A2COS safety certification

TOWARDS A NEW CERTIFICATION APPROACH FOR CHANGES IN THE TOTAL AVIATION SYSTEM

31 MARCH, 2015

Martijn.Stuip@nlr.nl , Edwin.van.de.Sluis@nlr.nl, Peter.van.der.Geest@nlr-atsi.nl, Hans.Post@nlr-atsi.nl

Aircraft Systems Department / Air Transport Safety Institute
National Aerospace Laboratory – NLR
Amsterdam, The Netherlands

NLR

ebeni

EADS APSYS

Project Background (see also ASCOS website: https://www.ascos-project.eu/)

- Many innovative technologies and operational concepts are not implemented due to issues arising with safety and certification
- Many operators and users are eager to use new developments
- To ease introduction of safety enhancement systems & operations, an innovative approach towards certification is required that:
  - Is more flexible with regard to the introduction of new products and operations;
  - Is more efficient, in terms of cost, time & safety, than current certification processes;
  - Considers safety impact of all aviation system elements and the entire system life-cycle in a complete integrated way.

ASCOS WP1 Proposed certification approach: staged application

1) Define the change
2) Define the certification argument
3) Develop/agree certification plan
4) Specification
5) Design
6) Refinement of argument
7) Implementation
8) Transfer into operation – transition safety assessment
9) Define arrangements for continuous safety monitoring
10) Obtain initial operational certification
11) Ongoing monitoring and maintenance of certification

WP4 Case Studies

ASCOS WP4 Case Studies

- RPAS failure management systems
- Automatic Aircraft Recovery System
- Certificate for de-icers
- ATM/CNS systems for improved surveillance

- Important aspects:
  - Logical safety argument approach
  - Total Aviation System approach
  - Complete life cycle

ASCOS WP4.2 Automatic Aircraft Recovery System
Some frequent characteristics of LOC accidents

- → Rare Failure modes
- → Lack of Situational Awareness
- → Rapid sequence of events
- → Erroneous recovery strategy

- → Example LOC cases
- → Air France AF447: Loss of airspeed indication en-route
- → Turkish Airlines TK1951 near Schiphol: Erroneous radio altimeter during approach

Potential hypothetical solution

- Automatic Aircraft Recovery System (AARS)
- Pioneered in Military Aircraft
  - F-22 Raptor
  - Eurofighter Typhoon:

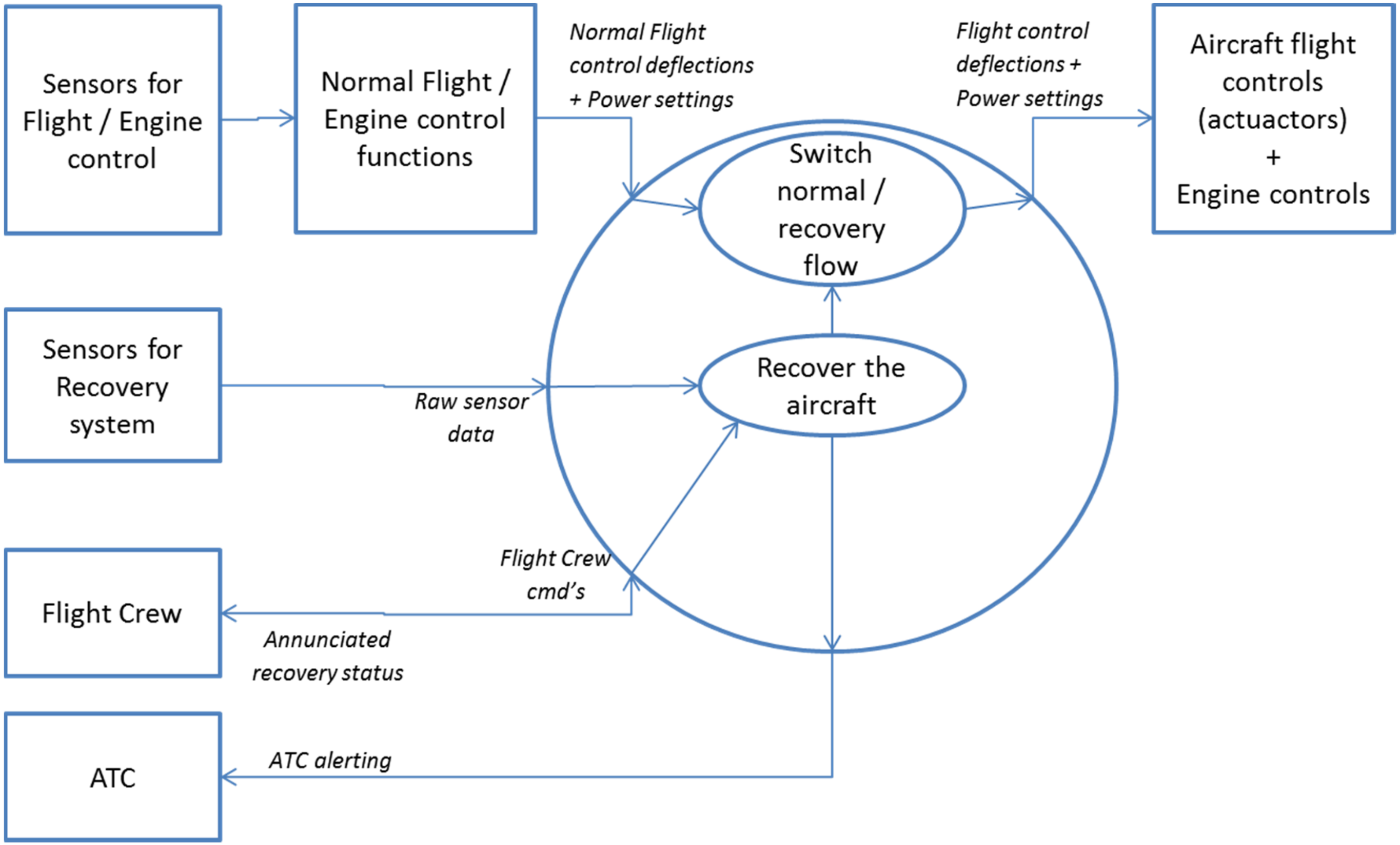
    In case of pilot disorientation, Eurofighter Typhoon's FCS allows for rapid and automatic recovery by the simple press of a button.
    On selection of this auto-recovery facility the FCS takes full control of the engines and flying controls, and automatically stabilises the aircraft in a wings level, gentle climbing attitude at 300 knots, until the pilot is ready to re-take control.
- Technology is transferable to Civil Aircraft
- Should take into account system failure conditions

Stage 1: Define the Change:
Auto Recovery System Functions

- To provide after pilot initiation a rapid and automatic recovery of the aircraft to a stable flight regime
- From any initial flight condition within or outside the normal flight envelope
- With or without failures to the automatic and/or primary flight control system and/or to engines
- To maintain stable flight regime for sufficient time for the pilot to
    - regain adequate situational awareness
    - diagnose any problem
    - to identify correct interventions to ensure continued safe flight

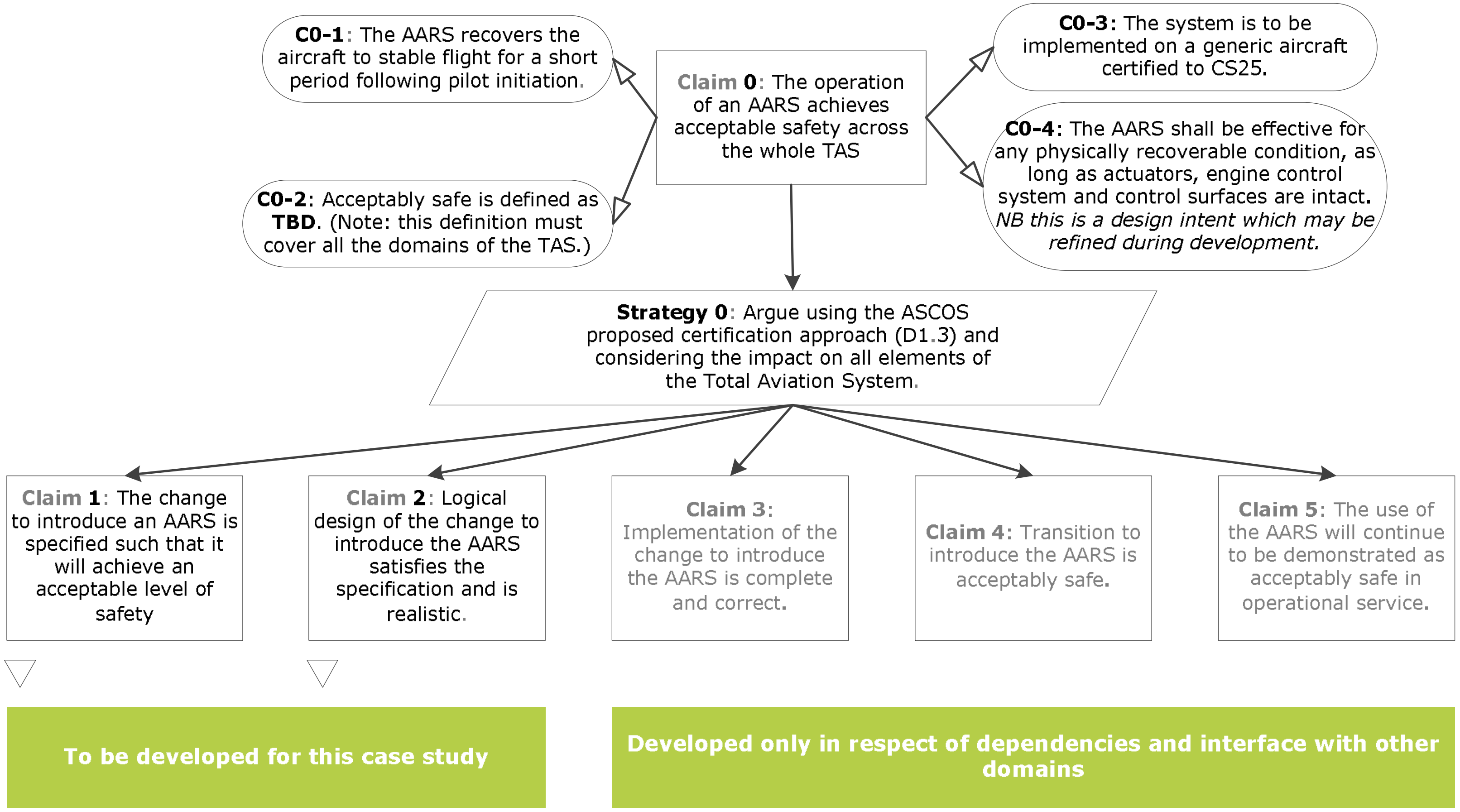
Stage 1: Define the Change:

The change is defined as the introduction of a technical device on-board of commercial aircraft (CS-25 type certified) that recovers the aircraft automatically from a loss of control or loss of situational awareness situation with one pilot button push.


Sensors for Flight / Engine control
Normal Flight / Engine control functions
Normal Flight control deflections + Power settings
Flight control deflections + Power settings
Aircraft flight controls (actuactors) + Engine controls
Switch normal / recovery flow
Sensors for Recovery system
Raw sensor data
Recover the aircraft
Flight Crew cmd's
Flight Crew
Annunciated recovery status
ATC
ATC alerting

Stage 2: Define the certification argument

- Representation: Goal Structuring Notation (GSN)
- Concept: generic logical argument used within ATM domain



C0-1: The AARS recovers the aircraft to stable flight for a short period following pilot initiation.

C0-2: Acceptably safe is defined as **TBD**. (Note: this definition must cover all the domains of the TAS.)

Claim 0: The operation of an AARS achieves acceptable safety across the whole TAS

C0-3: The system is to be implemented on a generic aircraft certified to CS25.

C0-4: The AARS shall be effective for any physically recoverable condition, as long as actuators, engine control system and control surfaces are intact. *NB this is a design intent which may be refined during development.*

Strategy 0: Argue using the ASCOS proposed certification approach (D1.3) and considering the impact on all elements of the Total Aviation System.

Claim 1: The change to introduce an AARS is specified such that it will achieve an acceptable level of safety

Claim 2: Logical design of the change to introduce the AARS satisfies the specification and is realistic.

Claim 3: Implementation of the change to introduce the AARS is complete and correct.

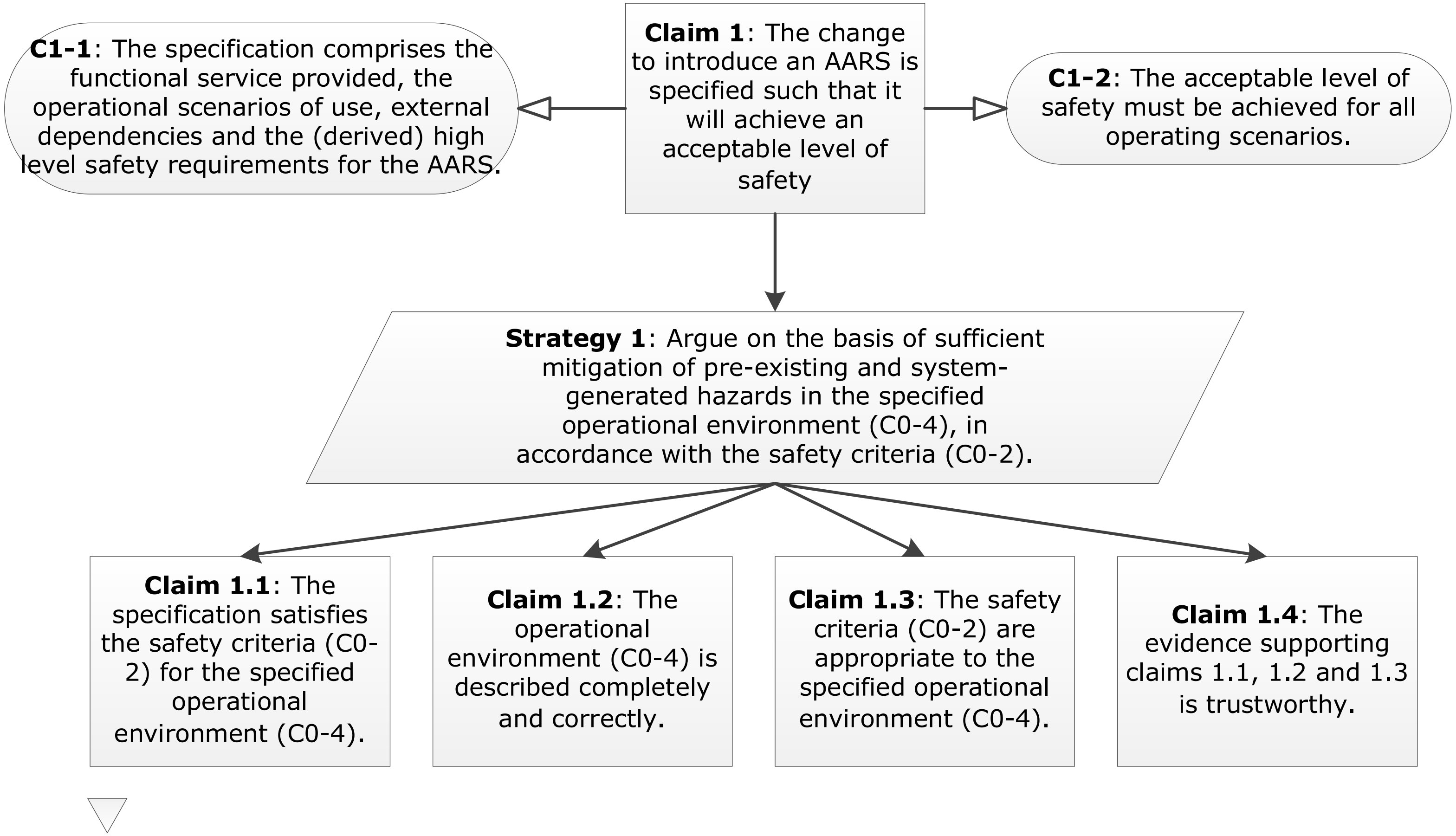
Claim 4: Transition to introduce the AARS is acceptably safe.

Claim 5: The use of the AARS will continue to be demonstrated as acceptably safe in operational service.

To be developed for this case study

Developed only in respect of dependencies and interface with other domains

Stage 2: Define the certification argument; Claim1



Claim 1: The change to introduce an AARS is specified such that it will achieve an acceptable level of safety

C1-1: The specification comprises the functional service provided, the operational scenarios of use, external dependencies and the (derived) high level safety requirements for the AARS.

C1-2: The acceptable level of safety must be achieved for all operating scenarios.

Strategy 1: Argue on the basis of sufficient mitigation of pre-existing and system-generated hazards in the specified operational environment (C0-4), in accordance with the safety criteria (C0-2).

Claim 1.1: The specification satisfies the safety criteria (C0-2) for the specified operational environment (C0-4).

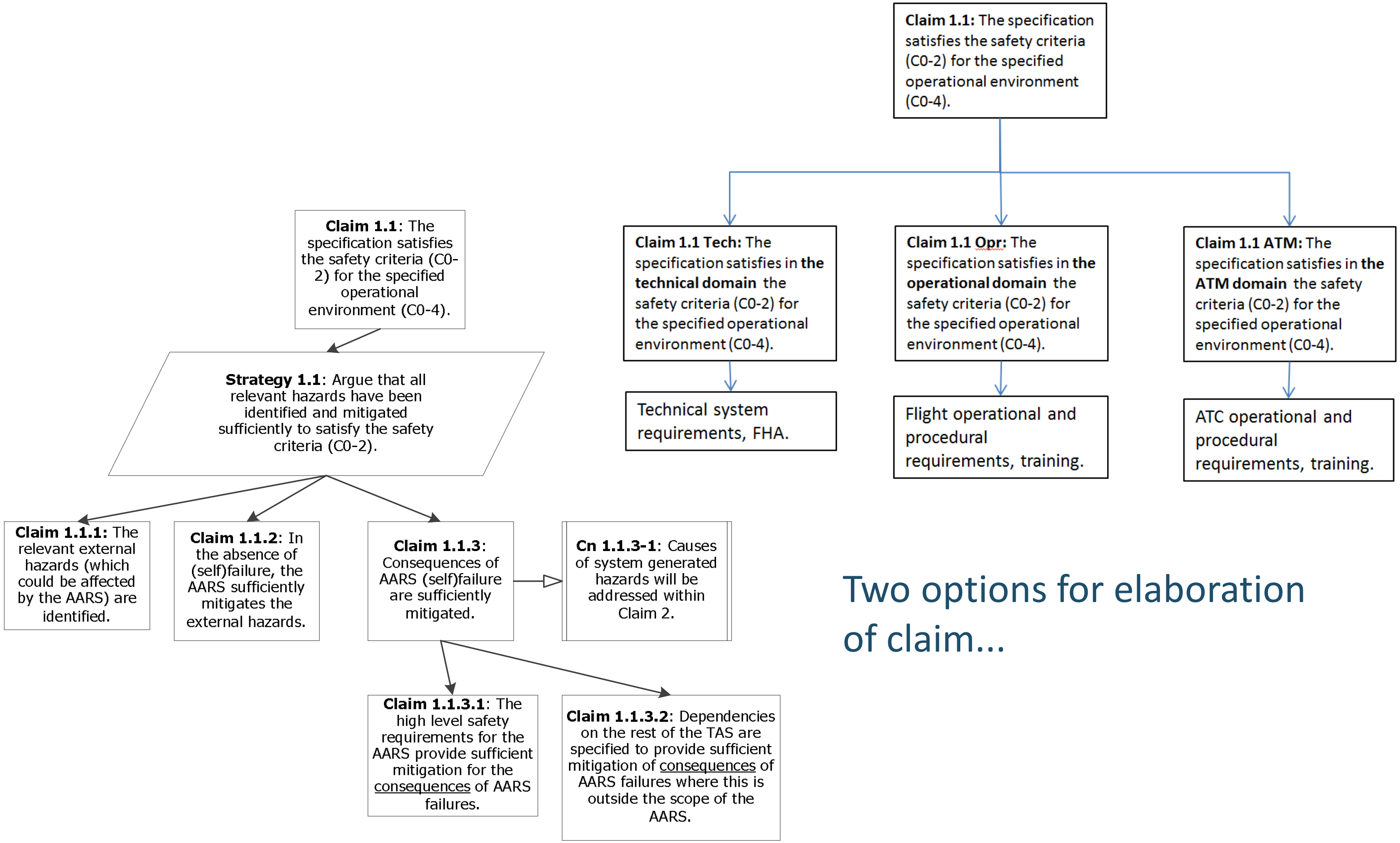
Claim 1.2: The operational environment (C0-4) is described completely and correctly.

Claim 1.3: The safety criteria (C0-2) are appropriate to the specified operational environment (C0-4).

Claim 1.4: The evidence supporting claims 1.1, 1.2 and 1.3 is trustworthy.

→ Claim1.1: Supported mainly by Functional Hazard Assessment (FHA);

Stage 2: Define the certification argument; Claim 1.1



Claim 1.1: The specification satisfies the safety criteria (C0-2) for the specified operational environment (C0-4).

Strategy 1.1: Argue that all relevant hazards have been identified and mitigated sufficiently to satisfy the safety criteria (C0-2).

Claim 1.1.1: The relevant external hazards (which could be affected by the AARS) are identified.

Claim 1.1.2: In the absence of (self)failure, the AARS sufficiently mitigates the external hazards.

Claim 1.1.3: Consequences of AARS (self)failure are sufficiently mitigated.

Cn 1.1.3-1: Causes of system generated hazards will be addressed within Claim 2.

Claim 1.1.3.1: The high level safety requirements for the AARS provide sufficient mitigation for the consequences of AARS failures.

Claim 1.1.3.2: Dependencies on the rest of the TAS are specified to provide sufficient mitigation of consequences of AARS failures where this is outside the scope of the AARS.

Claim 1.1: The specification satisfies the safety criteria (C0-2) for the specified operational environment (C0-4).

Claim 1.1 Tech: The specification satisfies in **the technical domain** the safety criteria (C0-2) for the specified operational environment (C0-4).

Technical system requirements, FHA.

Claim 1.1 Opr: The specification satisfies in **the operational domain** the safety criteria (C0-2) for the specified operational environment (C0-4).

Flight operational and procedural requirements, training.

Claim 1.1 ATM: The specification satisfies in **the ATM domain** the safety criteria (C0-2) for the specified operational environment (C0-4).

ATC operational and procedural requirements, training.

Two options for elaboration of claim...

Stage 3: Develop/agree Certification Plan (CP)

- Role: to show how the certification argument architecture will be developed and substantiated with evidence to the point where it can be presented for acceptance by the relevant authorities
- A given change may (currently) require endorsement from authorities from multiple domains (A/C, OPS, ATM); needs to be identified in argument
- For AARS CP will typically refer to EASA CS25.1309 (Equipment, systems and installations) and CS25.1302 (Human Factors), EU-OPS, ...

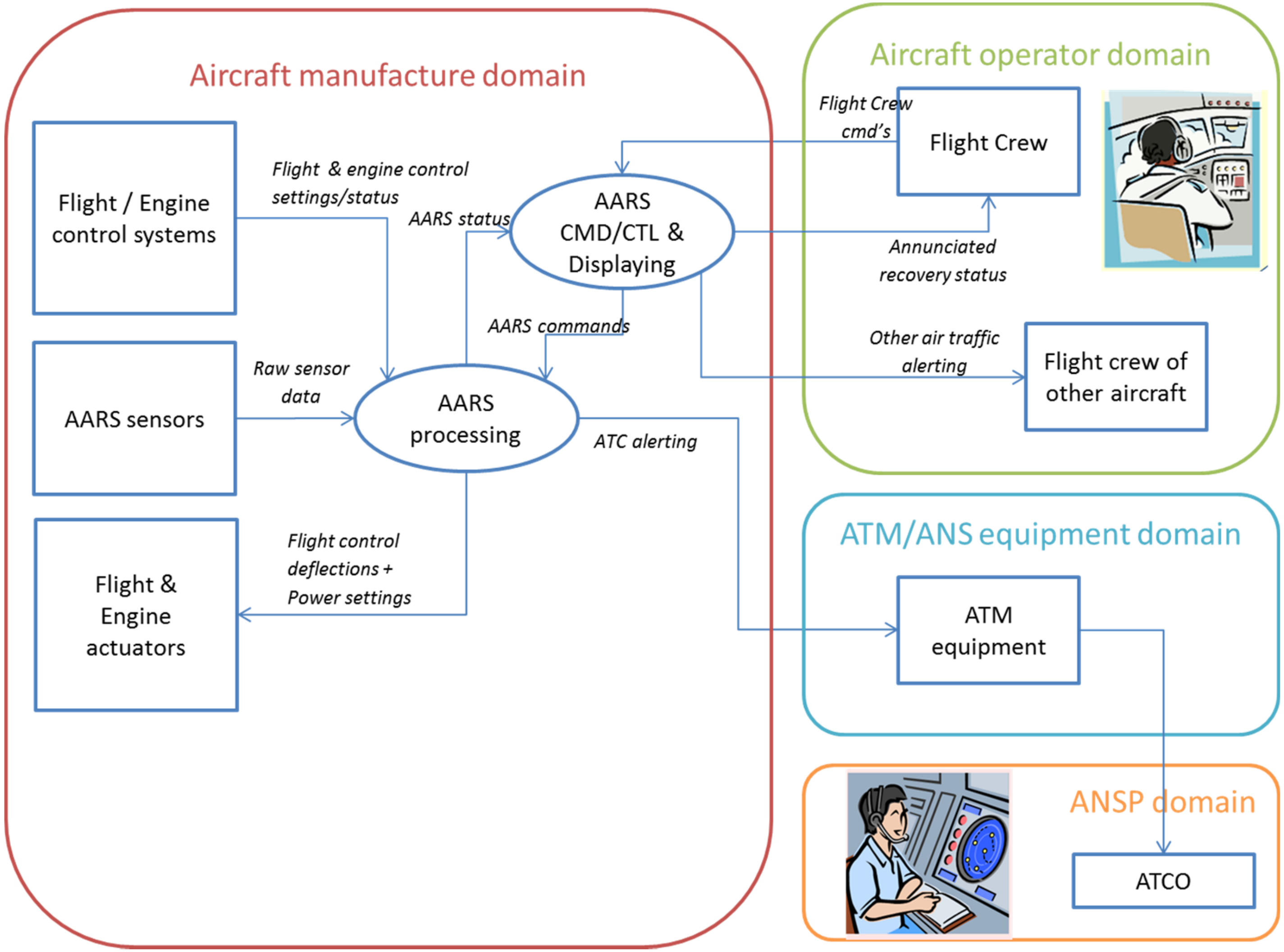
Stage 4: Specification

- Focuses on demonstrating Claim 1: change is specified to achieve an acceptable level of safety
- Safety assessment used to identify the hazards and assess their consequences on the safety of the Total Aviation System
- Broadly aligns with FHA process
- Exemplary identified hazards:
  - During recovery manoeuvre the aircraft deviates significantly from the assigned ATM clearance (laterally or vertically)
  - TCAS alert during recovery manoeuvre
  - Pilot follows EGPWS alert during recovery manoeuvre
  - The AARS drives one or more control surfaces or engine controls to the limit, at maximum rate (hard-over)

Stage 5: Design

- Focuses on demonstrating Claim 2: the logical design for the change satisfies the specification derived within Claim 1
- Safety assessment at this stage considers what the elements of the logical design need to do to ensure safety and the degree of assurance required (FDAL)
- Broadly aligns with early stage PSSA process
- Exemplary identified FDALs:
  - AARS -> FDAL B
  - ATC link -> FDAL C

Stage 5: Design (logical elements)


Aircraft manufacture domain
Flight / Engine control systems
Flight & engine control settings/status
AARS status
AARS CMD/CTL & Displaying
AARS commands
AARS sensors
Raw sensor data
AARS processing
ATC alerting
Flight & Engine actuators
Flight control deflections + Power settings
Aircraft operator domain
Flight Crew cmd's
Flight Crew
Annunciated recovery status
Other air traffic alerting
Flight crew of other aircraft
ATM/ANS equipment domain
ATM equipment
ANSP domain
ATCO

Prelimimary results and observations

- Total Aviation System approach puts early focus on importance of cross-domain interfaces.
- Set-up of logical argument structure is not without difficulties.
- How to define “acceptably safe” for a system that functions as an additional safety net (just like e.g. windshear detection) and that is not mandatory to install?
- Acceptable safety needs to be achieved across the whole TAS. This raises the question, if it is acceptable that increase of safety in one area of the TAS (e.g. reduction of LOC accidents) is balanced with reduced safety in another domain (e.g. increased probability of separation infringement), while the net gain in total safety is positive.
- The ATM equipment, ANSP and Aircraft operational domain currently lack the process for assignment of (F)DALs.
- Inconclusive from this case study whether approach is an actual improvement.
- Approach would require adaptations to current certifying organizations (who is responsible for TAS safety?)

A2COS
safety certification

Questions?

NLR THALES EADS APSYS CAAi Isdefe CERTIFLYER

avanssa ebeni DEEPBLUE consulting&research JRC EUROPEAN COMMISSION TUDelft IL