April 3, 2019

John T. Krzeszewski
Chief Engineer, Cybersecurity
Chair, “PG1: Risk Management” in ISO/SAE 21434

ISO/SAE 21434 AUTOMOTIVE CYBERSECURITY STANDARD

APTIV

AGENDA

- Overview of Aptiv and cybersecurity
- ISO/SAE 21434 “Road vehicles: Cybersecurity Engineering”
  - Why the standard is needed and general background
  - Key principles
  - Scope
  - ISO and SAE delegations involved in the development
  - Overview of the document structure
  - Timeline
  - Cybersecurity Assurance Level

We are a global technology company that develops secure, safer, greener, and more connected solutions, which enable the future of mobility.

APTIV

Aptiv Addressing Mobility's Toughest Challenges

Aptiv Provides End-to-end Solutions that Allow us to Commercialize New Mobility

SMART VEHICLE ARCHITECTURE

- SOFTWARE
- SENSING AND COMPUTING
- SIGNAL AND POWER DISTRIBUTION
- CONNECTIVITY

APTIV

SMART MOBILITY SOLUTIONS


ACTIVE SAFETY


USER EXPERIENCE

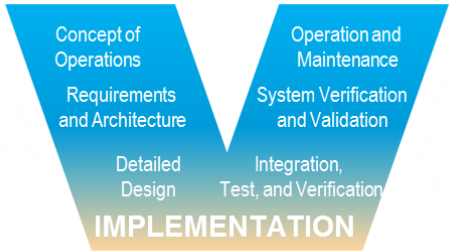

CONNECTED SERVICES


AUTONOMOUS SYSTEMS

Experience with Cybersecurity
Guidelines and Techniques

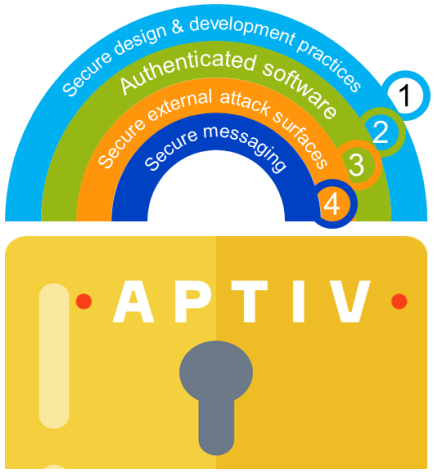
Security must be part of the entire product life-cycle

- Cybersecurity is a product architecture, a design, and a system qualification
- Cybersecurity follows the development v-cycle



We have a multi-layered guideline to protect products

- Proper protection is based on TARA (Threat Analysis / Risk Analysis) results



Aptiv's 4-levels of system security

Level 1 – Guidelines and best practices – TARA, reviews, code analysis

Level 2 – Authenticated software – secure boot, secure updates

Level 3 – Secure external attack surfaces – firewall, communication restrictions

Level 4 – Secure internal messaging – encrypt data, protect diagnostics

Experience with Cybersecurity

Established Cybersecurity Facility - CyberSEAL Lab

Operational World Class Cybersecurity Testing Facility

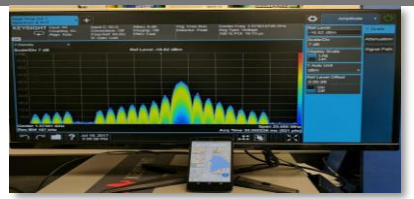
Lab Responsibilities

- Threat modeling (TARA)
- Vulnerability assessments
- Penetration assessments
- Development of advanced security tools
- Training & awareness in the art of exploitation (hands-on)
- Advanced cybersecurity R&D
  - Blockchain work group
- POC evaluations

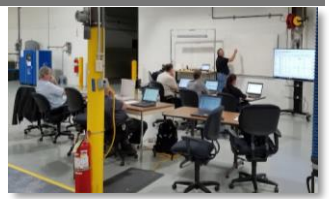
Lab Achievements

- Highly qualified security experts in place
- Completed penetration assessments
- Established lab test processes

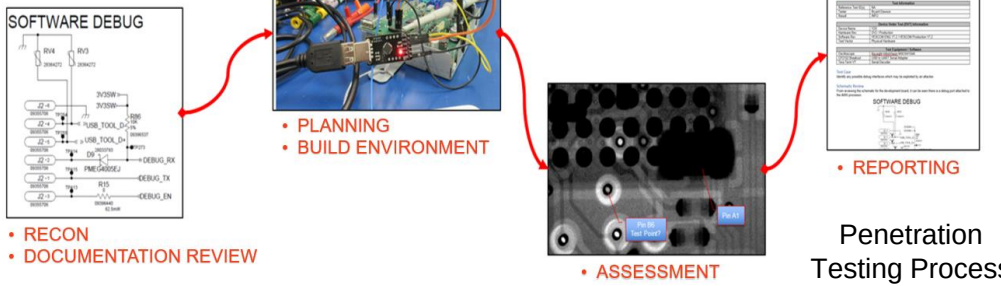
Test Benches



Advanced Tools (Aptiv GPS spoofing tool)



Training



Penetration Testing Process

Multiple Partnerships with Leading Cybersecurity Companies

APTIV

Why is Standard needed for Automotive Cybersecurity?

- Existing cybersecurity standards do not address unique automotive challenges
  - Safety
  - Long lifecycle
  - Use of embedded controllers
  - etc.

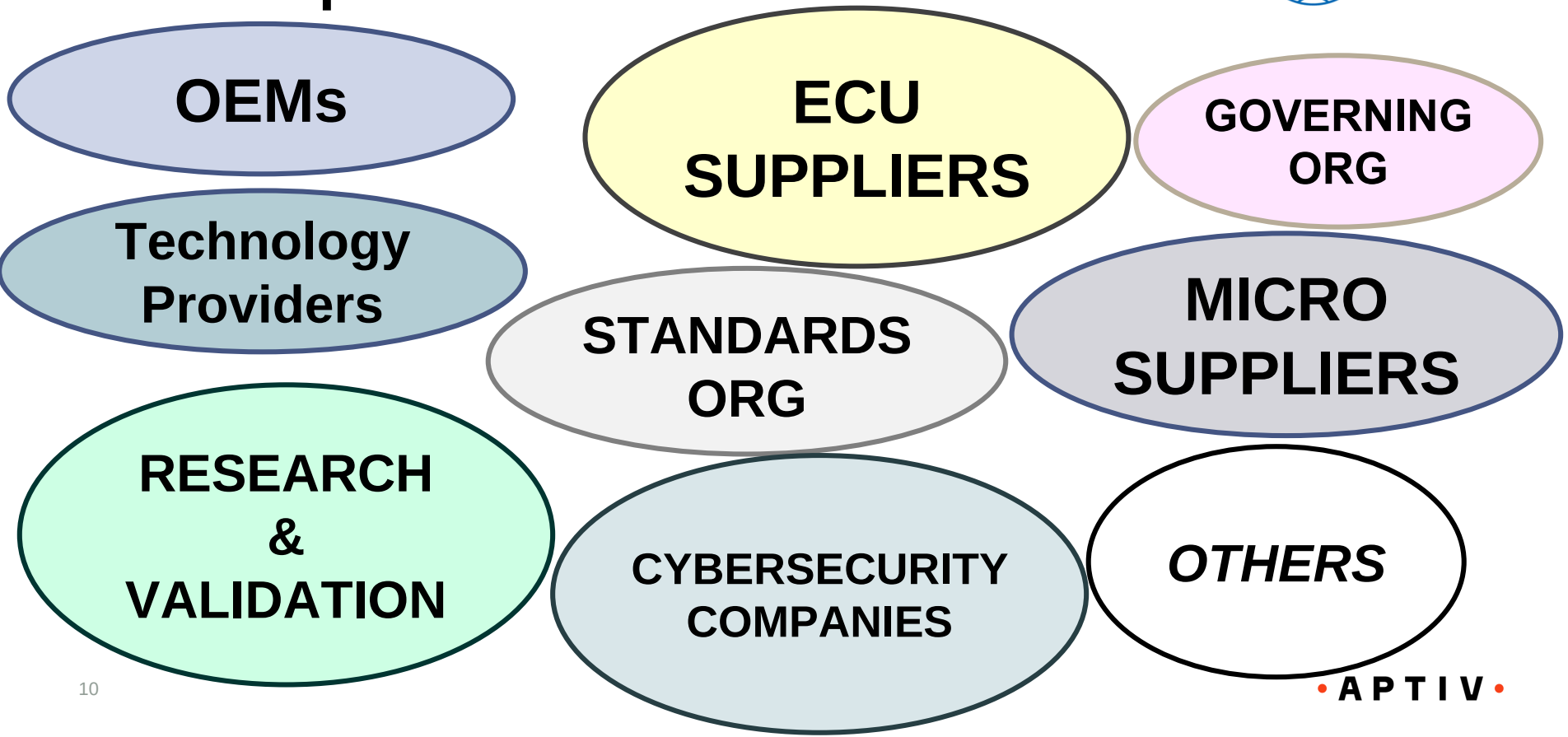
Benefit of Standard for Automotive Cybersecurity

- Define common terminology for use throughout supply chain
- Drive industry consensus on key cybersecurity issues
- Set minimum criteria for vehicle cybersecurity engineering
- Reference for regulators, etc. to minimize contradictions
- Provide evidence that industry is taking cybersecurity seriously

ISO/SAE 21434 – How Did This Begin?

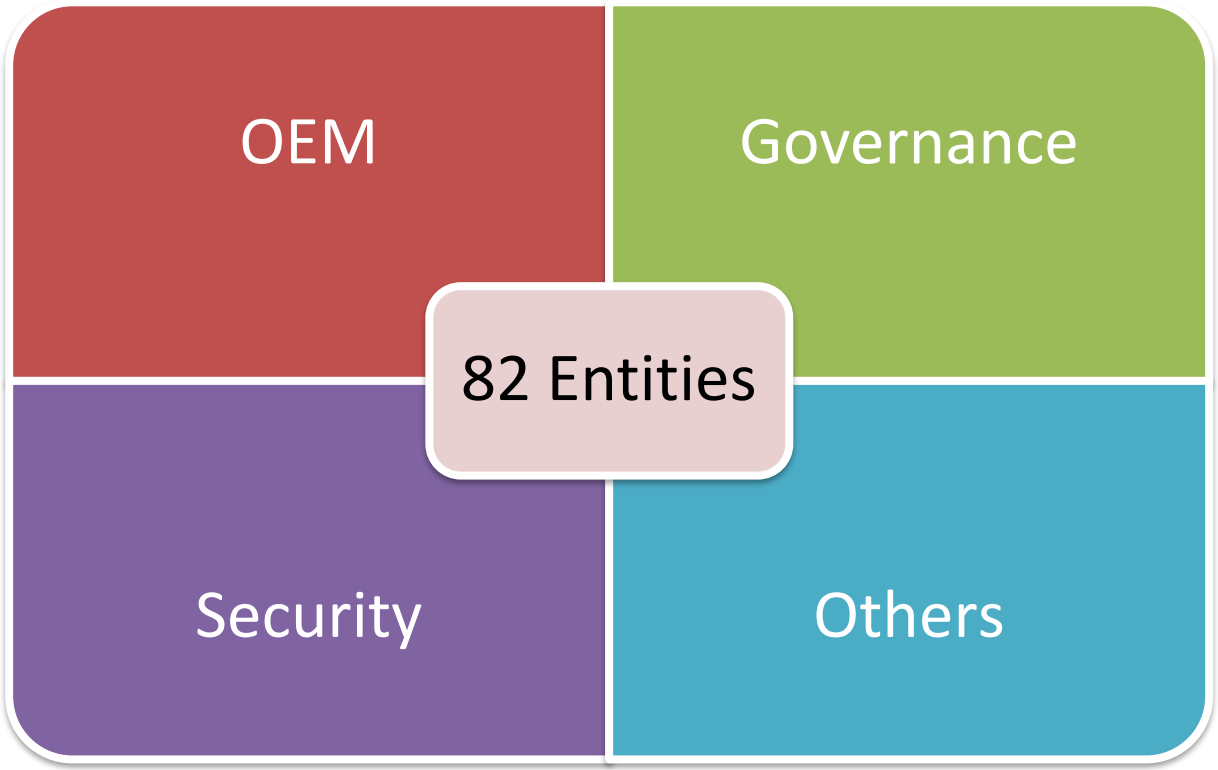
- SAE issued Best Practice document
  - J3061 “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”
  - Issued 2016-01-14
- ISO New Item Work Proposal 3556 “Automotive Security Engineering”
- Nov. 2016: Partnership Standards Development Organization (PSDO)
- Cooperation agreement between ISO and SAE in two areas:
  - Road Vehicles
  - Intelligent Transportation Systems
- SAE & ISO to work together to develop cybersecurity standard
- ISO/SAE 21434 = first standard to be created under new agreement
  - Will be jointly released by both SAE and ISO

ISO SAE 21434 Participation - 82 companies



APTIV

ISO SAE 21434 Participation



APTIV

ISO/SAE 21434 – Key Principles (1 of 2)

1. Applicable to **road-vehicles**
2. Goal of **reasonably secure** vehicles and systems
3. Automakers and suppliers can use to show “**due diligence**”
4. Focus on **automotive cybersecurity engineering**
5. Based on **current state-of-the-art** for cybersecurity engineering

ISO/SAE 21434 – Key Principles (2 of 2)

6. **Risk-oriented** approach
   - Risk is used for prioritization of action
   - Analyses of risk factors for methodical elicitation of cybersecurity requirements
   - Common language for communicating/managing cyber risk among stakeholders

7. **Management activities for cybersecurity**

8. Cybersecurity activities/processes for **all phases of vehicle lifecycle**:
   - Design and Engineering, Production, Operation by Customer
   - Maintenance and Service, Decommissioning

ISO/SAE 21434
What will it be applicable to?

- Applicable to:
  - Road vehicle,
  - its systems,
  - its components,
  - its software,
  - its connection from vehicle to any external device/network.

ISO/SAE 21434 – What is Out of Scope?

- ISO/SAE 21434 will:
  - **NOT** prescribe specific cybersecurity technology or solutions
  - **NOT** include requirements on specific remediation methods
  - **NOT** include requirements for telecommunications system
  - **NOT** specify requirements for connected back-office
  - **NOT** specify requirements for electric vehicle chargers
  - **NOT** specify unique requirements for autonomous vehicles

ISO/SAE 21434 -- Purpose

The purpose is to:

- Define a structured process to ensure cybersecurity is designed in upfront
  - Following a structured process helps reduce the potential for a successful attack, thus reducing the likelihood of losses
  - A structured process also provides a clear means to react to a continually changing threat landscape
- Maintain consistency across global industry
- Be complete and promote conscious decision making

ISO/SAE 21434 – Joint Working Group (JWG)

- Equal number of votes for SAE experts and ISO delegations:
  - 1 vote per ISO Delegation
  - 1 vote per SAE expert (limited to equivalent number of national delegations)
- Co-chaired by SAE & ISO
- Votes on key issues relative to 21434
- Coordinate work of Project Groups (PGs)

Delegations

- ISO
  - Austria
  - Belgium
  - China
  - France
  - Germany
  - Israel
  - Italy
  - Japan
  - Korea
  - Netherlands
  - Sweden
  - Switzerland
  - United Kingdom

- SAE Experts (13 votes)
  - Angela Barber
  - Lisa Boran
  - Jonathon Brookfield
  - Chris Clark
  - Gary English
  - Di Jin
  - John Krzeszewski
  - Susan Lightman
  - Bill Mazarra
  - Brian Murray
  - Dan Selke
  - Anuja Sonalker
  - Alan Tatourian
  - Giri Venkat
  - David Ward
  - André Weimerskirch

ISO/SAE 21434 – Project Groups (PGs)

- PG1: Risk Assessment Methods — 54 participants
- PG2: Product Development — 42 participants
- PG3: Production, Operations & Maintenance — 29 participants
- PG4: Process Overview and Interdependencies — 37 participants
- Drafting Team (ISO co-chair; SAE co-chair)
- Terms & Definitions Team (member from each PG)
- Use Case Team (members from each PG)

ISO/SAE 21434 – Committee Draft Outline
(1 of 4)

1.0 Scope
2.0 Normative References
3.0 Terms and Abbreviations
4.0 General Considerations
5.0 Management of Cybersecurity
6.0 Risk Assessment Methods & Trea
7.0 Concept Phase
8.0 Product Development
9.0 Production, Operations and Maintenance
10.0 Supporting Processes
Annexes

Mandatory elements of every ISO standard.

- What the standard does & its applicability
- External sources of mandatory contents

ISO/SAE 21434 – Committee Draft Outline
(2 of 4)

1.0 Scope
2.0 Normative References
3.0 Terms and Abbreviations
4.0 General Considerations
5.0 Management of Cybersecurity
6.0 Risk Assessment Methods & Treatment
7.0 Concept Phase
8.0 Product Development
9.0 Production, Operations and M
10.0 Supporting Processes
Annexes

Informative text – no requirements.
- Provides context
- Describes structure of the standard
- Explains interrelationships of clauses

Cybersecurity-specific or cybersecurity focused management activities:
- At corporate level
- For different phases of engineering lifecycle
- Over product lifetime

ISO/SAE 21434 – Committee Draft Outline
(3 of 4)

1.0 Scope
2.0 Normative References
3.0 Terms and Abbreviations
4.0 General Considerations
5.0 Management of Cybersecurity
6.0 Risk Assessment Methods & Treatment
7.0 Concept Phase
8.0 Product Development
9.0 Production, Operations and Maintenance
10.0 Supporting Processes
Annexes

Methodolgy for analysis, assessment and management of cybersecurity risk.

Processes and activities relative to cybersecurity engineering during concept phase.

ISO/SAE 21434 – Committee Draft Outline
(4 of 4)

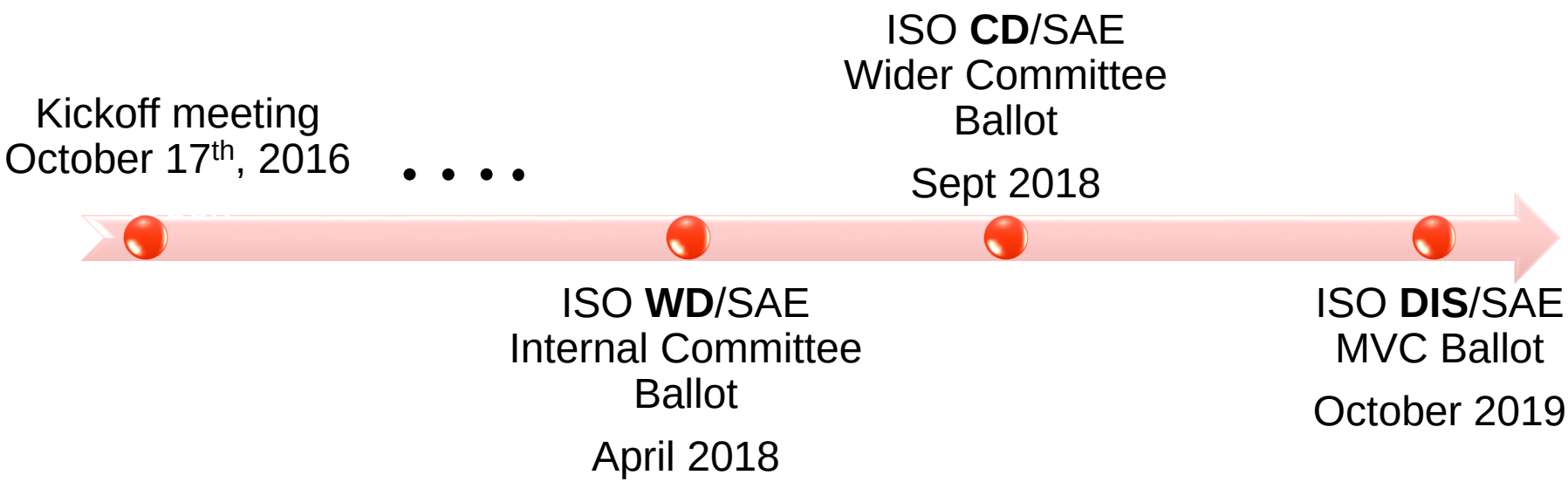
1.0 Scope
2.0 Normative References
3.0 Terms and Abbreviations
4.0 General Considerations
5.0 Management of Cybersecurity
6.0 Risk Assessment Methods & Treatment
7.0 Concept Phase
8.0 Product Development
9.0 Production, Operations and Maintenance
10.0 Supporting Processes
Annexes

Product Development phase processes and activities (not cybersecurity focused) that add to or support cybersecurity engineering.

Processes and activities relative to cybersecurity engineering in post-development phase.

General processes and activities (not cybersecurity focused) that add to or support cybersecurity engineering.

ISO/SAE 21434 – High-level Timeline



Expect a 2020 release
(Late in year, if DIS does not pass ballot)

APTIV

ISO/SAE 21434
Overview of Stages WD, CD, DIS

- **Working Draft (WD)**
  - Developed/reviewed by JWG participants
  - Informal comment resolution
- **Committee Draft (CD)**
  - Request for comments sent to ISO Technical Committee & SAE Committee
  - 8 weeks review period/ballot; approval by consensus
  - Formal comment resolution process
- **Draft International Standard (DIS)**
  - Request for comments sent to all ISO National Bodies and to SAE Committee
  - 12 weeks review period/ballot; 2/3 majority for approval
  - Formal comment resolution process (no technical comments for passage)
  - Publicly for sale

ISO/SAE 21434 – Committee Draft (CD)

- All CD comments received (3,534) must be formally addressed
  - Plan is to address majority of those by May for an internal draft
    - Internal draft review amongst 21434 delegates, resulting in DIS

- All normative clauses to be indicated by terms “shall” or “shall not”
  - Requirements to be strictly followed in order to meet ISO/SAE 21434
  - No deviation is permitted from these requirements

- Rationale will be provided for each normative clause
  - A short explanation of the purpose of a requirement, or group of requirements

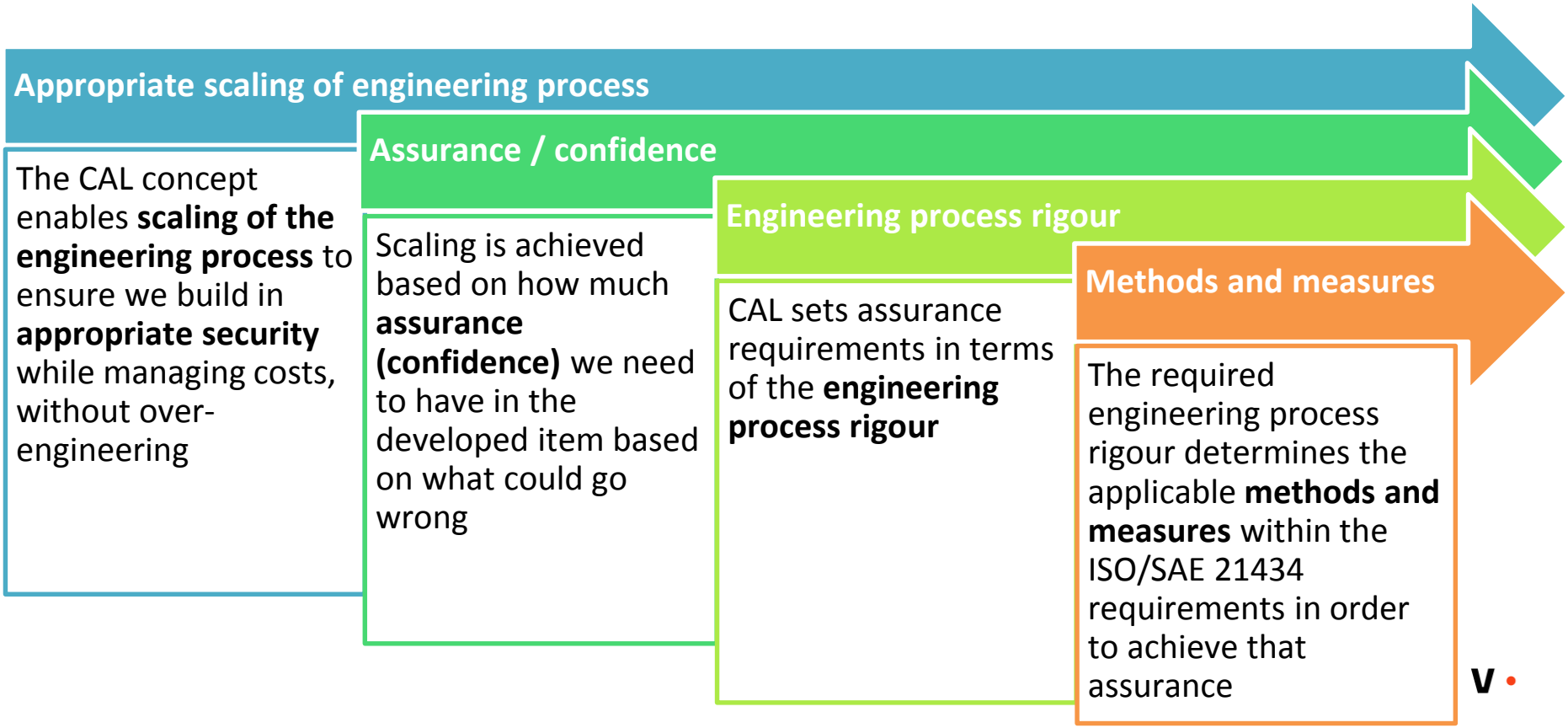
ISO/SAE 21434 – Committee Draft (CD)

- JWG has voted to have Cybersecurity Assurance Level (CAL) in 21434
- Decision made to including CAL:
  - CAL level would indicate the required level of cybersecurity process rigor
  - Methodology for determining CAL is defined in ISO/SAE 21434
  - CAL is **informational**
- CD has recently been released for comment

CAL Purpose and Benefits
- What problem does CAL solve?

- ISO/SAE 21434 is a single standard which is to be applied to many types of items, which contain assets with different levels of criticality
- Applying all requirements of ISO/SAE 21434 in all cases is neither appropriate nor feasible
- An appropriate means of scaling the effort and costs of implementing the cybersecurity engineering process requirements is required
- The automotive distributed development process requires a common means of communicating these process requirements through the supply chain, and also within an organization

CAL Purpose and Benefits - How CAL helps



1. CAL Purpose and Benefits
- Assurance – some definitions

- **grounds for confidence that a TOE meets the SFRs**
  - ISO/IEC 15408-1:2009
  - Information technology — Security techniques — Evaluation criteria for IT security

- **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

- **grounds for confidence that a deliverable meets its security objectives**
  - ISO/IEC 21827:2008
  - Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

- Assurance in this context means **confidence**, it does **not** imply **guarantee**

CAL Purpose and Benefits
- “Heritage” of CAL

- Assurance levels are **not** a new invention for ISO/SAE 21434
- Variants of integrity or assurance levels can be found in other established standards:
  - **Functional safety**
    - IEC 61508 – Safety Integrity Level (SIL)
    - ISO 26262 – Automotive Safety Integrity Level (ASIL)
    - DO-178 – Design Assurance Level (DAL)
  - **Security**
    - ISO/IEC 15408 – Evaluation Assurance Level (EAL)
    - IEC 62443 – Security Level (SL)

The different risk models adopted by these standards mean that their uses of levels are not directly comparable

- None of these is suitable to use **directly** in ISO/SAE 21434
- However the CAL takes **inspiration** from several of these

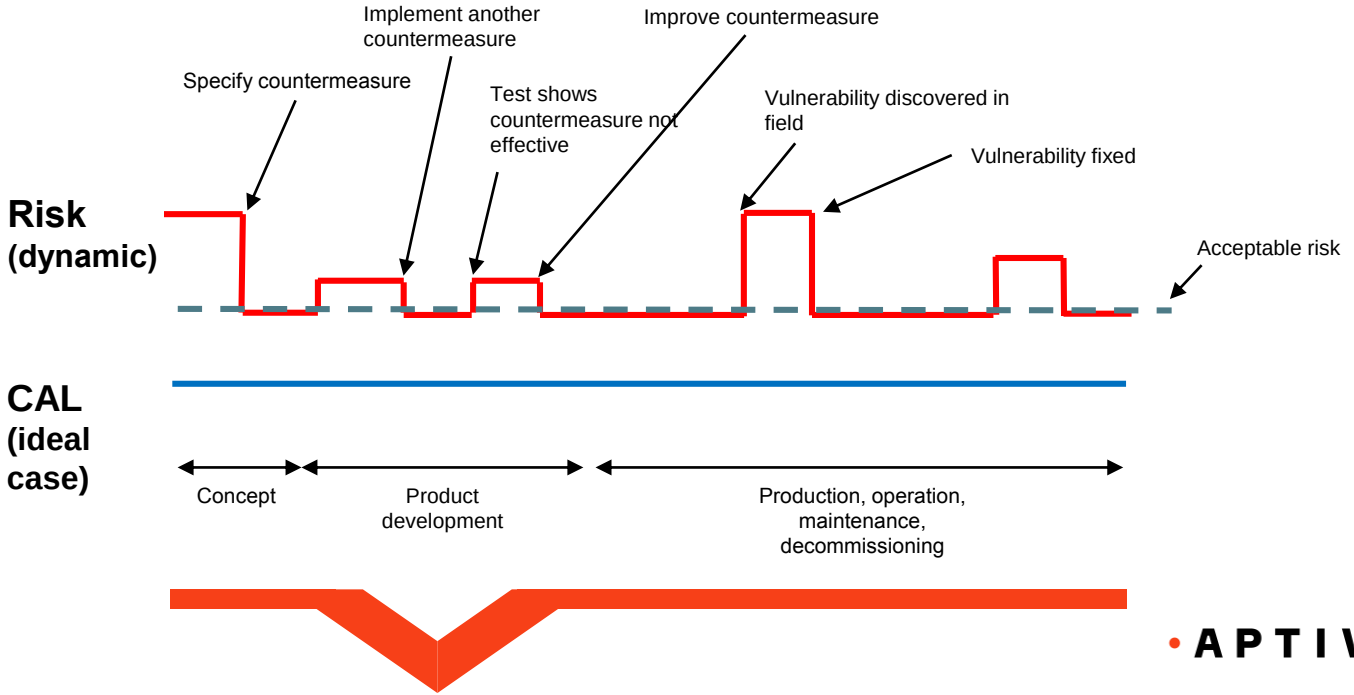
APTIV

How CAL relates to other concepts

- **CAL** and **Risk** have a connection, but are **not the same**
- Need to decouple CAL and dynamic Risk factors (so CAL remains as stable as possible)

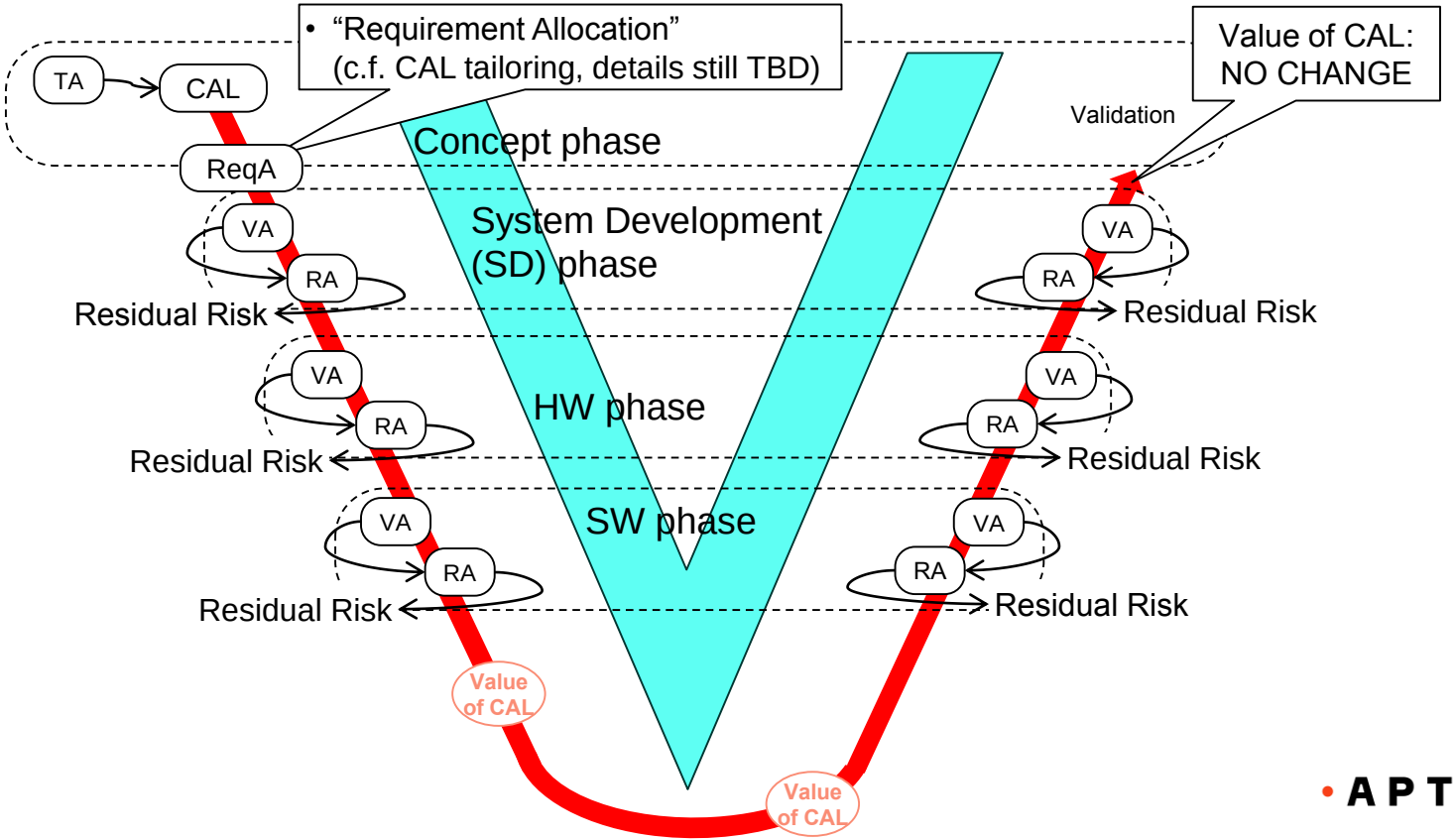
What is my current residual risk given the current spec / design / implementation?

What level of assurance do I need given the criticality of the assets I need to protect?



APTIV

How CAL relates to other concepts



Thank you

Questions?

John T. Krzeszewski
Chief Engineer, Cybersecurity Architecture
Aptiv
john.t.krzeszewski@aptiv.com

aptiv.com

Revisions

- Updated 19MAR19