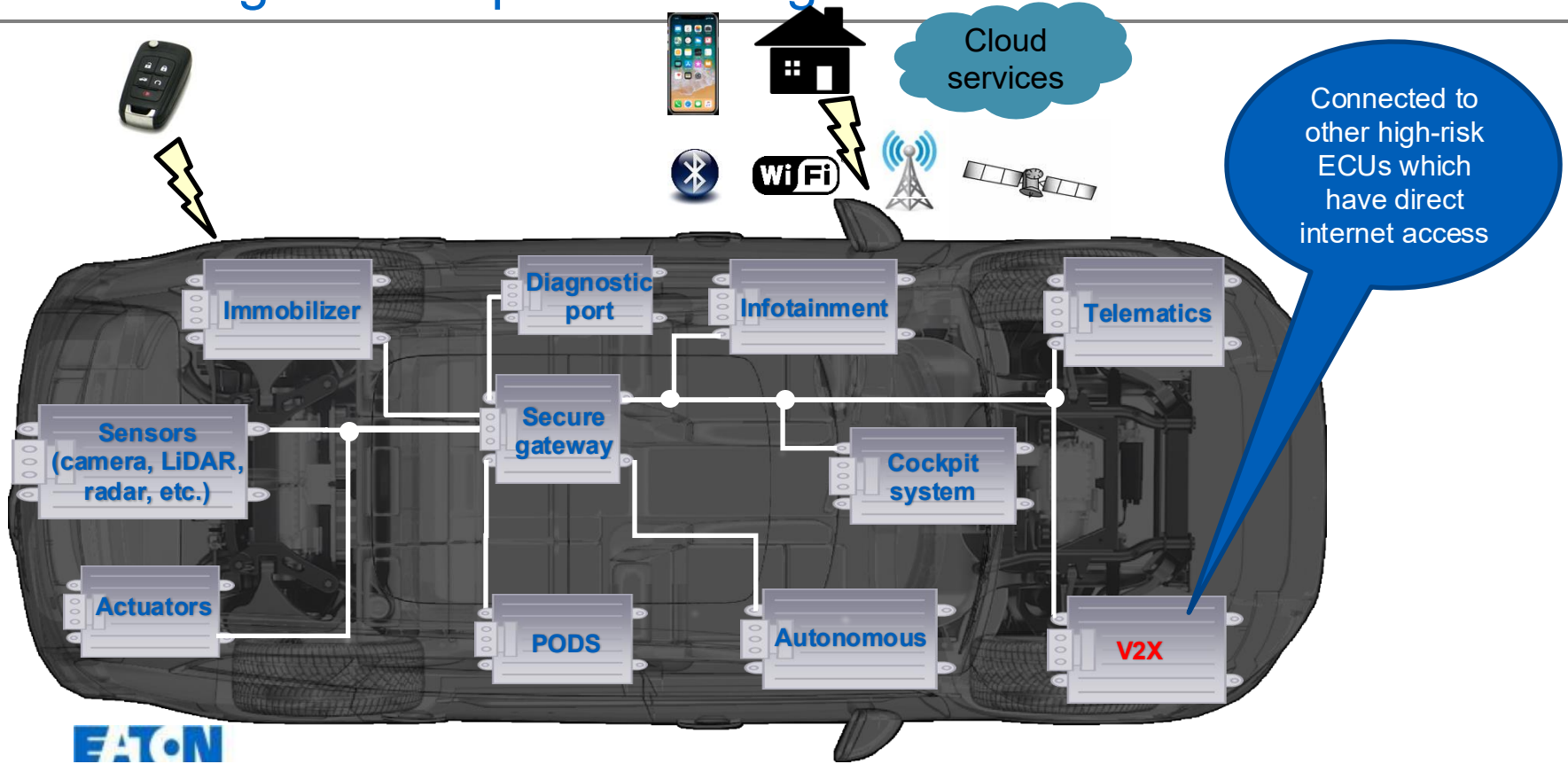
[1]**Submitted technical feedback on latest CD2**

Current state of CAL development

- CAL determination
  - Early in as possible - when all required inputs are available
    - ❖ Before activities that use CAL
  - Uses same parameters as defined in 21434
  - Optionally can include other static factors (with justification)
    - ❖ Architectural considerations
      - ➢ Depth, accessibility, exposure, degree of separation, operational environment, etc.
      - ➢ Examples on subsequent slides

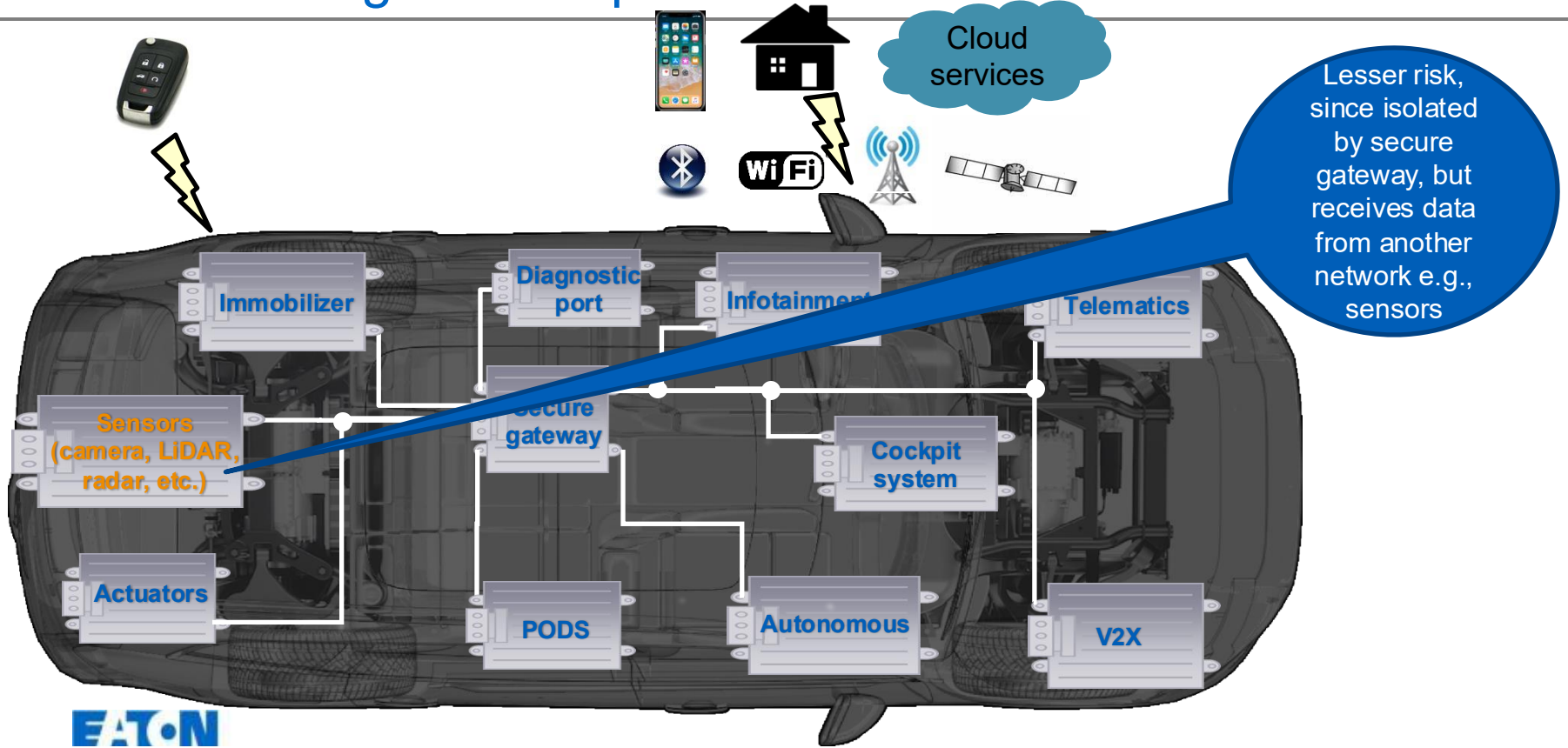
Powering Business Worldwide

V2X
- Low degree of separation: highest static risk

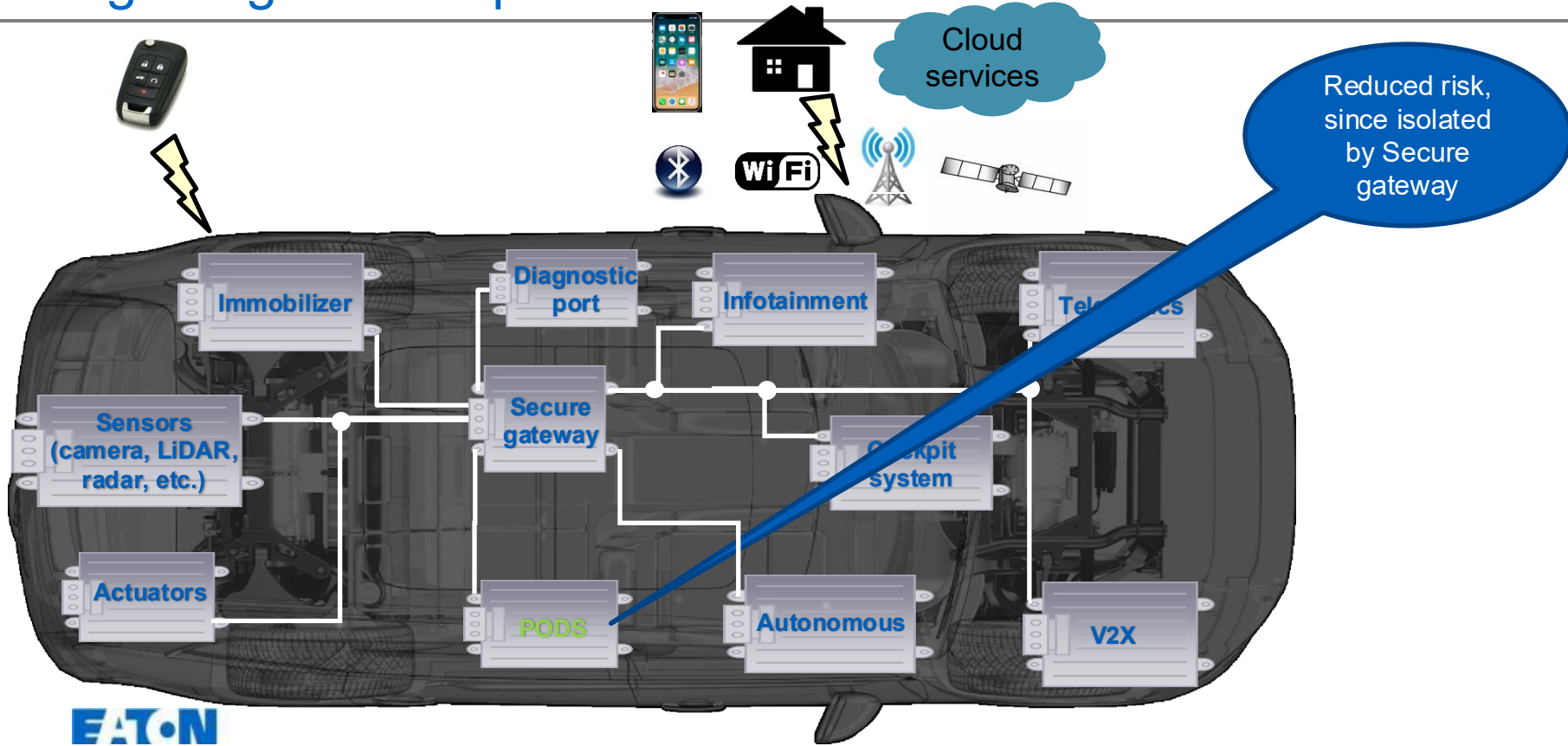


EATON
Powering Business Worldwide

Immobilizer
- Additional degree of separation: reduced static risk



PODS
- High degree of separation: lowest static risk



EATON
Powering Business Worldwide

Current state of CAL development

- Higher CAL ⇔ requires additional process rigor
- Expanding and clarifying applicability by clause/requirements of 21434
  - Applicable to the following
    - Some requirements in clause 9
    - Clause 10
    - Clause 11
  - Not applicable to the following
    - Clause 5
    - Clause 6 (except for independence of assessment)
    - TARA in clause 9
    - Clauses 8, 12, 13, 14 and 15

Powering Business Worldwide

Current state of CAL development

- Providing definitions of CAL levels and application
  - Now only 3-levels (CAL1 [basic], CAL2 [intermediate], CAL3 [advanced])
    - Tables to provide examples of how to apply i.e., activities/rigor per CAL
      - Can always do more than the specified CAL
  - Help ensure consistency in interpretation, while providing flexibility
- CAL is an attribute of a CS goal
  - Intended to be stable; required updates to be done via change mgt.
- No detailed guidance given for
  - Application in an out-of-context situation
  - Usage for off-the-shelf components

Powering Business Worldwide

ISO/SAE PWI 8475 project

Cybersecurity Assurance Level (CAL)
&
Targeted Attack Feasibility (TAF)

Powering Business Worldwide

Targeted Attack Feasibility

Concept origin & motivation

History

- ***Concept introduced during 21434 development***
- ***Postponed due to inadequate development time***

Motivation

- ***As a result of the TARA, the risk treatment decision for certain threats will be to 'reduce the risk'***
  - ✓ ***How do you specify the required strength of counter-measures?***
  - ✓ ***How do you know if the counter-measure strength is 'sufficient'?***
- ***Communicate required strength of countermeasures in supply chain***

EATON
Powering Business Worldwide

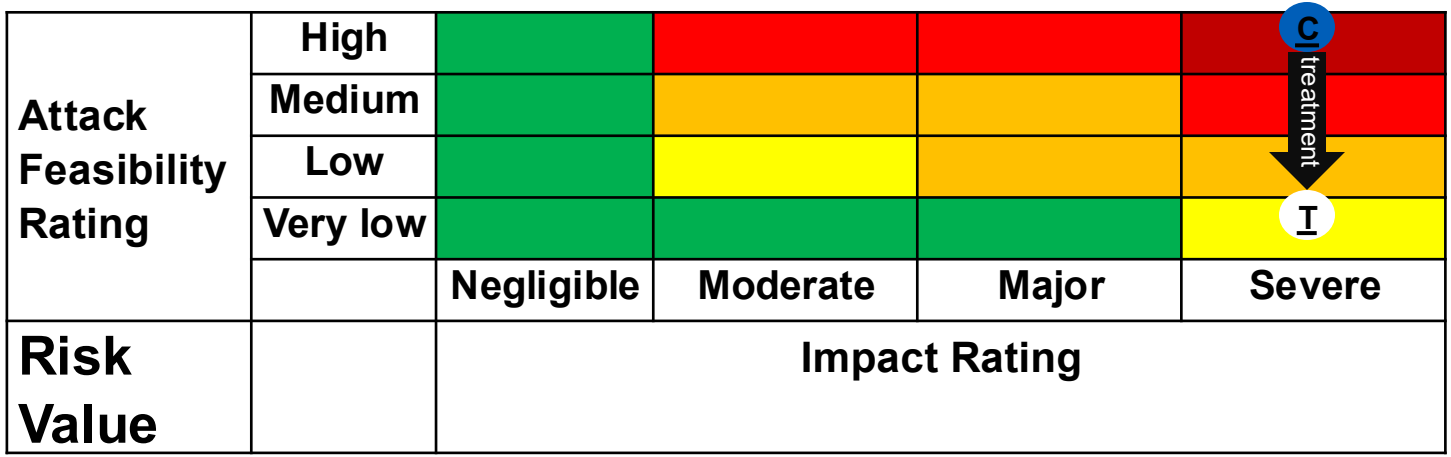
What is TAF?

- Based on attack feasibility (AF) as defined in 21434
  - ‘Attribute of an attack path describing the ease of successfully carrying out the corresponding set of actions’
- Current attack feasibility
  - Attack feasibility, considering current counter-measures, but before risk treatment
    - A factor to be considered when deciding risk treatment
- Targeted attack feasibility (TAF)
  - The target level of attack feasibility after implementation of countermeasures used to reduce residual risk to acceptable level
    - TAF and impact determine residual risk

Powering Business Worldwide

TAF selection

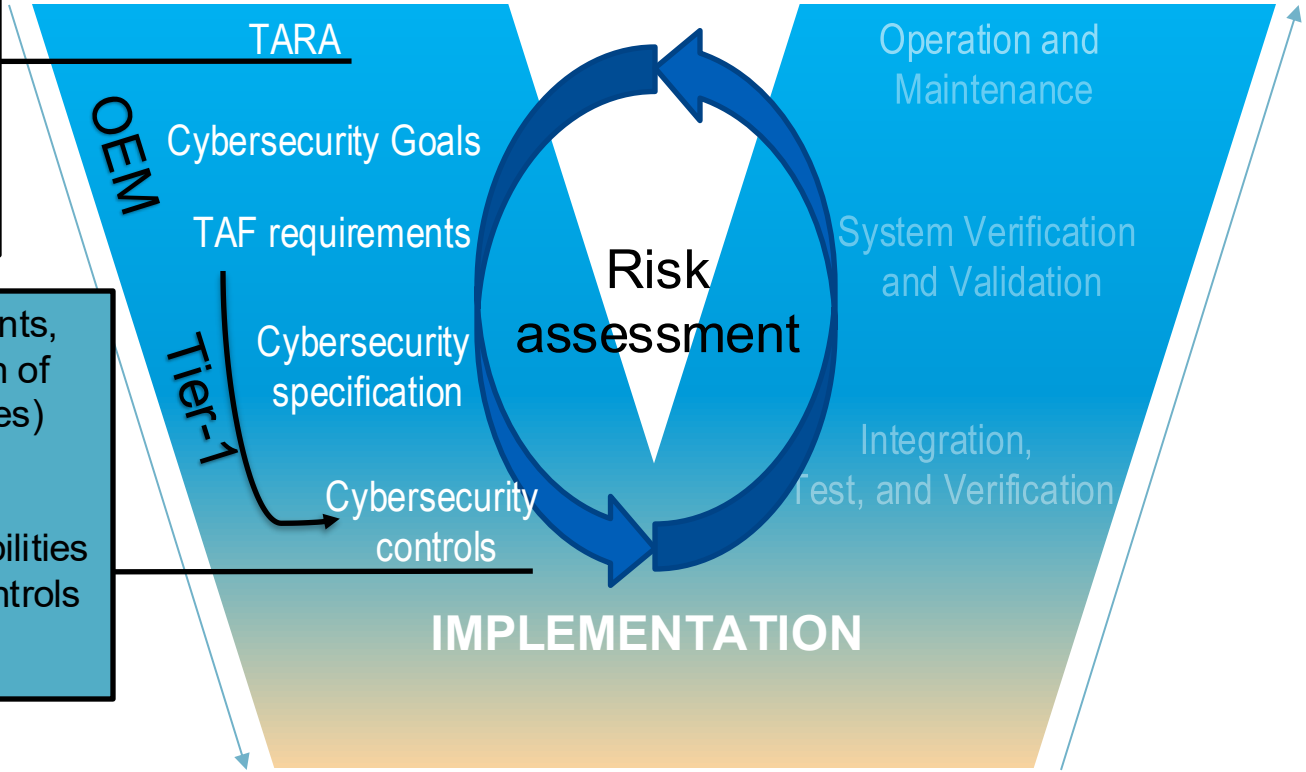
- The intent is to lower current attack feasibility
  - Selection of method to mitigate the risk could also reduce impact
  - Target level is communicated with supplier
    - TAF 1 (medium AF), TAF 2 (low AF), TAF3 (very low AF)
      - Illustrated below, where “C” is current, and “T” is targeted attack feasibility



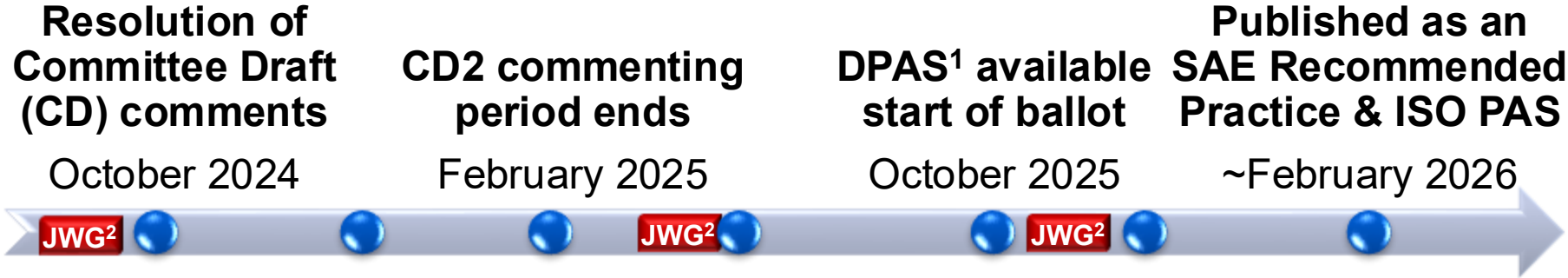
Potential application of TAF during design phase

- "TARA"=> output risk value, relative to threat/damage scenario (impact and attack feasibility)
- Derive CS goals and associated TAF
- Determines how to layer the protections (DiD)

- Refine & verify CS requirements, architecture, design: selection of controls (considering interfaces)
- Allocation of requirements to architectural elements
- Identify and manage vulnerabilities
- Selection of cybersecurity controls due to TAF (strength, depth)



ISO/SAE PWI 8475 CAL/TAF timeline



Expect a Q1 release in 2026

[1] Draft Publicly Available Specification (DPAS)
[2] ISO/SAE Joint Working Group (JWG) F2F meeting

ISO/SAE PWI 8477 V&V

Technical Report - Verification and Validation

Concept origin & motivation

History

- ***Some content originally in annex of earlier draft of 21434***
- ***Removed from 21434 before publication due to lack of content***

Motivation

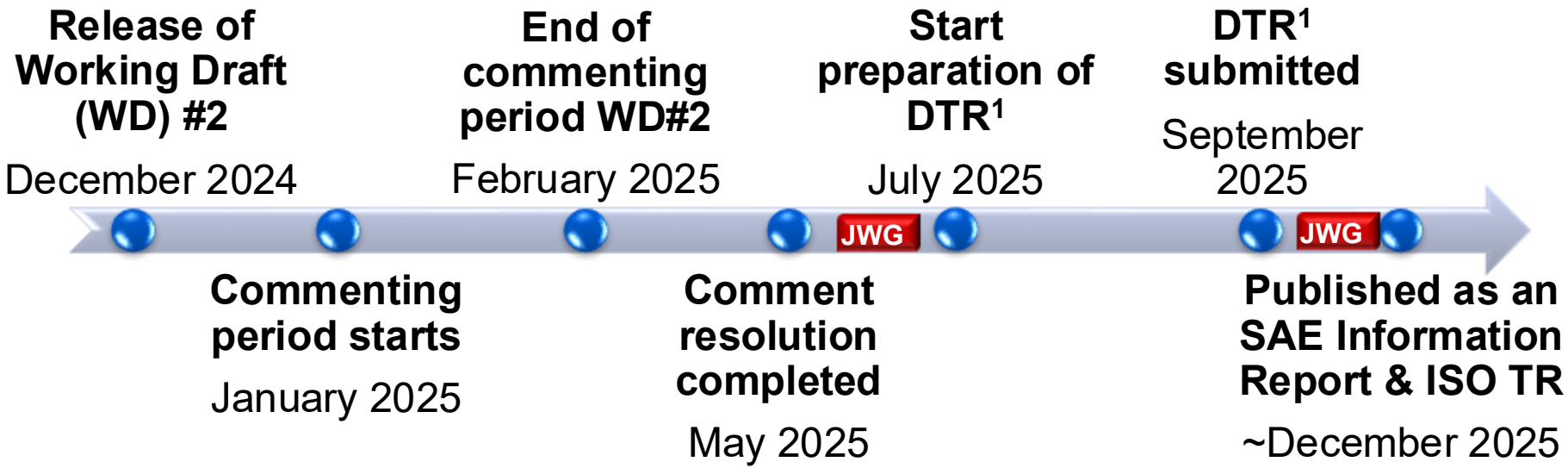
- ***Provide clarity on verification and validation and their relationship***
- ***Describe verification activities relative the 21434 requirements***
- ***Describe validation activities relative to cybersecurity goals, claims, etc.***
- ***Provide strategic guidance on V&V activities***

Powering Business Worldwide

Current state of V&V TR development

- Topics-current state
  - Defining verification and validation
  - Confirmation that CS requirements are adequate
  - Confirmation that implementation satisfies the CS requirements
  - Confirmation that assumptions hold true
  - Relationship between V&V and CS requirements, risk, activities
  - Example V&V methods
  - Application to off-the-shelf, reused & out-of-context components

ISO/SAE PWI 8477 V&V TR timeline



Expect a Q4 2025 release

[1]Draft Technical Report (DTR)

ISO/SAE 21434 2nd edition

ISO/SAE 21434 2nd edition

- Collected feedback from industry in 2024
- Content from current CAL, TAF and V&V projects will be leveraged
- Topics and concepts discussed during current projects as input
- Work delayed due to current joint ISO-SAE projects (CAL/TAF, V&V)

ISO/SAE 21434 v2 timeline

Comments submitted

August 2024

Key issues identified which can impact 21434 structure

May 2025

JWG decides on how key issues are to be addressed and scope

November 2025

Comments categorized

January 2025

Various options to address key issues documented

October 2025

Development starts

2026

Expect start of development 2026 (3+ years)

Opportunities to contribute to development of standards and publications

- Need experienced individuals
- Several SAE committees/task forces need volunteers
  - TARA task force
    - Best practices
    - Exchange of TARA information in supply chain (e.g., format of information)
  - Supply Chain BOM task force
    - Initially create an information report
    - Goal of publishing a best practice or standard
  - 21434 2nd edition (future need)
    - Output from above task forces may be included in 2nd edition

- Contact John Krzeszewski for additional information

Powering Business Worldwide

Questions?

Thank you!

John Krzeszewski, MSEE, GSEC

Senior Specialist, Functional Safety and Cybersecurity

jtk@eaton.com

Powering Business Worldwide

Eaton.com/WhatMatters