G34/WG-114 Spring 2020 Joint Plenary

31 March–1 April 2020 via WebEx

Christophe Gabreau, WG-114 Co-Chair
Sachin Jain, G34 Secretary
Santosh Mathan, WG-114 Secretary
Paula Olivio, G34 Vice Chair
Mark Roboff, G34 Chair
Christian Thurow, WG-114 Co-Chair
Welcome from the Leadership Team
Agenda

Day 1: Tuesday 31 March, 09:00 EDT
- 9:00 Welcome by Chairs
- 9:30 EUROCAE & SAE Slides
- 10:00 SC2 & SC3 Additions to SoC
- 10:30 SOC Comments Triage Report
- 11:00 Post-SOC Next Steps
- **11:30-11:45 BREAK**
- 11:45 Presentation by EASA
- 12:15 Presentation by Daedalean
- 13:00 Close

Day 2: Wednesday 1 April, 09:00 EDT
- 9:00 Report on AS6983 Skeleton
- 9:30 G-34/WG-114 Merger Presentation
- 10:30 Discussion and vote on Merger
- **10:45-11:00 BREAK**
- 11:00 Presentation on go-forward sub-committee structure
- 12:00 Liaison Activity Updates
- 13:00 Close
EuroCAE Mandatory Procedures
Any party participating in the work of EUROCAE is requested, in the timeliest possible manner and to the best of their knowledge, to draw attention to any known patent or to any known pending application on patent, either their own or of other organisations, that, according to their own judgment, may be considered to be or become an essential patent for the deliverable.

- Conditions for use of such material are further detailed in the EUROCAE Handbook.
- Final decision by EUROCAE Council is based on justification provided by WGs.
Participation in EUROCAE Working Group

EUROCAE is a membership-based organisation

Participation to EUROCAE activities is reserved for EUROCAE members.

Non-members are welcome to participate for a limited period of time to understand the scope of activities (1-2 meetings / 3 months max). After this period, should they wish to continue their participation, they must become members. Otherwise, WG membership and workspace access will be suspended.

EUROCAE Council has reaffirmed this principle at its 287th meeting (Nov 2015).
EUROCAE is committed to respecting your privacy. Any photos taken during the WG meeting may be used in one or several communication tools available at EUROCAE. Should you prefer that we do not include you in the photos that we publish, please advise us now.
Question?

Anna Guéган, CISSP
Technical Programme Manager
+33 1 49 46 19 67
anna.guegan@eurocae.net
SAE Anti-Trust, Patent Disclosure, and IP Statements
Anti-Trust Statement: In discharging their responsibilities, members of the Technical Standards Board, Councils/Division, and Technical Committees function as individuals and not as agents or representatives of any organization with which they may be associated, except that government employees participate in accordance with governmental regulations. Members are appointed to SAE Technical Committees on the basis of their individual qualifications which enable them to contribute to the work of the Committee.

Patent Disclosure: Each SAE Technical Committee or SAE working group member would be required to disclose at specified times during a development process all patents and patent applications that are owned, controlled or licensed by the member, member’s employer or third party and that the member believes may become essential to the draft specification under development. The member would make this disclosure based on the member’s good faith and reasonable inquiry. If SAE International receives a notice that a proposed SAE Technical Report may require the use of an invention claimed in a patent, the respective part of the SAE Technical Standards Board Policy will be followed.

IP Statement: SAE’s intellectual property is its most valuable asset. As such, the Society expends considerable resources maintaining and protecting its rights to its intellectual property. SAE reserves the right to copyright any of its print products, electronic products, databases, audio/visual products and any other subject matter. This is intended to protect SAE and its members from unauthorized copying and distribution of SAE intellectual property. SAE’s intellectual property may only be used in a manner that furthers the organization’s purposes.

It is also SAE policy that the copyrights and other intellectual property rights of third parties be respected and not infringed upon by SAE or any of its committees, or any employee, member or other person acting on behalf of SAE.

As a participant in SAE Technical Committees, individuals agree that the collective work of the committee(s) is the property of SAE, and SAE is charged with its publication, dissemination, and protection.
QUESTIONS?

Jordanna Bucciere
Aerospace Standards Specialist
Phone  +1.724.772.7517
Jordanna.Bucciere@sae.org
Report: SC2 & SC3 Additions to the SoC

(Statement of Concerns)

SC2 Chair - David Redman
SC3 Chair - Rey Nicholas
Report: SoC Comments Triage

Team 1 Chair - Alexis de Cacqueray
Team 2 Chair - Louis Fabre
Team 3 Chair - Eric Asselin
Team 4 Chairs - Baptiste Lefevre & Fateh Kaakai
SOC Chapter#1: Definitions and Classification of AI techniques

(Statement of Concerns)

SC5 Chair - Cory Laflin
TM1 Chair - Alexis de Cacqueray
Main AI Classification

- Symbolic AI
  - Logic
    - Non-temporal logic
    - Temporal logic
    - Probabilistic graphical models
  - Knowledge Engineering
    - Ontologies
    - Knowledge Bases
- Machine Learning
  - Supervised learning
  - Unsupervised learning
  - Semi-supervised learning
  - Reinforcement learning
  - Meta-learning
- Optimization
  - Operations Research
  - Population methods
  - State Estimation
  - Optimal Control
  - System Identification
  - Backpropagation Optimization
  - Data Clustering

Secondary classification: fields of application
- Computer vision
- Anomaly detection
- Natural Language Processing
- Decision making and Autonomy

ML bubble chart (to review)
• 35 comments received by comment forms on Draft 11 (24 SAE, 11 EUROCAE)
• 57% completely reviewed by SAE and EUROCAE team leaders
• Also many comments on the draft itself (around 70), answers during the sessions
• Deadline for comments extended to mid-April

General comments:
• Comments mostly about the definitions → please comment the classification
• This SoC: internal document → some changes will be taken into account for the released document
• Definitions: impossible to define every term → we focus on the needed ones for the other chapters
• For some topics: implicit agreements → difficult to change position now
• How do we include the other AI techniques in our SoC/Standard?

<table>
<thead>
<tr>
<th>Row Labels</th>
<th>Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>3</td>
</tr>
<tr>
<td>H</td>
<td>3</td>
</tr>
<tr>
<td>L</td>
<td>20</td>
</tr>
<tr>
<td>M</td>
<td>9</td>
</tr>
<tr>
<td>Grand Total</td>
<td>35</td>
</tr>
</tbody>
</table>
SOC Chapter#2: Gap Analysis

(Statement of Concerns)

SC1 Chair - Leon Gommans
TM3 Chair - Eric Asselin
A Common Standard for Airborne & Ground Systems

Iterative Offline Machine Learning as Core Scope

End-to-End Process from System to Item Implementation

Review status of Ch. 2
- 1 Life Cycle Assumption
- 20 Standards listed
- 5 Standards analysed
- 58 comments received
- 11 comments answered
- Target date: 15/04/2020

Functional Intent
Safety requirements
(Domain usage)

Source Code

Training Dataset

Learning

Test Dataset

ML model

Option A
Design Model

Option B
ML Architecture & Parameters as HLR

Verification

System Integration & Verification

Input for

Production

Model validation & verification

Dataset quality attributes check

Model design errors mitigation

Airborne: ED-12C/DO-178C with ED-218/DO-331, ED-80/DO-254

Airborne: ED-79/ARP-4754A
Ground: CIR (EU) 2017/373 with its AMC/GM

Development Assumption

Objectives covered by existing standards

Not covered by existing standards

Objectives not covered by existing standards
SOC Chapter#3: Areas of concerns

(Statement of Concerns)

TM2 Chair - Louis Fabre
ML & Data Sets System Life Cycle

- Safety
- Compliance demonstration
- Configuration management
- Security

Statement of Concerns
Chapter 3
# 40 concerns are identified in §3

5 H / 9 M / 2 L comments from Eurocae (inc. EASA)
11 H / 35 M / 13 L comments from SAE (inc. FAA)

Analysis is on going

“High” comments are related to new concerns / not understood concerns
“Medium” comments are related to improvements of existing concerns

SAE counter part could be beneficial
SOC Chapter#4: Areas of concerns

(Statement of Concerns)

TM4 Co-Chair - Baptiste Lefevre
TM4 Co-Chair - Fateh Kakai
A Common Standard for Airborne & Ground Systems

Iterative Offline Machine Learning as Core Scope

End-to-End Process from System to Item Implementation

Plan for certification / approval

System requirements definition and validation

Safety Considerations for AI-ML

Data Selection & Validation

Model Selection & Training

Model Validation

Machine Learning

Means for learning & development assurance

Learning assurance

Formal methods

Testing

Explanation

Licensing

In-service experience

System Safety assessment

Identification of safety risk mitigations

Development Assurance level assignment

Development of system architecture

ML-based Design Constraint Specification

ML-based Item Implementation & Verification

System Integration Verification & Validation

Review status of Ch. 4

- 96 comment received
- Balanced btw EUR/SAE
- 62 comments answered
- Progress metric: 65%
- Target date: 15/04/2020

Iterative Offline Machine Learning as Core Scope

End-to-End Process from System to Item Implementation

Trustworthiness analysis

Trustworthiness analysis

Learning assurance

Formal methods

Testing

Explanation

Licensing

In-service experience

SOP Chapter#4

SOC Chapter#4
Timeline

Internal Comments Due
Thursday, April 16

Comment Adjudication
April 16—May 14

Editing Process
May 14—May 31

Balloting Process
June 1—June 28

Internal Comments Deadline Extended
Now Due: Thursday, April 16
SOC Comments Adjudication

• Plan to leverage existing teams and sub-committees

<table>
<thead>
<tr>
<th>SOC Chapter</th>
<th>Teams</th>
<th>Leads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1 - Taxonomy*</td>
<td>Team 1 + SC 5</td>
<td>Alexis + Cory</td>
</tr>
<tr>
<td>Chapter 2 - Gap Analysis</td>
<td>Team 3 + SC 1</td>
<td>Eric + Leon</td>
</tr>
<tr>
<td>Chapter 3 - Areas of Concern</td>
<td>Team 2</td>
<td>Louis</td>
</tr>
<tr>
<td>Chapter 4 - Next Steps</td>
<td>Team 4</td>
<td>Baptiste + Fateh</td>
</tr>
<tr>
<td>Chapter 5 - Aircraft Use-Cases</td>
<td>SC 2</td>
<td>Dave + Steve</td>
</tr>
<tr>
<td>Chapter 6 - Ground Use-Cases</td>
<td>SC 3</td>
<td>Rey</td>
</tr>
<tr>
<td>Chapter 7 - Conclusions</td>
<td>Exec Team</td>
<td>Exec Team</td>
</tr>
</tbody>
</table>

* Includes Definition Section
The Editorial Committee

• Necessary to ensure the Statement of Concerns and future documents read well: edit for spelling, grammar, verbiage, tone, structure, and flow.

• Will commence on 15 May 2020, after comments adjudication has ended. Need to ensure technical content has solidified first.

• Mark Roboff to chair. Looking for 3-5 volunteers. Please e-mail mroboff@dxc.com if interested.
We will be back at:
End of Day 1 - Thank You!
Welcome to Day 2
Agenda

Day 1: Tuesday 31 March, 09:00 EDT
• 9:00 Welcome by Chairs
• 9:30 EUROCAE & SAE Slides
• 10:00 SC2 & SC3 Additions to SoC
• 10:30 SOC Comments Triage Report
• 11:00 Post-SOC Next Steps
• 11:30-11:45 BREAK
• 11:45 Presentation by EASA
• 12:15 Presentation by Daedalean
• 13:00 Close

Day 2: Wednesday 1 April, 09:00 EDT
• 9:00 Report on AS6983 Skeleton
• 9:30 G-34/WG-114 Merger Presentation
• 10:30 Discussion and vote on Merger
• 10:45-11:00 BREAK
• 11:00 Presentation on go-forward sub-committee structure
• 12:00 Liaison Activity Updates
• 13:00 Close
Report: AS6983 Skeleton

Skeleton Working Group Leader - Terri Hall
AS6983 Skeleton

• Working group met over four weeks to define outline

• Started with the applicable topics from the Statement of Concerns as well as ARP4754 as a starting point

• **Scope of document:** will address Machine Learning primarily; Some discussion of other AI techniques (on-line learning, etc.); More AI techniques in future revision; Organizational considerations

• Current version posted on StandardsWorks in AS6983 WIP area.
AS6983 Skeleton Top Level

- RATIONALE
- FOREWARD
1. SCOPE
2. PURPOSE
3. REFERENCES
4. DEVELOPMENT PLANNING CONSIDERATIONS FOR AI
5. SYSTEM DEVELOPMENT CONSIDERATIONS FOR AI
6. AI ITEM DEVELOPMENT
7. INTEGRAL PROCESSES ADDRESSING AI
8. MODIFICATIONS TO SYSTEMS OR AI ITEMS
9. APPENDICES
4. DEVELOPMENT PLANNING CONSIDERATIONS FOR AI

• No further definition at this time
5. SYSTEM DEVELOPMENT CONSIDERATIONS FOR AI

5.1 AI System Development Life Cycle

5.2 Requirement Definition
   5.2.1 System Requirements
      5.2.1.1 Types of Requirements
      Note: Consider Useability and Human-Computer Interaction
      5.2.1.2 Xx
   5.2.2 Item Requirements
      Note: Include here Explainability requirements, and Trustworthiness requirements - also Data Selection and Validation

5.2.3 Data Considerations
   5.2.3.1 Data Selection
   Note: Data Availability and Suitability should be considered
   5.2.3.2 Data Partitioning
   5.2.3.3 Data Cleansing
   5.2.3.4 Data Lineage
   5.2.3.5 Data Validation
   5.2.3.6 Data Provenance Review
5. SYSTEM DEVELOPMENT CONSIDERATIONS FOR AI

5.3 Development of System Architecture
5.4 Model Selection, Training and Validation
   5.4.1 Paradigm
   5.4.2 Topology

Note: Include here Explainability considerations
6. AI ITEM DEVELOPMENT

6.1 Machine Learning Based Design Constraint Specification
6.2 Machine Learning Component Implementation
7. INTEGRAL PROCESSES ADDRESSING AI

7.1 Requirement Validation
7.2 Safety Assessment and DAL Assignment
*Note: Include here Explainability considerations*
7.3 Machine Learning Component Verification
7.4 Machine Learning Component System Integration and Verification
7.5 Verification Methods/Techniques
   7.5.1 Testing
   7.5.2 Formal Methods
   7.5.3 In-Service Experience
7. INTEGRAL PROCESSES ADDRESSING AI

7.6 Configuration Management
7.7 Process Assurance
7.8 Certification Process
   7.8.1 Certification and Regulatory Authority Coordination
   7.8.2 Certification Planning
   7.8.3 Additional sections may be necessary
• Life Cycle Data
8. MODIFICATIONS TO SYSTEMS OR AI ITEMS

8.1 Machine Learning Based Operations and Maintenance
8.2 Data Selection and Utilization
*Note: Authors should consider Section 6 of ARP4754 for input*
8.3 Recertification
SAE G34 / EuroCAE WG-114 Merger Presentation

WG-114 Co-Chair - Christophe Gabreau
WG-114 Co-Chair - Christian Thurow
G34 Chair - Mark Roboff
G34 Vice Chair - Paula Olivio
G-34 / WG-114 Merger

• **Our Vision:** a fully merged group, with common goals, common sub committees, common meeting schedules, and merged and aligned leadership.

• What does that look like?
**Our Goal:** The development of a standard for the use and development of AI technology in aerospace systems (this entails both airborne and ground, e.g. ATC)

**Our Timeline:** Release of the V1 standard in the autumn of 2022, with the release of a statement of concerns report and a Taxonomy report in the summer of 2020
The entire group will be using **SAE Standard Works** as our main working tool and virtual environment

- As per EUROCAE policy, a copy of all Agendas/Calling Notices, Minutes, Drafts, and Milestones will also be placed on the EUROCAE website

- All documents on both websites should clearly state WG-144 and G-34
We will have three (3) face-to-face meetings a year
- Years 1+2 - alternate between North America and Europe
- Years 3+ - Expand to rest of the world
- Each meeting will be four (4) days in length

- Meetings will be run in an alternating fashion between leads from G-34 and WG-114
Leadership and Executive Committee meetings will continue in their established cadence.

General Body meetings will be renamed Virtual Plenary meetings and will be held monthly.

- The monthly cadence of Virtual Plenary meetings will be reviewed after six (6) months.

Meetings will be run in alternating fashion between G-34 and WG-114 leadership. Agendas will be shared within the leadership team 48 hours in advance to allow for comments by all leaders.
Sub-Committees and Teams will be renamed *Sub-Groups*

- Sub-Group meeting cadence will be based on need (a continuation of current practice)

- Each sub-group will be co-chaired, with one chair from G-34 and one chair from WG-114

- The current sub-committee and team structure will be dissolved upon completion of the Statement of Concerns. A new structure will be based on the AS6983 standard skeleton.
• SAE and EuroCAE have different means for decision-making: SAE votes and EuroCAE operates on consensus.

• For major items, voting will continue for SAE G-34 members. Each issue will be discussed until all comments have been addressed and consensus is achieved. Afterwards, an SAE G-34 vote can take place.

• Major items include:
  • Organizational structure: mergers, standing up committees, dissolving committees, leadership elections
  • Organizational direction: standing up AIRs, ARPs, and standards
• For document balloting, SAE and EuroCAE will continue to operate independently via existing procedures

• For minor items (i.e. passing of minutes, points of order,) we will continue to do an informal voice vote (aye vs nay)

• Face-to-Face meeting locations will be determined by the combined leadership team

• G-34 membership and voting requirements will not change
SAE G34 / EuroCAE WG-114 Merger Discussion and Vote

WG-114 Co-Chair - Christophe Gabreau
WG-114 Co-Chair - Christian Thurow
G34 Chair - Mark Roboff
G34 Vice Chair - Paula Olivio
We will be back at: 10:55 Eastern
Proposal for New Sub-Group Structure

WG-114 Co-Chair - Christophe Gabreau
WG-114 Co-Chair - Christian Thurow
G34 Chair - Mark Roboff
G34 Vice Chair - Paula Olivio
G34/WG114 Organizational Structure

G34 Chair / Vice Chair
WG-114 Co-Chairs
G34 & WG114 Secretaries
G34 & WG114 Tech Advisors
SAE & EuroCAE Admins

Subgroup Co-chairs
Sub Group 1
Sub Group 2
Sub Group 3
Sub Group N

Plenary Members
(Includes all G-34 and WG-114 participants on either roster. G-34 votes can only be taken by G-34 voting members.)

G-34/WG-114 Leadership Team

Standards Liaisons
G-32
S-18
ASTM
AVSI

Regulatory Liaisons
FAA
EASA
TCCA
ANAC
And More...

G-34/WG-114 Exec Team

G-34/WG-114 Plenary
Proposed Sub-Group Structure

Development

SG2: Data Management for ML

Methodology

SG3: ML Design & Implementation

Considerations

SG4: ML Validation & Verification

Inter-process Considerations

SG5: Safety considerations for AI (Architectural mitigation, Probabilistic assessment...)

Use Case Considerations

SG1: Aircraft, Ground, and ATM Applications

Leadership Team

Steering Board / External Liaisons / Future

Editorial Committee

Future SG: Modifications to ML Systems/Items

Future SG: Process Considerations (Planning, Configuration Management, Quality, Levelling, and Certification)
Considerations

• The Proposed Structure:
  • Aligns to the standards skeleton
  • Puts creating the development methodology at the core
  • Considers the interplay between AI development and systems engineering
  • Reflects the full aviation ecosystem from aircraft, to ATM, to ground
  • Reflects the full array of aircraft types: part-25, part-24, UAS/UAM/ETC, rotorcraft
  • Supports evolving needs, with future sub-committees standing by
In Summary

• Create:
  • SG-1: Aircraft, Group, and ATM Applications
  • SG-2: Data Management for ML
  • SG-3: ML Design and Implementation
  • SG-4: ML Validation and Verification
  • SG-5: Safety Considerations for AI

• Dissolve G34 SC-1, SC-2, SC-3, (once SoC is complete) and SC-5 (once taxonomy is complete)
• Dissolve TM-1 (once taxonomy is complete,) TM-2, TM-3, and TM-4 (once SoC is complete)
Proposed Timeline

- Discussion at next Virtual Plenary (Thursday, 16 April)
- Consensus and Vote at 7 May Virtual Plenary
- Chair Nominations to Occur 7 May through 14 May
- Chair Appointments by 15 May
- New Sub-Groups launched by 1 June
Liaison Presentations
Liaison Presentation Order

• S-18/WG-63/S-18 UAS - Steve Beland - 10 minutes
• G-32 - Chris Sunberg - 15 Minutes
• ISO/IEC JTC SC-42 Update - 15 Minutes
• AVSI - Dave Redman - 10 Minutes
• ASTM - Jonathan Daniels - 5 Minutes
• EuroCAE Liaisons Presentation - 5 Minutes
EXTERNAL ORGANIZATIONS AND STRATEGY DISCUSSION

Virtually in Brussels, April 1, 2020

G-34: Artificial Intelligence in Aviation
Chair: Mark Roboff
SAE Committee Trends and Industry Activity

<table>
<thead>
<tr>
<th>Organization</th>
<th>G-34 Liaison</th>
<th>Status</th>
</tr>
</thead>
</table>
| S-18 & WG-63 Aircraft and Sys Dev and Safety Assessment Committee | Steve Beland | • Main effort to finish & ballot **ARP4754B** and **ARP4761A** this year
• Also big effort to finish **AS7209**: Development Assurance Objectives for Aerospace Vehicles and Systems
• Also working Aerospace Information Reports at lower priority:
  • **AIR6219**: Use Of Modeling And Tools For Aircraft Systems Development – A Strategy For Development Assurance Aspects With Examples
  • **AIR6913**: Using STPA During Development and Safety Assessment of Civil Aircraft
  • **AIR7121**: Applicability of Existing Development Assurance and System Safety Practices to Unmanned Aircraft Systems (under S-18UAS (co-chaired by G-34’s Cory Laflin and Steve Beland)
• Monitoring other industry activities of common interest to G-34:
  • SAE G-32 Security
  • SAE HM-1 IVHM
  • WG-105 UAS
  • ANSI UAS Standards Collaborative Roadmap
  • ASTM F-38 Unmanned Aircraft Systems
• Next Joint meeting April 20-24 virtually (instead of in Budapest) |
| Overarching Properties Working Group (aka FAA Streamlining Assurance Workshop) | Steve Beland | • Defined 3 Overarching Properties (OPs) in 2016 that a system should possess to satisfy Development Assurance goals, and refined slightly since then. (see my November G-34 presentation for details)
• Most recent meetings were in April & September 2019 regarding Assurance Cases to show how OPs are satisfied, splitting work as:
  • develop ACs, related templates & evidence schemes,
  • define characteristics of good assurance cases
• Meeting April 21-22 Virtually (instead of in Seattle) |
G-32 CYBER PHYSICAL SYSTEMS SECURITY
Liaison Activity with G-34

Christopher Sundberg, GICSP
Woodward, Inc.
G-32 SwA Co-Lead
Agenda/Contents

What are Cyber Physical Systems?
The Connected World – Cyber Physical System Attack Surfaces
Industry Challenges
G-32 Goals and Structure
What are Cyber Physical Systems?

Technologies that combine the cyber and physical worlds and respond in real-time to their environments

Includes

• Electronic parts, assemblies, systems, and systems elements that operate as a single, self-contained device or within an interconnected network providing shared operations

Examples

• wearable medical devices, the smart grid, autonomous vehicles, Supervisory Control and Data Acquisition (SCADA) systems, industrial control systems (ICS), Internet of Things (IoT) systems, Industrial IoT (IIoT), telematics, vehicle charging systems, satellite communication systems, and embedded systems which include software, firmware, and electronics hardware
Vulnerabilities can include
• Software, hardware, firmware, adjacent systems in the network, energy supplies, users

System elements
• Integrated components
• Individual components including hardware, software, and firmware

Exploit paths for attackers
• Systems not adequately designed with security and resiliency
• Intent can range from economic espionage to denial of service to kinetic effect
Threat exists across multiple sectors:
  Defense, automotive, aerospace, healthcare, and many others
  Specific sectors have expertise in issues, however very low volume compared to other sectors

Commonality across industries
  Cyber Physical systems address the areas of concern
  Best practices for mitigating risk and implementing countermeasures
  Interconnections across sectors

- Electronic & Physical Security
- Information Assurance & Data Security
- Software Assurance & Application Security
- Asset Management & Access Control
- Hardware Assurance, Anti-Counterfeit & SCRM
- Life Cycle & DMSMS
- Anti-Malicious & Anti-Counterfeit
- Track & Trace
- Prognostics, Forensics, & Recovery Plans
- Information Sharing & Reporting
Technical experts
• Government
  • Regulatory authorities
  • Defense agencies
• Industry
• Academia

G-32 Subcommittees
• Software Assurance
• Hardware Assurance
• Risk Management
• Systems Security Engineering Overlay

Sectors
  Automotive
  Aerospace
  Defense
  Industrial Controls
  Medical devices
  Insurance

Documents
JA6678
  Cyber Physical Systems Security Software Assurance
  Drafts by July 4 2020, Finalize Dec 7, 2020

JA7496
  Cyber Physical Systems Security Engineering Plan (CPSSSEP)
  Drafts by July 4 2020, Finalize Dec 7, 2020
Structure of documents

**JA7496**
1. Scope
2. References
3. Terms and Definitions
4. Requirements
   1. CPSSEP
   2. System Engineering Design requirements tiers
      [this goes through the “system-v” and the security plan]
5. Appendix
   1. Illustrative Example(s)
6. NOTES

**JA6678**
1. Scope
2. References
3. Terms and Definitions
4. Software Assurance Framework for CPSS
“the level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.” –Defense Acquisition Guidebook

Define process, practice or methodology that can be employed to achieve the goal of Hardware Assurance

Early focus: the need for verification and validation tools that raise the level of assurance for hardware components

Focus on gaps and collaborate with industry standards experts enabling quick integration of the hardware assurance process into the overall CPSS framework
Software Assurance Security Process for developing and maintaining secured and trusted cyber physical software
Standardize approach for scoring vulnerabilities in cyber physical software
Standardize approach for scoring weaknesses in cyber physical software
Up-to-date repositories of best practices for developing software for cyber physical systems
Up-to-date database of tools, tips, and techniques for developing secured and trusted cyber physical software
“to provide a risk-based methodology for identifying key threats and vulnerabilities, as well as providing a process for the prioritization of risk treatment (i.e., avoidance, mitigation, transfer, and acceptance) initiatives for the organization. The risk management framework will be able to consider current and emerging risk sources across the entire system life cycle”

Where possible the framework will leverage existing standards, methods, and perspectives documented by other standards bodies, government institutions, academic researchers and industry groups

Integrated approach across physical, information, cognitive, and social domains to promote resilience
Systems and software engineering processes are the backbone of product development. There are multiple models in use today throughout industry and government, but all of these models rely, to varying extents, on the analytical thoroughness found in the technical processes described in ISO/IEC/IEEE 15288:2015, Systems and Software Engineering — System Life Cycle Processes. These technical processes form what is commonly referred to as the “Systems Engineering V”.

**Software and Hardware assurance associated with CPSS vulnerabilities**
- What tests for verification and validation
- How should rigor be verified and validated
- How to achieve confidence
- Measurement of confidence

**Triggering events**

**Integration of all areas of concern**
AVSI LIAISON ACTIVITIES
Dave Redman
Director, Aerospace Vehicle Systems Institute (AVSI)
1.04.2020
AFE 87 – Machine Learning

- Ran March 2018 – May 2019
- 10 participating organizations
- Final report approved for public release by project committee
  - Report is in final editing
- Overview presented at November 2019 G-34/WG-114 Kickoff Meeting
  (https://www.sae.org/servlets/works/meetingminuteResources.do?comtID=T/EAG34&resourceID=744733)
Recommended Safety Objectives

• Recommendations related to Machine Learning life-cycle
• Recommendations related to Datasets
• Recommendations related to Robustness
• Recommendations related to Safety Assurance
• Recommendations related to Run Time Assurance
• Recommendations related to AI Interpretability
• Recommendations for Community Standards
  – Objectives for training data set curation
  – Objectives for machine learning training
  – Objectives for using ML safety assurance case demonstration
  – Objectives for using simulation and modeling
Select uses cases that consider both a continuous system (e.g. control system) and a classifier (e.g. object detection). The objective of the follow-on work is to validate the processes and objectives recommended by this report. For each use case, the follow-on project should address the following:

• Work an example ML application
• Training dataset use, management, quality factors, and processes
• ML specification
• ML Validation and Verification
• Application of Overarching Properties to ML
• Simulation and Modeling for ML
A follow-on AVSI project is being planned with a target launch date of ASAP. AVSI recommends the following project development schedule:
Initial Considerations

The initial planning meeting expressed the following considerations:

• There may be one or more projects that could be useful

• At least one of these should be based on a use case
  – Appropriately scoped to exercise concerns/concepts outlined in the AFE 87 final report
  – Important to align selected use case with SAE/EUROCAE joint committee

• Other projects focused on promising technologies could be possible to accelerate the availability of tools that support certification of ML
Next Steps

• Next project planning meeting scheduled for 13 April
• AVSI SharePoint site set up to collect inputs.
• Can also email inputs to dredman@tamu.edu & mskerstetter@tamu.edu
• Discuss plans with SAE/EUROCAE joint committee to identify potential synergies (this presentation)

Contact Dave Redman (dredman@tamu.edu) if you are interested in participating in this project
STATUS OF ANSI UASSC ROADMAP V2.0

TO

G-34/WG-114 FIRST PLENARY MEETING

Virtual, 1 April 2020

SAE G-34/EUROCAE WG-114:
Artificial Intelligence in Aviation, Joint International Committee
Chairs: Mark R., Paula O., Christophe G., Christian T.
Others in Leadership: Sachin J., Terri H., Santosh M.
ANSI Unmanned Aircraft Systems Standardization Collaborative (UASSC) Mission and Deliverable

- **Mission**: To coordinate and accelerate the development of the standards and conformity assessment programs needed to facilitate the safe integration of unmanned aircraft systems (UAS) into the national airspace system (NAS) of the United States, with international coordination and adaptability.

- **Deliverable**: A comprehensive roadmap published in December 2018 describing the current and desired standardization landscape for UAS:
  - Publish Version 2.0 in June 2020
  - 60 gaps (no published standard) identified with accompanying recommendations
  - Available as a free download at www.ansi.org/uassc
Objectives of ANSI UASSC

- To foster coordination and collaboration among industry, standards developing organizations, regulatory authorities, and others on UAS standardization issues, including pre-standardization research and development
- To clarify the current and future UAS standardization landscape and enable stakeholders to better focus standards participation resources
- To provide a basis for coherent and coordinated U.S. policy and technical input to regional and international audiences on UAS standardization
- To support the growth of the UAS market with emphasis on civil, commercial, and public safety applications

UASSC is NOT developing standards
Catalyst of G-34, and SAE S-18 & AS-4 Committees’ support on Gap A19

- Gap A19: Enterprise Operations: Level of Automation / Autonomy / Artificial Intelligence (AI)
- **Gap A19 was one of the inputs during establishment of G-34**
- **SAE Committees Involved in Gap A19:**
  - S-18 **Aircraft and System Development and Safety Assessment Committee**
  - AS-4UCS **Unmanned Systems Control Segment Architecture**
  - AS-4JAUS **Joint Architecture for Unmanned Systems Committee**
  - Others
ANSI UASSC Roadmap (v1 dated Dec 2018):

**Significant Activity (Feb – April 2020)**

- v2 published on 4/1/2020 (public comments open for 30 days)
- Monthly Steering Committee (SC) and WGs Meetings
- Additions in v2 (UAS System Safety; Package Delivery UAS; Caro Transport UAS; Advanced Air Mobility; Pax Transport UAS; etc.)
- ANSI Participated in NATO Workshop on Use of Civil Standards, Greece, 25-27 Feb 2020

**Upcoming Activity**

- Standards Panel Presentation at AUVSI Xponential, Boston, 4-7 May 2020 (Moderator: Jim from ANSI)
- SC & WGs Activities, Feb – Jun, 2020
- Disposition of public comments, May – June 2020
- Outreach at FAA UAS Symposium, Baltimore, June 2020
- Publish ANSI UASSC Roadmap v2 in June 2020
Questions ?

Ritesh Ghimire
➢ Engineer, AUS-420 Technical Support Branch
➢ FAA Lead on All SAE UAS Activities
➢ Custodian of ANSI UASSC Roadmap on FAA’s behalf

FAA UAS Integration Office
ritesghimire@faa.gov
EUROCAE Targeted Liaisons

**EUROCAE WGs**
- WG-63 (Complex A/C systems)
- WG-72 (Aeronautical Systems Security)
- WG-103 (Independent Non-Cooperative Surveillance System)
- WG-104 (System-wide Information Management services)
- WG-105 (Unmanned A/C Systems - UAS)
- WG-112 (Vertical Take-Off and Landing – VTOL)

**Others**
- EUROCONTROL AI Group
- JARUS (Joint Authorities for Rulemaking on Unmanned Systems)
- ISO/IEC JTC 1/SC 42 (Artificial Intelligence)
- ANITI/DEEL (French Research project on Embedded AI)
- FAS (Forum for Aeronautical Software)
- High-Level Expert Group on Artificial Intelligence (AI HLEG)
Call for liaison members

- WG114 members will be identified from the table of competence (Santosh’s Survey)

- Liaison role: Coordination between both groups so that
  - No activities overlap
  - Progress awareness
  - Identification of potential impacts on both standards scope
WG-72 – Structure

EUROCAE Technical Programme Manager
Anna Guéган

WG-72 leadership
Chair: Cyrille Rosay (EASA)
Secretary: Clive Goodchild (BAE Systems)

Joint with RTCA SC-216
Chair: David Pierce (GE)
Secretary: Sam Masri (Honeywell)

WG-72 SG 2
SG Chair: Kristof LAMONT (EUROCONTROL)
SG Secretary: Matt Shreeve (Helios)
ED-205A to be launched

WG-72 SG 3
SG Chair: Judicaël Gros-Désirs (Airbus)
SG Secretary: Frédérique Dauvillaire (Thales)
ED-XXX
Industry Editor: TBD
ED-204A
Industry Editor: Kai Florian Tschakert (LH)

WG-72 SG 4
SG Chair: Stefan Schwindt (GE)
SG Secretary: Andy Boff (Helios)
ED-201A
Industry Editor: Clive Goodchild (BAE Systems)
The WG-72 Aeronautical Systems Security (ASS) shall address the cybersecurity for Aeronautical Information Systems (AIS) from an air-ground and end-to-end perspective from information production, processing, management, communication to operational usage and to maintenance. AIS cybersecurity therefore encompasses the aircraft, supporting infrastructure including communication and the supply chain.

WG-72 will develop Aeronautical Information System Security guidelines addressing the cybersecurity objectives and specifying the cybersecurity requirement including the operational concept rather than technological solutions in order to ensure their stability over time.

WG-72 will adopt a holistic approach, addressing cybersecurity and safety-related topics throughout the entire lifecycle of products/services developed, manufactured, operated and maintained by many different civil aviation stakeholders in both the air and ground segments.

Within the scope described above WG-72 will therefore address both the airborne systems and ground systems in their end-to-end interdependence from an operational and cybersecurity standpoint recognizing, however, that cybersecurity requirements may apply differently for airborne and ground systems.

WG-72 shall serve as a resource and coordinator for Aeronautical and ATM information security-related matters with all EUROCAE Working Groups. As part of its performance-based rulemaking, and in light of the emerging competency as per the new Basic regulation, EASA will increasingly rely on industry standards, including the ones on Cybersecurity in Aviation. Due to its long-term experience, WG-72 will play a pivotal role in this realm of industry standards.
The WG will in particular:

- develop and maintain acceptable processes and methods of compliance addressing security issues in support of existing safety processes and analytical methods (e.g. ED-79, ED-135), including associated methods/processes for ground-based systems.
- develop and maintain guidelines and objectives for evaluating security architectures and security procedures, demonstrating their compliance with security and safety objectives.
- determine and maintain design and operational compliance methods appropriate and adequate for the application of security solutions to safety-related functions.
- address the necessity and objectives for the management of security “events” and guidelines for “response” to detected or suspected attacks.
- address requirements and guidance for post-response recovery, including identification of affected systems, restoration of system configurations, notification requirements, and other related activities.
WG-72 – Published documents:

- ED-201: AISS Framework Guidance Document
- ED-203A/DO-356A: Airworthiness Security Methods and Considerations
- ED-205: Process Standard for Security Certification and Declaration of ATM/ANS Ground Systems
- ER-013: Aeronautical System Security Glossary
- ER-017: International Aeronautical Information Security Activity Mapping Summary


ED-205A: Process Standard for Security Certification and Declaration of ATM/ANS Ground Systems

ER-013A: Aeronautical System Security Glossary
The European Cyber security for aviation Standards Coordination Group

- Coordination of standardisation activities to ensure no duplicate
- Identification of gaps and overlaps, and observation of how other domains are addressing these (e.g.: ICT, Industry)
ECSCG - Membership

- ACI-Europe
- ARINC
- ASD
- ASTM
- A4E
- CANSO
- CEN
- EASA
- EC
- ECAC
- EDA
- ETSI
- EUROCAE
- EUROCONTROL
- IATA
- ISO
- SAE
- SESARJU
Thank you!

For any question, please contact:

Anna Guégan, CISPP
Technical Programme Manager

Phone: +33 1 49 46 19 67
Anna.guegan@eurocae.net

Le Triangle, 9-23 Rue Paul Lafargue
93200 Saint Denis - France
www.eurocae.net
Thank You / Stay Safe / Stay Healthy