RPAS Certification. Where the challenges lie

Military Airworthiness Conference 2014
Roma

Julio Jiménez López
Head of RPAS/UAS Airworthiness (Military Aircraft)
September 2014

AIRBUS
DEFENCE & SPACE

INDEX

Regulations

Safety, Complexity and Affordability

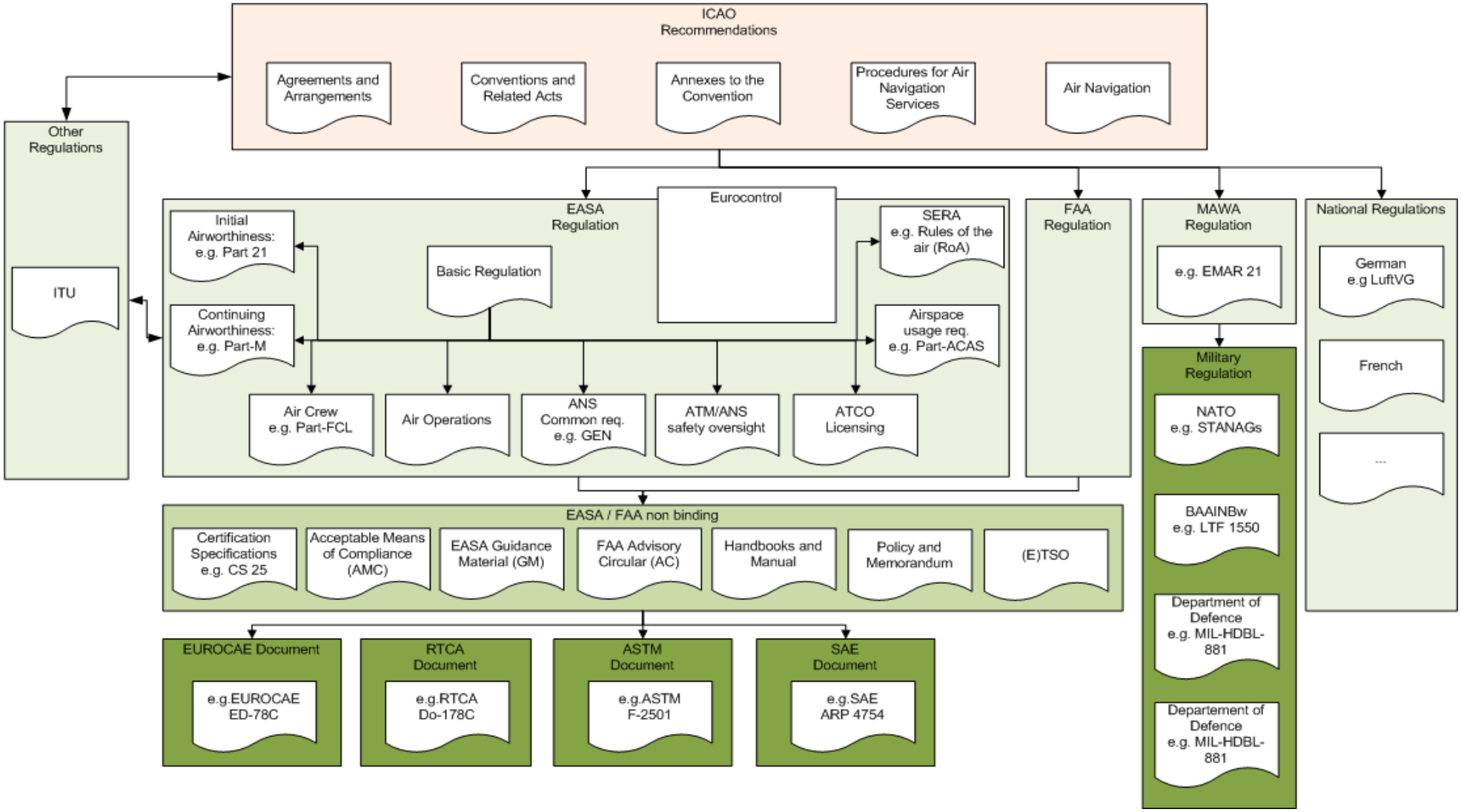
Regulations and Operational Suitability

AIRBUS DEFENCE & SPACE

Regulations

Slow Progress on UAS Regulation

Complex Regulations / Standards structure

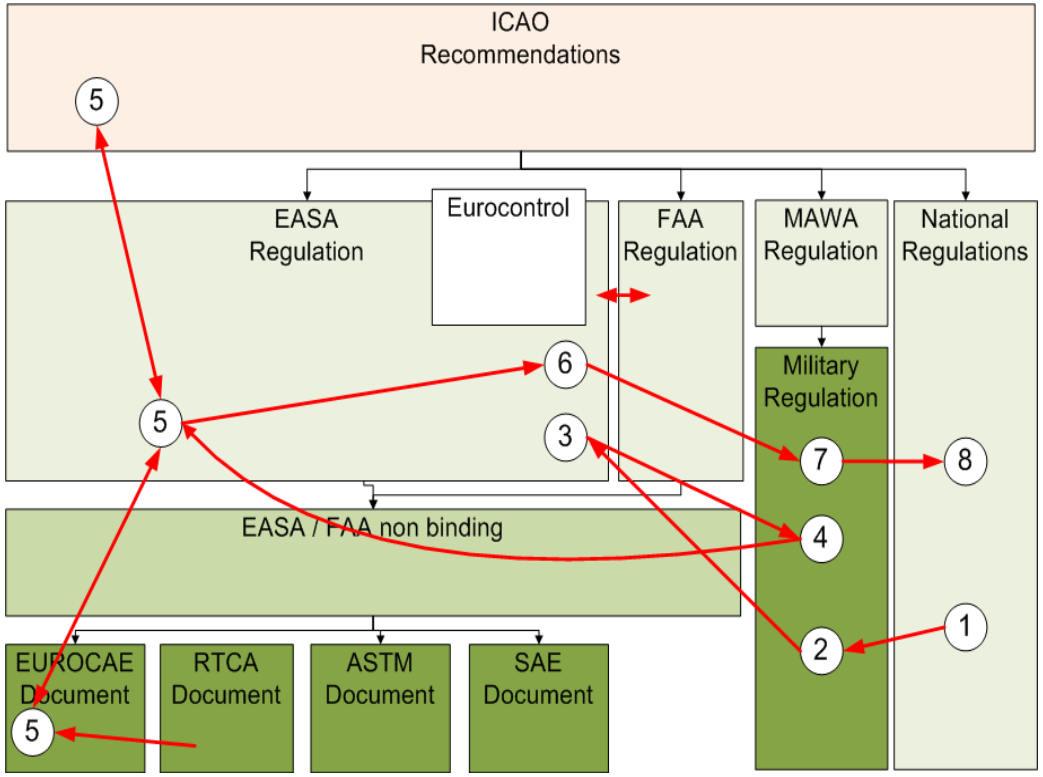


AIRBUS DEFENCE & SPACE

Slow Progress on UAS Regulation

The impact of how it has worked….

1. National Military Regulation (France USAR)
2. NATO level military regulation (Stanag 4671)
3. Review by FAA/EASA : non acceptance of safety objectives (E.Y013-01)
4. New Edition of Stanag 4671 by NATO
5. Current revision process of safety objectives:
   - EASA : ERSG
   - ICAO : RPASP
   - EUROCAE: WG 73 and WG 93
   - Discussion at NATO level
6. An agreement will be achieved at EASA and/or FAA and/or ICAO
7. The new safety objectives will require an update at NATO Level of Stanag 4671
8. The Stanag 4671 will be applied nationally based on agreement with national authorities



AIRBUS DEFENCE & SPACE

Slow Progress on UAS Regulation

Additional limiting factors

- Lot of Stakeholders:
  - Civil Aviation Industry
  - Military Aviation Industry
  - Operators
  - Regulation bodies

- Lot of Working groups with potential conflicts of interest:
  - BDLi
  - DFS „Working Group“
  - WTD61 „Working Group“
  - DACH
  - ERSG
  - EDA – MIDCAS
  - EDA - DESIRe
  - EDA - SINUE
  - EASA / EC public consultation
  - EUROCAE WG-72
  - EUROCAE WG-73
  - EUROCAE WG-75
  - EUROCAE WG-93
  - EUROCONTROL
  - UVS-International
  - ICAO / RPASP
  - ITU-R / WRC
  - JARUS
  - JARUS public consultation
  - ASD
  - NATO NIAG
  - ….etc

- Several initiatives are launched in parallel to bring solutions for RPAS certification / integration

- Missing of a REAL certification process: a RPAS project to apply the theory to the reality.

AIRBUS DEFENCE & SPACE

Military and Civil Regulations Evolution

Major Issues

- **A never ending story....since 2003 (French USAR)**
- **Proliferation of regulatory groups overtime, creating ever increasing number of documents**
- **Industry voice not enough listened, leading to stronger military safety requirements over time**
- **Worldwide accepted definition of Catastrophic RPAS event not yet available**

AIRBUS DEFENCE & SPACE

Safety, Complexity and Affordability

Intrinsic Safety, Ground Safety and Air Traffic Safety

- 1309 was historically a requirement to cover the Intrinsic Safety of an aircraft, and including some additional operational requirement on the safety in air traffic, which as a by-product results in the safety of third persons on ground.

- With the RPAS without any human being on board this intrinsic safety is not anymore the driving factor. This has lead to:
  - Mixing of operational requirement with airworthiness requirements:
    - Aircraft Loss (Airworthiness)
    - Ground fatalities (Operational)
    - Mid Air Collisions (Operational)

  - Comparison of non comparable safety objectives:
    - Probability of 1E-9 per Failure Condition in a passenger aircraft with a probability of 1E-9 for death of third parties on ground

- All of this in a context in which ARP4754A (civil certification of passenger aircraft) is being more considered in the military certification world.

AIRBUS DEFENCE & SPACE

What Industry Needs

- Clear requirements for the different safety:
  - Aircraft Loss (Airworthiness)
  - Ground fatalities (Operational)
  - Mid Air Collisions (Operational)

- Clear methodology to be able to apply this requirement on systems

AIRBUS DEFENCE & SPACE

Application of AMC1309 requirements

Definition of Catastrophic Event on STANAG 4671:

Catastrophic event definition for RPAS shall always be related to fatality

(i) Catastrophic: Failure conditions that are expected to result in at least uncontrolled flight (including flight outside of pre-planned or contingency flight profiles/areas) and/or uncontrolled crash, **where it can be reasonably expected that a fatality will occur**

Or Failure conditions which may result in a fatality to UAV crew or ground staff

Deviation from flight plan cannot be rated catastrophic

Catastrophic: Failure conditions that are expected to result in at least uncontrolled flight ~~(including flight outside of pre-planned or contingency flight profiles/areas)~~ and/or uncontrolled crash,

Or Failure conditions which may result in a fatality to UAV crew or ground staff

AIRBUS DEFENCE & SPACE

Evolution of STANAG 4671 safety objectives

- **Evolution from French USAR to STANAG 4671 editions has resulted in increased requirements for Failure Probabilities and DO178 SW DAL levels which impacts all RPAS systems**

- It is proposed to include in the Stanag 4671 ed3 a rational for proposed safety objectives using the three following arguments:
  1. Military Missions: objectives of the military aircraft are to **fulfill national priority mission**. This missions will require **specifics performances** and it should be accepted that this priority should be well balanced with the crash probability. In this context it should be accepted that military aircraft will define **lower safety objectives** to their aircraft than for a commercial aircraft.

  2. Higher Automation level: the high automation cannot be a **drawback** from an Airworthiness point of view. The higher the automation level is, the less pilot failure will be generated (in typical aircraft pilot failure are considered to be the source of 80% of the accident).

  3. Number of CAT Failure Conditions: In general a RPAS will have quite **less catastrophic failures** then a manned passenger aircraft.

AIRBUS DEFENCE & SPACE

Evolution of Stanag 4671 safety objectives

- **Comparison matrix with manned aircraft**

Aircraft category	No. of Potential catastrophic failure conditions	Acceptable probability of a single catastrophic failure condition (pfh)
Manned CS23 class I	10	1E-6
Manned CS23 Class II	10	1E-7
Manned CS23 Class III	10	1E-8
Manned CS25	100	1E-9
Military RPAS < 5,6t	10	1E-6
Military RPAS > 5,6t	100?	1E-7

RPAS Requirement Evolution over time

	Frequent	Probable	Remote	Extremely remote	Extremely improbable
USAR v3.0	> 10^{-2}	< 10^{-2}	< 10^{-3}	< 10^{-5}	< 10^{-6}
STANAG 4671 Ed. 1	> 10^{-3}	< 10^{-3}	< 10^{-4}	< 10^{-5}	< 10^{-6}
STANAG 4671 Ed. 3 Draft MTOM<5670	> 10^{-3}	< 10^{-3}	< 10^{-4}	< 10^{-5}	< 10^{-6}
STANAG 4671 Ed. 3 Draft MTOM>5670	> 10^{-3}	< 10^{-3}	< 10^{-4}	< 10^{-6}	< 10^{-7}
AC 23.1309-1C (1)	--	< 10^{-3}	< 10^{-4}	< 10^{-5}	< 10^{-6}
AC 23.1309-1C (2)		< 10^{-3}	< 10^{-5}	< 10^{-7}	< 10^{-8}
CS-25	--	< 10^{-3}	< 10^{-5}	< 10^{-7}	< 10^{-9}

AIRBUS DEFENCE & SPACE

Safety, Complexity and Affordability

- **To try to define an Equivalent Level of Safety and to apply the strict civil manned aviation process is bringing to over demanding military certification requirements:**

- **Consequences are:**
  - **High safety requirements**
  - **Higher complexity**
  - **Not affordable system for the required purpose**

Airbus DS has provided comments to draft 3 of STANAG 4671 and provided explanation of them on the "STANAG 4671 Industry Days" held in Mannheim in March 2014. Some examples are provided in the following slides

AIRBUS DEFENCE & SPACE

SW DAL Allocation for RPAS

Original text

DAL allocation for system and each portion of system architecture		Degree of redundancy
		Single failure/errors
Failure Condition Classification	Catastrophic	DAL B
	Hazardous	DAL C
	Major	DAL C
	Minor	DAL D
	No Safety Effect	DAL E

Proposed new text

DAL allocation for system and each portion of system architecture		Degree of redundancy	
		Single failure/errors	
Failure Condition Classification	Catastrophic	DAL B	
	Hazardous	DAL C	
	Major	DAL C	DAL D*
	Minor	DAL D	DAL E*
	No Safety Effect	DAL E	DAL E*

RPAS Requirement Evolution over time

	No safety effect	Minor	Major	Hazardous	Catastophic
USAR v3.0	E	D	C	C	C
STANAG 4671 Ed. 1	E	E / E	D / D	C / D	B / C
STANAG 4671 Ed. 3 Draft	E	D	C	C	B
AC 23.1309-1C (1)	--	D	C / D	C / D	C / C
AC 23.1309-1C (2)	--	D	C / D	C / C	B / C

AIRBUS DEFENCE & SPACE

SW DAL Allocation for RPAS

- **For Major Failure conditions:**
  - The aim of the new safety figures are to be more stringent with Hazardous and Catastrophic failure conditions. In line with this, for Major Failure Conditions the quantitative safety budget has not been changed (remains 10 E-4). Nevertheless, SW DAL requirement is not maintained for Major Failure Conditions as it has changed from DAL D to DAL C. This contradiction prevents use of any COTS, without benefit on performances.

- **For Minor Failure Conditions:**
  - A minor event it specify by a workload increase.
    UCS Designs rely significantly on existing technologies and COTS tools to provide advanced & user friendly & performance optimized functions which reduce operators workload.
    If DAL is raised up to DAL D, most of these COTS tools could not be used and thus, this change will just have the **opposite effect** to the intended one: **operator workload will be increased** due to design restrictions.

AIRBUS DEFENCE & SPACE

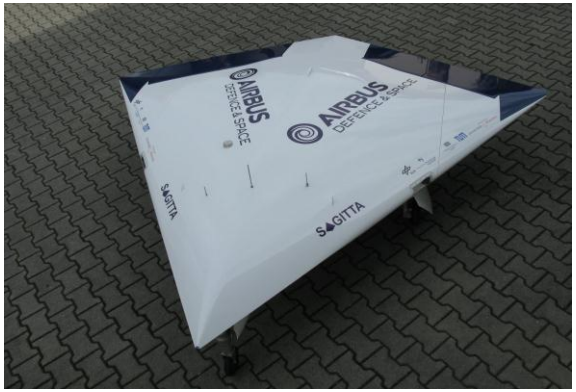
No DO-254 requirement for PLD, ASIC or COTS digital components

Book 2 – Section F, page 6. AMC.1309

Proposed new text

(e) In case of PLD (Programmable Logic Devices) or ASIC (Application Specific Integrated Circuit) development and/or use of COTS digital components, development assurance process as per RTCA DO-254 or possible equivalent guidance agreed with the Certification Authority should be applied.
Applicability of DO-254 can be excluded for PLD, ASIC or COTS digital component whose effects on safety are not Catastrophic nor Hazardous.

Compliance with DO-254 significantly reduces the scope of available COTS for UCS equipment, with the corresponding impact on performances. This is aligned with the software approach, which allows the use of DO-278 (instead of DO-178B) for COTS software whose effects on safety are limited to Major or Minor failure conditions.



AIRBUS DEFENCE & SPACE

Ground Control Station power supply

Book 1 – Section I, page 3, USAR.U1719

Proposed new text

- (a) Failure conditions of UCS power supply shall be assessed according to USAR.1309. **For COTS UCS power supply equipment not fulfilling the RTCA standards DO-178C and/or DO-254, a specific analysis should be used in agreement with the Certification Authorities.**

  However, Regarding AMC1309, section (6) the risk is to achieve compliance with DO-178B/DO-278 and DO-254 if required, due to the use of COTS battery backup systems, like UPS‘s. Its applicability will depend on internal equipment design, but is reasonable to expect that modern battery backup equipment implementations will use embedded software, but not necessarily to control most critical functions (that is, automatic switch to battery power on input power loss).

Regulations and Operational Suitability

Military and Civil certification standards

Differences for Military RPAS

- Civil Certification Standards are defined knowing that:
  - It should define the minimum requirement to maintain a suitable balance between:
    - Safety of users : a catastrophic event should happen with a probability more than 1E-9 per flight hours.
    - Safety of third person : safety of users and the Air Traffic Management rules ensure this safety.
    - Economical Feasibility : a change in the standards are often applicable for new Type only.
    - Technological Feasibility : no standards require the impossible.
  - The objective of user is to make benefits.
  - Around 1 000 000 flights (Commercial and General Aviation) per day world wide.

Military Certification Standards are defined knowing that:

- The military regulation should also consider :
  - Wartime Required Performances: in war time the mission objectives can have an high priority than some safety objectives.
  - Peacetime Required Performances : even in peacetime some military mission are necessary.
- The objective is to protect the nation and citizens.
- Around 100 000 flights per day world wide.

This differences have been considered in military manned aviation for decades. However for the new RPAS environment there is a tendency to use Civil certification requirements. Is this really appropriate For Mission or Combat RPAS?; Are we penalizing it too much?

AIRBUS DEFENCE & SPACE

Where the challenges lie?

Quote from “A new era for aviation”, Communication from the Commission to the European Parliament and the Council dated August 2014.
“The current division of the RPAS market between the very light and the heavy aircraft is questionable in view of a coherent RPAS safety policy”

THE BIGGEST CHALLENGE IS:

THE EVOLUTION FROM MANNED AVIATION MINDSET

AIRBUS DEFENCE & SPACE

Thank you for your attention!

AIRBUS DEFENCE & SPACE