Safecomp 2023

Certification Use Reliance when Integrating Machine Learning Solutions in Safety related and / or critical systems

Emmanuelle Escorihuela
AI transformation Leader for A/C systems
Airbus Commercial

Gary Brown
Advanced Aircraft Safety Specialist + AI Referent
Airbus Commercial

AIRBUS

Why Considering Machine Learning in A/C Systems ?

[Airbus Amber]

Landing
Generalised Autoland

Taxi
Assistances to manage crew workload

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.

Why Machine Learning is a challenge ?

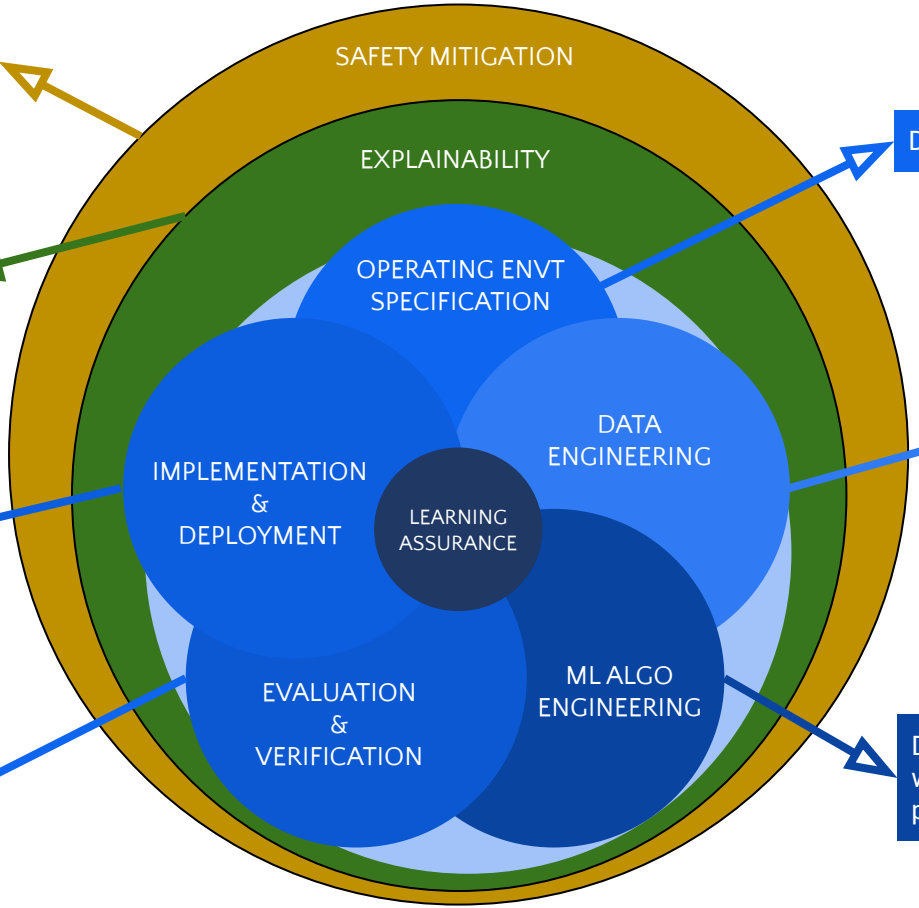
[Airbus Amber]

Design efficient **Monitoring function** to switch to **Fallback** safe solution

Ensure **Explainability** targeting Developers, Users, Auditors

Ensure same perfo on embedded HW target
Ensure **Real-time perfo** (WCET)

Characterise perfo on ODD
Robustness
Stability
Uncertainty



Define **Operational Design Domain**

Get the right data (**Representativeness, completeness**...)

Demonstrate the model **generalise** well and (good prediction on previously unseen data)

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.

The three pillars : Certification, Use, Reliance (CURe)

[Airbus Amber]

CERTIFICATION - The Regulator awards Approval with or without conditions against a set of defined requirements at an amendment of CS.25 (or other) under Modification Part 21 (Major, being Novel). For now likely specific Certification Review Item (CRI) or Paper driven from a Special Condition (SC)

Reliance - By adding the ML into the Aircraft product then its Credit or not must be RISK assessed to understand any uncertainties behind miss behaviours that are to be tolerated or independently functionally designed against or maintained. This is as per ARP 4761 FHA at 3.2 and ARP 4754A at 6.1

USE function - The functional design intent from learning is known and the solution is best served with by an AI ML supervised. It has a Problem statement "Selling Point", be it Aircraft operational Performance, Maintenance, Safety, or Environmental improvements that the customer would value

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.

Use – Obstacle Detection on a Runway

[Airbus Amber]

USE function - The Problem Statement here is that occurrence data indicates that some ground collision events are coming from human error in the Cockpit and/or ATC. The USE function here is, that, as a safety improvement, an alerting function based on ML-based computer vision will mitigate and reduce these future events

Airbus UpNext Dragonfly Demonstrator - Taxi Phase

<u>Design Intent</u>: Alert the cockpit crew of potential collision during taxi phase

<u>System Architecture</u>:

ML Constituent	Segmentation Task
Conventional SW	Estimation of the distance Collision risk Warning

<u>Benefits</u>: Safety enhancement

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.

Reliance – Obstacle Detection on a Runway

[Airbus Amber]

		Actual	
		Positive	Negative
Predicted	Positive	True Positive	False Positive
	Negative	False Negative	True Negative

For a Classification solution which is Image based as in the Ground Collision Avoidance then the RISK assessment must consider the *CONFUSION Matrix*.

The KEY need is to ascertain the worst case credible effects if the Prediction does not match the Actual real world as seen by the camera

A **False Positive** - provides a Prediction such as an impact with a stationary or moving object is likely and a Warning is issued (audio & visual HMI). There is no actual threat/hazard, so it is a False accusation and if frequent in occurrence would negate the "Selling Point" and trust

A **False Negative** - provides no Prediction, so no Alarm of audio and visual (attention getter) and the Pilot relies on normal situational awareness and Air Traffic Control (ATC), so its as if the ML function is NOT Available. There is a loss of "Selling Point" and a risk to safety if too much trust is placed

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.

Certification – Obstacle Detection on a Runway

[Airbus Amber]

Part 21 permits modification of already certified aircraft so long as the changes are not a regression to safety and airworthiness. ML is a novel integration so Major and thus not under Design Organisation Approval (DOA) privileges.

Adding a new Use function with an ML solution will be assessed under a **CRI** Approval and will be subjected to compliance to the following:

CS25.1301(a)1 - *Be of a kind and design appropriate to its **intended function***

CS25.1301(a)3 -*Be installed according to limitations specified for that equipment*

CS25.1309(a) - ***perform as intended under the aeroplane operating and environmental conditions**.*

CS25.1309(b) - *Behaviour under Failure (anomalous or aberrant)*

CS25.1309(c) - ***be designed to minimise flight crew errors** that could create additional hazards*

CS25.1302(d) - *To the extent practicable, installed equipment must enable the flight crew to manage errors resulting from the kinds of **flight crew interactions with the equipment that can be reasonably expected in service***

CS25.1319 - *Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary*

CS25.1322(d) - *The alert function must be designed to minimise the effects of **false and nuisance** alerts***.**

Assurance Level allocation by the safety process (ARP 4761/4754) will determine the ARP 6983 **objectives** for evidence substantiation (review, simulation, inspection, analysis, test). The **Performance Metrics** at **Inference acceptance are essential for safety development** Explainability (- uncertainties) supporting the normal System Safety Assessment MoC 3 demonstration. See ARP 4754A at 5.4 & table 6-1 for DAL assignment and read for Assurance Level equivalent (AL 3 = DAL C)

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.

Generalization – How confident to be ?

[Airbus Amber]

It is currently in debate and under research that a Failure Mode for an ML model can be expressed in a quantitative Failure Rate per Hour of Flight and added to a casual contribution inside a Failure Condition Model.

This notion implies that a compliance 1309(b) demonstration must include the ML prediction (False Positive or False Negative classification/linear regression) in the Safety Objective compliance as done for traditional hardware (deterministic) with random failures and satisfied by a Failure Modes & Effects Analysis (FMEA) & its Summary (FMES).

The current requirement of CS25.1309(b), ARP 4754A supported and DO-178C guidance do not offer the same notion to a software item, rather a development assurance approach is applied to ensure design intent correctness with any found defects either corrected or maintained in Open Problem Reports. A credit DAL is allocated in the Software item accomplishment summary and Declaration of Design Performance (DDP). The software item is considered as 0 (or 1).

The **right ML constituent balance** should be to maintain the same discipline as applied for software and complex electronic hardware, see ARP 4754A at 3.1, which is by review, simulation, inspection, test, analysis against defined learning objectives proportional to the safety contributions.

The MLC is from a learning process and not by the traditional design approach, at the inference test pass it is a single mathematical construct algorithm **black box** and its behaviour cannot be guaranteed other than the same input will always have the same output. Care must be taken to avoid amplification of the learning error when translating the ML mathematical construct algorithm into a software algorithm, mitigation strategies need to be applied.

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.

Generalization – How confident to be ?

[Airbus Amber]

The **Reliance** placed must be understood from the Functional Failure appreciation of the *Confusion Matrix*. Contributions to higher Safety Effect are permitted but alone the worst case credible effect is Limited. **LoC** is an outcome of the implementation from ARP 6983 allocation of objectives and any deviations.

Reliance - **Aircraft Safety Effect**	**Approval**	**Assurance Level**	**Level of Confidence (LoC)** Required - Qualitative tolerance
Potential Unsafe: ***EASA Concept Paper (draft 2.0) anticipates a limitation on validity at AL 1 & 2***	**Limitation**	**AL 1 (DAL A)**	Very HIGH
		AL 2 (DAL B)	HIGH
Major	Yes (conditions likely)	AL 3 (DAL C)	Medium
Minor	Yes alone	AL 5 (DAL D)	Low
No Safety Effect (NSE)	Yes alone	None (DAL E)	Very Low

Accident - *Catastrophic Hull Loss Impact at speed. Failure Condition - Loss of Aircraft from Collision*. Contribution of ML Use function reliance is a Major effect and thus a Medium LoC is required from ARP 6983 objectives substantiation with or without deviations

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.

Conclusions of **CURe**

The integration of ML unto Aircraft platforms must not cause a decrease in safety or airworthiness (Part 21).

ML predictions are an outcome of sufficient representative data, that through learning aim to be as close as possible to the ground truth or actual real world - but there will be residual errors from the bias verses variance trade-off.

Each ML Use function has a "Selling Point" which is more than just being novel, it should aim to be a safety improvement, or where not an operational or environmental gain or maintenance benefit etc.

Safety specialists, unlike in traditional design development with known solutions are faced with a learned mathematical construct algorithm that can only be influenced by development Öbjectives' allocated based on an assessment of the Confusion Matrix at supervised be it classification (binary) or linear regression (non binary).

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.

Conclusions of **CURe**

[Airbus Amber]

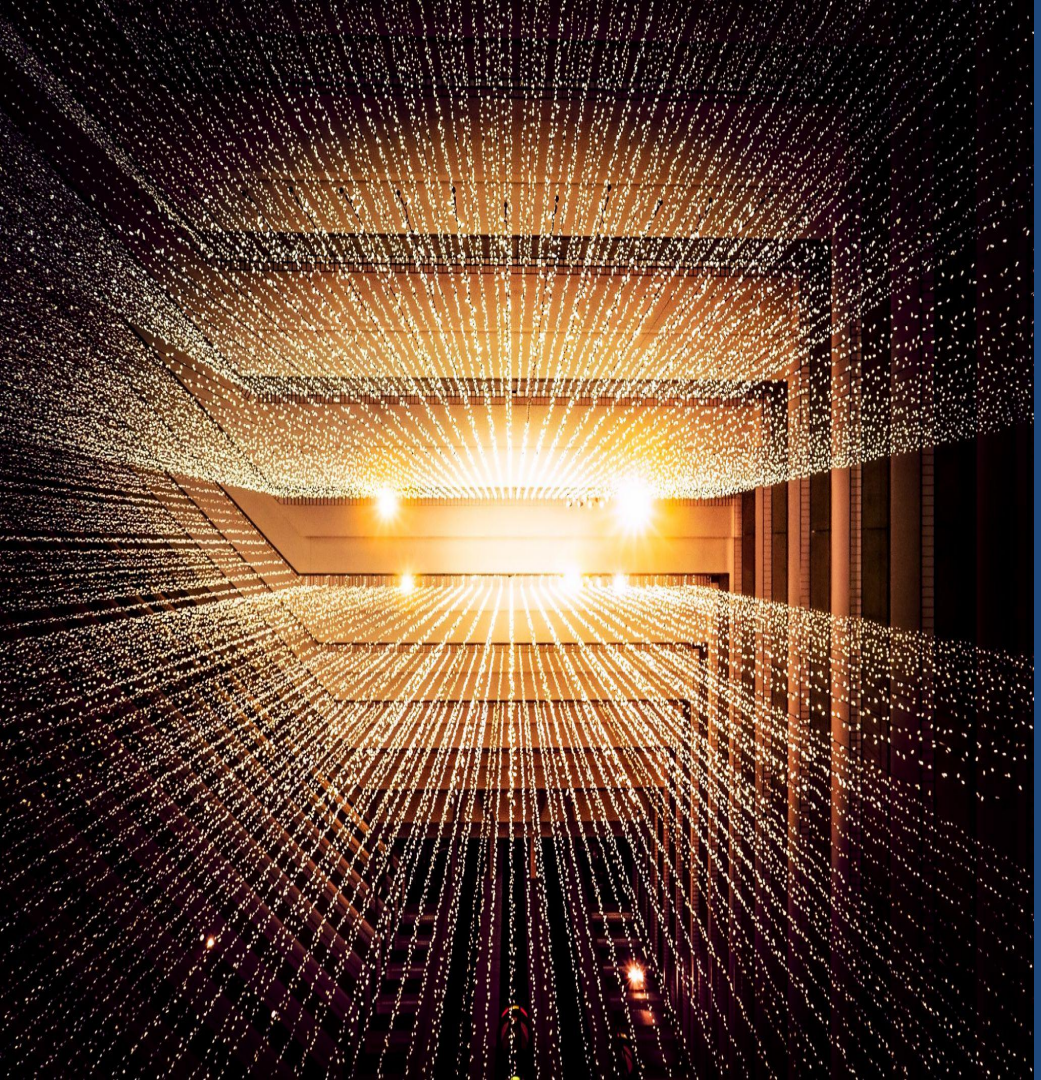
The forthcoming SAE/Eurocae **ARP6983** standard will set **objectives**, that Industry can wish to use to gain Approval. The objectives are to be proportionate to the safety risk so less harsh at AL 5 than AL 3.

Performance & safety are synonymous, Performance Metrics at classification like accuracy, precision, recall or F1 score are key measuring criteria for residual risk acceptance. They should be allocated as safety requirements in the specification.

Using the **three Pillars CURe approach** offers an holistic control of an ML Use function integration. By ensuring a fit for purpose ML Use function, that is understood by safety screening for miss behaviour and its platform **Reliance** then Certification can be better assured using a **Level of Confidence** qualitative credit as done for Software and complex items. The ML constituent Accomplishment Summary with the DDP will capture this credit, with any justified Open Problem Reports and Limitations or restrictions.

AIRBUS

Sept 2023 - This document and its content is the property of Airbus. It shall not be communicated to any third party without the owner's written consent. All rights reserved.



Q&A

AIRBUS

Thank you

© Copyright Airbus OPERATIONS - 2023) / Safecomp 2023 - Certification Use Reliance with ML

This document and all information contained herein is the sole property of Airbus. No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the expressed written consent of Airbus. This document and its content shall not be used for any purpose other than that for which it is supplied.
Airbus, its logo and product names are registered trademarks.