Status of Work in Process on ISO/SAE 21434 Automotive Cybersecurity Standard

Angela Barber

SAE Expert for ISO/SAE 21434; Co-author SAE J3061

Mitsubishi Motors R&D of America, Senior Advisor Product Cybersecurity

Why is Standard needed for Automotive Cybersecurity?

Existing cybersecurity standards do not address Automotive:

- Use of embedded controllers
- Long lifecycle of vehicles
- Safety implications
- etc.

Benefit of Standard for Automotive Cybersecurity

- Defines common terminology for use throughout supply chain.
- Drives industry consensus on key cybersecurity issues.
- Sets minimum criteria for vehicle cybersecurity engineering.
- Can be referenced by regulators, etc.
- Provides 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 January 14, 2016.

Early 2016: ISO NIWP 3556
“Automotive Security Engineering”

- Sept. 2016: Partnership Standards Development Organization (PSDO) defines 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

OEMs
Ford, GM, Volvo, Mitsubishi, FCA, Honda, Toyota, Volkswagen, BMW, Jaguar-Land Rover, Opel, Peugeot, Renault, Daimler, Nissan, Iveco, etc.

ECU SUPPLIERS
Continental, Valeo, Bosch, Lear, Delphi, ZF, Magna, Denso, Hella, Wabco, Actia, etc.

GOVERNING ORG
NIST, RDW, etc.

STANDARDS ORG
SAE, ISO, JSAE, VDA, etc.

MICRO SUPPLIERS
Infineon, Intel, Melexes, ON Semiconductor, etc.

RESEARCH/ VALIDATION
University of Warwick, Southwest Research Institute, AIT, Horiba Mira, UL, TUV, Bureau Veritas, etc.

CYBERSECURITY COMPANIES
Karamba, Vector, TowerSec, Synopsys, etc.

OTHERS
STEER, Thales, Method Park, BNA, Scania, etc.

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.
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.

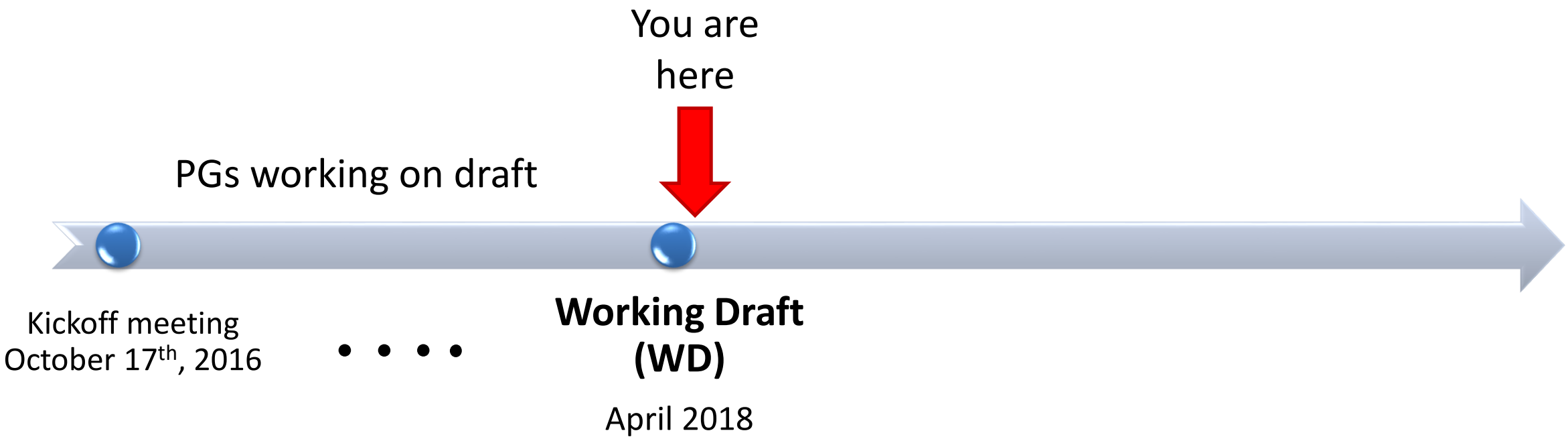
ISO/SAE 21434 – Joint Working Group (JWG)

- Equal number SAE experts and ISO delegations:
  - 1 vote per ISO Delegation (there are 12 ISO Nation Delegations)
  - 1 vote per SAE expert.
- Co-chaired by SAE & ISO.
- Votes on key issues relative to 21434.
- Oversees Project Groups (PGs).

ISO/SAE 21434 – Project Groups (PGs)

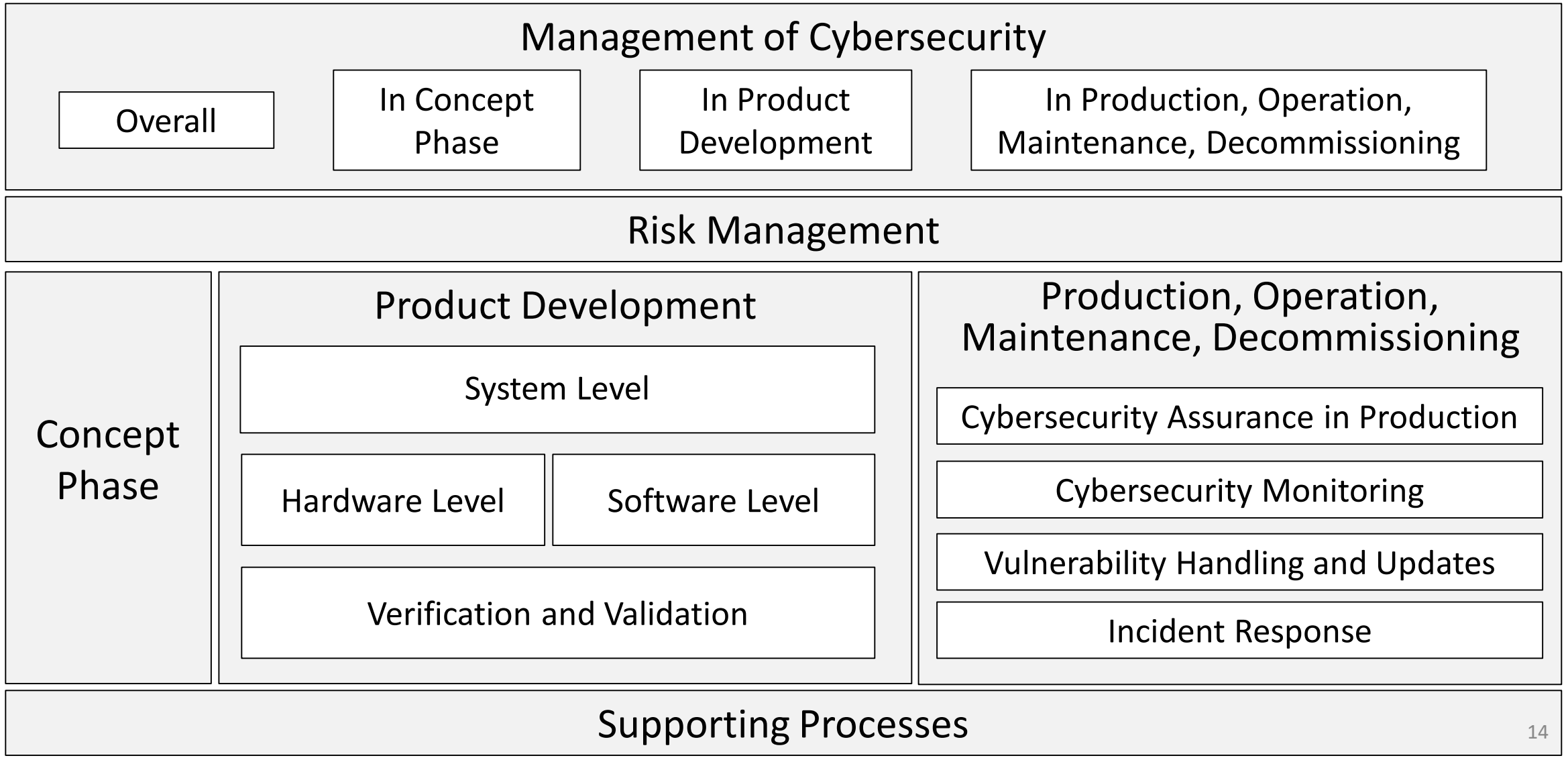
- PG1: Risk Management (SAE chair; ISO co-chair) 54 participants
- PG2: Product Development (ISO chair; SAE co-chair) 42 participants
- PG3: Production, Operations & Maintenance (SAE chair; ISO co-chair) 29 participants
- PG4: Process Overview and Interdependences (ISO chair; SAE co-chair) 37 participants
- Drafting Team (ISO co-chair; SAE co-chair)
- Terms & Definitions team (member from each PG)

ISO/SAE 21434 – High-level Timeline



3+ year timeline planned

ISO/SAE 21434 – Overview of Structure



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

1.0 Scope
2.0 Normative References
3.0 Terms and Definitions
4.0 Introduction
5.0 Management of Cybersecurity
6.0 Risk Management
7.0 Concept Phase
8.0 Product Development
9.0 Production, Operations and Maintenance
10.0 Supporting Processes
Annexes

Mandatory elements of every ISO/SAE standard.

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

ISO/SAE 21434 -- Working Draft Outline (2 of 4)

1.0 Scope
2.0 Normative References
3.0 Terms and Definitions
4.0 Introduction
5.0 Management of Cybersecurity
6.0 Risk Management
7.0 Concept Phase
8.0 Product Development
9.0 Production, Operations and Ma
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 -- Working Draft Outline (3 of 4)

1.0 Scope
2.0 Normative References
3.0 Terms and Definitions
4.0 Introduction
5.0 Management of Cybersecurity
6.0 Risk Management
7.0 Concept Phase
8.0 Product Development
9.0 Production, Operations and Maintenan
10.0 Supporting Processes
Annexes

Methodology for analysis, assessment and management of cybersecurity risk.

Processes and activities relative to cybersecurity engineering during concept phase.

ISO/SAE 21434 -- Working Draft Outline (4 of 4)

1.0 Scope
2.0 Normative References
3.0 Terms and Definitions
4.0 Introduction
5.0 Management of Cybersecurity
6.0 Risk Management
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 to cybersecurity engineering in post-development phase.

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

ISO SAE 21434 -- Working Draft (WD)

- **April 10, 2018**: WD released for comments to ISO & SAE participants.

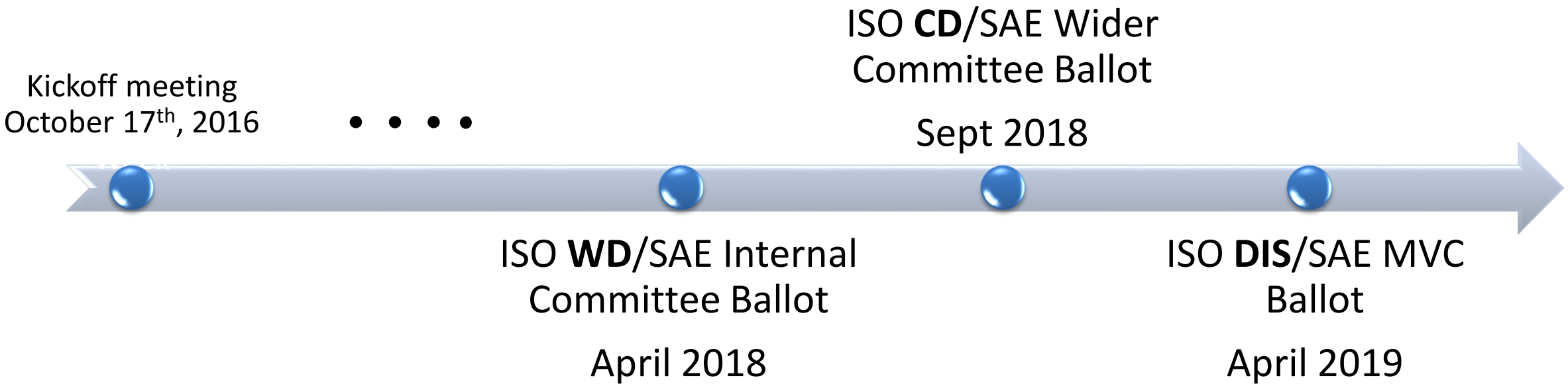
  "Note to readers:" have been added. Indicate parts of the text that are still being developed. Example:

  > NOTE TO READER: This clause is still being reworked and is not yet in its final state.
  > Topics which will be expanded are …

- **May 30, 2018:** deadline for comments on WD version.

- **Informal comment resolution**: Experts will focus on development.

ISO/SAE 21434 – High-level Timeline



Expect a late 2019 or 2020 release

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

- **Working Draft (WD)**
  - Developed/reviewed by JWG and PG 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
  - Publicly for sale

ISO/SAE 21434 – Steps to Committee Draft (CD)

- WD version will incorporate updates from PGs until CD stage.

- 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.

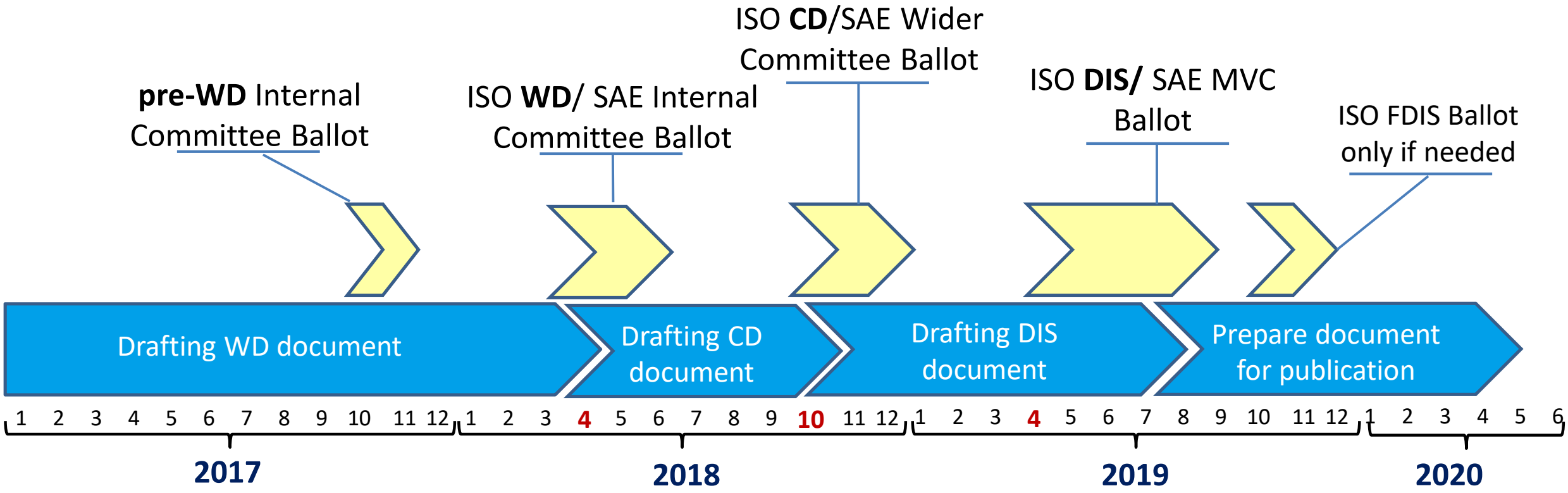
ISO/SAE 21434 – Steps to CD (continued)

- Decision to be made on including CAL:
  - CAL = Cybersecurity Assurance Level.
  - Methodology for determining CAL would be defined in ISO/SAE 21434.
  - CAL level would indicate the required level of cybersecurity process rigour.
  - Joint Working Group will vote on CAL in meeting in June 2018.

- CD version release for comment ~ Sept. 24, 2018.

ISO/SAE 21434 – Detailed Timeline

Per the PSDO and ISO's Fast Track procedure, only required ballot stage is DIS.



Balloting Process for ISO/SAE 21434 is much more rigorous than required by PSDO.

ISO/SAE 21434 – Questions??

ISO/TC 22/SC 32/WG 11/PG 1 **N**
122

ISO/TC 22/SC 32/WG 11/PG 1
Risk Management
E-mail of Secretary: kraehnert@vda.de
Secretariat: DIN

ISO SAE WD 21434 vers001 for commenting

Date of document 2018-04-10

Expected action Comment
Due Date 2018-05-30

Background

Dear All,
with this notification you will receive the WD draft for commenting.
As agreed during our last meeting, you can submit your comments (please use the comment sheet) to kraehnert@vda.de by due date mentioned above or you can also submit comments or further content directly to the project leader.
The document will be updated continuously. The explanation of the further procedure will published soon.
If you will have any questions please do not hesitate to contact me (kraehnert@vda.de).
Best regards,
Stephan Kraehnert

What questions does the audience have?