EASA
European Union Aviation Safety Agency

FAA
Aviation Safety

Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

Welcome to this webinar!

Eric DUVIVIER

This is all about ABSTRACTION LAYER

"A complete set of criteria used to assess development standards or methodologies for their use in complying with the applicable aircraft systems and equipment safety regulations"

Webinar OBJECTIVES

1. Present the work of the Task Force
2. Collect inputs from stakeholders from organizations that did not directly participate in the Task Force
   - Inputs provided during the webinar and
   - On published material after the webinar
     (eric.duvivier@easa.europa.eu)

The agenda

#	TIME	TITLE, SPEAKER
1	15:00-15:05	**Welcome to the webinar** Eric Duvivier [EASA]
2	15:05-15:15 15:15-15:20	**Presentation of the Task Force** **Q&A** Eric Duvivier [EASA] & George Romanski [FAA]
3	15:20-15:50 15:50-16:10	**Presentation of the AL** **Q&A** Anne Senechal [EASA], Mike Vukas [FAA] Maurizio Patriarca [Leonardo], Clay Barber [Garmin]
4	16:10-16:20 16:20-16:30	**The User Guide** **Q&A** Chris Hubbs [Collins], Bernie Newman [Astronautics]
5	16:30-16:55 16:55-17:05	**How to consider the AL within the current regulatory framework of EASA & FAA and** **Framework for recognition of alternate standards assessed using the AL** **Q&A** Anne Senechal [EASA], Mike Vukas [FAA], Brenda Ocker [FAA]
6	17:05-17:15 17:15-17:20	**Usage of the AL in the Feasibility Study** **Q&A** Chris Hubbs [Collins], Karen Brack [Boeing]
7	17:25-17:30	**Concluding remarks** Eric Duvivier [EASA] & George Romanski [FAA]

Questions & Answers

→ For sending questions and comments, please use the slido app, which is also accessible through WebEx:

- www.slido.com
- event code: 2106363
- Pass code: qi5vcz

Outcome

→ Webinar & Presentations will be recorded and made available at the EASA website after the event

Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

1 Welcome to the webinar
Eric Duvivier [EASA]

2 Presentation of the Task Force
Eric Duvivier [EASA] & George Romanski [FAA]

3 Presentation of the AL
Anne Senechal [EASA], Mike Vukas [FAA]
Maurizio Patriarca [Leonardo], Clay Barber [Garmin]

4 The User Guide
Chris Hubbs [Collins], Bernie Newman [Astronautics]

5 How to consider the AL within the current regulatory framework of EASA & FAA AND Framework for recognition of alternate standards assessed using the AL
Anne Senechal [EASA], Mike Vukas [FAA], Brenda Ocker [FAA]

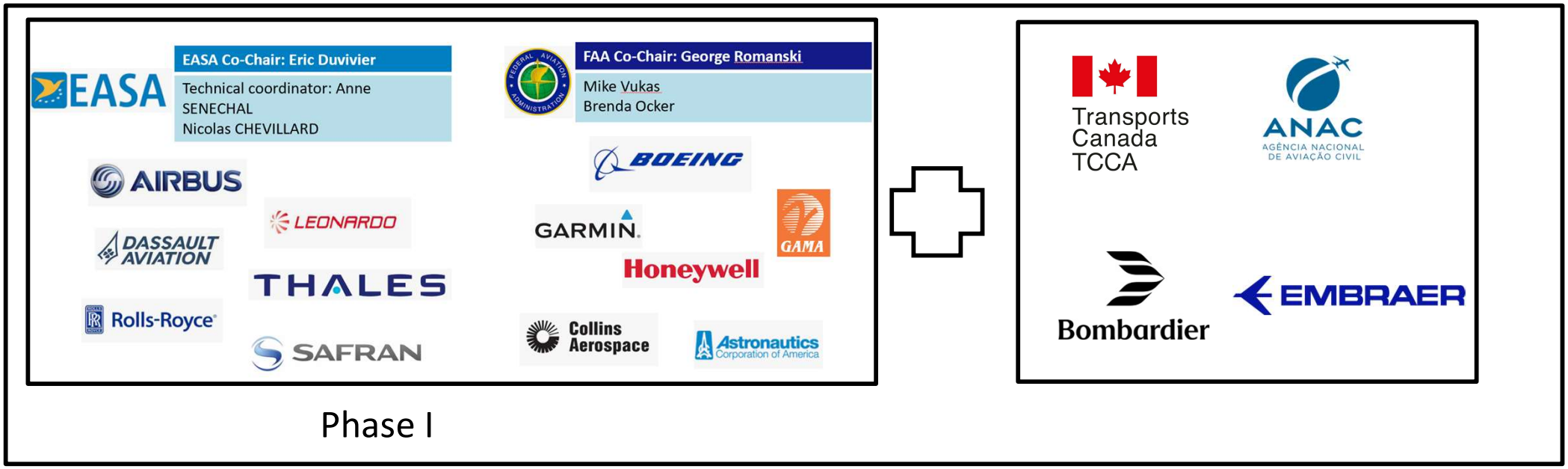
6 Usage of the AL in the Feasibility Study
Chris Hubbs [Collins], Karen Brack [Boeing]

7 Concluding remarks
Eric Duvivier [EASA] & George Romanski [FAA]

Background Information

- ToR: signed by the EASA and FAA Senior Management in June 2019
- The TF report to the EASA-FAA Management
- Work in 2 Phases:
  - → Phase I: June 2019-June 2021
    - Draft 1st version of an AL
    - 3 recommendations for a Phase II
  - → Phase II: June 2021-December 2023
    - Work to address the 3 recommendations
    - Team expanded: ANAC + Embraer, TCCA + Bombardier
    - Final deliverables

The Team


EASA
EASA Co-Chair: Eric Duvivier
Technical coordinator: Anne SENECHAL
Nicolas CHEVILLARD
AIRBUS
LEONARDO
DASSAULT AVIATION
THALES
Rolls-Royce
SAFRAN
FAA Co-Chair: George Romanski
Mike Vukas
Brenda Ocker
BOEING
GARMIN
GAMA
Honeywell
Collins Aerospace
Astronautics Corporation of America
Transports Canada TCCA
ANAC
AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL
Bombardier
EMBRAER
Phase I
Phase II

Phase I / Develop High Level criteria…

- Cover development assurance for Software and Airborne Electronic Hardware **simultaneously**
- Extract & abstract the fundamentals from ED-12/DO-178 & ED-80/DO-254 activities
- Find the right level of abstraction to accept alternate methods for development assurance processes
- Be assertive to detect process gaps , potential process escapes / insufficiency for safety

Phase I / Identify standards or methodologies that could be evaluated

- → The TF identified multiple existing industry standards that could be subject to evaluation against the Abstraction Layer criteria.
- → The following standards were selected, in priority order, as being the most practical and likely to be used in aerospace applications:
    1. ISO 26262 – Road Vehicles – Functional Safety (Automotive),
    2. ASTM F3201-16 – Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS),
    3. EN 50128 – Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems.

- → *Note: the above list is not meant to preclude other standards and methodologies that may be identified by industry or the authorities as good alternative candidates for evaluation.*

Phase II: address recommendations (3)

- **Recommendation #1**: Allow trial use of Abstraction Layer criteria on the automotive standard ISO 26262
- **Recommendation #2:** Publish the Abstraction Layer and define the usage context of the Abstraction Layer
- **Recommendation #3:** Framework for recognition of alternate standards assessed using the Abstraction Layer, for use into Avionics certification projects

Deliverables

→ 3 reports produced, 1 and 2 have been published

1. "Criteria for accepting alternative standards to ED-12C/DO-178C and ED-80/DO-254"
2. "How to consider the Abstraction Layer within the current regulatory framework of EASA and FAA" & "Framework for recognition of alternate standards assessed using the Abstraction Layer"
3. "Abstraction Layer Trial on ISO 26262"
   → *Not published, sole purpose is to validate the AL*

EASA
European Union Aviation Safety Agency

FAA
Aviation Safety

Questions?

Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

1 **Welcome to the webinar**
Eric Duvivier [EASA]

2 Presentation of the Task Force
Eric Duvivier [EASA] & George Romanski [FAA]

3 Presentation of the AL
Anne Senechal [EASA], Mike Vukas [FAA]
Maurizio Patriarca [Leonardo], Clay Barber [Garmin]

4 **The User Guide**
Chris Hubbs [Collins], Bernie Newman [Astronautics]

5 **How to consider the AL within the current regulatory framework of EASA & FAA AND Framework for recognition of alternate standards assessed using the AL**
Anne Senechal [EASA], Mike Vukas [FAA], Brenda Ocker [FAA]

6 **Usage of the AL in the Feasibility Study**
Chris Hubbs [Collins], Karen Brack [Boeing]

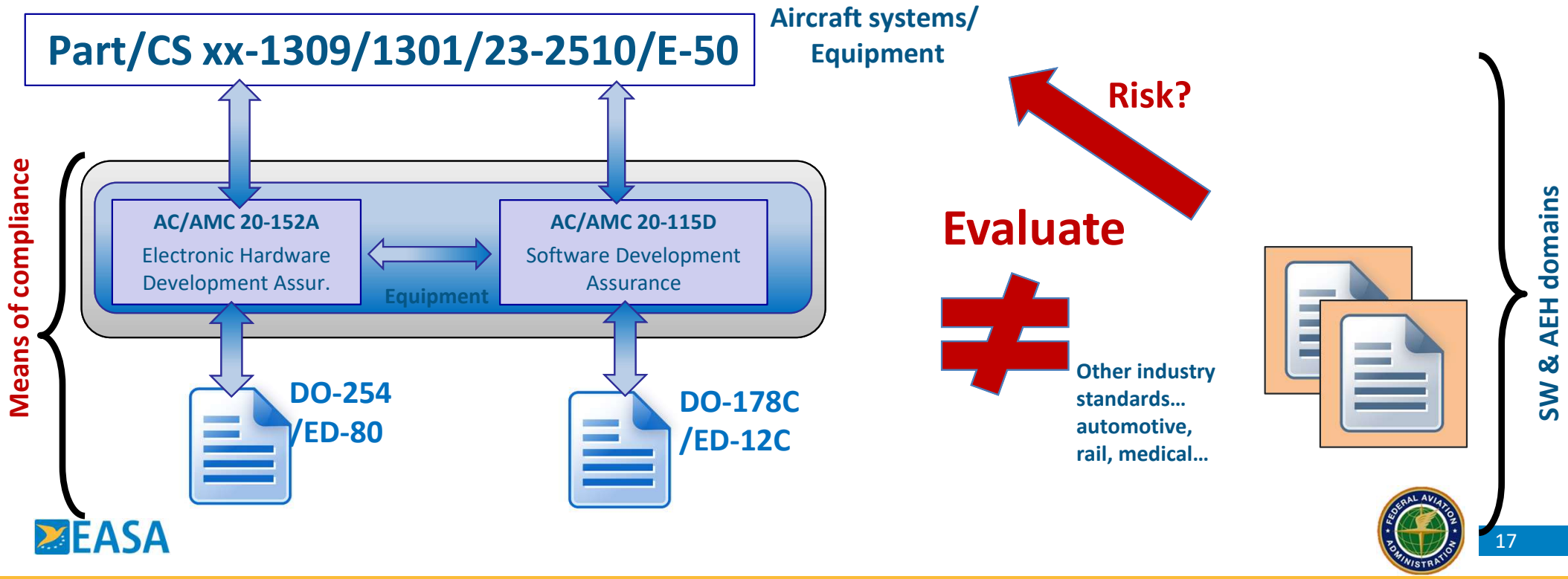
7 **Concluding remarks**
Eric Duvivier [EASA] & George Romanski [FAA]

Agenda

- Introduction & Scope
- Development of criteria for evaluating a standard or public methodology
- Present the Abstraction Layer
- Conclusion

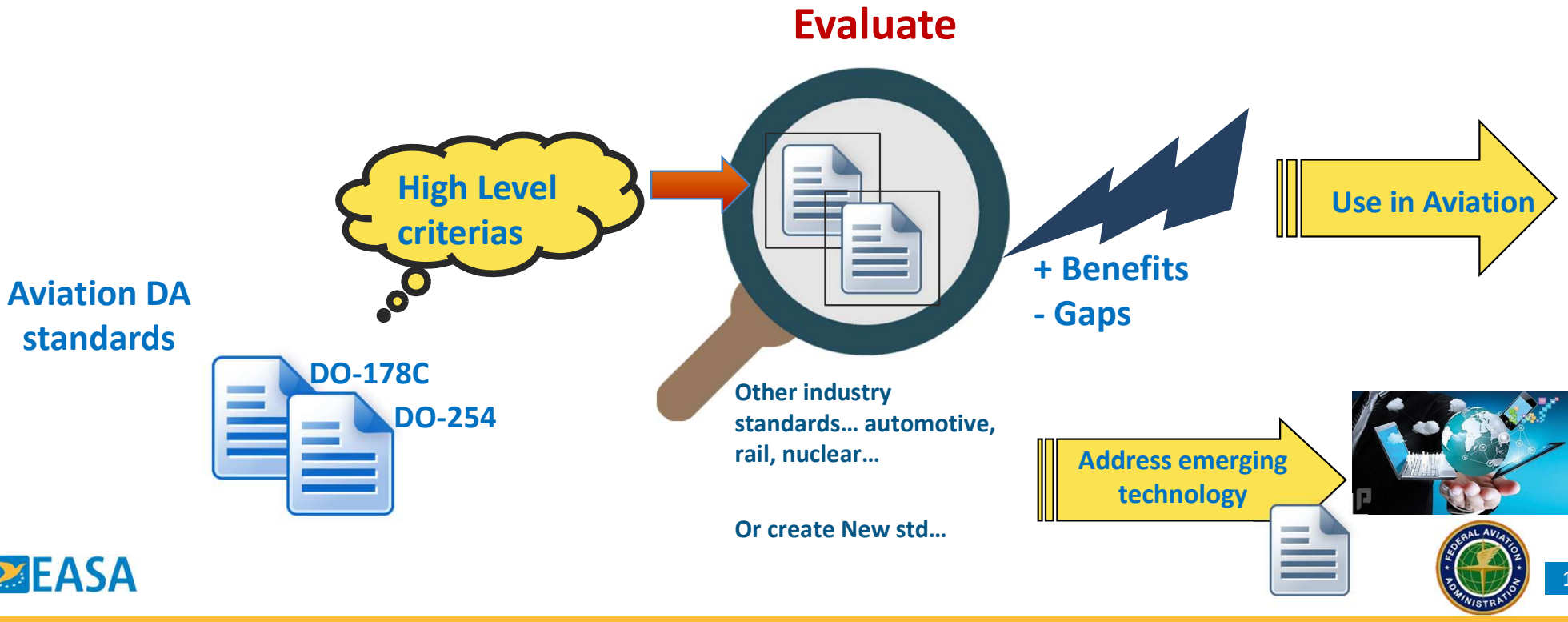
Abstraction Layer – Purpose (1/2)

- Have a mechanism to evaluate alternate standards or methodologies



Abstraction Layer – Purpose (2/2)

→ Develop means to evaluate alternative Development Assurance standards



Scope

- → Abstraction Layer is a method to assess alternate SW or HW standards or methodologies, in an objective manner and help identify any gaps.
- → AL doesn't replace industry standardization in the SW&AEH domain.
  - → Recognized industry standards will still be needed to describe in details the methods to satisfy the AL objectives in order
    - →to avoid subjective assessment on both side AA and industry
    - →to ensure level playing field
    - →To be efficient in time & resources (avoid endless discussions)

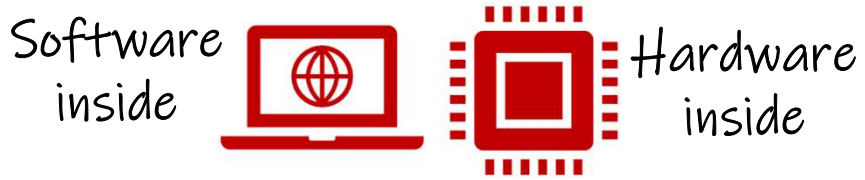
Development of the criteria for evaluating a standard or methodology

Challenges

- Extract & abstract the fundamentals & detach from ED-12/DO-178 & ED-80/DO-254 activities!
- Find the right level of abstraction to
  - Accept alternate methods for development assurance processes
  - Be assertive to detect process gaps , potential process escapes / insufficiency for safety
- Cover development assurance for Software and Airborne Electronic Hardware simultaneously

To develop criteria for evaluating a standard or methodology

→ Applied methodology:



Per DA process step

EASA

Capture key aspects of what is done

What to achieve?

↗ Criterion(s)

one goal

Why is it needed?

↗ Rationale

the intent of a criterion to facilitate its understanding

↗ Evaluation items

Key attributes of the process

Present the Abstraction Layer

SW&AEH TASK FORCE
"ABSTRACTION LAYER"

Issue 1

"Criteria for accepting alternative standards to ED-12C/DO-178C and ED-80/DO-254"

Abstraction Layer – overview (1/5)

Each criteria is documented based on the following structure

x. Criterion text

Rationale

- text

Evaluation items

1. Text…
2. Text …
   a. Text …

- Each Criterion has an identification number and a process-centric text (i.e., the process ensures/allows …)
- Rationale provides the reason why the criterion is necessary to support development assurance
- Evaluation
  - Specific attributes required for the process
  - Common text for SW and AEH as much as possible
  - All required to be met to fully satisfy a Criterion
  - Each evaluation item is specifically identified within the Criterion

Abstraction Layer – overview (2/5)

Safety level consideration

x. Criterion text

Rationale

- text

Evaluation items

1. [A/B] ……
2. [A/B/C][D(SW)] …

- 4 Safety Levels, defined in a similar manner as SAE ARP 4754A/ED-79A
  - Associated to each evaluation item
  - Same naming convention A/B/C/D as in SAE ARP 4754A/ED-79A
    - 'A' reflects the most demanding development assurance level and 'D' the lowest
  - Different Safety Levels may be allocated to SW and AEH

Abstraction Layer – overview (3/5)

Evaluation item “Check”

x. Criterion text

Rationale

- text

Evaluation items

x. [A/B/C][D(SW)] Check …

- Evaluation item “Check”
  - Requires a specific process to verify that other evaluation items are adequately performed/satisfied
  - Applicability depends on the safety levels of the evaluation items which the “check” process is confirming

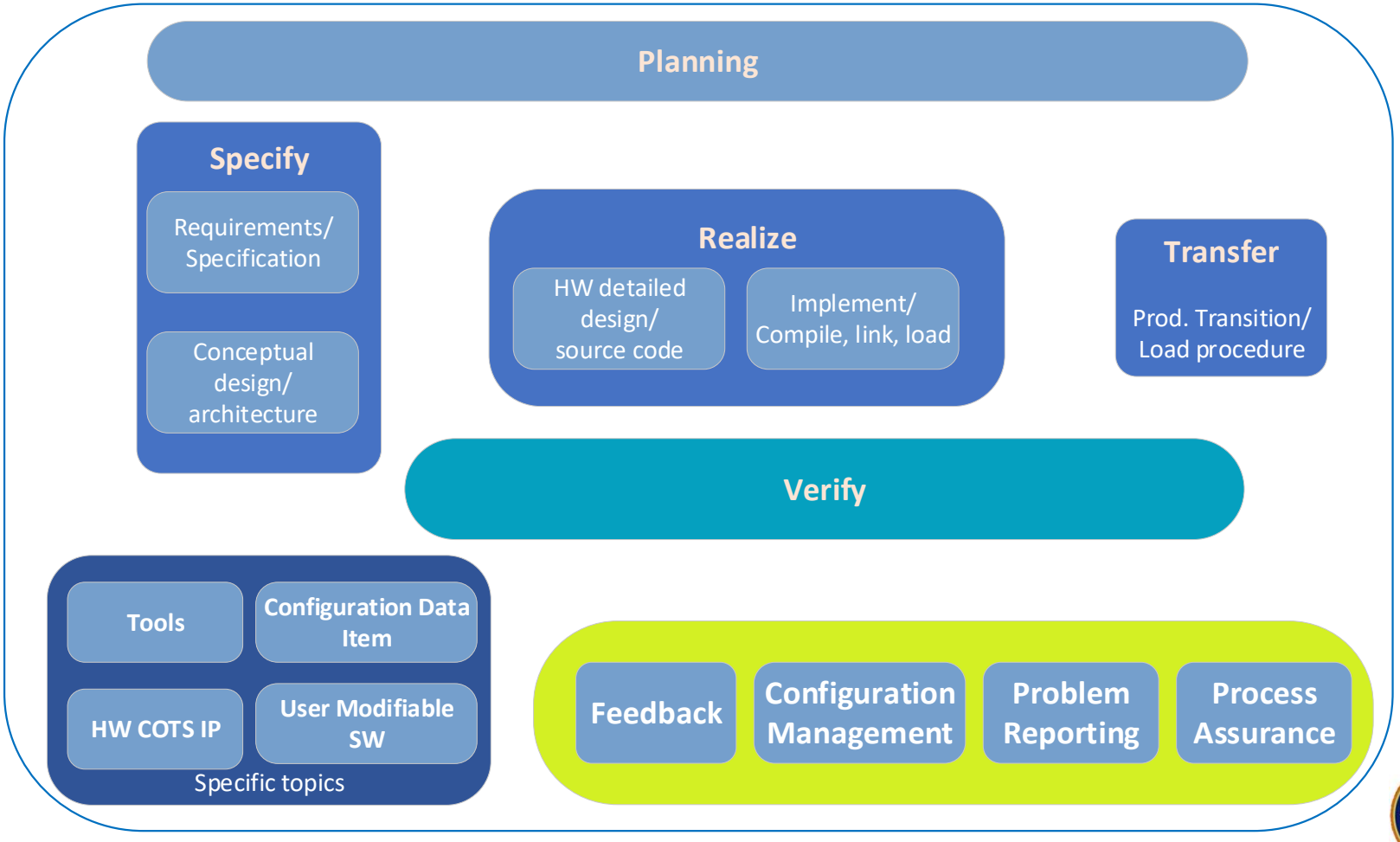
Abstraction Layer – overview (4/5)

Independence

- In order to minimize the risk of error, the following level of independence is required:
  - The process ensures that 'Check' of an evaluation item is performed with independence with the evaluation item(s) for safety level A & B.
  - The process ensures that VERIFY (*) process is achieved with independence from the REALIZE process.
  - The process ensures that PROCESS ASSURANCE (*) is achieved with independence from other processes.

(*) VERIFY and PROCESS ASSURANCE are two specific criteria

Abstraction Layer – overview (5/5)



Criteria Developed

PLANNING
1. PLAN DEFINITION
2. PLAN AGREEMENT

SPECIFY
3. SPECIFY REQUIREMENTS
4. COORDINATE EMERGING FUNCTIONALITY
5. SPECIFY DESIGN

REALIZE
6. REALIZE
7. TRANSFORMATION CONTROL
8. DOCUMENT FOR USE

VERIFY
9. VERIFY REQUIREMENTS
10. DETECT UNINTENDED FUNCTION

TRANSFER
11. TRANSFER

SPECIFIC TOPICS
12. TOOLS
13. DA FOR HW COTS IP
14. CONFIGURATION DATA ITEM
15. USER MODIFIABLE SOFTWARE

TRANSVERSE PROCESSES
16. FEEDBACK
17. CONFIGURATION MANAGEMENT
18. CHANGE MANAGEMENT
19. PROBLEM REPORTING
20. PROCESS ASSURANCE

Illustration of criteria (1/4)

SPECIFY process – defines an item's intended functions, expressed as requirements, and its conceptual design/architecture

Criterion 3 – SPECIFY REQUIREMENTS

A defined process ensures that a complete, correct, and detailed understanding of what the item is expected to do in its operating environment, is established and recorded.

Evaluation

1. A process completely and correctly defines the item functions, their performance and interfaces from the system-level requirements allocated to the item(s), from the design constraints and from the consideration of the safety related aspects. In particular the process ensures that:
    a. [A/B/C/D] All allocated system requirements are transformed correctly into item requirements.
    b. [A/B/C] For software, the item requirements are further developed into sufficiently refined requirements (typically one or more tiers) in order to enable that software code can be directly produced from the requirements. …

- Criteria written with open terminology that is decoupled from existing avionics development assurance standards
    - Provides opportunity for alternate standard's defined activities to meet criteria
- Each criterion is accompanied by evaluation items
    - Top-level evaluation items may have more detailed evaluation sub-items
    - Many evaluation items are common to both software and AEH domains, but some are applicable to only one domain

Illustration of criteria (2/4)

REALIZE process – creates the item in its final form from its requirements and the conceptual design/architecture by following transformation steps*

Criterion 6 – REQUIREMENTS REALIZATION

A defined process ensures that the item is correctly and completely realized from the requirements and the conceptual design/architecture into its final form, and can operate safely within the target operating environment.

Evaluation

…

5. [A/B/C (*)] Check REQUIREMENTS REALIZATION: the REALIZE process provides means for adding confidence in the generation of the final form, especially:
   a. Means to confirm that evaluation items 1 to 4 are met.
   b. Means for assessing compatibility with available resources

- Maintains requirements-based philosophy of existing avionics development assurance standards
- Some criterion have “Check” evaluation items that state an expectation for an alternative standard/methodology to confirm that a process is adequately performed

* “transformation steps” is a generic term used to refer to specific intermediate process steps from AEH or SW code to its final form

Illustration of criteria (3/4)

VERIFY process – refers to the verification processes of the item

Criterion 9 – VERIFY REQUIREMENTS

A defined process ensures that the item is completely and correctly verified against its requirements, when the item functions in its operating environment.

Evaluation

…

3. [A/B/C/D] The process ensures that any intermediate representation of the item, used to demonstrate correctness of the item, is correct.
   a. The process ensures that the limits of such verification activities are identified.

Note: for model-based development, if model simulation is used to verify the item, simulation cases are developed based on the layer of requirements specifying the model.

…

9. [A/B] The process ensures verification is performed with independence to REALIZE activities (…) to enforce the correctness demonstration.

- Requirement-based verification approach
- Verification with independence to REALIZE activities
  - General expectation of independence following ED-80/DO-254 concept, which Task Force acknowledges departs from ED-12C/DO-178C detailed allocation
- "Notes" are supporting information considered helpful to illustrate the intent of the words of the evaluation item or to provide additional information

Illustration of criteria (4/4)

VERIFY process – refers to the verification processes of the item

Criterion 10 – DETECT UNINTENDED FUNCTION

A defined process ensures that each element of the item has been verified through requirement-based verification, to preclude unexpected or undefined behavior.

Evaluation

1. …
   b. The method and associated criteria to measure the coverage of the item elements during requirement-based verification is defined and is appropriate to the type of elements.
   c. The results are analyzed and each gap identified is either justified or fed back to the appropriate process, particularly:
      i. elements 'not covered by requirement-based verification' are justified (the unused functions are identified with their deactivation means),
      ii. or feedback is provided to the REALIZE process to remove unintended function,
      iii. or feedback is provided to the VERIFY process.

- To preclude unexpected behavior of the item
- All evaluation items are required to be met to fully satisfy a Criterion, but evaluation sub-items may foresee alternatives

Conclusion – What Abstraction Layer Is/Is Not

Abstraction Layer is not …

- → intended to serve as a new alternative standard
  - → **Recognized industry standards are still required to describe in detail the methods to satisfy the AL objectives in order**
    - → **to avoid subjective assessment on both sides AA and industry**
    - → **to ensure level playing field**
    - → **to be efficient in time & resources (avoid endless discussions)**
- → intended to invalidate or put at risk current accepted industry development assurance standards in the SW&AEH domain

Conclusion – What Abstraction Layer Is/Is Not

Abstraction Layer is …

- → a ‘bridging tool’ to accept potential alternate standards or public methodologies used in other industry domains
- → a set of 20 criteria, providing an objective method to assess and help identify gaps in alternate standards or methodologies
- → accompanied by a User Guide describing ‘how to use the Abstraction Layer’ material

Conclusion

- Abstraction Layer represents a consensus opinion of the Task Force members comprised of representatives from industry and certification authorities

- Abstraction Layer usability has been demonstrated as a « proof of concept » with the test on ISO 26262 Automotive Functional Safety Standard.

- Abstraction Layer final version issued to FAA&EASA senior management in October 2023! We thank industry members for their active support and contributions.

EASA
European Union Aviation Safety Agency

FAA
Aviation Safety

Thank You

Any question?

Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

1 Welcome to the webinar
Eric Duvivier [EASA]

2 Presentation of the Task Force
Eric Duvivier [EASA] & George Romanski [FAA]

3 Presentation of the AL
Anne Senechal [EASA], Mike Vukas [FAA]
Maurizio Patriarca [Leonardo], Clay Barber [Garmin]

4 The User Guide
Chris Hubbs [Collins], Bernie Newman [Astronautics]

5 How to consider the AL within the current regulatory framework of EASA & FAA AND Framework for recognition of alternate standards assessed using the AL
Anne Senechal [EASA], Mike Vukas [FAA], Brenda Ocker [FAA]

6 Usage of the AL in the Feasibility Study
Chris Hubbs [Collins], Karen Brack [Boeing]

7 Concluding remarks
Eric Duvivier [EASA] & George Romanski [FAA]

How do you use the AL?

- → Scenario: you use or have identified an alternate industry standard that might provide value to the aviation industry
- → The Abstraction Layer may provide a route to get credit for use of that alternate standard
- → Where do you start?

The material in this presentation is formally captured as a User Guide in Appendix V of the Abstraction Layer report

We Tried This

- As a part of the TFAL, we did a “trial run” to validate the AL by conducting a proof-of-concept assessment of ISO 26262 (automotive standard)
  - This assessment is incomplete, but TFAL provided results in a report to FAA and EASA as an example of how an assessment might be performed
- We established methods and tools during this trial run that may be useful to the community

Form Task Force to Evaluate the Alt Standard

- Industry (likely via a trade association) forms an Assessment Task Force (ATF) to assess how the alternate standard meets the AL criteria
  - ATF should include industry and authorities
  - Authorities will want to see sufficient representation and interest to commit their own resources
- SMEs on the alternate standard should be included as trusted advisors, but not team members

Perform the Assessment

- → Gain an understanding of the alternate standard
- → Perform a detailed analysis using the AL worksheets per criterion
  - → Table 1: capture relevant guidance that seems to address assessment text
  - → Table 2: final assessment - met, not met, partial
- → Document a final assessment

Recognize Assessment Realities

- → It is likely that no alternate standard will fully meet the AL objectives
- → Document any suggested limitation to applicability per discipline or DAL
  - → E.g., a standard may only be applicable to HW or SW or only at DAL C/D, etc
- → Document the “gaps”
  - → important so that those gaps can be filled by additional activities

Submit the Final Assessment

- The completed assessment should be provided to the airworthiness authorities along with a statement of interest
  - Identified gaps
  - Statements of feasibility to address gaps
  - Suggestions to applicability limits (e.g., HW or SW, DAL D…)
  - Statement of interest to proceed or not

EASA
European Union Aviation Safety Agency

FAA
Aviation Safety

Questions?

Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

1 Welcome to the webinar
Eric Duvivier [EASA]

2 Presentation of the Task Force
Eric Duvivier [EASA] & George Romanski [FAA]

3 Presentation of the AL
Anne Senechal [EASA], Mike Vukas [FAA]
Maurizio Patriarca [Leonardo], Clay Barber [Garmin]

4 The User Guide
Chris Hubbs [Collins], Bernie Newman [Astronautics]

5 **How to consider the AL within the current regulatory framework of EASA & FAA AND Framework for recognition of alternate standards assessed using the AL**
Anne Senechal [EASA], Mike Vukas [FAA]

6 Usage of the AL in the Feasibility Study
Chris Hubbs [Collins], Karen Brack [Boeing]

7 Concluding remarks
Eric Duvivier [EASA] & George Romanski [FAA]

EASA
European Union Aviation Safety Agency

Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

FAA
Aviation Safety

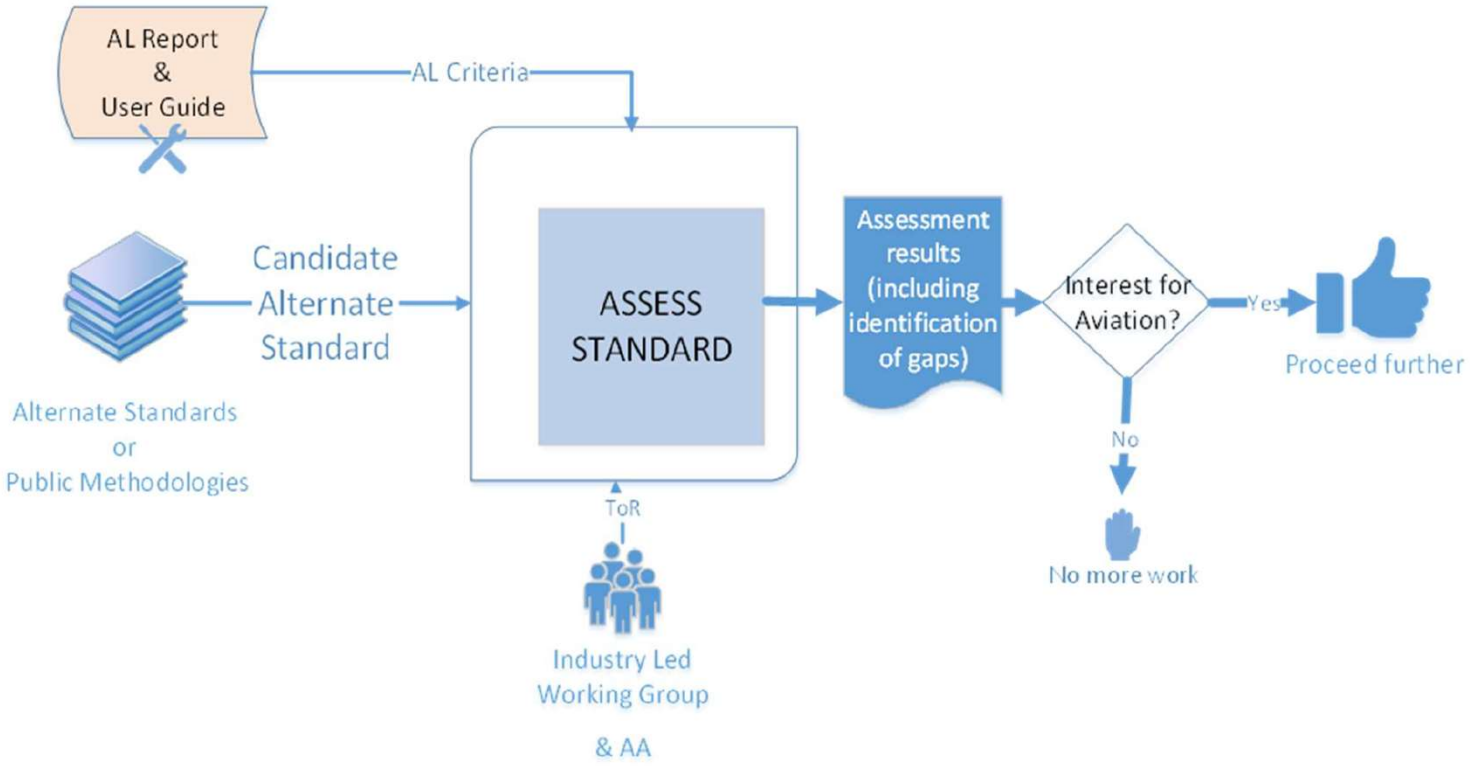
5-1: How to consider the AL within the current regulatory framework of EASA and FAA

Anne Sénéchal - EASA
Mike Vukas - FAA

Introduction

- The AL consists of criteria, formulated as goals, with associated evaluation items which state the expectations of what constitutes satisfying a criterion.
- The AL is not a standard itself for SW or AEH development, criteria are defined at a high-level.
- The AL doesn't detail a set of activities to develop SW&AEH.
  - AL doesn't replace standardisation activities in the SW&AEH domain.
- AL is considered as a "tool" to assess other standard against its criteria, to evaluate their relevance as alternate to current ED-12/DO-178 or ED-80/DO-254.

Framework for using the Abstraction Layer



Positioning of AL wrt regulatory framework

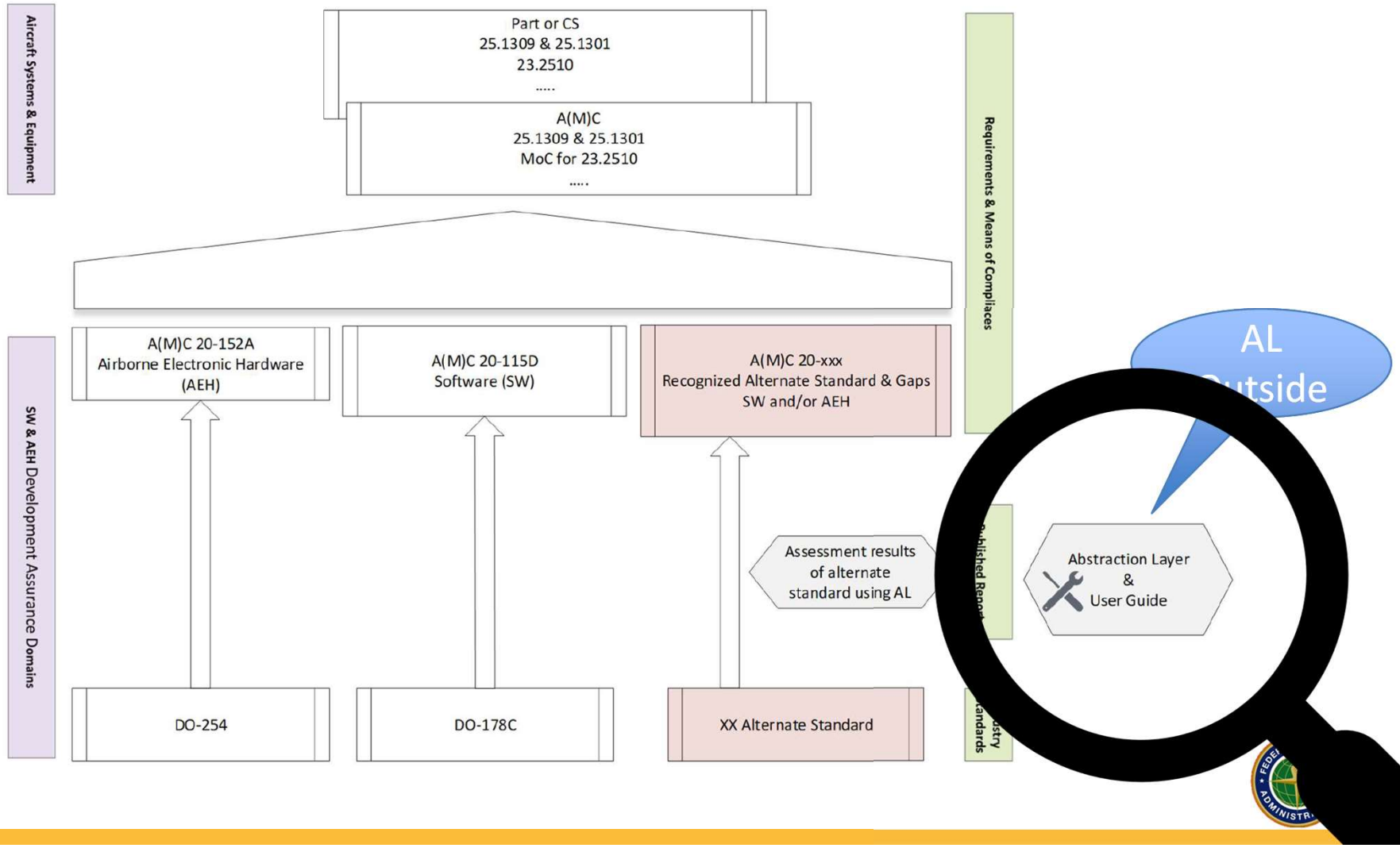
With its high-level definition,

→ the purpose of the AL is not to be placed in one EASA CS/FAA 14 CFR Part or accepted as a Means of Compliance (MoC) for a certification product(s).

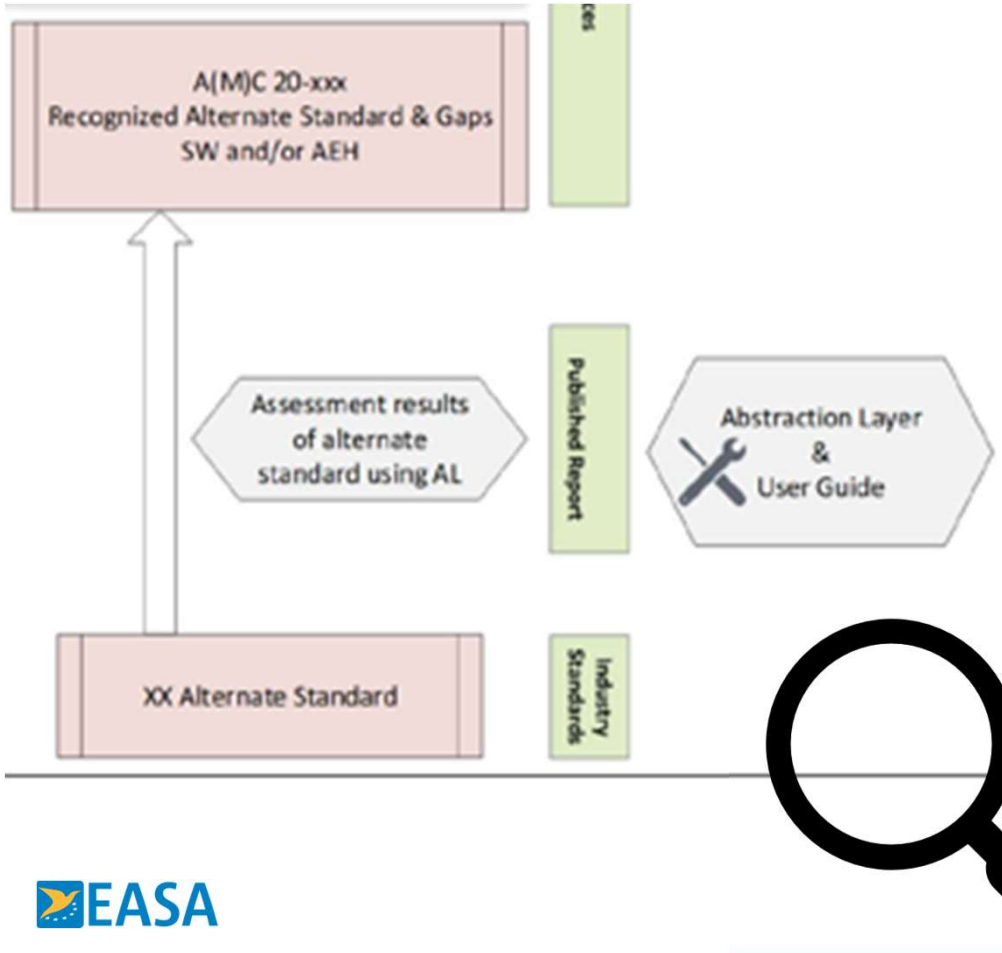
→ Consequently, the AL position is *outside* of the regulatory framework but

→ AL is available as a tool to assess alternative standards that could ultimately be introduced as MoC in the regulatory framework.

Positioning of AL wrt regulatory framework (1/2)



Positioning of AL wrt regulatory framework (2/2)



- AL is now published as a standalone document prepared by the Task Force.
  - Contains the AL material and the guidelines on how to use the AL material.
- Assessment results of alternate standards will be the start point of further recognition of an alternate standard into the regulatory framework.

EASA
European Union Aviation Safety Agency

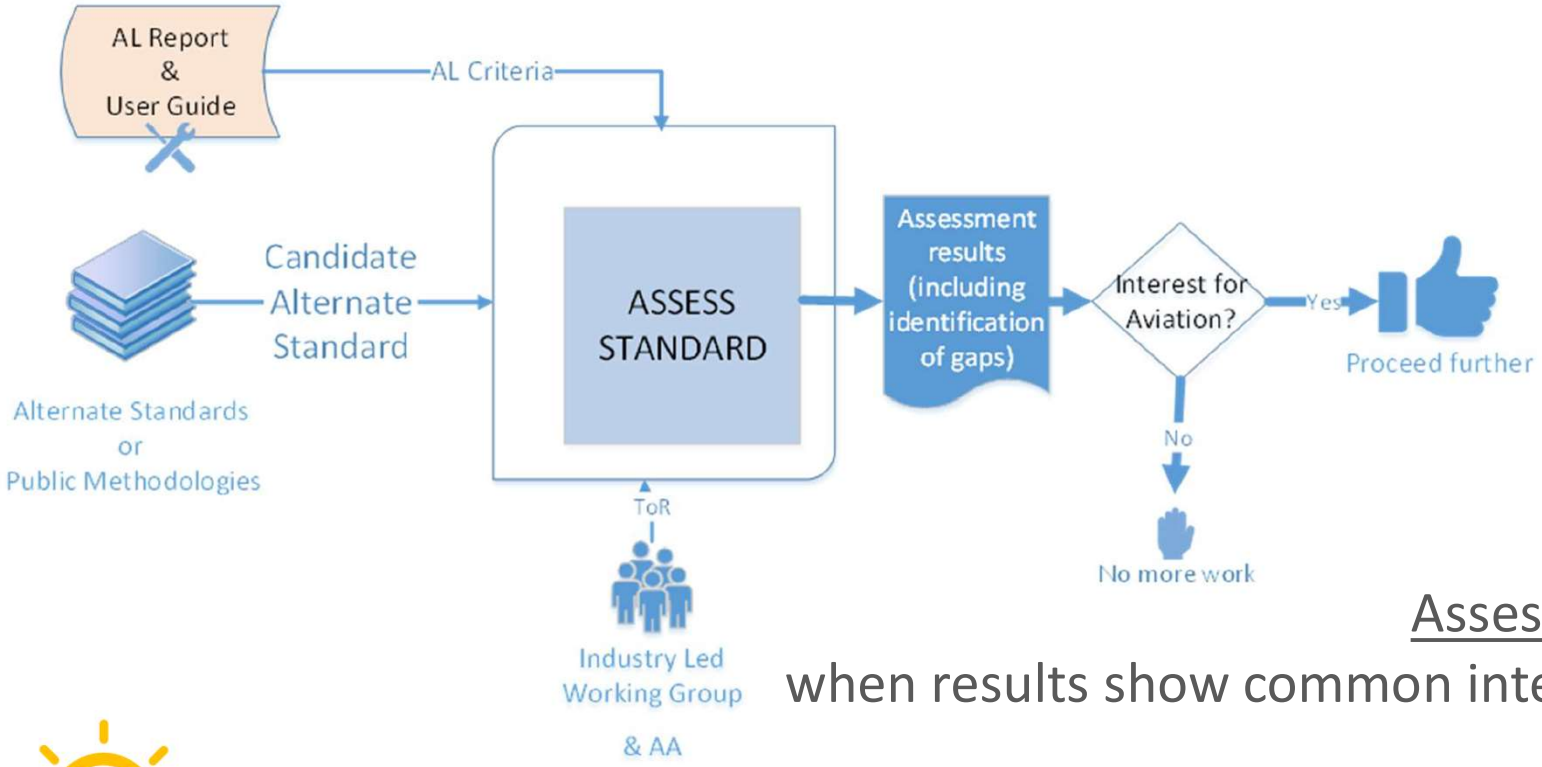
Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

FAA
Aviation Safety

5-2: Framework for recognition of alternate standards assessed using the AL

Anne Sénéchal - EASA
Mike Vukas - FAA

Introduction

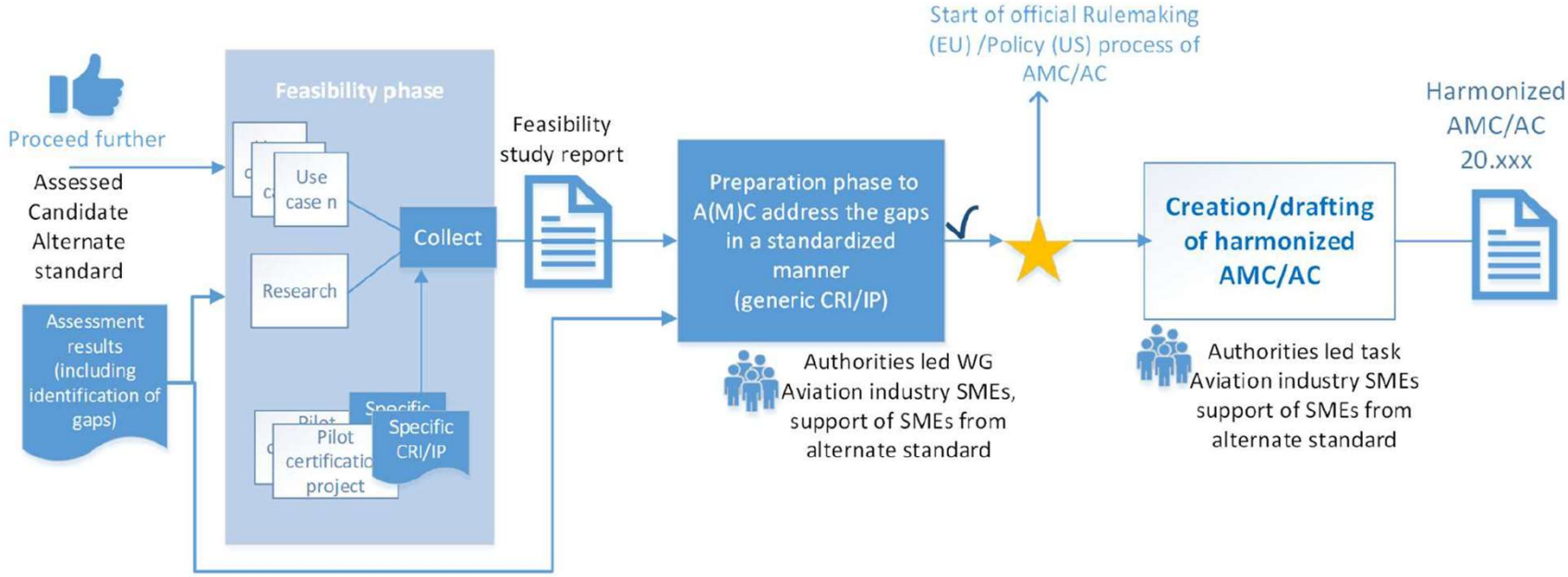


Assessment Framework

when results show common interest to proceed…

→ *First need to deepen knowledge in the alternate standard & concrete implementation & its practices*.

Process steps to enable recognition of alternate standard(s)



→ The Task Force proposes different phases before engaging in a formal AMC/AC process

Feasibility phase

The Feasibility phase is required in order to:

- Evaluate/understand in a concrete manner the challenges of using SW&AEH components developed according to the alternate standard in the Aviation context.
- Understand the benefits, the obstacles, and the artifacts produced.
- Understand the Development Assurance methods and foresee/evaluate solutions to address gaps.
- Confirm that the solution to use the alternate standard is cost effective beneficial for the aviation industry.

Feasibility study

- → is performed by the AA and Aviation industry in a coordinated manner.
- → is an investigation to collect all shared experience and lessons learned from the application of the alternate standard and actual practice in the alternate market.

The feasibility study may take different approaches, e.g.

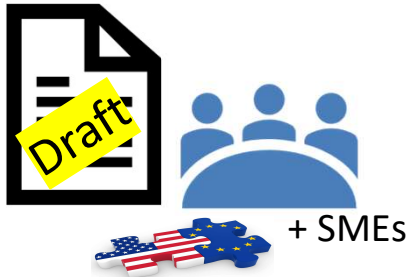
- → Use Case: proposed by Aviation industry member(s), shared with AA. To collect inputs
- → Research Project: Aviation industry member(s) propose a research project or request for information (RFI)
  - → to augment the experience in concrete usage of the alternate standard.
  - → to confirm the benefit/gaps as identified in the assessment of the std against AL.
- → Pilot Project: Pilot projects in a certification context, where the primary AA raises a specific CRI/IP paper to document a certification approach (including addressing the gaps) in a given project context.

Feasibility phase

- → includes a sharing forum where all stakeholders share their lessons learned, experience gained in practical development assurance process, artifacts, gap mitigation from the use cases and/or pilot projects.
- → Output is a Feasibility report

Preparation phase of AMC/AC

→ to address the gaps in a standardized manner



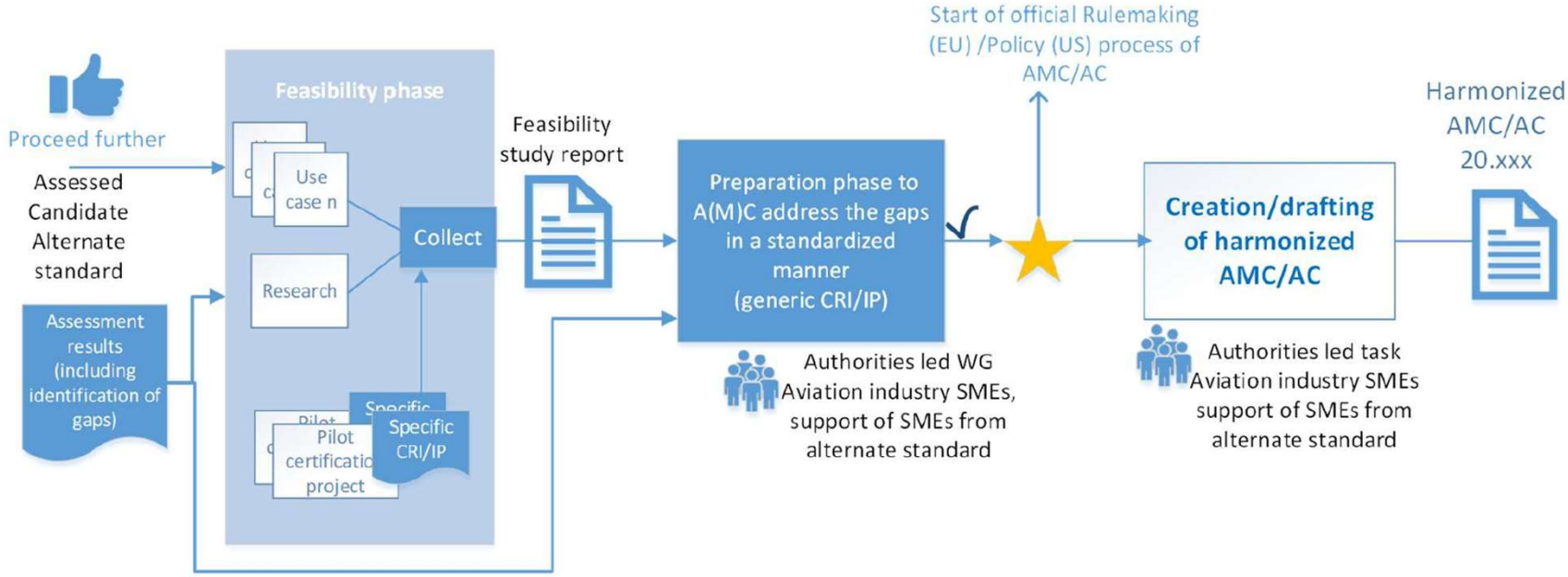
→ Develop initial AA material, as a generic EASA CRI / FAA IP, to recognise the alternate standard and define ways/activities to address any gaps.

→ AA engages with SMEs from alternate standard to discuss means to address gaps

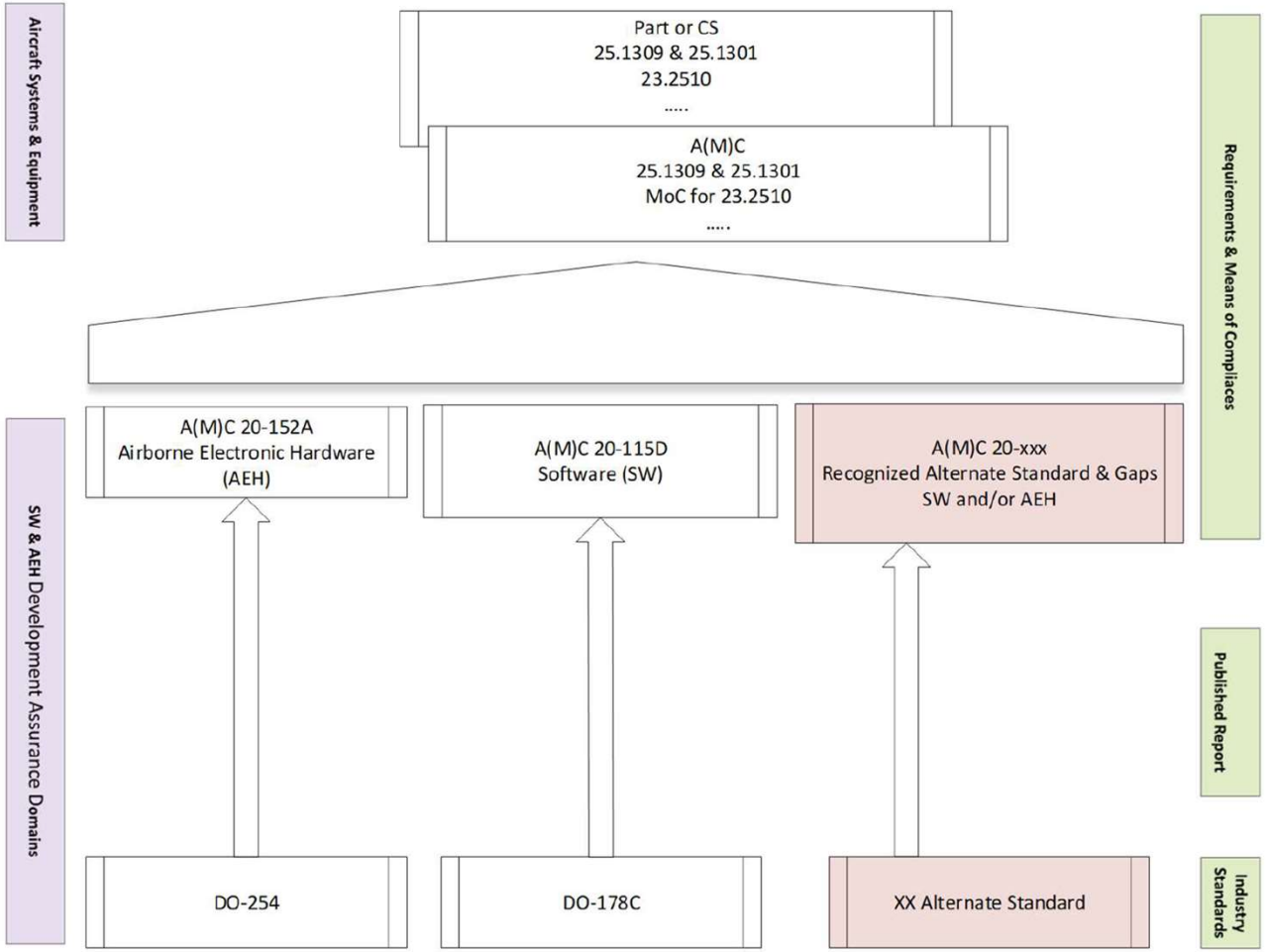
→ Gain experience and collect lessons learned with the process (alternate standard + additional gap mitigating activities) through pilot certification projects.

Mature the developed material (CRI/IP) benefiting from the gained experience, and generalize.

Proposed process …
to finally recognize the alternate std



Recognition of alternate standard



As proposed by the Task Force to EASA&FAA Management

EASA
European Union Aviation Safety Agency

FAA
Aviation Safety

Questions?

Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

1 Welcome to the webinar
Eric Duvivier [EASA]

2 Presentation of the Task Force
Eric Duvivier [EASA] & George Romanski [FAA]

3 Presentation of the AL
Anne Senechal [EASA], Mike Vukas [FAA]
Maurizio Patriarca [Leonardo], Clay Barber [Garmin]

4 The User Guide
Chris Hubbs [Collins], Bernie Newman [Astronautics]

5 How to consider the AL within the current regulatory framework of EASA & FAA AND Framework for recognition of alternate standards assessed using the AL
Anne Senechal [EASA], Mike Vukas [FAA], Brenda Ocker [FAA]

6 Usage of the AL in the Feasibility Study
Chris Hubbs [Collins], Karen Brack [Boeing]

7 Concluding remarks
Eric Duvivier [EASA] & George Romanski [FAA]

Test Project to Leverage Supplier Activities under ISO 26262

Collins Aerospace
An RTX Business

Chris Hubbs
Director, Avionics Advanced Technology Certification

22 May 2024

Collins Avionics Use Case

- Collins has challenges to procure components (HW, firmware, embedded software) that have a DO-178() or DO-254 pedigree
- Many suppliers, though, do serve the automotive industry and provide ISO 26262 compliance for some components
- Leveraging ISO 26262 approval via the Abstraction Layer (AL) makes it easier to get cooperation from the supplier for a safety certification

Current Collins project

- We currently have an Avionics product under development for a DAL D function
- A supplier from the automotive industry has software, firmware, and AEH available that has an existing ISO 26262 pedigree
- Our plan is to integrate the supplier components into a Collins design, taking advantage of the ISO 26262 compliance substantiation in place of “traditional” DO-178/254 reverse engineering

Current Status

- We have held preliminary discussions with the FAA specialist to introduce the topic
- We are working with the supplier to gain access to their ISO 26262 compliance data so we can assess it for acceptability
- We are working to understand the gaps between ISO 26262 and Abstraction Layer objectives and how the supplier's process maps to those gaps
  - Some gap filling may be needed at the integration level

Perceived Risks Using An Alternate Standard

- The first time for anything is risky – many unknowns!

- The supplier's substantiation data may not be of sufficient quality or fidelity to be acceptable to the airworthiness authorities
  - If the evidence is deemed good by the auto industry, is it good enough for us?

Perceived Benefits of Using An Alternate Standard

- Eliminate expensive reverse engineering activities for non-DO-178/254 components
- Opens pathways to make use of more supplier components
- Gives us opportunities to explore alternative development assurance methodologies
  - This is needed to move the industry forward!
  - Our industry would benefit from having a path to use alternatives to DO-178 & DO-254

EASA
European Union Aviation Safety Agency

Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

FAA
Aviation Safety

Usage of the Alternate Standard in the Feasibility Study

Karen G Brack

Likely Interest in Performing Assessment

- When avionics industry identifies component(s) developed for an alternate industry that can be used in Avionics
- When component developer(s) follow an alternate standard
  - Examples:
    - ISO 26262
    - IEC 61508
    - Nuclear Regulatory Commission standard
- Likely that the alternate standard is followed because use of the component requires addressing reliability or safety concerns

Likely Interest in Performing Assessment

- When the alternate standard or methodology to be evaluated shares fundamental principles of the Abstraction Layer
- Examples
  - Specification of desired operation
  - Structured design process
  - Testing based on specification
  - Documented development process

Feasibility Phase for Hardware

- After applying the Abstraction Layer to assess the alternate standard, a feasibility phase should be conducted

  Reference: "How to consider the Abstraction Layer within the current regulatory framework of EASA and FAA" & "Framework for recognition of alternate standards assessed using the Abstraction Layer"

- Use cases, research projects and pilot projects are requested to evaluate use of the alternate standard and resulting outputs
- ISO 26262 has been assessed

  Reference: "Abstraction Layer Trial on ISO 26262"

- The timing is right for a Feasibility Phase

Feasibility Phase for Hardware

- Potential Use Cases to study ISO 26262: airborne hardware component(s) have common aspects of the hardware architecture with applications in other industries
- Examples
  - Digital bus interface
  - Microprocessor interface
  - Signal processing function
  - Data processing function
  - Encryption

EASA
European Union Aviation Safety Agency

FAA
Aviation Safety

Questions?

Webinar *Task Force SW&AEH*
"Abstraction Layer"
May 22, 2024

1 Welcome to the webinar
Eric Duvivier [EASA]

2 Presentation of the Task Force
Eric Duvivier [EASA] & George Romanski [FAA]

3 Presentation of the AL
Anne Senechal [EASA], Mike Vukas [FAA]
Maurizio Patriarca [Leonardo], Clay Barber [Garmin]

4 The User Guide
Chris Hubbs [Collins], Bernie Newman [Astronautics]

5 How to consider the AL within the current regulatory framework of EASA & FAA AND Framework for recognition of alternate standards assessed using the AL
Anne Senechal [EASA], Mike Vukas [FAA], Brenda Ocker [FAA]

6 Usage of the AL in the Feasibility Study
Chris Hubbs [Collins], Karen Brack [Boeing]

7 Concluding remarks
Eric Duvivier [EASA] & George Romanski [FAA]

EASA
European Union Aviation Safety Agency

FAA
Aviation Safety

Thank YOU!