AISafety 2021
IJCAI-21 | Virtual | Aug 19-20, 2021

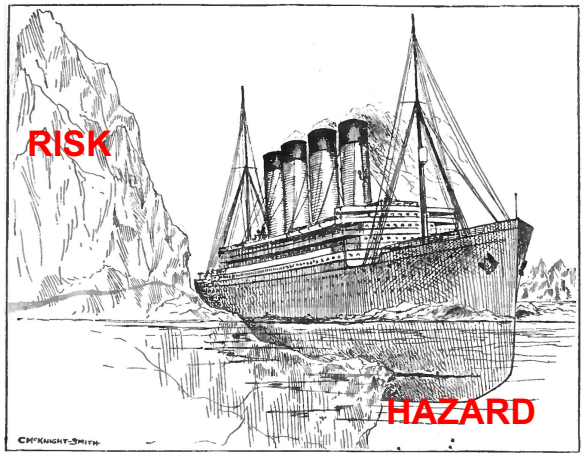
Simulation Qualification for Safety Critical AI-Based Systems

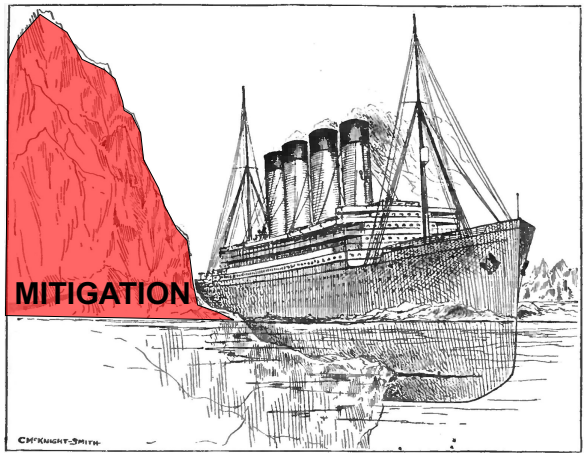
Prof. Dr. Umut Durak

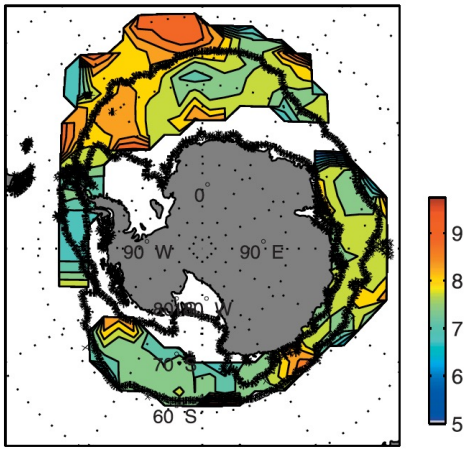
German Aerospace Center (DLR)

DLR

Safety Critical Software and Development Assurance







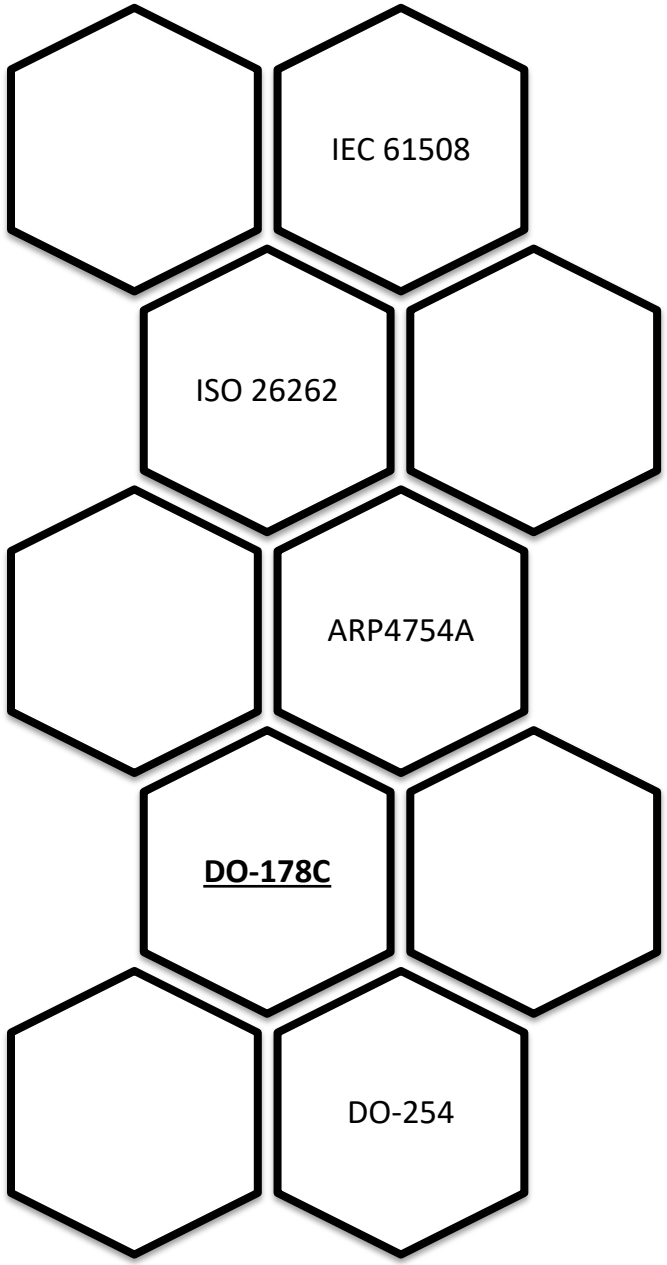
Development Assurance is building confidence in the process that it identifies and removes the errors before the product is delivered

Tournadre, J., Whitmer, K. and Girard-Ardhuin, F., 2008. Iceberg detection in open water by altimeter waveform analysis. *Journal of Geophysical Research: Oceans*, *113*(C8).

Functional Safety Standards

The **required level of rigor** in development assurance depends on failure condition severity and probabilities.

The **standards** provide the guidelines for setting the assurance levels and specify the associated requirements.



Airborne Software Assurance with Objectives

	Objective		Activity	Applicability by Software Level				Output		Control Category by Software Level			
	Description	**Ref**	**Ref**	**A**	**B**	**C**	**D**	**Data Item**	**Ref**	**A**	**B**	**C**	**D**
1	High-level requirements comply with system requirements.	6.3.1.a	6.3.1	●	●	○	○	Software Verification Results	11.14	②	②	②	②
2	High-level requirements are accurate and consistent.	6.3.1.b	6.3.1	●	●	○	○	Software Verification Results	11.14	②	②	②	②
3	High-level requirements are compatible with target computer.	6.3.1.c	6.3.1	○	○			Software Verification Results	11.14	②	②		
4	High-level requirements are verifiable.	6.3.1.d	6.3.1	○	○	○		Software Verification Results	11.14	②	②	②	
5	High-level requirements conform to standards.	6.3.1.e	6.3.1	○	○	○		Software Verification Results	11.14	②	②	②	
6	High-level requirements are traceable to system requirements.	6.3.1.f	6.3.1	○	○	○	○	Software Verification Results	11.14	②	②	②	②
7	Algorithms are accurate.	6.3.1.g	6.3.1	●	●	○		Software Verification Results	11.14	②	②	②	

DO-178C Failure Categories and Assurance Levels

Category	Description	fDAL	iDAL	Assurance Level
Catastrophic	Multiple fatalities, usually with the loss of the aircraft	→	→	Level A
Hazardous	Serious or fatal injury to a relatively small number of the occupants other than the flight crew	→	→	Level B
Major	Physical distress to passengers or cabin crew, possibly including injuries	→	→	Level C
Minor	Routine flight plan changes, or some physical discomfort to passengers or cabin crew	→	→	Level D
No Safety Effect	No affect the operational capability of the aeroplane or increase crew workload	→	→	Level E

Current Airborne Software Landscape

Level A
- Flight Control
- Engine Control

Level B
- Guidance
- Performance

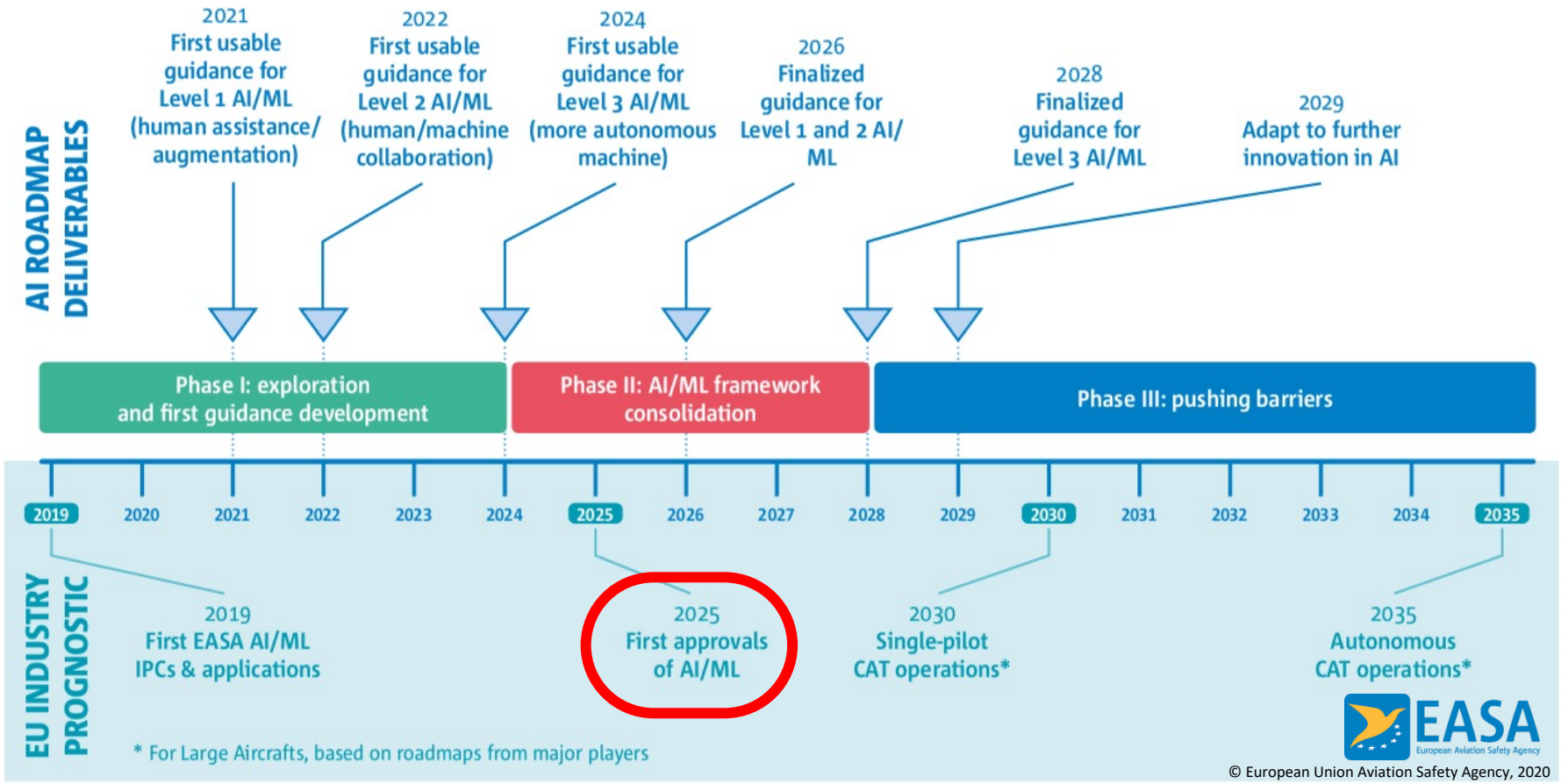
Level C
- Terrain Avoidance
- Maintenance

Level D
- Water Control
- Cabin Lights

Level E
- In Flight Entertainment

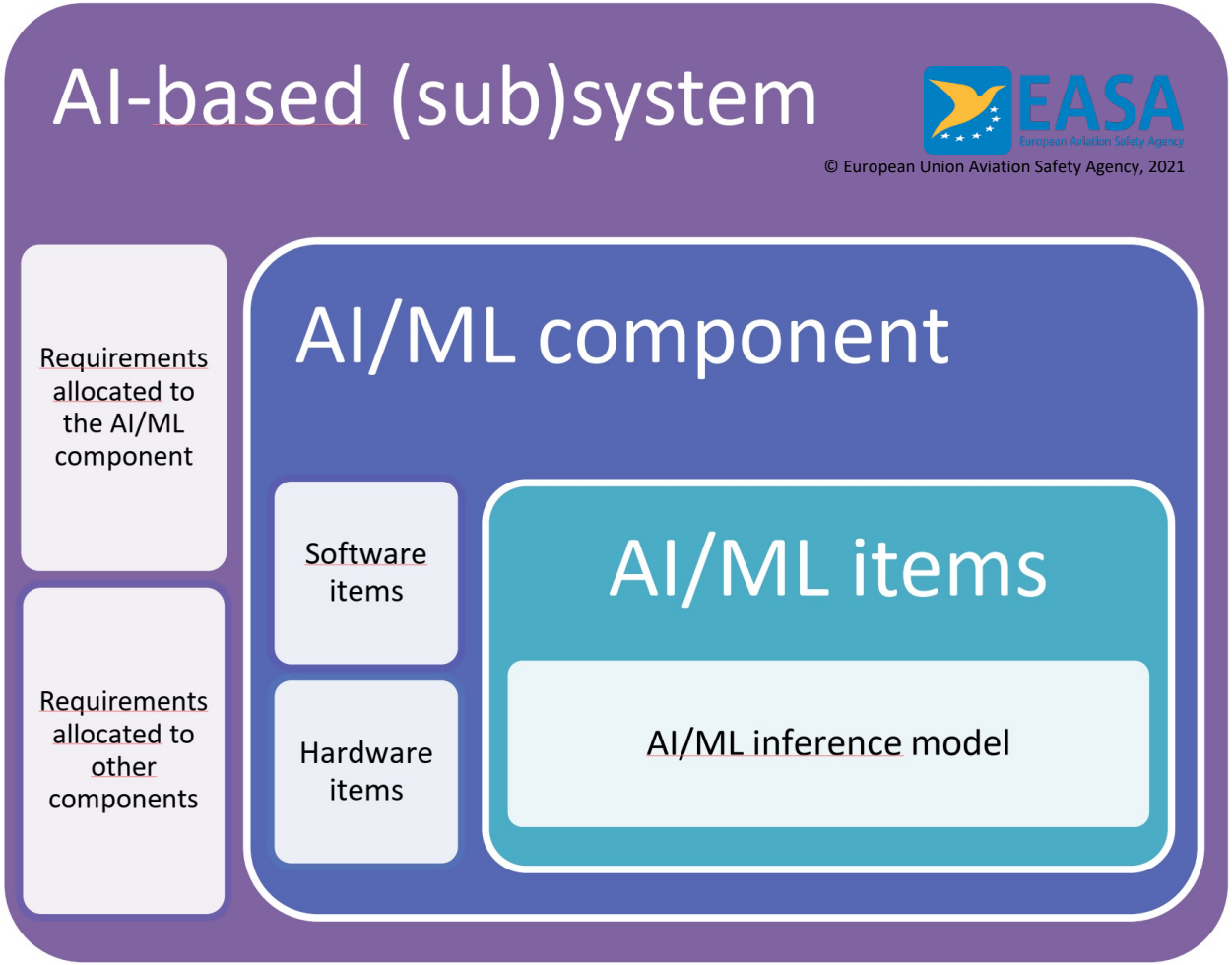
Future Airborne Software Landscape

Level 1 AI/ML : assistance to human	Level 2 AI/ML : human/machine collaboration	Level 3 AI/ML : more autonomous machine
• Level 1A – Routine assistance • Level 1B – Reinforced assistance	• Level 2A – Human performs a function / Machine monitors • Level 2B – Machine performs a function / Human monitors	• Machine performs functions with no human intervention in operations. Human is in the loop at design and oversight time



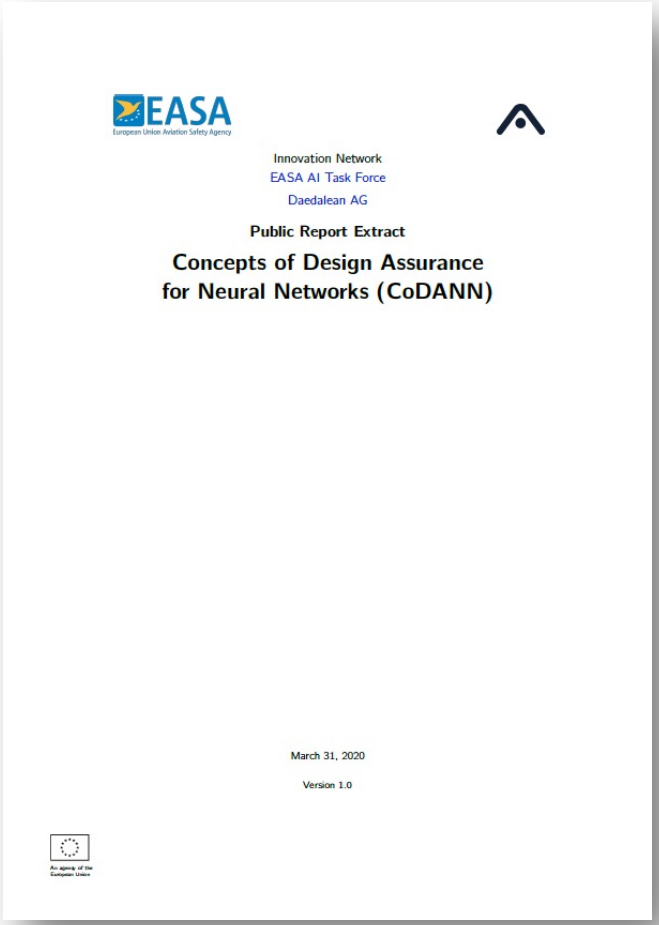
EASA AI Roadmap

AI-Based System



CoDANN

Concepts of Design Assurance for Neural Networks

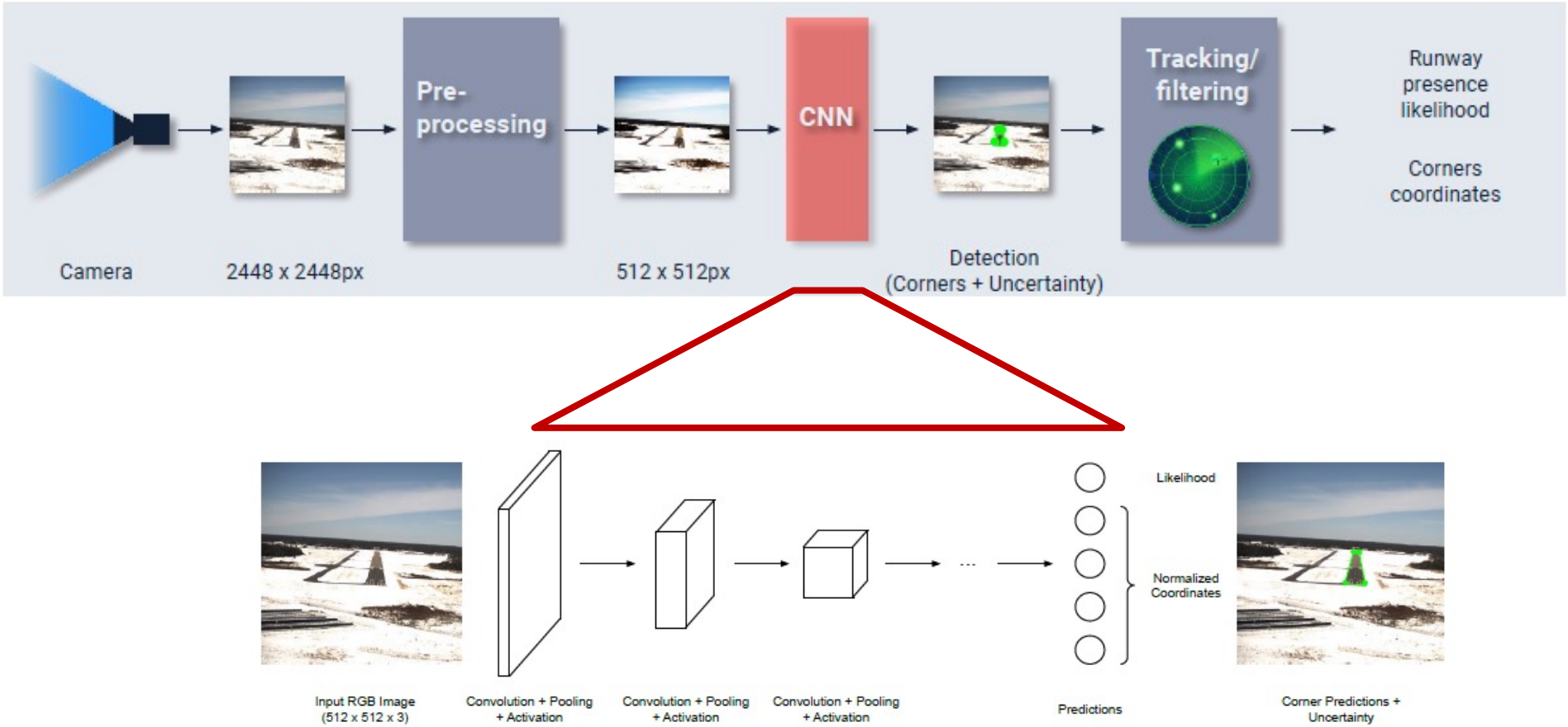


DAEDALEAN
APPLIED INTELLIGENCE

EASA Innovation Partnership Contract (IPC) to Daedalean AG for examining the **challenges posed by the use of neural networks in aviation**

DLR

CoDANN Use Case – Visual Landing Guidance



Simulation in CoDANN

7.2 Synthesized data

Acquiring high-quality data satisfying the requirements of Section 5.1 can be very costly, while it is crucial that machine learning algorithms are tested and trained on a very large amount of data. Consequently, the design and testing of safety-critical machine learning models should rely on *simulated/synthesized data*, for which new data can be acquired at a very low cost once a system is setup. By synthesized data, it is meant *any data that was computer-generated or any data from the target sensors that underwent a processing step that is not included in the target operational system.*

(a) Real image

(b) Synthetic image

Simulation-based Testing AI/ML Drougue Detection Algorithms

AIAA SciTech Forum
6-10 January 2020, Orlando, FL
AIAA Scitech 2020 Forum

10.2514/6.2020-0670

Check for updates

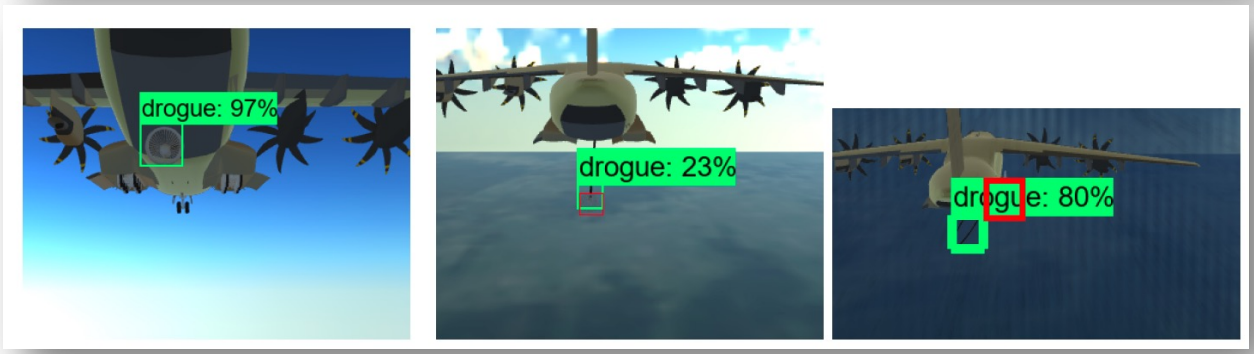
Simulation Based Verification of Drogue Detection Algorithms for Autonomous Aerial Refueling

Oliver Ellis *
Clausthal University of Technology, Department of Informatics, Clausthal-Zellerfeld, Germany

Umut Durak†
German Aerospace Center (DLR), Institute of Flight Systems, Braunschweig, Germany

Drogue detection algorithms are object detection algorithms that are used to detect the drogue basket using a camera in order to automate the docking phase of aerial refueling. Deep learning techniques, particularly Convolutional Neural Networks (CNNs) are receiving more and more interest for the drogue detection problem. The verification of such networks is a recent challenge. This paper proposes a simulation environment to generate test data, a test scenario generation approach to achieve a broad coverage, and an evaluation strategy. It not only integrates them in a testing workflow, but also demonstrates them with an example case.

4/6.2020-0670



Certification with Simulation Data

"Partial certification credits may still be granted while using a non-conformed test article, provided that the item to be evaluated is simulated with an adequate level of representativity."

[EAS19] EASA. *EASA Generic Means of Compliance Certification Review Item (MOC CRI): Certification credit for Simulator and Rig Testing.* Tech. rep. 2019.

"In order to ensure that credit may be taken from the [simulator/test rig] tests, the [simulator/test rig] must be adequately representative for aircraft systems and flight dynamics. At the same time the limitations for using the [simulator/test rig] must be established. This objective can be achieved by a combination of a controlled development process of the [simulator/test rig], simulator configuration management, system models behavior (crosschecked when necessary with partial system bench or flight test results, analysis, desktop simulation) and engineering/operational judgment. Currently, there is no detailed guidance available on the qualification of simulators or test rigs for use as a Means of Compliance for certification. [...] Relying upon simulation results in arguing safety is typically a practical necessity. Simulation results can be used so long as their accuracy is justified, simulation run coverage is justified, and an appropriate non-zero amount of physical testing is used to validate simulation results."

[UL-4600] Edge Case Research Inc. "UL-4600: Standard for Safety for the Evaluation of Autonomous Products". Work in progress. 2019.

Tool Qualification Considerations

"However good the design and however accurate its implementation, the integrity of the system relies on the correct operation of the tools used to create it" *

In simulation based design and test of AI-Based Systems

Correctness of Simulation is a Safety Concern!

*Hobbs, C. 2019. Embedded software development for safety-critical systems. CRC Press.

DO-330 Software Tool Qualification Consideration

“an error in the tool may have a negative impact on software functionality if the tool inadequately performs its intended functions”

Tool Qualification guarantees that the tool is developed and verified using an adequate process in order to obtain a confidence in the tool functionality .

DO-330 specifies the tool life cycle process requirements with respect to each Tool Qualification Level (TQL), TQL-1 being the most rigorous and TQL-5 being the least.

Tool Qualification Level Determination

Software Level	Criteria		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

Criteria 1: A tool whose output is part of the airborne software and thus could insert an error.

Criteria 2: A tool that automates verification process(es) and thus could fail to detect an error, and whose output is used to justify the elimination or reduction of:

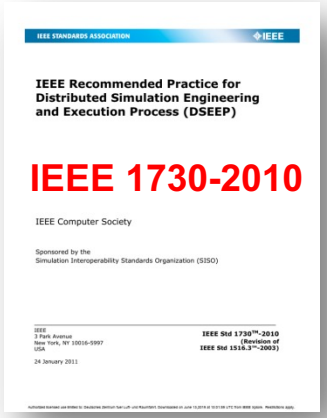
1. Verification process(es) other than that automated by the tool, or
2. Development process(es) that could have an impact on the airborne software.

Criteria 3: A tool that, within the scope of its intended use, could fail to detect an error.

DO-330 Objectives for the Tool Design Process

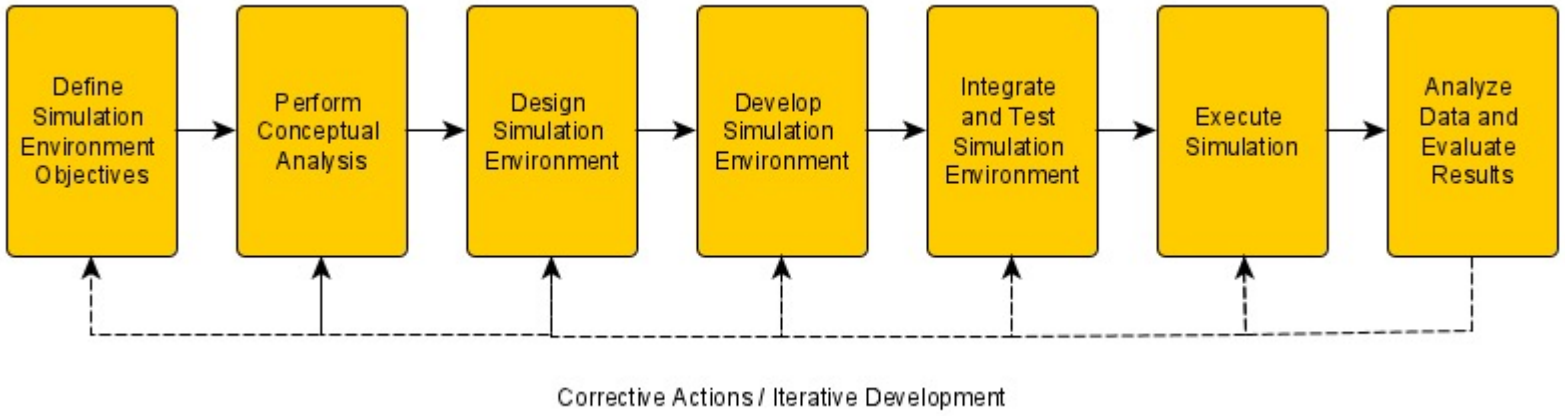
Objective		Activity	Applicability by TQL					Output		Control Category by TQL				
Description	**Ref.**	**Ref.**	**1**	**2**	**3**	**4**	**5**	**Description**	**Ref.**	**1**	**2**	**3**	**4**	**5**
Tool architecture is developed.	5.2.2.1.a	5.2.2.2.a 5.2.2.2.b 5.2.2.2.e 5.2.2.2.f 5.2.2.2.g	❍	❍	❍	❍		Tool Design Description	10.2.2	①	①	①	②	
Low-level tool requirements are developed.	5.2.2.1.b	5.2.2.2.c 5.2.2.2.e 5.2.2.2.f 5.2.5.b	❍	❍	❍			Tool Design Description Trace Data	10.2.2 10.2.7	① ①	① ①	① ①		
Derived low-level tool requirements are defined.	5.2.2.1.c	5.2.2.2.c 5.2.2.2.d	❍	❍	❍			Tool Design Description	10.2.2	①	①	①		

Simulation Engineering Process

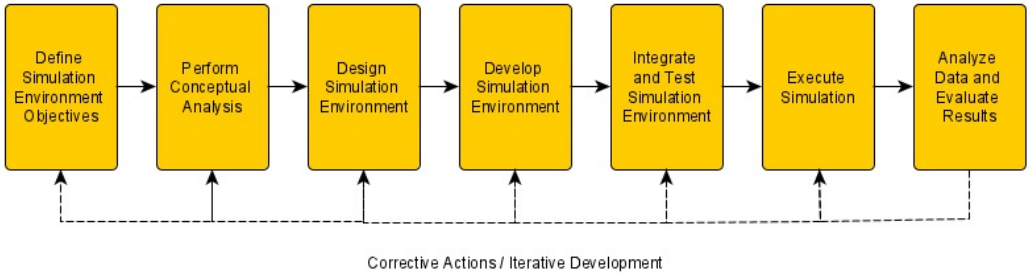


IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process

A generalized process for building and executing distributed simulations



Proposed Simulation Qualification Framework



IEEE 1730 DSEEP as Simulation Qualification Process

Criteria	Development Assurance Level			
	A	B	C	D
1	SQL1	SQL2	SQL3	SQL4
2	SQL4	SQL4	SQL5	SQL5
3	SQL5	SQL5	SQL5	SQL5

Simulation Qualification Levels

Objective		Recommended Tasks	Applicability by SQL					Output		Control Category by SQL				
Description	Ref.	Ref.	1	2	3	4	5	Description	Ref.	1	2	3	4	5
Develop scenario	4.2.1	4.2.1.2	❍	❍	❍	❍		Scenario(s)	4.2.1.3	ⓘ	ⓘ	ⓘ	ⓘ	
Develop conceptual model	4.2.2	4.2.2.2	❍	❍	❍	❍		Conceptual Model	4.2.2.3	ⓘ	ⓘ	ⓘ	ⓘ	
Develop simulation environment requirements	4.2.3	4.2.3.2	❍	❍	❍	❍		Simulation Environment Requirements Simulation Environment Test Criteria	4.3.3.3	ⓘ	ⓘ	ⓘ	ⓘ	

Simulation Engineering Objectives

Simulation Qualification Level Determination

Criteria	Development Assurance Level			
	A	B	C	D
1	SQL1	SQL2	SQL3	SQL4
2	SQL4	SQL4	SQL5	SQL5
3	SQL5	SQL5	SQL5	SQL5

Criteria 1: A simulation whose output is part of the system and thus can introduce an error.

Criteria 2:. A simulation that is used in verification and validation of the system and this could fail to detect an error, and whose output is used to justify the elimination or reduction of another validation and verification effort

Criteria 3: A simulation, within the scope of its intended use, could fail to detect an error.

Perform Conceptual Analysis Step Objectives

Objective		Recommended Tasks	Applicability by SQL					Output		Control Category by SQL				
Description	**Ref.**	**Ref.**	**1**	**2**	**3**	**4**	**5**	**Description**	**Ref.**	**1**	**2**	**3**	**4**	**5**
Develop scenario	4.2.1	4.2.1.2	❍	❍	❍	❍		Scenario(s)	4.2.1.3	①	①	①	①	
Develop conceptual model	4.2.2	4.2.2.2	❍	❍	❍	❍		Conceptual Model	4.2.2.3	①	①	①	①	
Develop simulation environment requirements	4.2.3	4.2.3.2	❍	❍	❍	❍		Simulation Environment Requirements Simulation Environment Test Criteria	4.3.3.3	①	①	①	①	

Sample Use Case

AI-Based System: Autonomous Aerial Refueling

Assurance Level: A

Simulation Utilization: Data Generation for Training

Qualification Criteria: 1 **(**simulation output is part of the system and thus can introduce an error)

Simulation Qualification Level: SQL1

Example Objectives:

- Simulation Conceptual Model (IEEE 1730-2010 Section 4.2.2) need to be developed.
- Simulation Conceptual Model (IEEE 1730-2010 Section 4.2.2) need to be verified independently that it represents the domain adequately.

Summary

Future AI-based systems will rely on simulation, probably for both design and verification

Simulation fidelity itself is not an adequate (easy) measure

Development assurance techniques need to be applied for engineering simulations for safety-critical AI-based systems

IEEE 1730-2010 DSEEP is a good point to start

AISafety 2021
IJCAI-21 | Virtual | Aug 19-20, 2021

Simulation Qualification for Safety Critical AI-Based Systems

Questions and Answers

Prof. Dr. Umut Durak
German Aerospace Center (DLR)

DLR