EASA
European Union Aviation Safety Agency

Rotorcraft and VTOL Symposium

Development Assurance and Safety Assessment Processes (AMC 2510)

10-12-2019

Arne Malcharowitz

Guillaume Soudain

VTOL.2500 General requirements on systems and equipment function

(a) Requirements SC VTOL.2500, SC VTOL.2505 and SC VTOL.2510 are general requirem… able to systems and equipment installed in the aircraft, and should not be used to supersede any oth… requirement.

(b) **Equipment and systems** required to comply with type certification re… ements or operating rules, or whose improper functioning would lead to a h… **ed so that they perform their intended function throughout the operati…** aircraft is certified.

VTOL.2510 Equipment, systems a…

(a) The equipment and sy… red separately and in relation to other systems, must be designed

(1) eac… ly improbable and does not result from a single failure;

(2) ea… xtremely remote; and

(3) eac… is remote.

(b) The oper… pment and systems not covered by SC VTOL.2500 must not cause a hazard to the aircraft or its occupants … ghout the operating and environmental limits for which the aircraft is certified.

(c) For Category Enhanced, provisions for in-service monitoring of equipment and systems which failure may have hazardous or catastrophic consequences must be established.

This AMC focuses on 2510 (a) and (b), as well as 2500 (b)

Outline of AMC to 2500/2510

1. Purpose
2. Scope
3. References
4. Definitions
5. **Failure conditions classifications and probability terms**
6. **Safety objectives**
7. **Safety assessment process**
8. **Development Assurance processes**
9. **Lift Thrust system considerations**
10. Crew and maintenance considerations

Failure conditions and probability terms

→ VTOL.2510 Equipment, systems, and installations

The equipment and systems identified in SC VTOL.2500, considered separately and in relation to other systems, must be designed and installed such that:

(1) each catastrophic failure condition is extremely improbable and does not result from a single failure;

(2) each hazardous failure condition is extremely remote; and

(3) each major failure condition is remote.

→ AMC 2510 defines the failure conditions and probability terms

→ Similar approach compared to known AMCs

Safety Objectives

→ For **Category Enhanced**, failure conditions that would prevent continued safe flight and landing of the aircraft are considered catastrophic.

→ For **Category Basic**, failure conditions that would prevent a controlled emergency landing of the aircraft are considered catastrophic.

Safety Objectives

	Maximum Passenger Seating Configuration	Failure Condition Classifications			
		Minor	Major	Hazardous	Catastrophic
		Allowable Qualitative Probability			
		Probable	Remote	Extremely Remote	Extremely Improbable
Category Enhanced	-	$\leq 10^{-3}$ FDAL D	$\leq 10^{-5}$ FDAL C (see Note B)	$\leq 10^{-7}$ FDAL B	$\leq 10^{-9}$ FDAL A
Category Basic	7 to 9 passengers	$\leq 10^{-3}$ FDAL D	$\leq 10^{-5}$ FDAL C (see Note B)	$\leq 10^{-7}$ FDAL B	$\leq 10^{-9}$ FDAL A
	2 to 6 passengers	$\leq 10^{-3}$ FDAL D	$\leq 10^{-5}$ FDAL C	$\leq 10^{-7}$ FDAL C (see Note A)	$\leq 10^{-8}$ FDAL B (see Note A)
	0 to 1 passenger	$\leq 10^{-3}$ FDAL D	$\leq 10^{-5}$ FDAL C	$\leq 10^{-6}$ FDAL C (see Note A)	$\leq 10^{-7}$ FDAL C (see Note A)
[Quantitative safety objectives are expressed per flight hour]					

Note B: For FDAL C **no further DAL reduction**, in case the possible alleviation in item development assurance for IDAL D is used

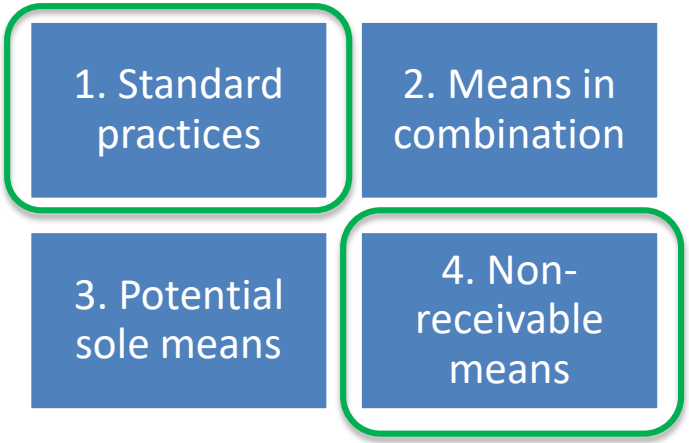
Note A: **no** considerations of the system architecture for a **DAL reduction**

Safety Assessment

- As for any product:
  - The safety assessment process is an **iterative process**, requiring **preliminary assessment steps** to ensure that the proposed system architecture(s) can reasonably be expected to meet the safety objectives
  - The **rigor** of the assessment depends on the system criticality and/or complexity
  - Guidance on **how to** perform the Safety Assessment process can be found in ED-79A/ARP-4754A and ARP4761
  - Other means of compliance can proposed, provided they are comparable and meet the intent of ARP4761
  - **Early and regular coordination** with the authority on the different process steps necessary

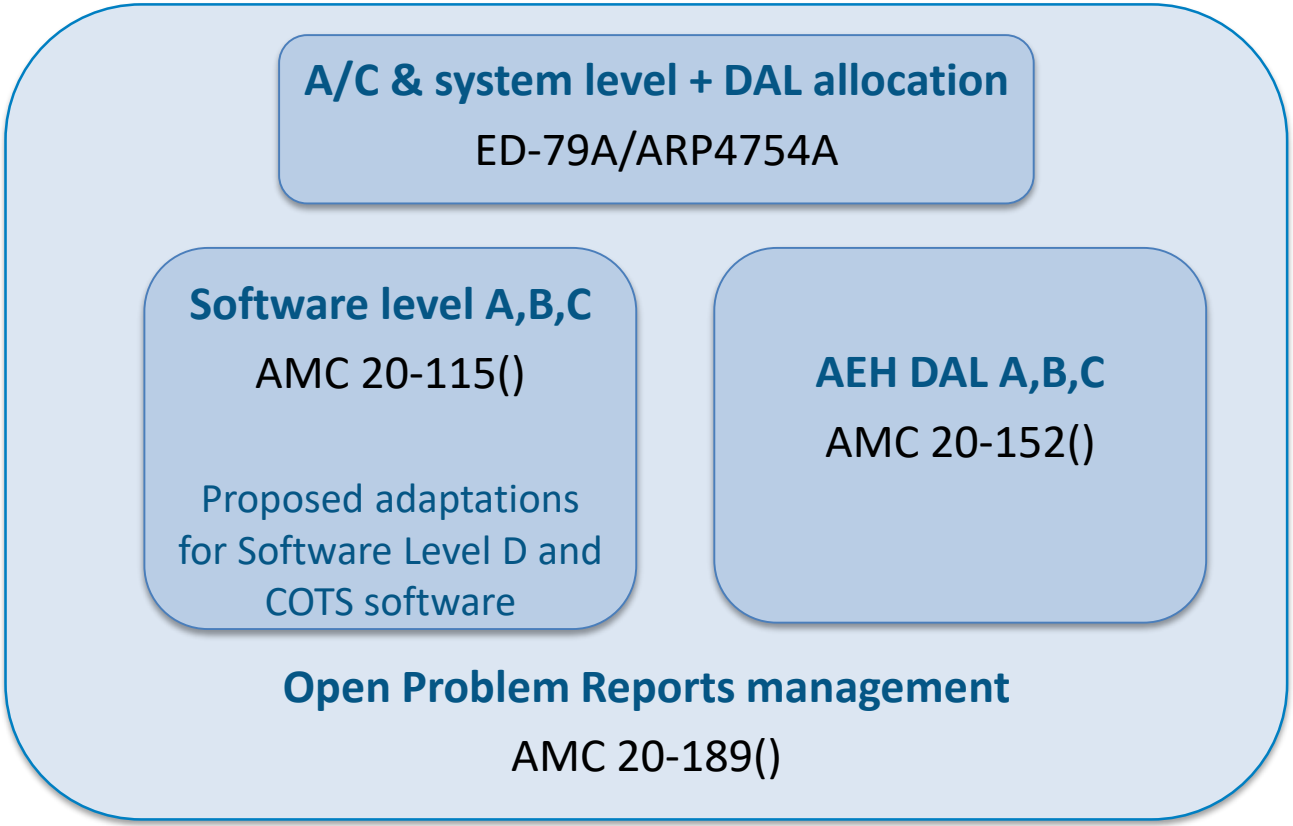
Concept for CMA guidance

→ Possible grouping of mitigation means to Common Mode Failures (CMFs) in 4 classes:



→ EASA is working on evaluation of this concept on the basis of CMA review in projects and with EUROCAE WG-112

Development Assurance (DA)

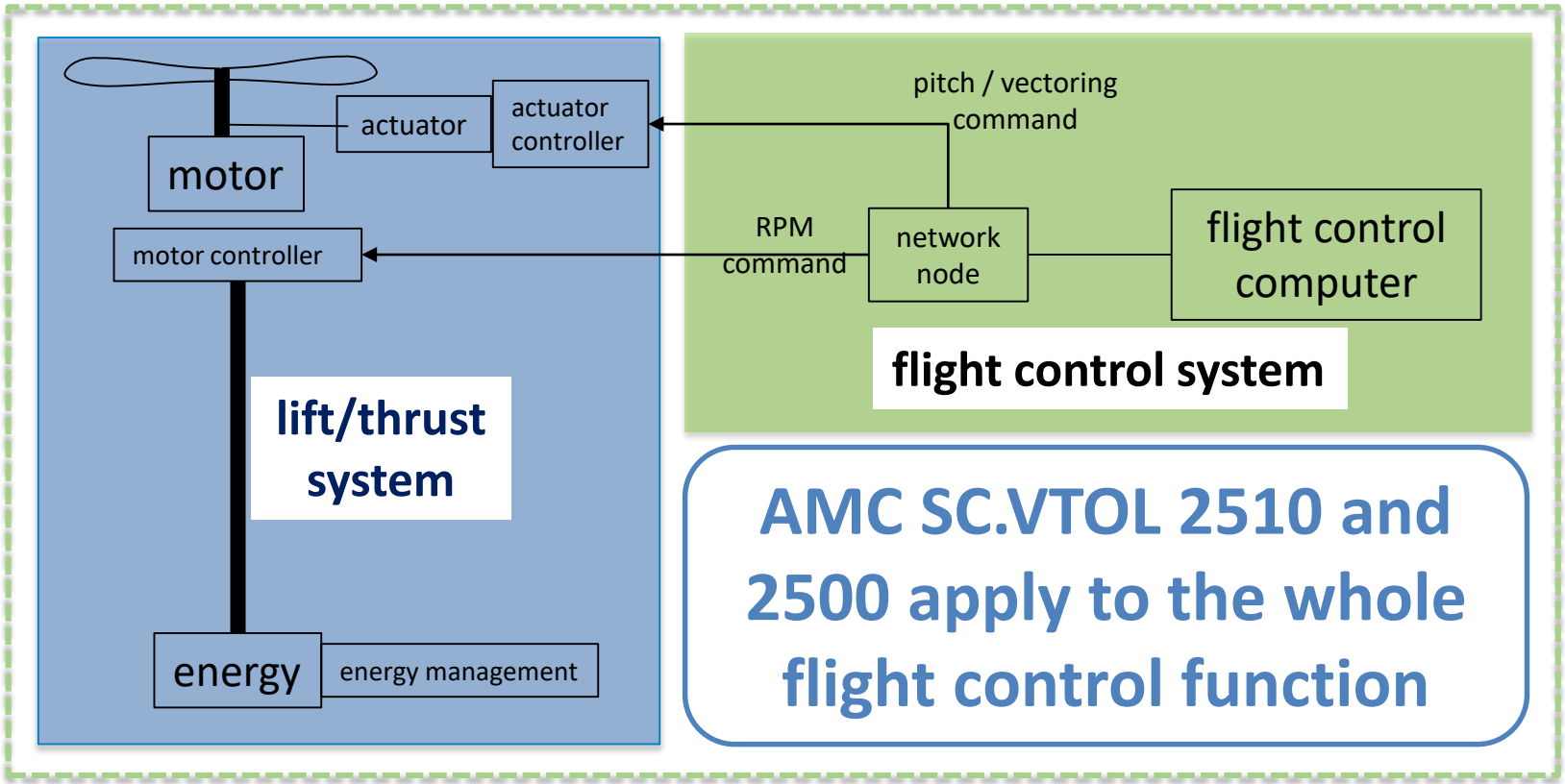


Adaptations for Software DA

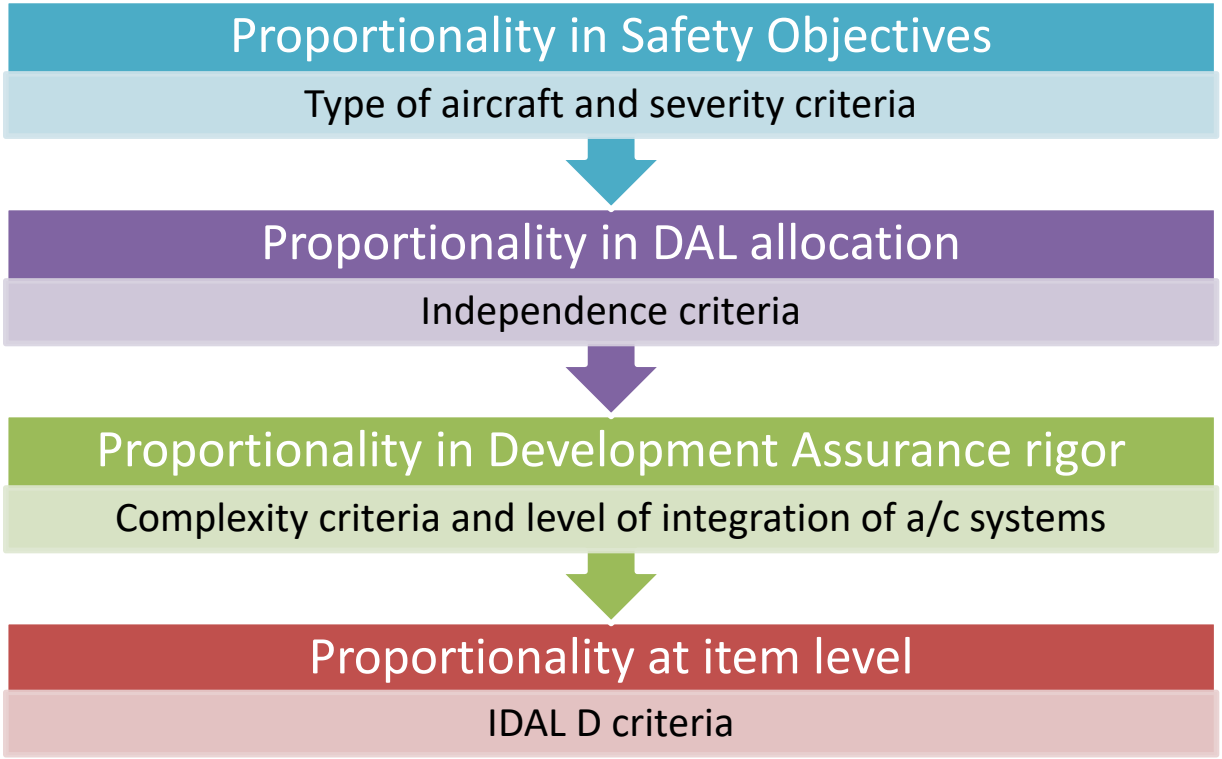
- For Software IDAL/Level D
  - AMC 20-115() is applicable and can be used
  - However system level DA processes may be sufficient provided adequate derived requirements management

- For COTS Software
  - Recognizing that ED-109A/DO-278A section 12.4 guidance can be useful beyond limits of CNS/ATM applications
  - Specific guidance to be developed in dedicated working groups

Lift Thrust system considerations



Proportionality approach



Status of the activity / next steps

- First draft AMC ready including provisions of this presentation
- Work planned with WG-112
  - Sharing this first draft for review and discussions
  - Concept for the CMA
- Consistency with other AMC, in particular:
  - 21xx for Handling Qualities
  - 2300 for Flight Controls
  - 2500 for Cybersecurity
  - 2505 for Equipment limitations
- Topics to be further investigated
  - Framework for quick deployment of safety updates

Thank you for your attention!

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union