EUROPEAN AVIATION SAFETY AGENCY
AGENCE EUROPÉENNE DE LA SÉCURITÉ AÉRIENNE
EUROPÄISCHE AGENTUR FUR FLUGSICHERHEIT

7th ROTORCRAFT Symposium

Safety Assessment and Development Assurance process for current and future helicopters: EASA view

Alexandra FLORIN
Certification Directorate
Development Assurance and Safety Assessment expert

2013-12-05

Your safety is our mission.

Table of content

1. Regulatory background
2. Focus on ED-79/ARP-4754 standard
3. Missions of the DASA experts in EASA
4. Involvement of the DASA experts in the certification process
5. Relation with other authorities

1. Regulatory background (1/6)

- Current trend in rotorcraft design is an increasing level of complexity and integration between the R/C functions and the systems implementing them.
- A typical example is the use of Integrated Modular Avionics (IMA) architectures integrating many of the traditionally federated systems and functions, e.g.:
  - *Automatic Flight Control Systems (AFCS),*
  - *Air Data and Inertial Reference System,*
  - *Vehicle and Engine Management System (VMS),*
  - *Digital Map, Synthetic Vision, …*

1. Regulatory background (2/6)

- Another typical example is the use of Advanced Flight Controls architectures such as fly-by-wire systems.
- In some cases, those fly-by-wire systems even integrate the engine control functions.

1. Regulatory background (3/6)

- Increased complexity leads to the possibility of development errors (i.e. mistakes in requirements, design, or implementation) that are not systematically detectable by tests as they used to be for conventional systems.
- Those development errors have been traditionally addressed using development assurance techniques at SW and AEH levels (DO-178C/DO-254).
- But DO-178C/DO-254 standards do not address potential development errors at rotorcraft level or system level.

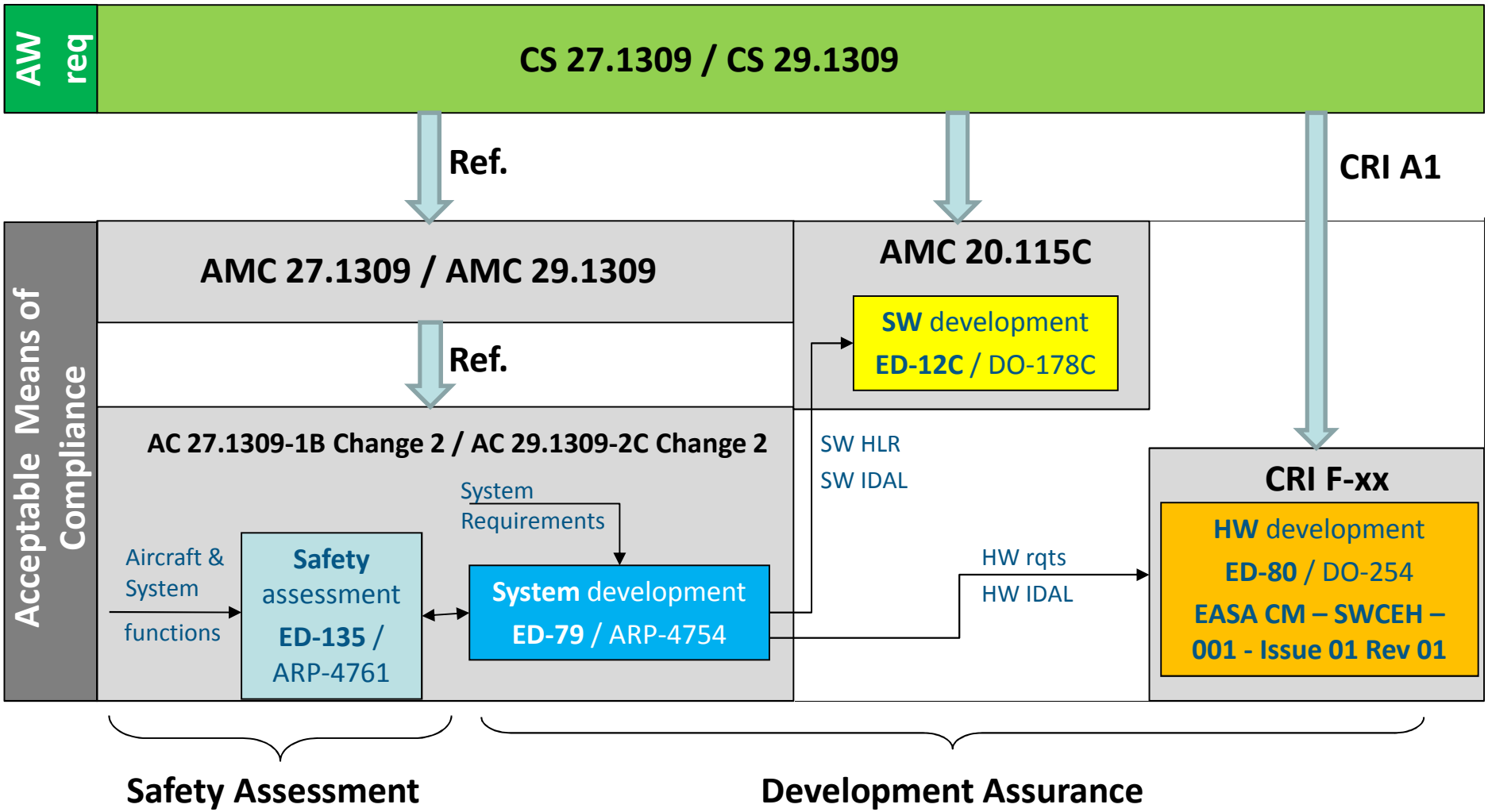
1. Regulatory background (4/6)

- In this context, the industry (through Eurocae/SAE working groups) has published two standards:
  - ED-135/ARP-4761: "Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment"
  - ED-79(-)/ARP-4754(-): "Certification Considerations for Highly-Integrated or Complex Aircraft Systems"

1. Regulatory background (5/6)

- ED-135/ARP-4761 standard addresses safety assessment methodologies (Functional Hazard Assessment, Common Mode Analysis, …).
- ED-79/ARP-4754 standard provides guidelines considered as an acceptable means of addressing potential ***development errors*** at rotorcraft or system level:
  - Is the risk of a development error limited to a level commensurate with its most severe effect?
  - Are unintended functions or behaviours prevented?
- Both activities are necessary to show compliance with 1309 requirement.

1. Regulatory background (6/6)



1. Regulatory background
2. Focus on ED-79/ARP-4754 standard
3. Missions of the DASA experts in EASA
4. Involvement of the DASA experts in the certification process
5. Relation with other authorities

2. Focus on ED-79/ARP-4754 standard (1/4)

- Increased complexity leads to the possibilities of development errors that are not systematically detectable via tests.
  - How to ensure an acceptable risk?
  - How to ensure absence of unintended function or unintended behaviour?

2. Focus on ED-79/ARP-4754 standard (2/4)

- ED-79 provides development assurance activities guidelines to be used while developing a rotorcraft and its systems.
- The Development Assurance Processes provide means to establish confidence that rotorcraft and system development have been accomplished in a sufficiently disciplined manner to limit the likelihood of development errors that could impact aircraft safety.
- The development assurance activities described in ED-79 standard are process-based activities:
  - *Requirement capture process,*
  - *Validation & Verification processes,*
  - *Configuration Management process, …*

2. Focus on ED-79/ARP-4754 standard (3/4)

- Requirement Validation Process
  - Ensures correctness and completeness of requirements
  - Are we building the right aircraft and the right systems?
- Implementation Verification process
  - Confirms that the intended functions have been correctly implemented and the requirements have been satisfied
  - Have we built the aircraft and its systems right?
- Process Assurance activities:
  - Are pillars of Development Assurance activities
  - Ensure that the necessary DA plans are in place,
  - Ensure that development assurance activities are conducted in accordance with the plans.

2. Focus on ED-79/ARP-4754 standard (4/4)

- Traditional development assurance techniques at SW and AEH levels (DO-178C/DO-254) do not address potential development errors at rotorcraft or system level.
- Additional development assurance activities are therefore necessary to reduce and mitigate development errors.
- ED-79 guidelines are considered by EASA as acceptable means of compliance with CS-29.1309.
- Development Assurance activities at rotorcraft level and system level need to be performed in addition to the more traditional safety assessment techniques.

1. Regulatory background
2. Focus on ED-79/ARP-4754 standard
3. Missions of the DASA experts in EASA
4. Involvement of the DASA experts in the certification process
5. Relation with other authorities

3. Missions of the DASA experts in EASA (1/3)

- Since the 1309 requirement is applicable at rotorcraft level and to all rotorcraft systems, the EASA Department of Experts has decided to involve the Development Assurance and Safety Assessment (DASA) experts to ensure a coordinated and consistent approach within the Agency in terms of safety assessment and development assurance activities for all systems, including at the rotorcraft level.

3. Missions of the DASA experts in EASA (2/3)

- The EASA DASA experts are thus in charge of investigating, as part of the certification team, rotorcraft level compliance with xx.1309 airworthiness requirements.

- From 2012, all on-going CS-29 type-certification/type-validation projects have an assigned DASA expert:
  - Agusta AW169 & AW189,
  - Eurocopter X4,
  - AWTRC AW609.

3. Missions of the DASA experts in EASA (3/3)

- The DASA experts are as well in charge of providing advice in the development of new airworthiness requirements in co-operation with the EASA Rulemaking Directorate, for instance:
  - Participating in Inter-Agencies (FAA/TCCA/EASA) discussions on the FAA proposed AdFC Handbook on FBW,
  - Participating in discussions with the FAA on the new FAA Policy Statement on NORSEE (NOn Required Safety Enhancing Equipment),
  - …

1. Regulatory background
2. Focus on ED-79/ARP-4754 standard
3. Missions of the DASA experts in EASA
4. Involvement of the DASA experts in the certification process
5. Relation with other authorities

4. Involvement of the DASA experts in the certification process (1/3)

- The involvement of the DASA experts in the certification process depends on the product being certified:

	CS-25, CS-29	CS-23, CS-27, CS-E	Other CS-xx
Case #1 **Panel 12 creation**	recommended	possible	N/A
Case #2 **DASA Focal Point**	possible	recommended	possible
Case #3 **No DASA expert involvement**	N/A	possible	recommended

- Case #1 - Depending on the complexity of the project, Panel 12 is composed of one or two DASA experts. When more than one DASA expert is working on a dedicated project, a Panel 12 coordinator is nominated.
- Case #2 - When no Panel 12 is created, the PCM or a system expert from the team will be nominated to deal with 2x.1309 verification activities at rotorcraft level. He/she should liaise with and get support from a DASA expert focal point.
- Case #3 - Limited to projects with limited verification xx.1309 activities at A/C level.

4. Involvement of the DASA experts in the certification process (2/3)

- The DASA experts' certification activities involve reviewing and accepting, after coordination with the other panels, the rotorcraft level documents, e.g.:
  - the Rotorcraft Safety Plan, the Rotorcraft Development Assurance Plan, the Rotorcraft level safety compliance documents (rotorcraft FHA, PASA, and ASA), …
- They also coordinate the review of the safety assessment methodologies used to perform:
  - Aircraft / System Functional Hazard Assessments (FHAs),
  - Preliminary Aircraft / System Safety Assessments (PASA/PSSA)
  - Aircraft / System Safety Assessments (ASA / SSA),
  - the Common Cause Analyses (CMA, ZSA),
  - the FDAL and IDAL (Functional and Item Development Assurance Levels) assignment from aircraft to items.

4. Involvement of the DASA experts in the certification process (3/3)

- The other panels of the certification team:
  - Participate in the aircraft level activities coordinated by the DASA expert;
  - For the systems they are responsible for:
    - Review and accept the methods, tools and formats proposed by the rotorcraft manufacturer related to the Particular Risk Analyses;
    - Monitor the proper application of the agreed procedures and methodologies;
    - Are responsible for the relevant system compliance documents (e.g. system FHA, PSSA, SSA, PRA, …);
    - Assess the need for system development assurance audits.

- The coordination between the DASA expert, the other System experts and the rotorcraft manufacturer can be done through Safety Interface Meetings, either internally or with the applicant.

1. Regulatory background
2. Focus on ED-79/ARP-4754 standard
3. Missions of the DASA experts in EASA
4. Involvement of the DASA experts in the certification process
5. Relation with other authorities

5. Relation with other authorities

- FAA:
  - John Vanhoudt is the FAA focal point for ROT AdFC activities.
  - FAA AC 20-174 recognizes ED-79A/ARP-4754A as an acceptable method for establishing a development process.

- TCCA:
  - Jim Marko (Manager, Aircraft Integration & Safety Assessment) is the TCCA focal point for the DASA activities.
  - Safety Interface Meetings have been introduced for the first time for the C-Series.

Thank you for your attention

Questions?

List of abbreviations

- **AdFC:** Advanced Flight Controls
- **ARP** : Aerospace Recommended Practice
- **ASA**: Aircraft Safety Assessment
- **CCA**: Common Cause Analysis
- **CMA**: Common Mode Analysis
- **CS**: Certification Specification
- **DA**: Development Assurance
- **DASA**: Development Assurance & Safety Assessment
- **EUROCAE**: European Organisation for Civil Aviation Equipment
- **FDAL**: Function Development Assurance Level
- **FHA**: Functional Hazard Assessment
- **FTA**: Fault Tree Analysis
- **HLR**: High Level Requirements
- **IDAL**: Item Development Assurance Level
- **PASA**: Preliminary Aircraft Safety Assessment
- **PRA**: Particular Risk Analysis
- **PSSA**: Preliminary System Safety Assessment
- **RTCA**: Radio Technical Commission for Aeronautics
- **SAE:** Society of Automotive Engineers
- **SSA**: System Safety Assessment
- **ZSA**: Zonal Safety Analysis