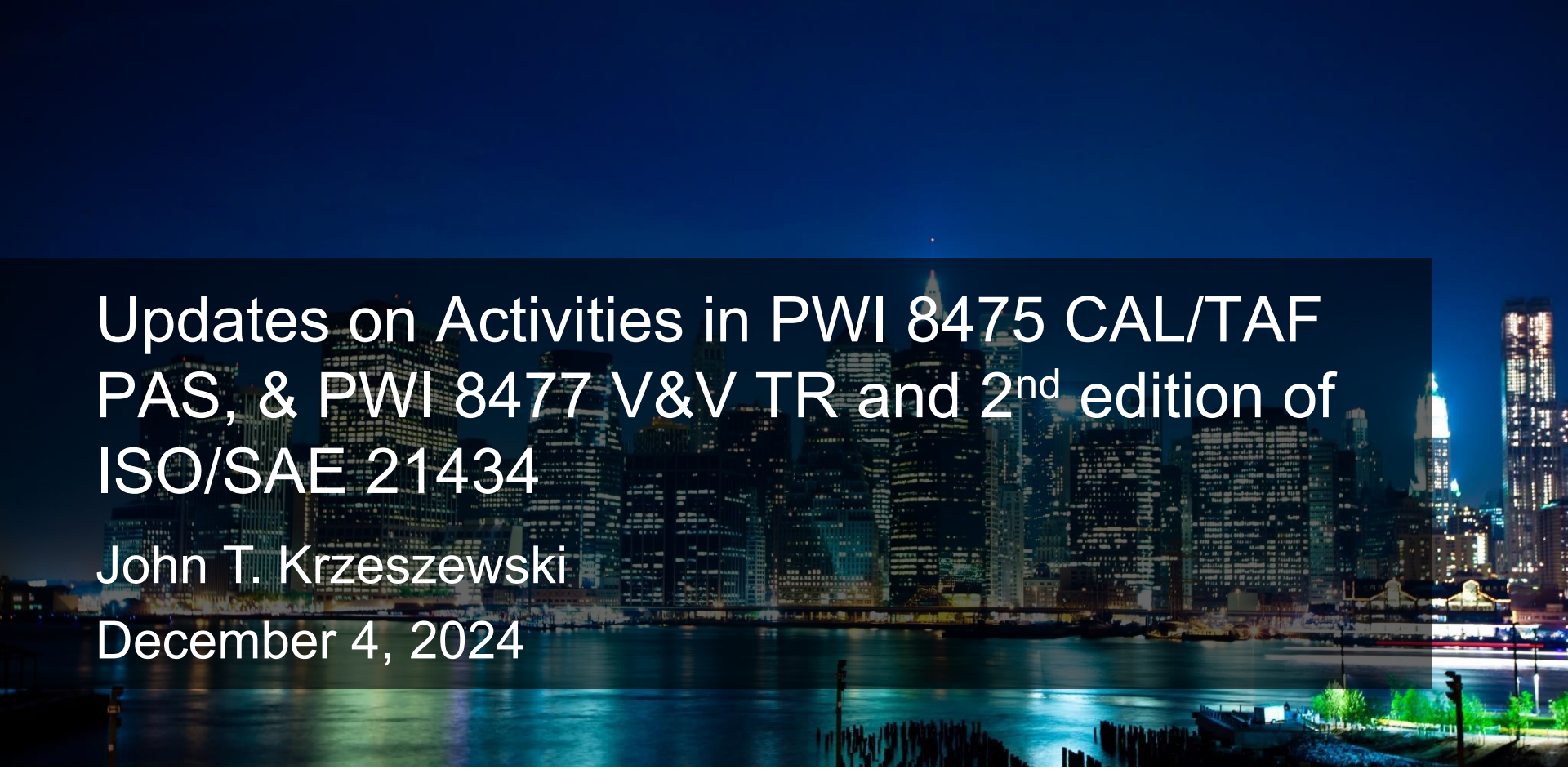


Updates on Activities in PWI 8475 CAL/TAF PAS, & PWI 8477 V&V TR and 2nd edition of ISO/SAE 21434

John T. Krzeszewski

December 4, 2024

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
- Previous 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*

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***

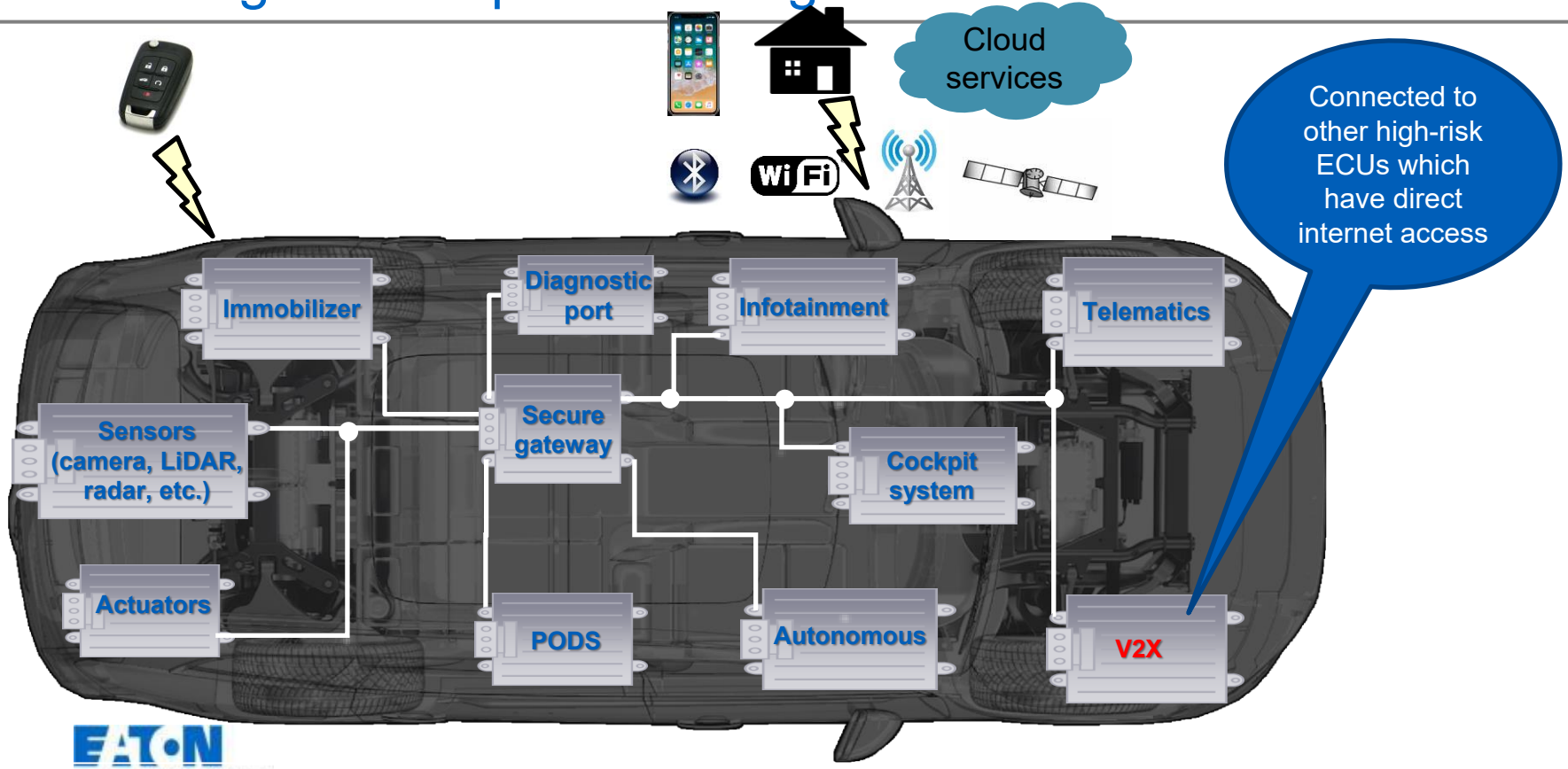
Powering Business Worldwide

6

Current state of CAL development

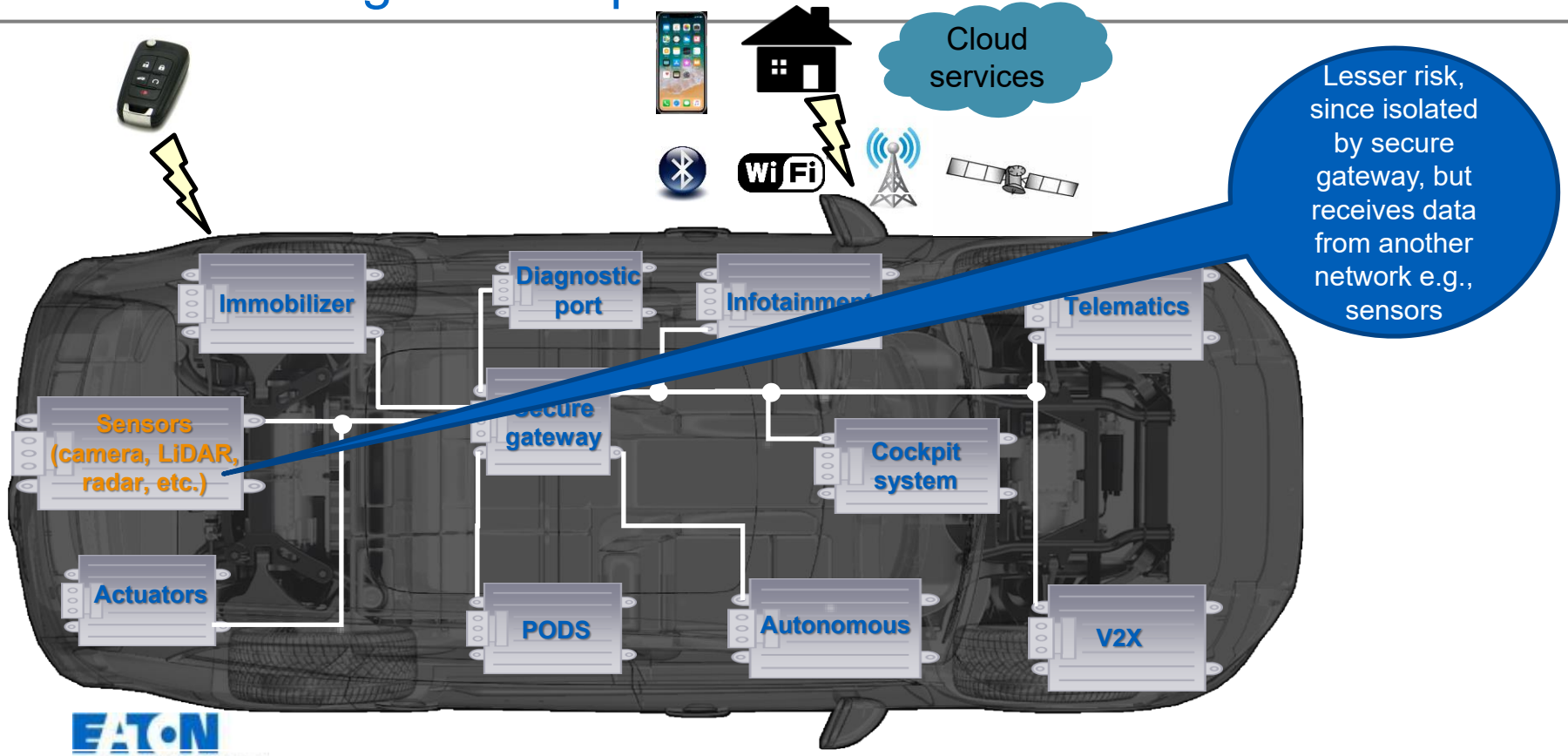
- CAL determination
  - Early in as possible - when all required inputs are available
    - ❖ Before activities that use CAL
  - Uses same parameters as defined in 21434
  - Optionally can include other static factors (with justification)
    - ❖ Architectural considerations
      - ➢ Depth, accessibility,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

V2X
- Low degree of separation: highest static risk

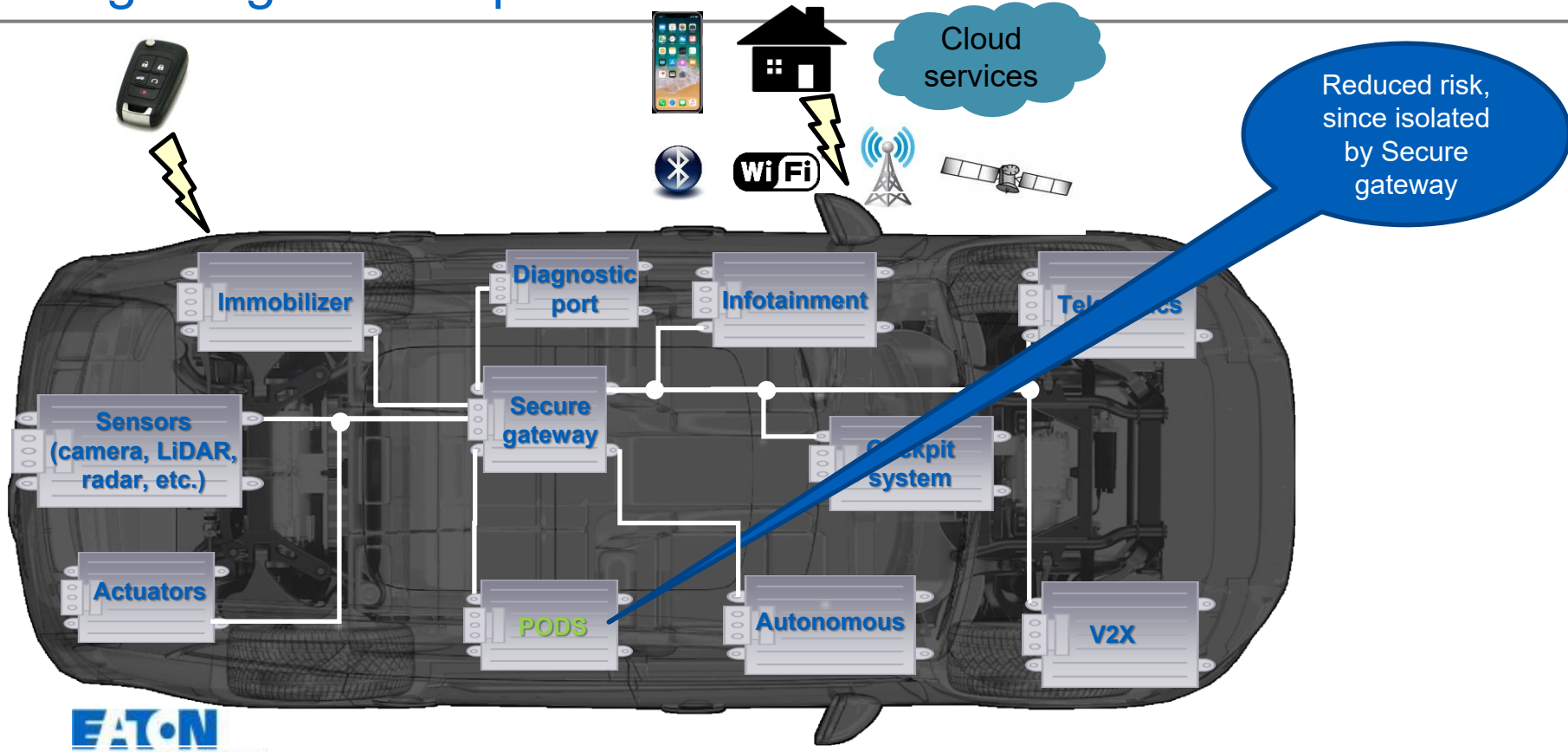


EATON
Powering Business Worldwide

Immobilizer
- Additional degree of separation: reduced static risk



PODS
- High degree of separation: lowest static risk



Current state of CAL development

- Higher CAL ⇔ requires additional assurance measures / effort
- 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 simple 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 discussion of
  - Application in an out-of-context situation
  - Usage for off-the-shelf components

Powering Business Worldwide

CAL open items

- Examples of deriving test cases based on CAL
- How isolation can impact CAL assignment

PWI 8475 CAL/TAF group members

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

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

16

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

TAF selection

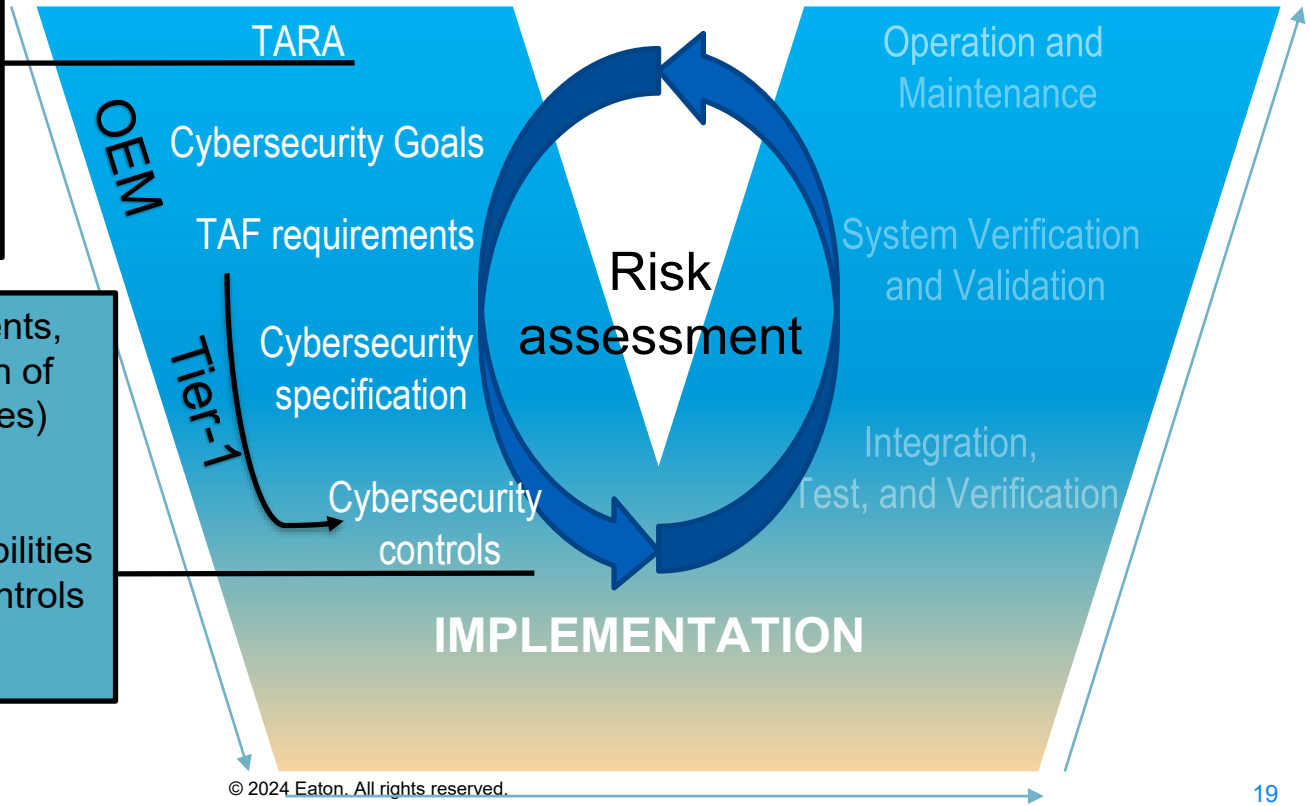
- The intent is to lower current attack feasibility
  - Selection of method to mitigate the risk could also reduce impact
  - Target level is communicated with supplier
    - TAF 1 (medium AF), TAF 2 (low AF), TAF3 (very low AF)
      - Illustrated below, where “C” is current, and “T” is targeted attack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

Attack Feasibility Rating	**High**				C
	Medium				treatment
	Low				
	Very low				T
		Negligible	**Moderate**	**Major**	**Severe**
Risk Value		**Impact Rating**			

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)



Current state of TAF development

- Will be included as an informational concept in an annex
- Agreed upon TAF concept principles
  - TAF determined for each threat scenario necessitating ‘reduction’ of risk
  - Used to determine controls (technical, perhaps procedural)
  - Can be used to describe strength of controls
  - For distributed development
    - ❖ Can be applied in an out-of-context situation
  - Inputs to TAF determination
    - ❖ Attack feasibility and corresponding attack path
    - ❖ Further supporting info
      - ➢ Architectural design information; CS requirements; stakeholder defined parameters

TAF open items

- TAF concept may be renamed e.g. “Required Attack Feasibility (“RAF”), Necessary Attack Feasibility (“NAF”)
- Improvement in examples of TAF usage

ISO/SAE PWI 8475 CAL/TAF timeline

Resolution of Committee Draft (CD) comments

October 2024

CD2 commenting period ends

February 2025

DPAS[1] available start of ballot

July 2025

PAS Publication

October 2025

CD2 released for comment

December 2024

Resolution of CD2 comment resolution complete

May 2025

End DPAS ballot

September 2025

Expect a Q4 release in 2025

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

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***
- ***Publish as a Technical Report (TR)***

Powering Business Worldwide

24

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
  - Discussion of pros/cons of various types of testing
  - Application to off-the-shelf, reused & out-of-context components

ISO/SAE PWI 8477 V&V TR timeline

Release of Working Draft (WD) #2

December 2024

Commenting period starts

January 2025

End of commenting period WD#2

February 2025

Comment resolution completed

May 2025

Start preparation of DTR[1]

June 2025

JWG

DTR[1] for internal JWG review

July 2025

JWG

TR Publication

~October 2025

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 projects (CAL/TAF, V&V)

ISO/SAE 21434 v2 timeline

Comments submitted

August 2024

Comment resolution proposals-initial draft

April 2025

JWG decision on scope

November 2025

Comments categorized

January 2025

Updated draft of comment resolution proposals

September 2025

Development starts

2026

Expect start of development 2026 (3+ years)

Questions?

Thank you!

John Krzeszewski, MSEE, GSEC
Senior Specialist, Functional Safety and Cybersecurity

jtk@eaton.com

Powering Business Worldwide

Eaton.com/WhatMatters