SEVENTH FRAMEWORK PROGRAMME

ASCOS certification case study: Automatic Aircraft Recovery System (AARS)

Case study for the testing of a novel certification approach

P.J. van der Geest, J.A. Post, M. Stuip, E. van de Sluis (NLR),

S. Bull (Ebeni), G. Temme (CertiFlyer), S. Bravo Muñoz (Apsys)

ASCOS safety certification

This document presents a novel aircraft system, called an Automatic Aircraft Recovery System (AARS). The objective of AARS is to reduce the number of Loss of Control accidents by providing an on-board system that can recover the aircraft automatically from Loss of Control or Loss of Situational Awareness events. The certification of this novel aircraft system has been specified as a use case within ASCOS to demonstrate the applicability of the new certification methodology and to expose potential benefits and drawbacks of the proposed ASCOS certification approach.

Coordinator	L.J.P. Speijker (NLR)
Work Package Manager	A.L.C. Roelen (NLR)

Grant Agreement No.	314299
Document Identification	D4.2
Status	Approved
Version	1.1
Date of Issue	5/11/2015
Classification	Restricted

This page is intentionally left blank

Document Change Log

Version	Author(s)	Date	Affected Sections	Description of Change
1.0	P.J. van der Geest et al.	21-02-2015	All	Version for approval by PMT
1.1	P.J. van der Geest et al.	11-05-2015	Title, Executive Summary	Minor corrections

Review and Approval of the Document

Organisation Responsible for Review	Name of person reviewing the document	Date
NLR	A.L.C. Roelen	21-02-2015
TATM	H. Neufeldt	21-02-2015
TR6	B. Pauly, F. Orlandi	21-02-2015
APSYS	J.P. Heckmann	21-02-2015
CAA UK	A. Eaton	21-02-2015
CertiFlyer	M. Heiligers	21-02-2015
Avanssa	N. Aghdassi	21-02-2015
Ebeni	A. Simpson	21-02-2015
Deep Blue	L. Save	21-02-2015
Organisation Responsible for Approval	Name of person approving the document	Date
NLR	A.L.C. Roelen	21-02-2015
NLR	L.J.P. Speijker	11-05-2015

Document Distribution

Organisation	Names
European Commission	M. Kyriakopoulos
NLR	L. Speijker, A. Rutten, M.A. Piers, P. van der Geest, A. Roelen, J.J Scholte, J. Verstraeten, R. Wever, E. van de Sluis, M. Stuip
Thales Air Systems GmbH	G. Schichtel, J.-M. Kraus, H. Neufeldt
Thales Air Systems SA	B. Pauly, F. Orlandi
Airbus Defence and Space APSYS	S. Bravo Muñoz, J.P. Heckmann, M. Feuvrier
Civil Aviation Authority UK	L. Young, A. Eaton, T. Longhurst, S. Barker, C. Gill
ISDEFE	I. Etxebarria, C. Regidor Gil
CertiFlyer	G. Temme, M. Heiligers
Avanssa	N. Aghdassi
Ebeni	A. Simpson, J. Denness, S. Bull, M. Shuker
Deep Blue	L. Save
JRC	W. Post, R. Menzel
JPM	J. P. Magny
TU Delft	R. Curran, H. Udluft, P.C. Roling
Institute of Aviation	K. Piwek, A. Iwaniuk
CAO	A. Ortyl, R. Zielinski
EASA	E. Isambert
FAA	J. Lapointe, T. Tessitore
SESAR JU	P. Mana
Eurocontrol	E. Perrin
CAA Netherlands	R. van de Boom
JARUS	R. van de Leijgraaf
SRC	J. Wilbrink, J. Nollet
ESASI	K. Conradi
Rockwell Collins	O. Bleeker
Dassault Aviation	B. Stoufflet, C. Champagne
ESA	T. Sgobba, M. Trujillo
EUROCAE	A. n'Diaye
TUV NORD Cert GmbH	H. Schorcht
FAST	R. den Hertog

Acronyms

Acronym	Definition
AARS	Automatic Aircraft Recovery System
ADS-B	Automatic Dependent Surveillance Broadcast
ANSP	Air Navigation Service Provider
AoC	Area of Change
APFCS	Automatic and/or Primary Flight Control System
ASAS	Airborne Separation Assurance System
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATM	Air Traffic Management
CAT	Commercial Air Transport
CAT	Catastrophic
CFIT	Controlled Flight Into Terrain
CMD	Command
CS	Certification Specification
CTL	Control
DAL	Development Assurance Level
DSR	Design Safety Requirements
EASA	European Aviation Safety Agency
ED	Eurocae Document
EGPWS	Enhanced Ground Proximity Warning System
ESD	Event Sequence Diagram
FADEC	Full Authority Digital Engine Control
FAST	Future Aviation Safety Team
FCL	Flight Crew Licensing
FCS	Flight Control System
FDAL	Functional Development Assurance Level
FHA	Functional Hazard Assessment
FMS	Flight Management System

Acronym	Definition
FT	Fault Tree
HAZ	Hazardous
HW/SW	Hardware/Software
JSAT	Joint Safety Analysis Team
LOC-I	Loss of Control In-flight
LSA	Loss of Situational Awareness
MAJ	Major
MIN	Minor
PFCS	Primary Flight Control System
PSSA	Preliminary System Safety Assessment
SSA	System Safety Assessment
STC	Supplemental Type Certificate
SWAL	Software Assurance Level
TAS	Total Aviation System
TAWS	Terrain Avoidance Warning System
TBD	To Be Determined
TCAS	Traffic alert and Collision Avoidance System
UML	Universal Modelling Language

This page is intentionally left blank

Executive Summary

The ASCOS project aims to outline a newly proposed approach to certification that is more flexible and efficient than the current certification processes and considers the impact on safety of all elements of the Total Aviation System (TAS). In order to assess the potential benefits and shortcomings of the new approach a number of use cases have been defined. These use cases define a particular product, system or organisation that needs to be certified. For this certification process the ASCOS approach is followed, according to the newly proposed ASCOS certification approach (as documented in ASCOS D1.3).

The particular use case in this report concerns the certification of an Automatic Aircraft Recovery System (AARS). The objective of AARS is to reduce the number of Loss of Control accidents by providing an on-board system that can recover the aircraft automatically from Loss of Control or Loss of Situational Awareness events. Currently, such a system does not exist for civil aircraft and no specific certification requirements have been specified, as yet. This case intends to highlight potential safety and efficiency gains of using the ASCOS approach when applied to a novel aircraft system. Moreover, this use case is of particular interest when the certification approach takes into account the Total Aviation System, because the safety benefits of the system at aircraft level may be –to some extent- offset by possible safety decrease in for instance the ATM domain. The ASCOS approach has been designed to address such issues from the start.

It is shown that the new approach allows incorporating existing certification methods and tools, such as a Functional Hazard Assessment and Preliminary System Safety Assessment within the new approach. In that sense the new approach is sufficiently flexible. The use of a logical argument structure to define the certification basis (defined as the combined set of applicable claims) and the acceptable means of compliance (the combined set of evidences to substantiate the claims) appears to add structure to the certification process of a novel system. At the same time, the set-up of the logical argument structure and the associated use of goal-structured-notation is not without problems. More guidance and more experience would be needed to be able to define the logical argument structure to the required depth and completeness.

A clear advantage of the new approach is that novel systems are not designed and certified in isolation, but that from the start the impact on the Total Aviation System is taken into account. However, this raises a number interesting questions, such as

- Who is the certifying authority when a system is certified over various domains in the TAS?
- How to deal with different definitions of the acceptable safety level across domains?
- Can a safety benefit in one domain (e.g. reduction in LOC accidents) be accepted at the expense of a (small) safety reduction in another domain (e.g. increased probability of Mid-Air Collision)?

Such questions would need to be addressed before the ASCOS approach can be applied in practice. In this context it is suggested that adoption of the proposed ASCOS certification approach would have to be accompanied with organisational changes in the current certification process, such that responsibilities of certifying authorities and stakeholders are clearly defined within the Total Aviation System.

This page is intentionally left blank

Table of Contents

List of Figures

List of Tables

This page is intentionally left blank

1 Introduction

1.1 Background

Fundamental changes in the institutional arrangements for aviation regulation in Europe, the introduction of new technologies and operations, and demands for higher levels of safety performance call for the adaptation of existing certification processes. The European Commission (EC) Project 'Aviation Safety and Certification of new Operations and Systems' (ASCOS) contributes to the removal of certification obstacles and supports implementation of technologies to reach the EU ACARE Vision 2020 [7][8][9] and Flight Path 2050 [10] goals. ASCOS aims to outline a newly proposed approach to certification that [11]:

- Is more flexible with regard to the introduction of new operations, systems and products;
- Is more efficient, in terms of cost, time and safety, than the current certification processes;
- Considers the impact on safety of all elements of the Total Aviation System (TAS) and the entire system lifecycle in a complete and integrated way.

Based on ASCOS D1.1's [12] analysis of existing regulations and certification processes and ASCOS D1.2's [13] development and evaluation of a long-list of innovative certification approaches, ASCOS D1.3 [14] proposes an outline certification approach. Complementary ASCOS documents present supporting safety methodologies and tools, including a tool for safety risk assessment [25], a tool for continuous safety monitoring [26], and an Area of Change list [15]).

The objectives of ASCOS Work Package (WP) 4 "Certification case studies" are:

- to apply the proposed certification approach and supporting safety based design systems and tools in a number of example case studies, which focus on key safety priority areas.
- to evaluate the practical application of the proposed certification process adaptations
- to assess the overall safety impact of bringing safety enhancements in operational use

ASCOS WP4 consists of 5 sub-tasks, of which WP4.1 through 4.4 consider individual certification case studies, and WP4.5 an evaluation of the results of the results of these.

1.2 Objective and scope

This ASCOS D4.2 document describes a certification case study. Primary objective of this certification case study is to test and evaluate the proposed certification approach of ASCOS D1.3 [14] and supporting safety tools to a practical case in the aircraft systems domain. The case study includes testing the feasibility of the practical application, and collecting feedback of the experience with application of the certification methodology in this field.

The proposed certification approach and supporting safety tools considered are [24]:

- The certification approach proposed in ASCOS D1.3 [14].

- The tool for safety risk assessment selected by ASCOS.
- The Area of Change list from FAST.

The potential safety enhancement selected for this case study is the certification of new safety system on-board of the aircraft with the objective to reduce the probability and consequences of Loss of Situational Awareness (LSA) and Loss Of Control situation in-flight (LOC-I) . The system is referred to as an Automatic Aircraft Recovery System (AARS). This system is a hypothetical system, for which currently no certification basis exists for civil aircraft. However, the technology for implementation of the AARS does already exist for military aircraft. So, the focus in this certification case does not focus on the technical aspects, but mainly addresses the issues concerning the transfer of this technology to civil aircraft, and in particular the certification of such system for a civil aircraft using the new methodology.

In this document, specific use case observations and potential feedback to the proposed certification approach and supporting safety tools is presented in boxes. Where possible, the feedback indicates to which element (i.e. certification approach or supporting safety tool) it applies.

1.3 Document structure

This document is structured as follows:

- Section 2 introduces the proposed certification approach and supporting safety tools being tested and evaluated in this case study.
- Section 3 describes the definition of the case study.
- Sections 4 through 9 describe the application of the stages of the proposed certification approach to this case study, with Section 4 describing the change (Stage 1), Section 5 the definition of the certification argument (Stage 2), Section 6 the development and agreement over the certification plan (Stage 3), Section 7 the specification (Stage 4), Section 8 the design (Stage 5), and Section 9 the refinement of the argument.

2 Proposed certification approach and supporting safety tools

2.1 Stages of the proposed certification approach

ASCOS D1.3 proposes the certification approach. It consists of the following stages:

1. Define the change
2. Define the certification argument (architecture)
3. Develop and 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

This case study considers the first 5 stages.

2.2 Safety risk assessment tool

ASCOS D3.3 [25] describes a risk assessment tool that enables the safety practitioner to model risk scenarios in order to derive safety requirements and safety objectives. The tool model describes accident scenarios and accident avoidance scenarios as event sequence diagrams (ESDs) and fault trees (FT).

The tool is flexible and can be tailored at different levels of details. In this document, the tool is used – as far as practicable – to provide information to stage 4 and stage 5. It is suggested that the ESD elements may be used to support stage 4 and the Fault Tree to support stage 5. This allocation is an a priori hypothesis and can be modified along the development of this case study. In more detail, this is as follows:

- Stage 4: This stage is focused on demonstrating that Claim 1 of the generic argument is met, namely that the change is specified to achieve an acceptable level of safety.[…] The safety assessment in this stage broadly aligns with the FHA process [14].

  The safety practitioner can create the reference scenario as well as the abnormal scenarios. The failure scenarios can be modelled by introducing a probability of failure of the element composing the reference and the abnormal scenario.

  The hazards can be understood as the end state element. The pivotal element corresponds to potential safety barriers.

The safety practitioner can repeat this process with the abnormal and the failure scenario and to create a set of high level safety requirements to avoid these failures.

- Stage 5: Safety assessment at this stage broadly aligns with the PSSA process [14]. The objective of the PSSA process is to devise a number of preliminary concept designs, implementing the proposed functionality, and check whether such design would meet the safety objectives, resulting from the Functional Hazard Assessment. It considers what the elements of the logical design need to do to perform the intended function and to ensure safety and the degree of assurance required. This stage identifies failure modes of each of the preliminary system components and verifies whether the failure probability matches with the criticality of the implemented function. This produces a set of Design Safety Requirements" (DSRs). Fault trees can be applied in this process to assess the failure propagation. These fault trees may work in combination with ESDs (a high level requirement). In this context the ESDs may need to be adapted to reflect the functioning of the preliminary system design (as a new element in the the ESD) and to interface with the fault tree.

> Safety objectives follow from the functional hazard analysis (FHA) as result of the criticality of the hazards. For that only the end states of the scenarios are of interest. E.g. "Crew does not regain control" leads to loss of control. The severity of this hazard can be: catastrophic, hazardous, major or minor. From that follows the safety objective of the functional failure that caused the hazard. This can be: extremely improbable, extremely remote, etc.
>
> It is not clear what is meant by "The D3.3 tool can provide inputs to the safety objectives and the safety requirements that the FHA derives from the analysis of the failure conditions …etc."

2.3 Continuous safety monitoring tool

ASCOS D3.4 describes the tool for continuous safety monitoring.

The scope of the case study described in this document is limited to stages 1 to 5 of the ASCOS method and does not include a elaboration of stage 9, that deals with arrangements for continuous safety monitoring. Consequently, the continuous safety monitoring tool is not used or tested in this case study.

2.4 FAST Area of Change list

The FAST Area of Change list (version 15 November 2013, [30], pp. 15-92) describes per Area of Change a description, associated potential hazards, and a source and comments. The assessment of the FAST Areas of Change (AoC) is an inherent part of the new certification methodology and is addressed in the context of the AARS development in Chapters 4.6 and 4.7.

3 Definition of the case study

This section introduces the case study. Section 3.1 describes the potential safety enhancement considered, and Section 3.2 provides the rationale for its selection for this case study. Section 3.3 describes how the proposed certification approach is applied for this potential safety enhancement.

3.1 The potential safety enhancement

Not so long ago Controlled Flight Into Terrain (CFIT) and Mid-Air Collision MAC) were dominant aircraft accident categories. However, by the introduction of new technical systems, such as Enhanced Ground Proximity Warning Systems (EGPWS) and Traffic alert and Collision Avoidance Systems (TCAS), the number of CFIT and MAC accidents have been greatly reduced. Currently, Loss of Control In-flight (LOC-I) has taken over as the dominant accident category, see the figure below.

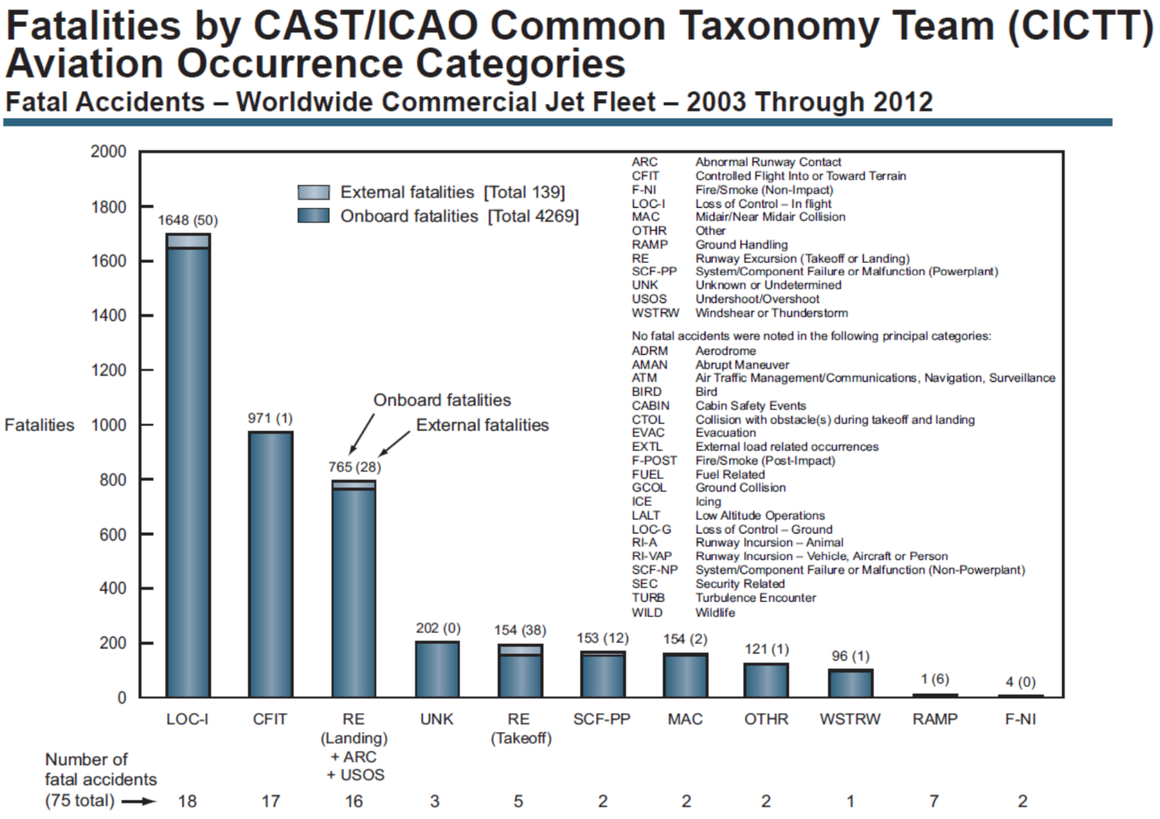


Figure 3-1: LOC-I is today the dominant accident category (© Boeing)

Therefore reducing the number of LOC-I incidents would lead to a major safety enhancement. However, as yet no technical device has been invented in the commercial aircraft domain, that would have the potential to reduce the number of LOC-I accidents, as EGPWS and TCAS have realised for CFIT and MAC accidents.

For this reason, systems and techniques have been investigated that could realise this potential safety enhancement by effectively reducing the number of LOC-I accidents. In 2000 CAST installed the so-called Joint Safety Analysis Team (JSAT) to specify potential interventions that could reduce LOC-I accidents [6].

In the final report of this JSAT, interventions were suggested to develop automatic and manually activated recovery systems. Intervention 245 specifically recommended that manufacturers should develop systems that could return aircraft to normal attitude with one pilot button push (pilot initiated auto-recovery systems)

If such system would only be 50% effective, it has the potential to reduce the total number of accidents with over 10% and save around 80 fatalities per year.

3.2 Rationale for selection

ASCOS and the ASCOS User Group jointly selected the certification of the Automatic Aircraft Recovery System as the potential safety enhancement considered in this case study. The rationale for this selection is based on the considerations given in the previous paragraph. In addition it is important to note that the technology to design and implement such system is currently available for military aircraft.

For instance the Eurofighter Typhoon is equipped with an automatic recovery system, which is described as follows:

> *"In the unlikely event of pilot disorientation, Eurofighter Typhoon's Flight Control System 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."*

A similar system is currently under develoment for the F-22 Raptor.

So, from a technological viewpoint this military technology would merely need adaptation to commercial aircraft.

It is important to note that disorientation, or loss of situational awareness indeed plays an important role in a number of recent LOC-I accidents (such as in Air France AF447 and Turkish Airlines TK1951 near Schiphol). From such accidents it is observed that they are often triggered by insufficient situational awareness in combination with rare failure modes. It is often an unexpected and rare failure that startles the flight crew, leading to distraction from the primary flying tasks and degrading the flight crew situational awareness to the point that erroneous control inputs may lead to extreme, and sometimes unrecoverable, flight conditions.

This may include situations with very low speed, high angle of attack, high pitch attititude and excessive roll angle. In many cases the aircraft is physically (from a control viewpoint) still recoverable from the extreme flight condition. However pilots may become so confused that inproper control inputs are given, such that the flight condition evolves to an unrecoverable situation.

It is very difficult to train pilots sufficiently to cope with these conditions, due to the vast amount of rare failure modes in modern aircraft. Therefore, pilots are today trained in a general way to cope with recovery from upsets. However, this training is usually limited to simulator or in-flight aerobatics training, where the element of surprise to an unexpected failure mode is in generally lacking. The degradation of situational awareness is therefore difficult to simulate and, although upset recovery training certainly has it value, it will not provide a solution to the event that a pilot is confronted with control problems after an unexpected failure mode.

A common factor in the mentioned loss of control accidents is also that a seemingly normal operation may develop into an uncontrollable situation in a very short period of time after a failure has occurred. Therefore, in general there is very little time to diagnose the problem and to identify the proper failure response. The rapid sequence of events, including the associated array of aural and visual alerts and warnings, is a major cause for reduced situational awareness. This in combination with time pressure to resolve a safety critical situation has led in practice to pilots providing improper control and aggravating the situation. In many accident reports this has led to the conclusion of pilot or human error. However, in reality this should be regarded as a system error, due to a system that is insufficiently resistant against failures, and in case of a failure, provides insufficient time to the pilot to diagnose the problem and identify the required recovery control actions.

The potential solution to these problems is the automatic aircraft recovery system (AARS). The function of such system is to restore automatically the aircraft from any potential upset or any other deviation from a normal control regime, after an unexpected system failure or any other flight disturbing event, to a stable flight condition, within the normal flight envelope of the aircraft, and maintain this situation for a sufficient period of time to diagnose the potential problem and to restore situational awareness.

The certification of an AARS is selected as a use case to demonstrate the functioning of the new certification methodology

3.3 Application of the proposed certification approach

To test and evaluate the certification approach of ASCOS D1.3 [14] and supporting safety tools, this case study intends to follow the ASCOS D1.3 guidance closely. This section explains a number of non-trivial issues in the application. An important aspect of the certification approach is that it implicitly addresses the Total Aviation System. In the context of the certification of AARS this is of significant importance. The primary function of the AARS (automatic recovery) may indeed improve safety in the area of LOC-I accidents, but at the same time may interfere in wider areas of the TAS in a sense that it might induce reduced safety in the CFIT or MAC area. Therefore this particular use case is of interest to determine how the new methodology may support certification, such that it achieves acceptable safety within the Total Aviation System.

4 Stage 1: Definition of the change

This chapter describes the application of Stage 1 of the certification approach, and hence aims to ensure that the subject of certification in the TAS is fully understood.

4.1 Application of stage 1

The core of the ASCOS D1.3 [14] guidance for this stage is as follows:

This stage is focussed on ensuring that the proposed change to the TAS is fully understood. This includes defining / identifying:

- the overall goal of the change;
- definition of the change to be made, including the intended functions and an operational concept;
- initial high level architecture for the change, sufficient to allocate requirements between the domains of the TAS;
- definition of the time frame for the actual implementation of the change (target year);
- what Areas of Change (AoC) within the TAS are expected within the defined time frame;
- which of the AoCs, expected within the time frame, would possibly affect the change to be made;
- what part(s) of the system will be changed (including operational processes, products, roles for human actors), or affected by the change – this includes, but is not limited to, identifying the domains changed or affected;
- what organisations are involved in making the change (e.g. introduction of a new ATM system will involve, at least, the ANSP and the equipment manufacturer);
- how the external environment may be affected by the change;
- initial argument architecture related to the change based on the above including identification of assurance contracts
- what existing regulations, certification specifications, standards, AMCs or other relevant guidance material are applicable to the change;
- what requirements (including safety requirements) the change needs to fulfil."

The next paragraphs addresses all these issues sequentially.

4.2 Overall goal of the change

The overall goal of the change is to enhance safety by reducing Loss of Control accidents with potentially 50%, when fully implemented within the commercial air fleet.

The safety risk assessment tool [25], as developed within ASCOS, can be used to provide further detail on what the overall benefits of the AARS may be. In total the risk model contains 28 event sequence diagrams that together model all possible events that contribute to unsafe events. From these 28 events 14 events contribute to Loss of Control in Flight, with as ultimate consequence a collision with the ground.

These events are:

- Incorrect configuration during take-off (ESD-ASC-5)
- Aircraft takes off with contaminated wing (ESD-ASC-6)
- Aircraft encounters wind shear after rotation (ESD-ASC-8)
- Fire, smoke, fumes onboard aircraft (ESD-ASC-11)
- **Flight crew member spatially disoriented (ESD-ASC-12)**
- Flight control system failure (ESD-ASC-13)
- **Flight crew member incapacitation (ESD-ASC-14)**
- Ice accretion on aircraft in flight (ESD-ASC-15)
- **Airspeed, altitude or attitude display failure (ESD-ASC-16)**
- **Aircraft encounters thunderstorm, turbulence, or wake vortex (ESD-ASC-17)**
- Aircraft weight and balance outside limits during approach (ESD-ASC-21)
- **Loss of control due to poor airmanship (ESD-ASC-38)**
- **Single engine failure in flight (ESD-ASC-18)**
- **Unstable approach (ESD-ASC-19)**

The events presented in **Bold-face** indicate cases where the AARS is expected to be effective. Analysis with the risk assessment tool indicates that these cases cover approximately 80% of all Loss-of-Control accidents. By far the largest contribution to the risk of loss of control results from ESD-ASC-19 “Unstable approach” (roughly 55% of the total LOC risk), followed by ESD-ASC-16 “Airspeed, altitude or attitude display failure” (roughly 13% of the total LOC risk). Clearly the AARS would be aimed to provide a risk reduction in those specific areas. So, even when the AARS would not be successful in all cases it appears that an overall risk reduction of 50% for LOC cases may be achievable.

4.3 Definition of the change

This section describes the definition of the change to be made, including the intended functions and an operational concept.

4.3.1 The proposed change

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

4.3.2 Intended Function

The proposed function to be provided by the auto-recovery system is:

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

4.3.3 Functional Requirements

Functional requirements for the system, at highest level, are:

1. The system shall be initiated by the pilot;
2. The recovery shall be performed without any further intervention of the pilot;
3. The recovery shall be performed succesfully, from any intial condition, in the presence of failures in the automatic and/or primary flight control system and/or engines.
4. The recovery shall result in restoring a stable flight regime for some period of time.

4.3.4 List of assumptions

The system design will take into account the following (initial list of assumptions):

Ident	Assumption	Comment
A.1	The AARS will always in hot stand by, when the aircraft is airborne	
A.2	Actuation systems are fully operational	
A.3	The AARS will be installed in large aircraft (CS25)	
A.4	The recovery system can be used in case of failures to the automatic and/or primary flight control system and/or engines, but also in case there are no failures and the flight crew has lost control or when the flight crew is disorientated. It is assumed that the automatic and/or primary flight control system provides “commands” to the actuators (whatever type they are, electrically or hydraulically), which are assumed to function correctly. When the automatic recovery system is activated it will also generate commands to the actuators. If there are failures in the actuators the recovery system will not be able to recover stable flight. The same applies to the control surfaces, which are assumed to be intact. It is assumed that the engine control system is a dedicated system (such as FADEC) to control the engines. When the automatic recovery system is activated it will generate commands to the engine control system, which must be available and working such that (remaining) engines can still be controlled.	

4.4 Initial high level architecture

The initial high level architecture is defined below by means of structograms. The level 0 functional architecture shows the intended function of the change and the interactions with its functional environment. The successive levels show the internal functional architecture of the functional processes.

4.4.1 Level 0 / Context

At the highest level the functioning of the AARS is shown in the context diagram below.

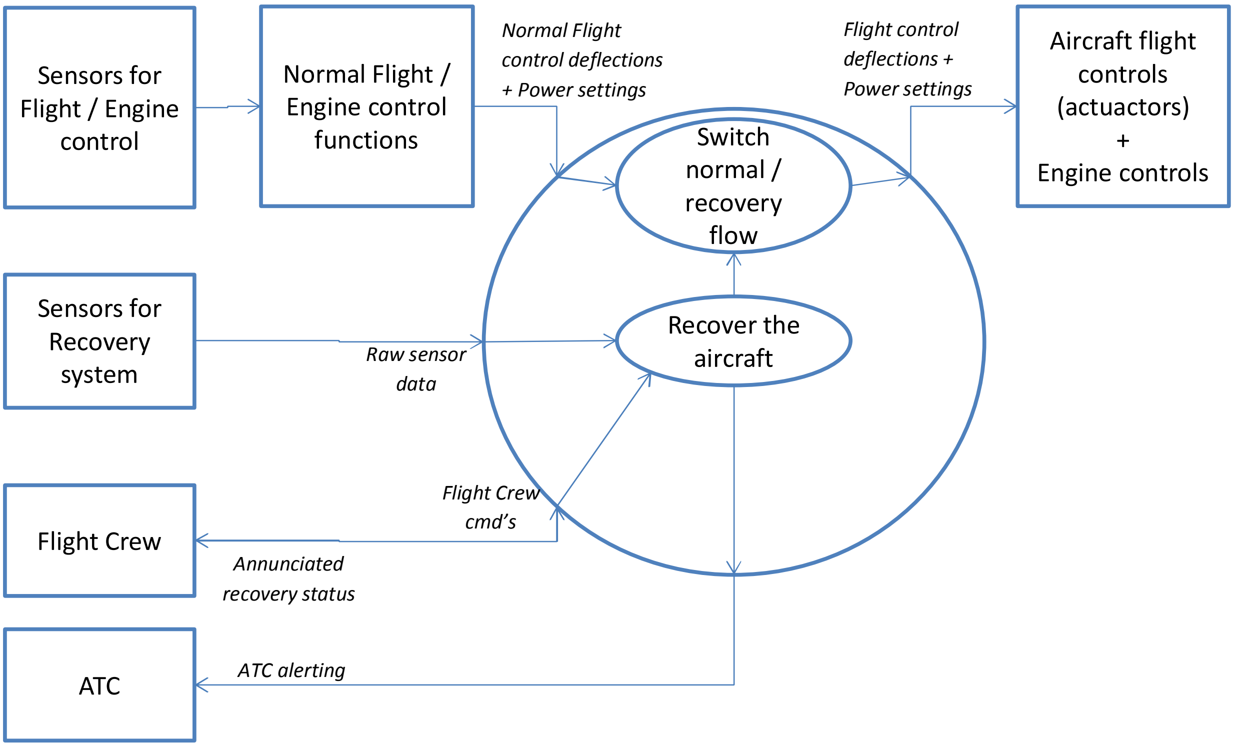

Sensors for Flight / Engine control
Normal Flight / Engine control functions
Normal Flight control deflections + Power settings
Flight control deflections + Power settings
Aircraft flight controls (actuators) + Engine controls
Switch normal / recovery flow
Sensors for Recovery system
Raw sensor data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

Figure 4-1: Aircraft Auto Recovery System: Context diagram

4.4.2 Interaction with domains

The initial high level architecture interacts with the following domains (from D1.3 Appendix B):

- ANSP
- ATM/ANS (possible; depending on design)
- Aircraft manufacturer and certification
- Aircraft operator

See also Paragraph 4.8 and Figure 4-4

4.4.3 Level 1: Main Function: aircraft recovery

The main function of the AARS is to recover the aircraft to a stable and safe flight regime, after pilot inintiation.

The main function is illustrated in Figure 4-2, below.

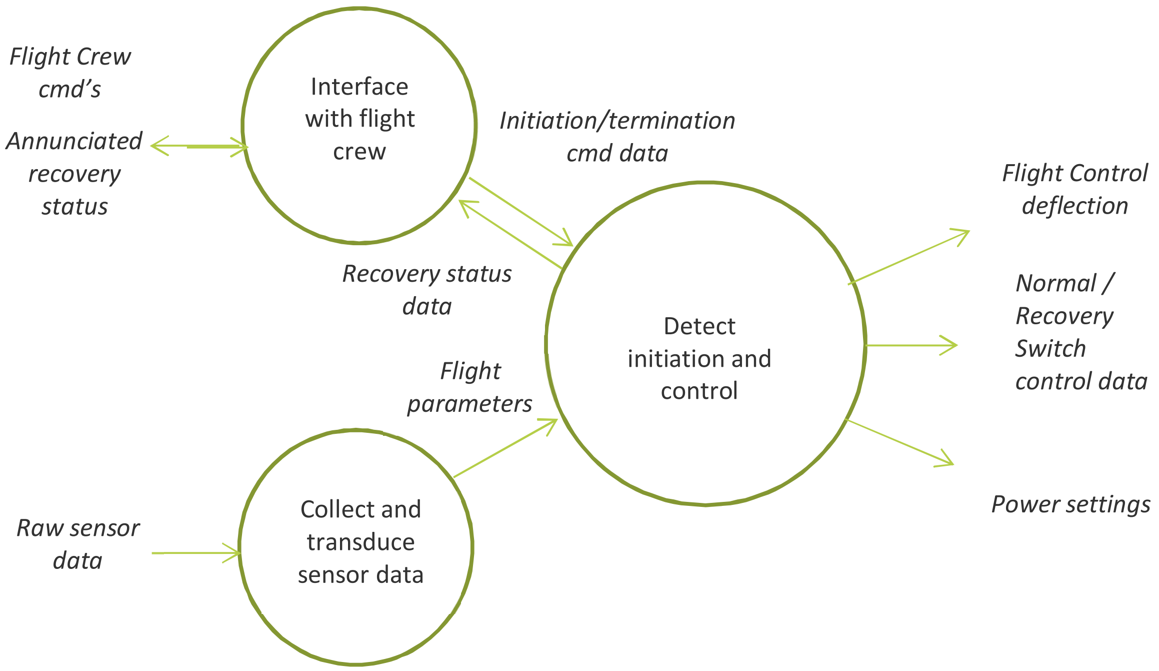

Flight Crew cmd's
Annunciated recovery status
Interface with flight crew
Initiation/termination cmd data
Recovery status data
Flight parameters
Detect initiation and control
Flight Control deflection
Normal / Recovery Switch control data
Power settings
Raw sensor data
Collect and transduce sensor data

Figure 4-2: The main function of AARS: Recover the aircraft

4.4.4 Level 2: Pilot interface function

The AARS can be only initiated by the pilot, and therefore needs a functional interface. Also the recovery status has to be fed back to the flight crew, such that informed decisions can be made concerning termination of the recovery manoeuvre and restoring control to the flight crew. This function is illustrated in the diagram in Figure 4-3 below.

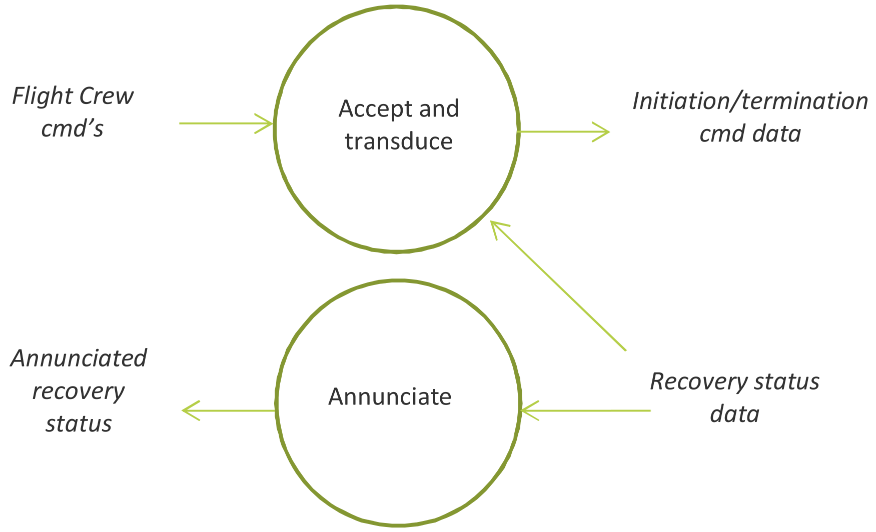


Figure 4-3: Function: Interface with flight crew

4.4.5 Entities, processes and data flow

Based on the high level functions and functional requirements, as described in the previous paragraphs a summary can be made of all entities that are involved in the performance of the functions, related to the AARS. The processes that take place to perform the Auto Recovery function can be listed. The data flow between the various entities, that support the various processes, can subsequently derived.

The involved entities, processes and related data flows are given in the following tables.

Table 4-1: List of involved entities in the Auto Recovery function

Ident	Entity	Domain	Functional requirements
E0.1	Flight crew	Aircraft operator	Crew flying the aircraft and initiating / terminating the Aircraft Auto Recovery system (P0.1).
E0.2	Aircraft Flight controls	Aircraft manufacture and certification	System including flight controls and actuation system. Flight control surfaces and actuation system are operating and can be applied by the Aircraft Auto Recovery system (P0.1). Failures of the actuation systems are excluded.
E0.3	Aircraft Engine Controls	Aircraft manufacture and certification	System including Engine(s) and engine power actuator(s). Engines and actuator are operating and can be applied by the Aircraft Auto Recovery system (P0.1). Failures of the actuator excluded.
E0.4	Sensor 1	Aircraft manufacture and certification	Airspeed sensor
E0.5	Sensor 2	Aircraft manufacture and certification	Attitude & Attitude rate sensor
E0.6	Sensor 3	Aircraft manufacture and certification	Position Sensor
E0.7	Sensor n	Aircraft manufacture and certification	TBD-Sensor
E0.8	Air Traffic Control	ANSP	Ensure safe separation when auto recovery is in progress

Table 4-2: List of processes

Ident	Process	Functional requirements
P0.1	Recover the aircraft	The recovery shall be performed successfully, from any initial condition within or outside the normal flight envelope whereas: • the aircraft is physically (from a control viewpoint) still recoverable from the extreme flight condition; • failures in the automatic and/or primary flight control system and/or engines may be present; and • flight control surfaces are still operating and can be applied by the recovery system. The recovery shall result in restoring a stable flight regime for a TBD period of time; The Aircraft Auto Recovery system should ensure sufficient robustness against failures in the automatic and/or primary flight control system and/or engines The system shall be initiated by the flight crew; The recovery shall be performed without any further intervention the flight crew;
P1.1	Interface with flight crew	The system shall incorporate a flight crew interface to engage the system. The flight crew interface shall be unambiguous and easy to access for the flight crew, even under stress and disorientating conditions. A clear indication to the flight crew shall be given that the system is functional. This requires the system to annunciate when the recovery is complete. It requires also to provide a means and procedure to transfer flight control back to the flight crew after recovery. If a specific initial condition would prevent a successful recovery, the system shall provide an unambiguous annunciation, that it cannot be activated in this condition
P1.2	Detect and control	
P1.3	Collect and transduce sensor data	The sensor system will deliver flight parameter values in a sufficient way and with sufficient accuracy for the automatic recovery system to fulfill its function as specified in P0.1. The sensor system will fulfill its function with or without failures to the automatic and/or primary flight control system and/or engines.
P1.1.1	Accept and transduce	Not further addressed
P1.1.2	Annunciate	Not further addressed

Table 4-3: List of Data Flows

Ident	Data flow	Functional requirements
D0.1	Flight Crew cmd's	The flight crew commands will comprise: • Engage recovery • Disengage recovery • Etc?
D0.2	Annunciated recovery status	A clear indication to the flight crew shall be given that the system is functional. This requires the system to annunciate when the recovery is complete. If a specific initial condition would prevent a successful recovery, the system shall provide an unambiguous annunciation, that it cannot be activated in this condition
D0.3	Flight Control deflection	A flight control deflection command to the flight control actuator
D0.4	Power setting	A power setting command to the engine control system
D0.5	Normal / Recovery Switch control data	Data that controls the disengaging of the normal flight/engine control system and engaging of the recovery control and vice versa.
D1.1	Initiation/termination cmd data	Data that controls the initiation and termination of the recovery action.
D1.2	Recovery status data	Data that represents the status of the recovery
D1.3	Flight parameters	Data that represents the value of flight parameters conform TBD standard.
D1.2.1	Raw sensor data	Raw output from a sensor depending on the type of sensor.

4.5 Time-frame

It is estimated that the implementation of the change will take at least five years. So the target year will be around 2020.

4.6 Expected Areas of Change

According to the outline of the new certification approach (D3.1) the definition of the change has to take into account the Areas of Change, as defined by FAST, in order to assess whether anticipated future developments may introduce additional hazards. The assessment of the AoCs is done in two steps: first it has to be identified which of the AoCs may materialize within the timeframe of the novel system, and secondly from this list those AoCs need to be identified that are relevant for the change at hand. The list of Areas of Change comprises more than 200 items. Many of these might be expected to be to be (partly) realized within the defined time frame.

It would be very helpful if FAST would provide some assessment of the timeframe within which the future hazards are expected to develop. This would prevent applicants to do such assessment based on their own perception without knowing the precise background of the AoC. Moreover, this would increase consistency among results from various applicants.

It is therefore judged not meaningful to list them all in this paragraph. The list below shows the firs 18 items as an example.

Within timeframe 2020 the following AoC are expected to be (partly) realized:

- AoC_1: Introduction of new A/C types: A/C designed and built to accommodate retrofits that can be made without degrading safety;
- AoC_3: Changes in design responsibility and design roles among manufacturing organizations
- AoC_11: Increasingly heterogeneous aircraft fleets (varying software, equipment, capabilities, etc.)
- AoC_13: Increasing crew reliance on flight deck automation for flight-path management, separation assurance and terrain avoidance
- AoC_14: Increasing reliance on automated vehicle health management systems
- AoC_18: Increasing implementation of new cockpit surveillance/recording systems
- AoC_22: Changing approaches to cockpit warning and alert systems
- AoC_31: Increasing implementation of glass-cockpit designs in general aviation aircraft.
- AoC_36: Increasing dependence on Electronic Flight Bag (EFB) for efficient and safe operations
- AoC_39: Increasing use of composite structural materials
- AoC_41: Ongoing electronic component miniaturization
- AoC_43: Increasing implementation of highly-integrated, interdependent aircraft systems
- AoC_47: Changing human factors assumptions for implementing automation
- AoC_51: Delegation of responsibility from the regulating authority to the manufacturing, operating or maintaining organization
- AoC_53: Trend toward privatization of government ATC systems and airports
- AoC_58: Shift toward performance-based solutions and regulations
- AoC_66: Increasing societal pressure to find individuals and organizations criminally liable for errors in design and operations
- AoC_78: Increasing availability and quality of incident, maintenance, ATM, and operations data
- Etc. etc.

4.7 Affected Areas of Change

From the Areas of Change expected to be to be (partly) realized within the defined time frame those listed below may possibly affect the change to be made.

- AoC_13: Increasing crew reliance on flight deck automation for flight-path management, separation assurance and terrain avoidance
- AoC_14: Increasing reliance on automated vehicle health management systems

- AoC_22: Changing approaches to cockpit warning and alert systems
- AoC_43: Increasing implementation of highly-integrated, interdependent aircraft systems
- AoC_47: Changing human factors assumptions for implementing automation
- AoC_95: Changing approaches to ATM warning and alert systems
- AoC_202: Increasing pressure to shorten and compress pilot training

A multitude of potential hazards may arise from those AoCs, such as:

- Failure of the flight crew to remain aware of automation mode and aircraft energy state
- Unfamiliar modes of aircraft automation may result in a perfectly normal flying aircraft suddenly taking on characteristics that the pilot has seldom or never previously encountered
- Pilots may not be adequately trained to understand the philosophy of the automation design when the functionality is being automatically degraded in particular situations for reasons know only to the software
- Latent flaws in the displays or primary flight control system may go undetected, because not enough human-in-the-loop testing is performed
- Systems of such complexity that they are unable to yield to software certification techniques that exist today. In some cases it is not the software itself that is the issue it is the failed logic that drives annunciations and/or changes especially following system degradation/failures.
- Proliferation of caution/warning systems and alerts overwhelming the perceptual and cognitive abilities of the flight crew in critical phases of flight
- Lost or erroneous inputs can result in a cascade of effects on the aircraft.
- Proliferation of caution and warning systems and alerts may overwhelm the controllers in periods of heavy workload
- Shortened type rating may not provide opportunities to detect weaknesses in basic pilot skills among the candidates

All these potential hazards are relevant in the context of the development of the AARS. Clearly the inherent objective of the AARS will be such that these potential hazards are sufficiently mitigated in the sense that the AARS will provide a means to prevent serious consequences to arise from mentioned hazards. It is interesting to note that FAST implicitly addresses the Total Aviation System. In particular the potential hazard that "*the proliferation of caution and warning systems and alerts may overwhelm the controllers in periods of heavy workload*" requires devoting sufficient attention to the interface between the aircraft and ATM in case an auto-recovery is in progress. Downlinking another caution or warning to controller may indeed contribute to information overload in periods of heavy workload and therefore may be counterproductive.

Therefore, the use of applicable AoCs in the change definition is considered useful as it may direct attention to areas otherwise easily overlooked, in particular in the area of the Total Aviation System.

4.8 Domains and organisations

4.8.1 Affected domains

The following domains are identified to be affected by the change. Below each domain the affected parts of the system are mentioned:

- ANSP
    - Air Traffic Management / Surveillance / RPAS contingency procedures
- ATM/ANS equipment
    - Data communication
- Aircraft manufacture and certification
    - ACAS/ASAS
    - EGPWS
- Aircraft operator
    - Aircraft Operations
    - Training
    - Maintenance

The following figure presents the dependencies of the AARS within the Total Aviation System:

Figure 4-4: Dependencies of the AARS within the Total Aviation System

4.8.2 Involved organizations

The following organizations are involved in making the change:

- Aircraft manufacturer
- Avionics/Equipment manufacturer
- Aviation Authority (Certifying entities)
- Training organizations
- ANSP
- Maintenance organisations

4.9 Effect on external environment

No significant relevant effects on the external environment have been identified.

4.10 Initial argument structure

The following figure provides an initial argument structure for the certification of an Aircraft Automatic recovery System (AARS). Chapter 5 details and enhances this initial structure.

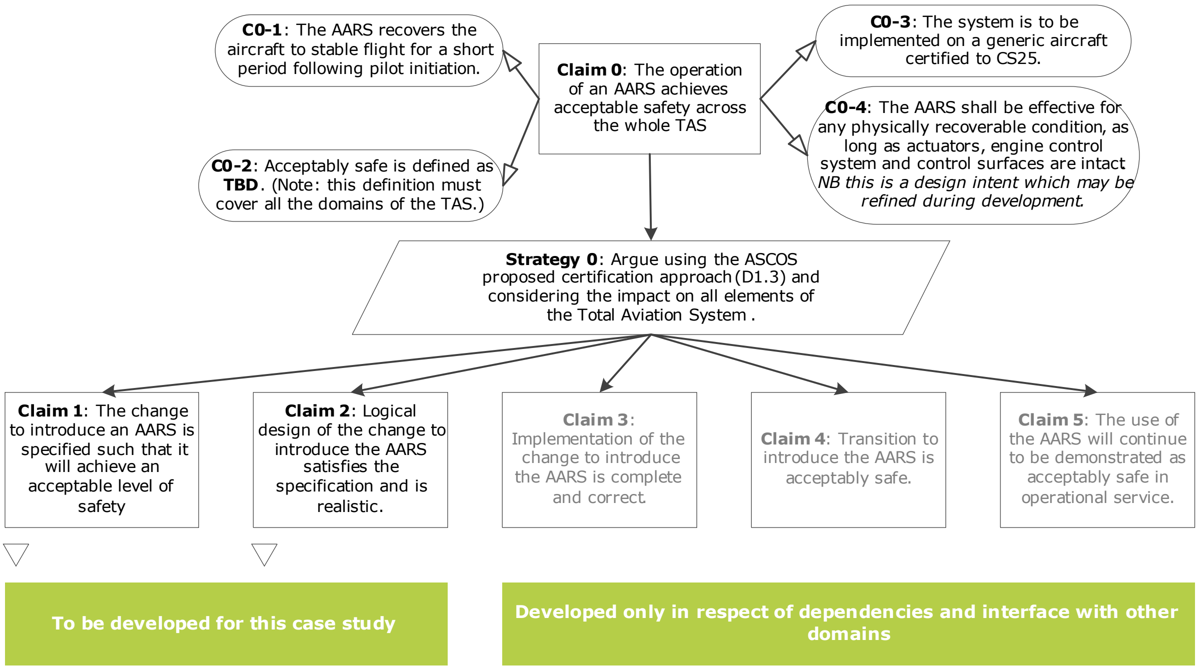

C0-1: The AARS recovers the aircraft to stable flight for a short period following pilot initiation.
C0-2: Acceptably safe is defined as **TBD**. (Note: this definition must cover all the domains of the TAS.)
Claim 0: The operation of an AARS achieves acceptable safety across the whole TAS
C0-3: The 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

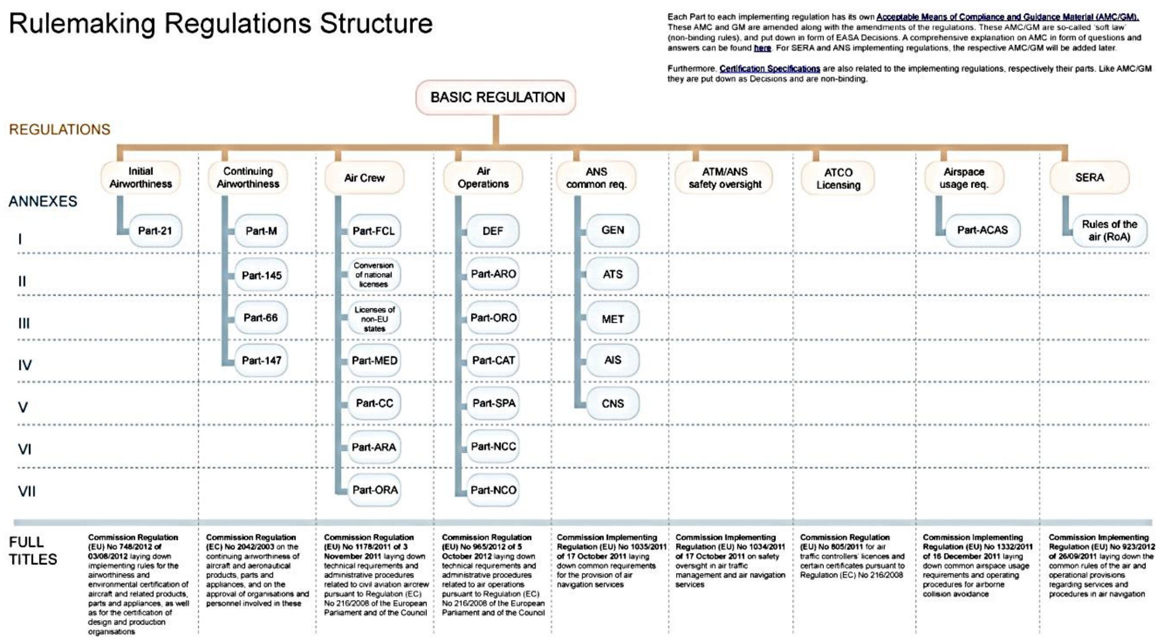
Figure 4-5: Initial argument structure for the certification of the AARS

4.11 Regulations, means of compliance and guidance

As mentioned CO-3 of the initial argument structure the system is to be implemented in aircraft certified to EASA CS-25. Correspondingly, it is evident that EASA will also be the certifying authority, and will be responsible for issuing the Supplemental Type Certificate (STC) for the AARS. However it is less clear which organisation would be responsible for approval of aspects outside the STC, such as the interface with ATC. Although the authority of EASA covers the ATM domain, it is not clear whether such interface would be certified under the authority of EASA or as a local implementation by a National Authority.

> It is observed that adoption of the ASCOS certification approach would have to be accompanied with organisational changes in the current certification process, such that responsibilities of certifying authorities and stakeholders are clearly defined within the Total Aviation System.

The general regulatory structure in Europe is shown in the figure below:


Rulemaking Regulations Structure

Each Part to each implementing regulation has its own Acceptable Means of Compliance and Guidance Material (AMC/GM). These AMC and GM are amended along with the amendments of the regulations. These AMC/GM are so-called 'soft law' (non-binding rules), and put down in form of EASA Decisions. A comprehensive explanation on AMC in form of questions and answers can be found here. For SERA and ANS implementing regulations, the respective AMC/GM will be added later.

Furthermore, Certification Specifications are also related to the implementing regulations, respectively their parts. Like AMC/GM they are put down as Decisions and are non-binding.

Commission Regulation (EU) No 748/2012 of 03/08/2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations

Commission Regulation (EC) No 2042/2003 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these

Commission Regulation (EU) No 1178/2011 of 3 November 2011 laying down technical requirements and administrative procedures related to civil aviation aircrew pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council

Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council

Commission Implementing Regulation (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services

Commission Implementing Regulation (EU) No 1034/2011 of 17 October 2011 on safety oversight in air traffic management and air navigation services

Commission Regulation (EU) No 805/2011 for air traffic controllers' licences and certain certificates pursuant to Regulation (EC) No 216/2008

Commission Implementing Regulation (EU) No 1332/2011 of 16 December 2011 laying down common airspace usage requirements and operating procedures for airborne collision avoidance

Commission Implementing Regulation (EU) No 923/2012 of 26/09/2011 laying down the common rules of the air and operational provisions regarding services and procedures in air navigation

Figure 4-6: EU rulemaking regulations structure

Based on this regulatory umbrella the following regulations are applicable:

- Initial Airworthiness, Part 21; the AARS will be a new system and therefore will affect the Type Certificate
- Part M; the AARS will require maintenance instruction to ensure continued airworthiness

Remark Concerning Part-21: It is assumed that the change concerns large aeroplanes. Then CS-25 (amendment 15) is the applicable certification basis and the main applicable certification requirements are CS 25.1309 (Equipment, Systems and Installations) and CS 25.1302 (Installed systems and equipment for use by the flight crew).

Other applicable EU regulations are to be further determined. It is possible that introducing the AARS will affect for instance flight crew licensing (Part FCL), as the pilot may have to be specially trained to operate the AARS, and this training requirement may be part of the pilot license. Also Part-CAT (Commercial Air Transport Operation) could be affected; for instance regulations dealing with interfacing with the flight data recorder (CAT.IDE.A.190) and data link recording (CAT.IDE.195) could be affected. Furthermore it should be noted that introduction of the AARS might affect the required Air Navigation Services (ANS), as Air Traffic Control personnel may have to be trained and ATC procedures may have to be adapted. Therefore, possibly also part-ANS may be affected.

Because the AARS is a novel system, there will be no a priori specific guidance material available.

Associated EUROCAE / SAE docs can be part of the airworthiness certification base, in particular:

- ED 12C Software considerations in airborne systems and equipment certification
- ED 14G Environmental conditions and test procedures for airborne equipment
- ED 18 Audio systems characteristics and MPS covering microphones (except carbon), headsets, handsets and loudspeakers, audio selector panels and amplifiers (in case of audio alerting of flight crew)

4.12 Requirements

The system requirements are derived from the functional description, as given in Chapter 4.3.

The high level system requirements are related to the main functions identified, i.e.

1. The system shall be initiated by the flight crew;
2. The recovery shall be performed without any further intervention the flight crew;
3. The recovery shall be performed successfully, from any initial condition whereas:
    a. the aircraft is physically (from a control viewpoint) still recoverable from the extreme flight condition;
    b. failures are present in the sensor systems, the automatic and/or primary flight control system and/or engines;
    c. flight control surfaces are still operating and can be applied by the recovery system;
4. The recovery shall result in restoring a stable flight regime for a TBD period of time;

The preliminary system requirements derived from these functional requirements are as follows:

1. A) The system shall incorporate a pilot interface to engage the system.

B) The pilot interface shall be unambiguous and easy to access for the pilot, even under stress and disorientating conditions.

C) A clear indication to the pilot shall be given that the system is functional.

D) Clear operational procedures must be put in place concerning the system activation and termination.

2. A) After system activation, the system must invalidate any control input from any other flight system;

B) Clear operational procedures must be put in place that the pilot should refrain from giving pilot inputs during the recovery, until a stable and safe flight regime is restored. This requires the system to annunciate when the recovery is complete. It requires also to provide a means and procedure to transfer flight control back to the pilot after recovery.

3. A) The recovery capability shall be robust against, and independent of, failures in the automatic and primary flight control system. Because the system must have control over the actuation systems (engine control and primary control surfaces) the failure conditions are limited to sensor failures and system failures (H/W and S/W) in the mentioned control systems, but failures to actuation systems are excluded.

B) The system shall provide a means to define indepently the safe flight envelope and shall provide a control strategy to restore the aircraft flight condition to within this safe flight envelope, from any given initial condition. If a specific initial condition would prevent a succesful recovery, the system shall provide an unambiguous annunciation, that it cannot be activated in this condition.

C) The recovery manoeuvre shall be performed within the performance and structural limitations of the aircraft.

4. A) A stable flight regime shall be defined as a straight and level –or gently climbing- flight, with wings level and airspeed with a fair margin above the stall speed and below the maximum operating speed.

B) The stable flight shall be maintained for sufficient time (around 2-4 minutes).

C) The stable flight shall be mainained in the presence of engine failure.

D) Means shall be provided to annunciate that the stable flight regime is achieved.

C) Means shall be provided that the pilot can disengage the auto-recovery after the stable flight regime has been established.

5 Stage 2: Definition of the certification argument

5.1 Application of stage 2

This section shorty summarises the ASCOS D1.3 [14] guidance for this stage.

“The generic argument to be adopted should be chosen and developed into an argument architecture. It is proposed that, for each of the case studies, the generic argument (*cf. Section 4.10*) is initially adopted, unless it is evident from the outset that an alternative argument is appropriate. (In the event that alternative top level arguments are identified during the case studies, these will be documented in the presentation of the refined approach.). Note however, that variation in the argument approach is not likely to affect the modularisation of the argument as this is driven more by the existing commercial and physical partitions within the TAS. It may affect the links between modules but this should be avoided especially if it affects an existing assurance contract. At this stage the argument should identify any potential impact either on or from existing assurance contracts or modules outside the initial scope of the change. Note the full impact may not be realised until later (e.g. during implementation) but consideration should still be given to any known impacts at this stage, as they may alter or undermine key assumptions in the design of the change.

The development of the argument architecture should follow the principles identified in [14] section 2.2 and section 3.3. The architecture will follow existing established certification approaches where these remain appropriate (e.g. compliance with CSs for airborne equipment) while ensuring that any consequences of using this approach are fully understood and managed – for example the need to establish that the CS remains applicable within the context of the specific change. The argument should then be developed by the argument architect (see [14] section 2.2.1). It remains the argument architect’s responsibility to maintain the argument throughout the lifetime of the change. The level to which the argument can be developed at this stage is limited until the assessment activities associated with Specification (Stage 4; *cf. Section 7*) and Design (Stage 5 – *cf. Section 8*) have been completed. However, it is important to develop the initial argument to provide a basis for development and agreement of the certification plan.

5.2 Overall structure

The argument structure presented in D1.3 [14] (section 3.2) will be used as the basis for this case study. The scope of the case study is to develop (only) claims 1 and 2 of the argument. However, we will also consider the impact which the case study will have on the other parts of the argument.

5.3 Responsibility for Parts of the Argument

5.4 Evidence Types

Direct evidence is the evidence that a particular claim is satisfied – this is evidence relating directly to observable properties of an output or product.

The argument must also be supported by *backing* evidence, which is the evidence there is sufficient confidence in the direct evidence, i.e. that the processes followed were suitable and that they were undertaken by suitably competent people. Backing evidence will be presented separately within the claim structure.

This is captured in the argument as claims that the evidence used to support the argument is *trustworthy*. (See Claim 1.4; there will also be similar claims under Claim 2.)

5.5 The Argument

The argument is described in the sections below. The argument is developed into several levels. Each level is described by means of a **claim** which is supported by **items of context**. The claim is then decomposed in **subclaims**, where the subclaims form the claims of the subsequent level. The decomposition takes place by means of a strategy.

5.6 Claim 0: Automatic aircraft recovery system is acceptably safe

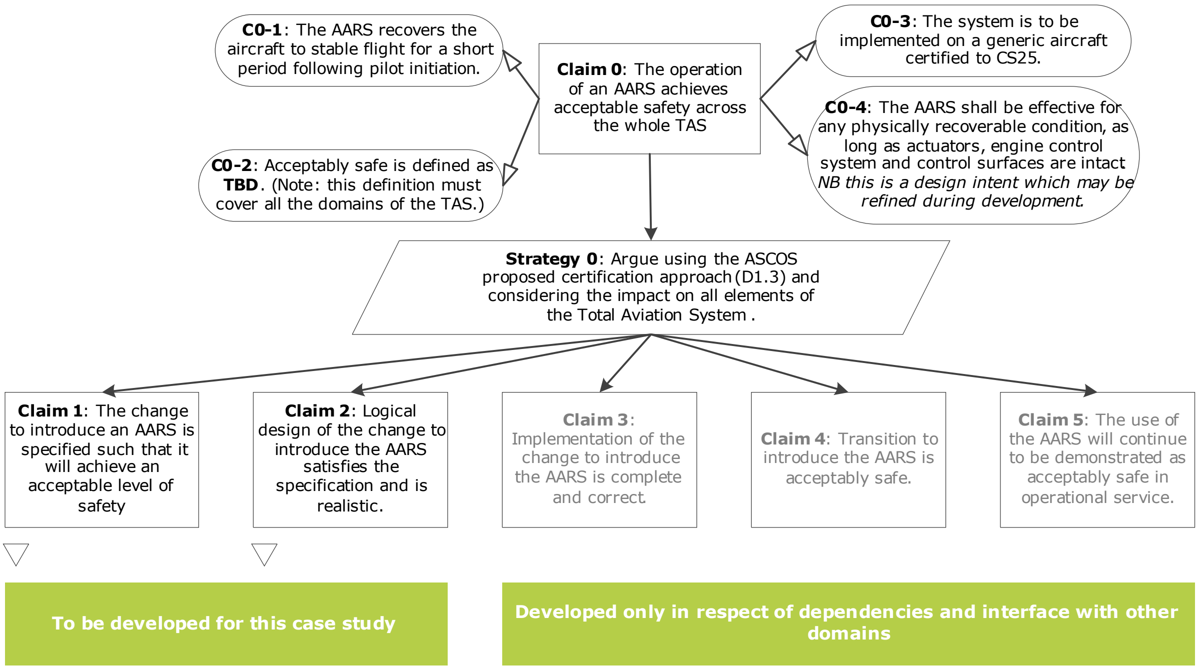

C0-1: The AARS recovers the aircraft to stable flight for a short period following pilot initiation.
C0-2: Acceptably safe is defined as TBD. (Note: this definition must cover all the domains of the TAS.)
Claim 0: The operation of an AARS achieves acceptable safety across the whole TAS
C0-3: The system 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

Figure 5-1: Top level argument structure (claim 0) for the certification of the AARS

Figure 5-1 shows the adaptation of the top level of the D1.3 argument to this case study.

Claim 0 is the top level claim being made by the argument, namely that the operation of an Automatic Aircraft Recovery System (AARS) is acceptably safe across the whole TAS.

Note the following points.

1. *The claim covers the lifecycle of the change* – i.e. it covers specification, design and implementation of the AARS; it also covers transition into operation and monitoring while in operation. Each of these elements is covered in a separate subclaim.
2. *We do not claim that operations of the aircraft as a whole are acceptably safe* – we are only considering how the AARS contributes to the safety of the operation of the aircraft. To make a claim for aircraft operations as a whole, we need to consider significant areas outside the scope of the case study;
3. *We will consider both the positive and negative effects of the AARS on the safety of the aircraft* – i.e. we consider how the AARS benefits the aircraft by “rescuing” it from loss of control, as well as how failure of the AARS itself may threaten the aircraft (and the wider TAS).

Use Case observation:

- How to define “acceptably safe” for a system that functions as an additional safety net (just like e.g. WS detection/guidance) and that is not mandatory to install? It must be inferred that the TAS is considered already acceptably safe by current standards. The added safety by the AARS does in itself not change the level of acceptable safety; otherwise there would have been a mandate for the system. In other words the top-level claim is inherently achieved by AARS whether it functions or not (assuming that the net effect of the introduction does not lead to reduced safety). Therefore, to use this generic top-level claim may become a hollow phrase.
- 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.

We define the following items of context, to add detail to the claim being made; in theory all these items of context could be combined with the claim to make one very long sentence – although this would then make the claim very difficult to understand! These items of context are defined further in the following sections.

- **C0-1** provides (a pointer to) the definition, at an abstract functional level, of the operation of the AARS.
- **C0-2** defines the level of safety which needs to be achieved by the introduction of the AARS.
- **C0-3** identifies that the AARS is conceived as an adaptation of an existing civil piloted fixed wing cargo aircraft (certified under CS-25).
- **C0-4** defines the operational environment to which the safety argument applies.

The top level claim (Claim 0) is then decomposed into subclaims (Claims 1 – 5), each making a “smaller” claim about the change. The premise of the argument is that, when taken together, the subclaims are sufficient to demonstrate that the top level claim has been achieved. Strategy 0 documents the approach which is taken in subdividing the claim – i.e. the approach proposed in ASCOS D1.3 [14] – which considers specification, design, implementation, transition into operation and operational service.

5.6.1 Context C0-1: Definition of the operation of the AARS

In order to undertake the safety analysis, we need a high level, abstract definition of the operation of the AARS and its effect on the other parts of the TAS.

The initial description is made up from:

- a functional description of the operation – see section 5.6.1.1;
- an expansion of this functional description in the form of operational scenarios – see section 5.6.1.2;
- the operational environment in which the AARS is to operate – see section 5.6.4.

This description has been developed from the description in this. It will be further developed during the assessment, in particular to identify:

- the sequence of events following the detection of a failure;
- the interactions between the AARS and the rest of the TAS (via the aircraft systems), including those which take place via the remote pilot.

5.6.1.1 *Abstract Functional Description*

The function of the AARS is to provide after pilot initiation a rapid and automatic recovery of the aircraft to a stable flight regime within the flight envelope from any initial flight condition within or outside the normal flight envelope and with or without failures to the automatic and/or primary flight control system and/or to engines. The stable flight regime should be maintained for sufficient time for the pilot to regain adequate situational awareness, to diagnose any problem and to identify correct interventions to ensure continued safe flight.

5.6.1.2 *Operational Scenarios*

The analysis within the argument is based on scenarios of operation of the AARS and the associated description of the sequence of events in each scenario.

Scenarios describe the operation of the AARS at a functional level, without considering its internal architecture. In other words, this case the scenarios describe the operation of the AARS as seen from the outside showing the effect on the rest of the total aviation system (TAS).

Scenarios are divided into three types:

- Normal scenarios describe the operation of the AARS in an "ideal" environment: i.e. in normal conditions of the external system, where the AARS itself has not failed in any way:
  During normal conditions of the external system the AARS will always be in hot stand by, when the aircraft is airborne. In these conditions the AARS can be initiated by the pilot (see section 4.3).

- Abnormal scenarios – where the AARS is operating outside the usual envelope of the external system (e.g. this could be due to (inter alia) incorrect maintenance, incorrect actions by the pilot, severe weather conditions, busy traffic conditions) but the AARS itself has not failed in any way:
  The AARS can be used in case of failures to the automatic and/or primary flight control system and/or engines, but also in case there are no failures and the flight crew has lost control or when the flight crew is disorientated. This can be within or outside the normal flight envelope of the external system (see section 4.3).
- (Self)failure[1] scenarios – where the AARS itself has failed. Note: at the initial stage of the analysis we can only consider the consequence of these failures; the causes are considered later.
  These scenarios are typically treated in a functional hazard analysis, which is described in section 7.3. In this analysis three types of failure are addressed:
  - Detected failure of the AARS to perform its intended function.
  - Undetected failure of the AARS to perform its intended function.
  - Erroneous operation of the AARS.

5.6.2 Context C0-2: Level of Safety

C0-2 defines the level of safety which needs to be achieved by the change. The level of safety must be defined for all domains within the TAS, and the criteria may be different in each domain. This item is adequately described for this level in sections 6.1 up to 6.5 and will be elaborated further in the next stages.

5.6.3 Context C0-3: Adaptation of existing aircraft

C0-3 identifies that the wider certification context is an aircraft otherwise compliant with CS-25 [23]. Any new certification specification for the AARS would be developed in this context.

5.6.4 Context C0-4: External System Conditions

C0-4 defines the conditions of the Total Aviation System (TAS) (including, but not limited to, the condition of the aircraft itself) within which the AARS is capable of operating. The case study definition (see section 4: Stage 1: Definition of the change) aspires to a system able to recover from any condition which is physically recoverable, as long as the actuators and engine control system are functional and the control surfaces are intact. However, this may not be achievable, and C0-4 may require refinement during the development of the argument as scenarios are identified from which the AARS will not be able to recover. This may include scenarios where activating AARS causes an accident which would not otherwise have occurred.

5.7 Claim 1: AARS specified to achieve an acceptable level of safety

Claim 1 (see Figure 5-2) is that the AARS is specified to achieve an acceptable level of safety.

[1] Note, in this context, (self)failure refers to failure of the AARS to function as specified, not to an external failure leading to the requirement for an action from the AARS.

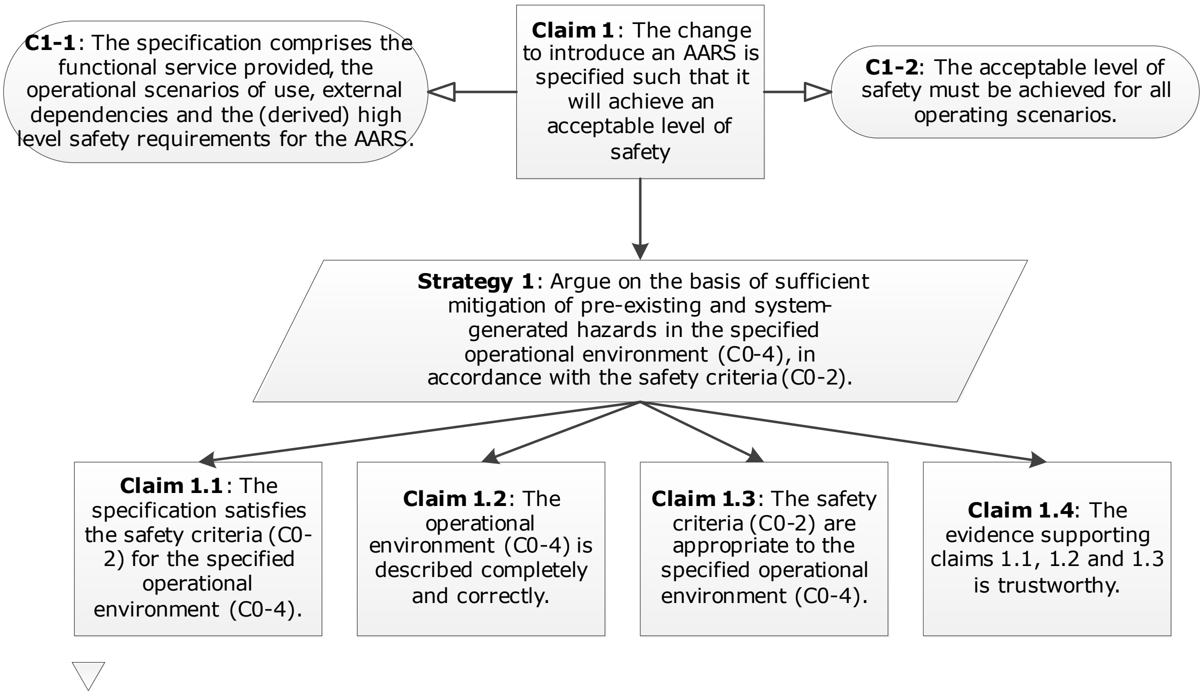

C1-1: The specification comprises the functional service provided, the operational scenarios of use, external dependencies and the (derived) high level safety requirements for the AARS.
Claim 1: The change to introduce an AARS is specified such that it will achieve an acceptable level of safety
C1-2: 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.

Figure 5-2: AARS specified to achieve acceptable level of safety (Claim 1)

Claim 1 is supported by the following items of context[2]:

- Context **C1-1**: explains that the specification of the AARS (at the functional level; section 4 “Stage 1: Definition of the change”) comprises the following items:

a.	the overall goal of the AARS:	section 4.2
b.	a high level description of the intended function:	section 4.3.2
c.	description of the operational scenario’s:	section 4.3.2
d.	the functional requirements for the AARS:	section 4.3.3
e.	the initial high level functional architecture:	section 4.4
f.	the interaction with domains:	4.4.2
g.	the initial requirements:	4.12

Note: at this level we do not consider how the AARS is actually implemented[3]; thus there is no consideration of equipment or specific human roles, just what the AARS will achieve and how it will interact with the rest of the TAS.

Note: the specification referred to here is developed as part of the work to support claim 1, it is not required (or possible) for it to be complete before the stage 4 assessment starts.

[2] These items of context are in addition to the context already defined for Claim 0: in the GSN notation, context from higher level claims is automatically “inherited” by the lower level claims.

[3] It is obviously important that the concept is capable of being implemented: thus achievability is addressed in claim 2.

- Context **C1-2**: clarifies that the acceptable level of safety (defined in **Context 0-2**) must be achieved for all the operating scenarios, including normal, abnormal and (self)failure scenarios.

> The purpose of C1-1&2 is not entirely clear as it repeats is already described in stage 1 (section 4). Also: This kind of refinement of the context does not bring in new information since all known details are already presented in stage 1. When new specification details would come up due to the development process these also should be mentioned in stage 1. In that case C1-1 could be used as an administration of that fact.

This claim (Claim 1) is then decomposed into subclaims (Claims 1.1 – 1.4); together these claims combine to satisfy claim 1, in the same way that claims 1-4 combine to satisfy claim 0. The main claim is Claim 1.1 (that the specification satisfies the safety criteria for the specified operational environment): this is elaborated further below. The other claims may seem obvious, but they are listed to emphasise that we also need to demonstrate that:

- Claim 1.2: the description of the operational environment (C0-4) is complete and correct;
- Claim 1.3: the safety criteria (C0-2) are at the correct level and match the operational environment;
- Claim 1.4: sufficient backing evidence (see section 5.4) is in place to show that the direct evidence supporting the claims can be relied upon – i.e. used suitable processes which were correctly applied by competent personnel.

Claim 1.1 (see Figure 5-1) is that the specification of the AARS satisfies the safety criteria (C0-2) when operating in the specified operational environment (C0-4). The main assessment to support this claim will be a form of **functional hazard assessment** (FHA). This FHA is performed in Stage 4: Specification (section7.3).

As specified in the description of the certification methodology (D1.3), it is important that in that stage the argument for Claim 1 is fully developed and substantiated with relevant evidence.

Strategy 1.1 explains that the strategy for demonstrating Claim 1.1 is to show that all relevant hazards have been identified and that the specifications (safety objectives) guarantee that when the system performs as designed, all identified hazards are mitigated sufficiently, both in the absence of (self) failure and in the event of (self)failure of the AARS.

Each of the sub-claims 1.1.1 to 1.1.3 is described further in the sections below.

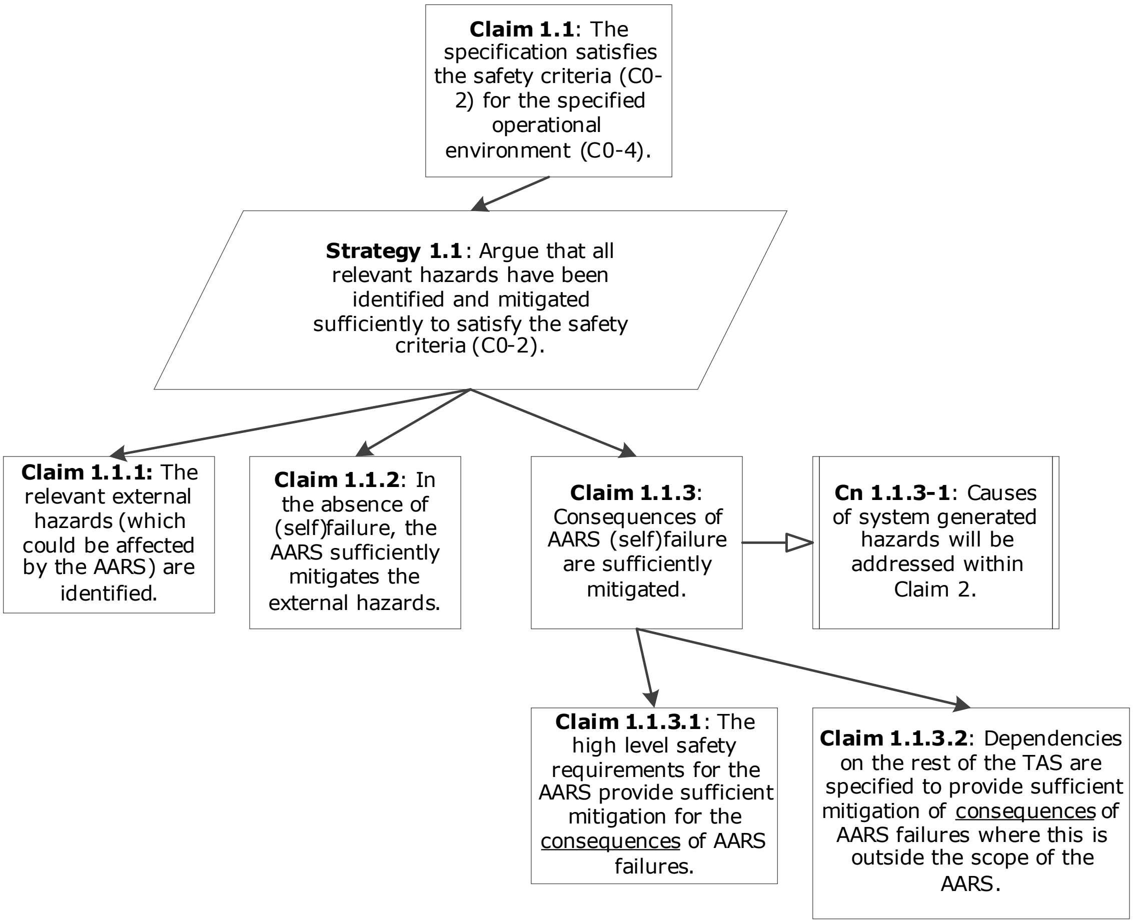

Claim 1.1: The specification satisfies the safety criteria (C0-2) for the specified operational environment (C0-4).
Strategy 1.1: Argue that all relevant hazards have been identified and mitigated sufficiently to satisfy the safety criteria (C0-2).
Claim 1.1.1: The relevant external hazards (which could 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.

Figure 5-3: Argument that AARS specification satisfies the safety criteria (Claim 1.1)

5.7.1 Claim 1.1.1: Relevant external hazards are identified

In line with the characteristics of the FHA process, the following requirements apply:

- The FHA should establish how safe the AARS needs to be;
  The required safety level depends on the criticality of the intended functional failure conditions (minor, major, hazardous or catastrophic) ;
- The FHA should be conducted at the functional level and therefore is largely independent of the actual implementation;
- The FHA should also address the impact of external factors and of interaction among the various domains on the intended function of the AARS.

At this stage the assessment is performed independent of the implementation of the system and so failures of the system are related to specification-level functions only. However, it should be noted in some cases consideration must also be given to concept of operations, modes of operation or other operational definitions which depict the intended use of the system in several domains of the TAS.

.

The intended functions of the system and the associated functional requirements have been listed in Chapter 4.3. This information is used together with a number of reference scenarios, defined in Chapter 7.2, to determine the functional hazards and their consequences. It is the purpose of the intended function to mitigate the pre-existing hazards[4]. In this particular case the pre-existing hazards that are aimed to be mitigated are:

- Loss of Control
- Loss of Situational Awareness,

These hazards could possibly be initiated by aircraft system failure. It is assumed (which is to be demonstrated in later stages) that when the system performs as designed, the pre-existing hazards are mitigated. Unsafe conditions can only arise from the system not performing its intended function. Therefore the hazard analysis focuses on system generated hazards and functional failures.

5.7.2 Claim 1.1.2: AARS provides sufficient mitigation of external hazards

This claim is about showing that the AARS, when operating without (self)failure, provides sufficient safety benefit to the aircraft (and TAS). Essentially, this answers the question of whether the AARS is "good enough" at doing the job it is intended for, when it is operating correctly. The high level safety requirements are derived through identification and assessment of normal and abnormal conditions of the external system. What the AARS should do in these conditions is established in the intended function(s) (see section 4.3.2) of the AARS which in brief are formulated below.

- During normal conditions of the external system the AARS will always be in hot stand by, when the aircraft is airborne. In these conditions the AARS can be initiated by the pilot (see section 4.3).
- The AARS can be used in case of failures to the automatic and/or primary flight control system and/or engines, but also in case there are no failures and the flight crew has lost control or when the flight crew is disorientated. This can be within or outside the normal flight envelope of the external system (see section 4.3).

The safety aspects of the intended function(s) are covered in the FHA in Stage 4: Specification (section 7). For the non-failed AARS this only considers the **system-generated hazards** that are related to the system performing its intended function. These are described in section 7.4.2. A system-generated hazard is one which is generated (or affected) by the introduction of the new function, but which is not a hazard which the function is designed to mitigate.

The resulting safety objectives which are the high level safety requirements that are derived from the results of the Functional Hazard Analysis are presented in sections 7.4.67.4 and 7.5.

No further high level safety requirements exist for the intended functioning of the AARS. The system is optional to attempt to enhance safety by reducing Loss of Control accidents, with potentially 50% when fully

[4] A pre-existing hazard is one which is already present in the environment prior to the introduction of the function under consideration, which the function is designed to mitigate.

implemented within the commercial air fleet. However, there are no (regulatory) requirements for this amount. Therefore the target of 50% is more to be considered as an economical target.

5.7.3 Claim 1.1.3: Sufficient mitigation of AARS (self)failure

This claim is about showing that the consequences of failures of the AARS itself are sufficiently mitigated. As with Claim 1.1.2, the output of this part of the assessment is still at a high level, yielding high level safety requirements for the AARS function. (Design of the solution to meet those requirements is covered in stage 5 of the assessment.)

The high level safety requirements are derived through the identification and assessment of (self)failure scenarios[5], following the process defined in "Briefing on Stage 4 Assessment for WP4.2" [24].

The high level safety requirements developed to support this claim form part of the specification of the AARS, as defined in Context **C1-1**.

Claim 1.1.3 is subdivided into two subclaims to emphasise that, as well as deriving requirements on the AARS itself (Claim 1.1.3.1), it is necessary to define any interactions (at the "black box" level) with other parts of the system (Claim 1.1.3.2), including: ATM, other aircraft, pilot.

Because the assessment is at the "black box" level, it is not possible, within Claim 1, to assess the causes of the AARS failures. Assessment of causes is undertaken in the assessment to support claim 2.

5.7.3.1 *Claim 1.1.3.1: Sufficient mitigation of consequences of AARS (self)failure*

The safety aspects of the intended function(s) are covered in the FHA in Stage 4: Specification (section 7). For the (self)-failed AARS these are described in section 7.4.3 - 7.4.5. In this analysis the following types of failure are addressed which cover the whole range of possible failures:

- Detected failure of the AARS to perform its intended function (section 7.4.3)
- Undetected failure of the AARS to perform its intended function. (section 7.4.4)
- Erroneous operation of the AARS in performing its intended function. (section 7.4.5)

The consequences of these failures have been elaborated into safety objectives which are the high level safety requirements that are derived from the results of the Functional Hazard. The resulting safety objectives are presented in sections 7.4.67.4 and 7.5.

5.7.3.2 *Claim 1.1.3.2: Dependencies on rest of TAS of AARS (self)failure*

The safety aspects of the intended function(s) are covered in the FHA in Stage 4: Specification (section 7). Because it is important that acceptable safety must be achieved over the relevant domains in the TAS, in

[5] Note, in this context, (self)failure refers to failure of the AARS to function as specified, not to an external failure leading to the requirement for an action from the AARS.

section 7.1 this is represented by dividing Claim 1.1 into parallel claims, each covering an element of the TAS. Based on the identified domains (see paragraph 4.8), three main domains have been discriminated:

- the **technical domain**, addressing the technical aspects of implementing the AARS in the aircraft (thus assuring that the technical implementation, including the interface with other technical systems, is safe);
- the **operational domain**, addressing the operational aspects of implementing the AARS (thus are all aspects related to people, procedures and training for the operation addressed and ensured to be safe);
- the **Air Traffic Management** domain, addressing all aspects related to Air Traffic Services and Control (thus are all aspects that may affect the safety of air traffic control, aircraft separation, controller workload, ATC procedures, etc. sufficiently addressed to ensure the safety of the ATM system).

In the further course of the FHA consequently the three domains have been taken into account in all aspects of the assessment.

5.8 Claim 2: Realistic logical design satisfies specification

Claim 2 is that the logical design of the AARS satisfies the (functional) specification (which was defined in support of Claim 1) and is realistically achievable. This considers the AARS as an abstract black box: it does not consider the internal architecture. At this level the interaction of the AARS with other elements of the TAS (including, but not limited to, the aircraft) is defined and analysed. A detailed initial description has been provided in the Stage 1: Definition of the change (section 4) and it is expected that this will be developed further during the case study.

The main assessment to support this claim will be a form of preliminary system safety assessment (PSSA) of the logical design, using techniques which are well-established in assessing concepts (rather than equipment). The form of assessment will be explained in more detail in a later version of this document.

5.9 Claims 3-5: Implementation, Transition and Monitoring

The remaining claims will not be elaborated in the case study, but are described here to explain how the argument will be completed in a full application of the approach.

Claim 3 is that the AARS has been implemented completely and correctly in accordance with its specification and logical design. The assessment of the physical implementation considers the evidence that the specific equipment (hardware and software), procedures and any associated human competence requirements fully and correctly implement the AARS. This includes an assessment of any emerging properties to ensure that they do not compromise the safety of the system. The development of many systems encounters a major problem at this point, namely the limited ability of test-based V&V to show with sufficient confidence that the required safety integrity properties of the system have been met. This leads to the adoption of an assurance based approach.

Claim 4 is that the AARS can be brought into operational service safely and includes confirmation that preparation for operation is complete (procedures have been published, resources procured, personnel trained); that the arrangements for ongoing safety management are in place; that the switchover process has been fully defined and assessed and any appropriate mitigations are in place. Given that the AARS is being introduced into an existing system and that no detailed switchover is required, the main focus of this claim would be on the first point, i.e. that preparation for operation is complete.

Claim 5 is that the AARS will continue to be demonstrated to be safe during operation. This claim would be supported by demonstrating: (a) that continuous safety monitoring will collect appropriate metrics to confirm the results of the safety assessments undertaken under earlier claims; (b) that processes are in place to report, investigate and (where appropriate) correct any safety-related incidents and (c) that processes are in place to assess any interventions (e.g. maintenance) and demonstrate that risks are known and acceptable.

6 Stage 3: Development of and agreement over the certification plan

6.1 Develop and agree a Certification Plan

This section describes how the approach proposed by ASCOS D1.3 to organise the demonstration of safety can be used to develop and agree the plan for certifying the introduction of an onboard Automatic Aircraft Recovery System. The certification plan is the reference for communication between the stakeholder which is seeking for certification of the change and the certification authority, which needs to be entirely satisfied with the application by the stakeholder of applicable regulatory requirements and accompanying evidence before granting the certificate. The Certification Plan needs to contain at least the following elements:

- An overall description of the change, its limits and the way it is interfaced with other domains. This description is primarily intended for the experts of the authority. It may highlight relevant aspects as technical novelties, and, for changes involving multiple stakeholders, relationship with other domains;
- Agreement with the authority on a full and consistent set of applicable regulatory requirements and related guidance material. This may require establishing a common agreement between the different authorities involved;
- A framework to the authority on how to seek agreement on any further technical issues related to the interpretation of the regulatory requirements that may arise during the development of the change;
- A comprehensive description of how the evidences will be produced to show that all the regulatory requirements are complied with;
- Agreement with the authority on the organisation of Certification Deliverables. The Certification Deliverables are documents or data items that need either to be approved or agreed or received by the authority prior to granting the certificate. They are to be considered as the core part of the Certification Plan.
- An overall description of how the “Continuing Safety activities” will be organized in compliance with the reference standards as the response to the mandatory requirements on safety, introducing actors, activities and key documents as output of these activities, including safety activity interface with partnering stakeholders;

6.2 General Description of the change

The certification plan needs to include an overall description of the change, the involved stakeholders and domains, their limits and the way they are interfaced with the other, unaffected or affected domains. This description is primarily for the experts of the authority who may have to undertake the supervision of the change and activities performed by the applicant. It may highlight relevant aspects as technical novelties, and for changes involving multiple stakeholders, relationship with changes in their organisations. Basically, all the aspects of the change as described in section 4: “Stage 1: Definition of the change” would be covered.

6.3 Claims and arguments

This part describes and develops the generic claims that are generated in stage 2 and how these claims need to be satisfied by logical arguments.

6.3.1 High level claim

The certification plan is presented to the relevant authorities and other stakeholders, to gain their agreement that, if the plan is followed and the evidence is presented, they will accept the change into service. Although lack of agreement at this stage does not prevent progress to later stages, the benefit of gaining agreement is to reduce the risk to the certification programme at later stages. This approach can be developed further into requirements. These requirements may all (or mostly) be beneficial, but they introduce significant cost increases if they are introduced progressively through the project.

The ASCOS D1.3 approach proposes to structure the demonstration of safety by building upon the approach of the initial argument architecture as per stage 2, suggesting a top-level safety claim (Claim 0) that could be of the form:

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

and then cascading this higher level claim in sub-claims.

Besides, and as part of their overall duty of protecting the public in general and the environment, the authorities of the aviation system continuously develop common safety and environmental rules. These rules are usually formulated as a structured argument of safety requirements. In some domains the argument is more formulated as a performance requirement than as a defined means of compliance (e.g. in the ATM domain).

As a consequence, it must be checked whether the current rules and standards are an adequate argument to satisfy the claims. It must also be checked whether the assumptions that are used between the domains are adequately addressed.

Means of compliance argument for Claim 0:

- It will be shown by testing that the AARS fulfils the required functionality of stabilizing the aircraft after for a short period after pilot initialization. (CO-1)
- The required level of safety will be defined by the current level of safety combined with the required improvement as defined by EASA in their Safety Plan. The safety objective for the addition of an Aircraft Recovery System is described as “acceptably safe”. This needs to be further refined in order to be able to set the safety standard in the Certification plan. Each domain will constitute an argument on a lower level with its correlated CO’s. The total safety level of this change will then be built from the safety levels achieved in the different domains that are considered to be involved:
  1. Aircraft certification

2. Air operator certification
3. ATM certification

- It would be logical to use the current certification methods that are used in the different domains and focus for ASCOS on the combination of these. This would enable the application of the new certification method (as in D1.3) on this level. If there is then a problem detected with the fusion of these domains, a further investigation on the applicability in a particular domain can be made. This will then require a much more detailed description of the impact in that domain. In order not to lower the current safety standard it may be necessary to include EGPWS and TCAS in the system definition. Otherwise, an uncontrolled move of the aircraft could infringe on the margins of terrain clearance and aircraft separation. (CO-2)
- The conditions in which the service provider takes action are not crisply defined currently, but the service provider must take action based on the inspection of aircraft if the conditions are "conducive to ice accretion". This philosophy is not like to change in the near future. There have been attempts to design systems that can measure ice accretion on aircraft services, but these have not been found acceptably reliable yet. (CO-3)
- The current standards and practices are designed based also on previous accidents and incidents. All the knowledge and experience from these accidents and incidents is condensed in these standards and practices and therefore it is advised to use these in order to comply with CO-4. If the way of working will be different from the current standard, the applicant will argue the level of safety to the Authority by means of established techniques (e.g. FHA / PSSA / HF evaluations etc.)

The main difference lies in the division of responsibilities. These will have to be defined in detail and laid down in the compliance documents.

6.3.2 Sub claims

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

Means of compliance argument:

- The main assessment to support this claim will be an assessment of the operations at a conceptual level, using a technique (established in the air traffic control domain) which assesses the change to introduce an AARS and establishes safety objectives for those operations.
- For the domain of aircraft certification EASA CS 25 will be applicable. In particular CS25.1309 (system safety assessment) and CS25.1302 (Human Factors) would have to be complied with. Here the safety level for the subject change is defined. The FHA (Functional Hazard Analysis) will define the hazard level for the different Failure Conditions. It should be noted that for current, modern, aircraft the safety level required by CS 25 is already achieved and a factor 10 better than required. The mere fact that we are adding a safety feature to the existing fleet means that we are not satisfied with the current safety level. EASA also identifies controlled flight into terrain as one of the epic accident causes. We could therefore consider this aircraft modification as one of the opportunities to increase the safety level in this aircraft certification domain. It is still to be decided how much the modification could reasonably contribute to a higher safety standard.

- The trajectory to improve the safety standard could possibly involve a more comprehensive Human Factors development.
- The safety standard for operational certification (required equipment, training etc.) is more difficult to numerically define than for aircraft certification. It will therefore be assumed that the common compliance based method will be applied for this domain with the same safety level as currently achieved.
- Especially the training component will need to be covered.
- As the approach to certification in the ATM domain is primarily performance based, fusion with the other domains may be difficult. It is not ruled out that the ASCOS method needs to be extended into this domain in order to develop standards that are easier to apply by the applicant and that may contribute to better standardization between ANSP's. It may also contribute to a more defined safety level that may facilitate fusion with the other domains in terms of safety level.
- As the description of the modification includes a provision to inform ATC on the activation of the recovery mode, this functionality will need to be certified.
- Furthermore, the possible influence on aircraft separation (TCAS) and ground clearance (EGPWS/TAWS) needs to be taken into account.

Claim 2: The AARS shall be effective for any physically recoverable condition as long as actuators, engine control systems and control services are intact

Means of compliance argument:

- The main assessment to support this claim will be an assessment of a logical model of the change and the establishment of requirements
- This model needs also to take into account all the assumptions that are coming from the other domains
- In the scenarios that are being developed for stage 4, it will be defined which conditions are considered to be “physically recoverable”. It will then be established by a combination of analysis and testing that the AARS is able to recover the aircraft from those conditions

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

Means of compliance argument

- The applicant will show that the actual system fulfils the requirements as derived in claim 2
- The applicant must show that all the assumptions as coming from other domains are fulfilled

Claim 4: The transition to introduce the AARS is acceptably safe

Means of compliance argument:

- The equipment has been procured and tested, any required spares are available and arrangements are in place to ensure suitable use and maintenance of the equipment
- Staff has been trained to maintain the equipment

- Pilots have been trained in use of the system
- Any arrangements for interfacing with other organisations (e.g. ATC) are in place and any affected staff has been suitably briefed
- The transition to introduce the AARS is properly documented and organized.

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

Means of compliance argument:

- Continuous safety monitoring to collect appropriate metrics to confirm the results of the safety assessments undertaken under earlier claims
- reporting and investigating any safety-related incidents and making any changes required as a consequence of the investigations
- Maintaining staff competence (e.g. through refresher training);
- Maintaining equipment;
- Assessing any subsequent changes to the system.

6.4 Coordinated approaches between domains

For changes requiring coordination between the service provider and other domains within the TAS, it is important to ensure that the certification process engaged by an applicant and its partner(s) towards their respective authorities is consistent and coordinated. The assumptions between the domains need to be carefully addressed.

6.5 Content of the certification baseline

The certification baseline that can be proposed for agreement in a first step by the applicant of the proposed change will be the following:

- EASA CS25
- EASA IR-OPS (EU 965/2012 [1], amended by EU 800/2013 [2] and EU 71/2014 [3]), which lays down technical requirements and administrative procedures related to air operations.
- TBD ATM requirements

In addition, for those topics for which it can be known in the first step of the change that a discussion and agreement needs to be conducted with the authority, due to the specifics of the change, a list of “Review Items” or “Issues” will be appended to the baseline. For example, the following topics can be presumed to be open in order to agree on interpretation material:

- Tests for Certification (planning and extent of tests to be conducted

- Human Factors considerations;
- Relationship with Certification Requirements used in different aviation domains
- Finally, as all aspects of certification cannot realistically be completed prior to the starting of design activities, the certification plan should propose to the authority a framework on how to seek agreement on any further technical issues related to the interpretation of the regulatory requirements and the need to consolidate the certification baseline that may arise during the design and development of the change.

6.6 Compliance Demonstration

The certification plan should give a comprehensive description of the means of compliance arguments (see 6.2.1 and 6.2.2) and how the evidences will be produced that all the regulatory requirements and standards are complied with. This can for example take the form of an assembly of plans shown to be consistent in a Means Of Compliance checklist.

The certification plan should also propose an organisation of Certification Deliverables together with their certification status. Depending on this status, the Certification Deliverables are documents or data items that need either to be approved or agreed or received by the authority prior to granting the certificate. They can be considered as the core part of the Certification Plan. A separate document describing the assumptions coming from other domains and how these are being covered must be part of the document deliverables. If testing is part of the certification baseline, a summary of the test results must be part of the document deliverables.

A Functional Hazard Assessment (FHA) may be part of the compliance demonstration in order to analyse which safety hazards need to be considered. The FHA can be the basis for fixing the Design Assurance Levels. The FHA report itself must be a Certification Deliverable.

Any Human Factors considerations and assumptions that are the result of compliance activities must be compiled in a document in order to be useable in the Continuing Safety activities for personnel training requirements.

6.7 Agreement on the certification plan

Early agreement on the certification plan and the means of compliance with the operational authorities is important in order to avoid unnecessary “surprises” during the compliance period.

6.8 Continuing Safety activities

Understanding and monitoring how the demonstration of continuing safety will be managed and achieved is of utmost importance for the authority. As a consequence a special focus is to be put in the certification plan on how the requirements and standards will be implemented and monitored, giving sufficient details on:

- the design organisation and the actors in charge;
- the organisation of safety activities, their inputs and outcomes, how they interface;
- the key documents produced as output of these activities
- personnel training requirements

The description of safety activities should also include safety activities and output documents interfacing with partnering stakeholders.

6.9 Example outline of a Certification Plan

1.General Description

1.1.Overview of change

1.2.Interface with other stakeholders

1.3Interface with other domains

2.Applicable Requirements, Standards and Related Guidance

2.1. Certification Basis (Claims and Argument architecture)

2.2. Special Conditions & Issue Papers & Equivalent Safety Findings

2.3. Interpretative Material

2.4. Listing of required tests for Certification

2.5. Other requirements and reference documents

2.6 Means of compliance checklist

2.7 Relationship with Certification Requirements in neighbouring domains (Assumptions)

3.Compliance Demonstration

3.1 List of certification deliverables

3.2.Summary of the Functional Hazard Assessment

3.3.Determination of Levels for the Assurance of the change (Design Assurance Levels)

3.4 Compliance deliverables (including assumptions)

3.5 Test results

3.6.Human Factors considerations

4. Transition requirements

4.1.Transition document .

5.Continuing Safety activities

5.1.Scope of the Safety activities

5.2.Main Safety actors and outputs

5.3. Relationship with Certification Requirements in neighbouring domains

5.4. Personnel training requirements

7 Stage 4: Specification

7.1 Application of stage 4

This stage is focused on demonstrating that Claim 1 of the generic argument is met, namely that the change is specified to achieve an acceptable level of safety. This addresses the functional behaviour of the system both in the absence of failure as well as in the presence of functional failure conditions.

Safety assessment in this stage is used to identify functional hazards relevant to the system and assesses the consequences of these hazards on the safety of the TAS. This assessment is used to derive definitions of:

- Functional requirements of the system which specify what the system is required to do (not how it does it) in order perform its intended function
- The safety requirements for the system;
- The degree of assurance required that the system will meet its requirements;
- Any additional functional requirements or assumptions to capture any external means of mitigating the consequences of the hazards caused by failure of the system.

As specified in the description of the certification methodology (D1.3), it is important that in this stage the argument for Claim 1 is fully developed and substantiated with relevant evidence.

In chapter 5 Claim 1 has been developed into several sub-claims. It was concluded that the main assessment to support Claim 1.1 will be a form of Functional Hazard Analysis process. Because the methodology is aimed to address the TAS (and the pre-existing hazards in the TAS), it is important that acceptable safety must be achieved over the TAS. This is represented by dividing Claim 1.1 into parallel claims, each covering an element of the TAS. Based on the identified domains (see paragraph 4.8), three main domains have been discriminated:

- the **technical domain**, addressing the technical aspects of implementing the AARS in the aircraft (thus assuring that the technical specification and implementation, including the interface with other technical systems, is safe);
- the **operational domain**, addressing the operational aspects of implementing the AARS (thus are all aspects related to people, procedures and training for the operation addressed and ensured to be safe);
- the **Air Traffic Management domain**, addressing all aspects related to Air Traffic Services and Control (thus are all aspects that may affect the safety of air traffic control, aircraft separation, controller workload, ATC procedures, etc. sufficiently addressed to ensure the safety of the ATM system).

This is reflected in

Figure 7-1 below. In the further course of the FHA consequently the three domains have been taken into account in all aspects of the assessment.

Figure 7-1: Development of Claim 1 into sub-claims in the relevant domains

7.2 Reference scenarios

In order to facilitate the hazard assessment reference scenarios are defined, that indicate how, under which conditions and in which environment the system is intended to operate. These reference scenarios can be used to identify the relevant functional hazards in the various domains, and how they are interrelated. Moreover these scenarios can be used to test the usability of the risk assessment tool as developed in ASCOS D3.3.

Two main scenarios have been defined. These scenarios address cases that according to the risk assessment tool (see also Chapter 3.1) relate to the main scenarios, causing loss of control events.

Scenario1

The first reference scenario is derived from the accident with Air France flight AF 447 en-route from Rio de Janeiro to Paris [21]. In this reference scenario it is assumed that a speed sensor failure leads to complete loss of airspeed indication. The loss of situational awareness due to this rare loss of critical information, combined with a consequential failure of the auto-pilot and reversion of the manual flight control system to a degraded back-up mode, without envelope protection, leads to a situation where the flight crew is confused and unable to determine the correct recovery strategy, leading to an unnoticed increase of angle-of-attack. In response to this situation the AARS will be employed by the pilot-flying. If the system performs its intended function the aircraft will return to stable, wings level, horizontal flight. The aircraft will not necessarily fly at its assigned flight level, during the recovery. It is furthermore assumed that surrounding traffic is present, with a vertical separation of 1000 ft from the assigned flight level of the incident aircraft. Potentially a TCAS alert will be given during the recovery manoeuvre.

Scenario2

The second scenario is derived from the accident with Turkish Airlines flight TK1951 near Schiphol [22]. In this reference scenario, the radio altimeter fails during the final approach and transmits an erroneous value of zero ft. This failure is not detected by the on-board fault detection and isolation system, and therefore the erroneous value is transmitted as a valid signal to the auto-throttle and auto-flight system. The auto-throttle system interprets the erroneous signal as being very close to the ground and initiates an automatic throttle retard (which is normal behaviour of the auto-throttle system close to the ground). This remains unnoticed to the flight crew, who is relying on the auto-throttle system for speed control. As a consequence, the aircraft decelerates quickly, and approaches a stall condition. The flight crew performs an unstabilised approach and is confused by the sequence of events. Finally the crew is surprised by an imminent stall condition. In response to this situation the pilot flying engages the AARS. If the system performs its intended function, the aircraft recovers from the imminent stall condition and re-engages the engine controls in order to provide the appropriate power level for a slightly climbing flight. It is assumed that in this scenario high terrain surrounds the airport, and that potentially an EGPWS alert is given during the recovery. Also it is assumed that surrounding traffic is present, at minimum radar or wake vortex separation. Finally, it is assumed that Air Traffic Control is informed about the abnormal behaviour of the aircraft, and provides air traffic control instructions to surrounding traffic to avoid separation infringement during the recovery.

7.3 Functional Hazard Analysis

As mentioned in the description of Stage 4 of the certification methodology, the assessment broadly aligns with the Functional Hazard Analysis process. In line with the characteristics of the FHA process, the following requirements apply:

- The FHA should establish how safe the AARS needs to be;
  The required safety level depends on the criticality of the intended functional failure conditions (minor, major, hazardous or catastrophic) ;
- The FHA should be conducted at the functional level and therefore is largely independent of the actual implementation; and
- The FHA should also address the impact of external factors and of interaction among the various domains on the intended function of the AARS.

At this stage the assessment is performed independent of the implementation of the system and so failures of the system related to specification-level functions only. However, it should be noted in some cases consideration must also be given to concept of operations, modes of operation or other operational definitions which depict the intended use of the system.

The intended function of the system, and the associated functional requirements have been listed in Chapter 4.3. This information is used together with a number of reference scenarios, defined in Chapter 7.2, to determine the functional hazards and their consequences. From these the high-level safety requirements can be derived. It should be noted that the purpose of the intended function is to mitigate the pre-existing hazards[6]. In this particular case the pre-existing hazards that are aimed to be mitigated are Loss of Control and Loss of Situational Awareness, possibly initiated by a system failure. It is assumed that when the system performs, as designed, the pre-existing hazards are mitigated. Unsafe conditions can only arise from the system not performing its intended function. Therefore the hazard analysis focuses on system generated hazards and functional failures.

The functional hazard analysis basically addresses four elements:

1. What are the **system generated hazards**, that are related to the system performing its intended function. A system-generated hazard is one which is generated (or affected) by the introduction of the new function, but which is not a hazard which the function is designed to mitigate. Examples are: when the AARS is engaged it might interfere with TCAS or EGPWS and introduce a hazard (such as increased probability of CFIT or MAC) that otherwise would not exist (in the technical or operational domain), or it might interfere with the function of ATC to provide separation (in the ATM domain).
2. What are the hazards, related to a **detected failure of the system** to perform its intended function.

[6] A pre-existing hazard is one which is already present in the environment prior to the introduction of the function under consideration, which the function is designed to mitigate.

For example: the system is not functional and the flight crew is aware of the unavailability of the system. In other words, when a LOC situation occurs the flight crew cannot rely on the system to perform a recovery manoeuvre. This is related to the reliability of the system.

3. What are the hazards, related to **an <u>undetected failure of the system</u>** to perform its intended function. For example: the system is not functional and the flight crew in not aware of the loss of functionality of the system. In other words, when a LOC situation occurs the flight crew will rely on the system to perform a recovery manoeuvre. However, the system will not perform its intended function. This is related to the integrity of the system.
4. What are the hazards, related to **<u>erroneous operation of the system</u>.**

   For example, the system provides erroneous control inputs (e.g. soft or hard over), or provides misleading information, before or after engagement of the system.

This is further elaborated in the next chapter, addressing the basic elements of the FHA per domain.

7.4 Hazard Severity Assessment

7.4.1 Generic hazard severity definitions

For the severity classification the following generic definitions have been used. The term “generic definition” is used here to express that the definition applies for the Total Aviation System.

Table 7-1: Generic hazard severity definitions

Severity	Description
No Safety Effect	Conditions that would have no effect on safety; that would not affect the operational capability of the aeroplane or increased flight crew or ATC workload.
Minor	Conditions which would not significantly reduce aeroplane safety, and which involve crew/ATC actions that are well within their capabilities. May include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew/ATC workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.
Major	Conditions which would reduce the capability of the aeroplane or the ability of the crew/ATC to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew/ATC workload or in conditions impairing crew efficiency, or discomfort to the flight crew, of physical distress to passengers or cabin crew, possibly including injuries.
Hazardous	Conditions, which would reduce the capability of the aeroplane or the ability of the crew/ATC to cope with adverse operating, conditions to the extent that would be: A large reduction in safety margin or functional capabilities;

	Physical distress or excessive workload such that the flight crew/ATC cannot the relied upon to perform their tasks accurately or completely, or; Serious or fatal injury to a relatively small number of the occupants other than flight crew
Catastrophic	Conditions which would result in multiple fatalities, usually with the loss of the aeroplane.

7.4.2 System generated hazards

A system-generated hazard is one which is generated (or affected) by the introduction of the new function, but which is not a hazard which the function is designed to mitigate.

System generated hazards in the technical domain

Hazard TS.1: Traffic separation infringement during recovery manoeuvre: Based on reference scenario 1, a system generated hazard is that the AARS is engaged and performs the recovery manoeuvre and deviates, due to the recovery, from the assigned flight level, such that vertical separation with surrounding traffic is reduced. This may lead to a collision avoidance alert (e.g. a TCAS Resolution Alert both for the recovering aircraft and the surrounding traffic). It is assumed that the recovery procedure to prevent immediate loss of control takes priority over the collision avoidance alert. Therefore, the flight crew shall not react to the collision avoidance alert (that even may be suppressed for this reason during the recovery).

It is assumed that traffic surrounding can avoid a conflict by the following the TCAS Resolution Alert, but that it may lead to significant work load, because a successful avoidance manoeuvre depends on the proper action of the conflicting aircraft only.

Therefore hazard TS.1 is major, in case the TCAS RA is followed by the conflicting traffic.

Hazards TS.2: Ground/obstacle proximity during recovery manoeuvre; based on scenario 2 it is possible that the recovery manoeuvre at low altitude may lead to a conflict with high terrain. This may lead to an EGPWS alert. It is assumed that the recovery procedure to prevent immediate loss of control takes priority over the EGPWS alert. The options for the pilot are however limited in this case; loss of control or controlled flight into terrain might the consequence of any pilot action taken. It is possible that when the initial recovery is successful, the pilot might respond to the EGPWS alert to prevent CFIT. This will lead to very high workload.

Therefore hazard TS.2 is assessed as hazardous.

System generated hazards in the operational domain

Hazard OS.1: Pilot follows TCAS alert during recovery manoeuvre: If the pilot responds to a TCAS alert during a recovery manoeuvre, this may interfere with the recovery and lead to an unsuccessful recovery. Pilots must therefore be trained to ignore the TCAS alert in this case, or the TCAS alert must be suppressed altogether. An unsuccessful recovery may lead to loss of control.

Therefore hazard OS.1 is assessed as catastrophic.

Hazard OS.2: Pilot follows EGPWS alert during recovery manoeuvre: If the pilot responds to an EGPWS alert during a recovery manoeuvre, this may interfere with the recovery and lead to an unsuccessful recovery. Ignoring an EGPWS alert close to the ground may however be equally dangerous. Therefore, it should be left to the pilot to decide which action takes precedence, and therefore the EGPWS alert will not be suppressed. It will be however very difficult to train pilots for this scenario. An unsuccessful recovery may lead to loss of control.

Therefore hazard OS.2 is assessed as catastrophic.

Hazard OS.3: Pilot does not recognize LOC or LSA condition properly and fails to engage AARS. It might be counter intuitive for a pilot to transfer control to an automatic recovery system, in a stressfull condition involving LOC or LSA conditions. Pilots must be properly trained in recognizing the conditions for usage of the AARS. If the training is not sufficient, pilots may be reluctant to engage AARS, and the safety benefits will not be achieved. A manual recovery may be successful. However this will result in a very high level of workload.

Therefore hazard OS.3 is assessed as hazardous.

System generated hazards in the ATM domain

Hazard AS.1: During recovery manoeuvre the aircraft deviates significantly from the assigned ATM clearance (laterally or vertically)**:** When the aircraft performs a recovery manoeuvre it may deviate from the assigned flight level or the assigned route, potentially leading to separation infringement. Without ATC intervention this might lead to conflicts. It may be assumed that TCAS is capable to solve such conflicts. However, it may be required that ATC takes the appropriate action to clear the area of the recovery manoeuvre from conflicting traffic, until the recovery procedure is completed. It is therefore required that ATC is informed as soon as possible that a recovery procedure is in progress. This can be done by the flight crew through voice communication (“mayday, automatic recovery in progress”) or by downlinking an annunciation that a recovery is in progress.

It is assumed that if ATC is informed immediately, that surrounding traffic can be instructed such that conflicts are avoided. This may lead to some increased workload for the Air Traffic Controllers.

In this case hazard AS.1a (with informed ATC) is considered major.

In case ATC would not (or too late) be notified that the recovery procedure is in progress, ATC might get confused concerning the occurrence, in particular due to the fact that the recovering aircraft would not respond to ATC instructions. This will give rise to high workload.

Therefore, in this case hazard AS.1b (with uninformed ATC) is considered hazardous.

7.4.3 Detected failures

A detected failure concerns the situation that the system is not functional and that this state is known to the flight crew, so that they will not try to engage the system in conditions where they otherwise would do so. In general a detected failure refers mostly to the detection by the systems itself (built-in test, fault detection and isolation, etc.). In some cases the flight crew is able to detect un-flagged failures themselves by means of cross-monitoring. However, in the case of AARS there is no way the pilot can establish the failure of the system, other than by an annunciation of the system itself.

The consequence of a detected failure is that the system will not perform its intended function. At the same time the pilot is aware of this failure, and therefore he may cope by not relying on the system, and in case of LOC or LSA conditions returning to a manual recovery strategy. Clearly, the probability of successful recovery is reduced in this case. It may be expected that for this reason the unavailability of the system is not allowed to be permanent. However, dispatch with a failed system will most likely be allowed for a certain period of time. This will be covered in the Minimum Equipment List. The criticality of the detected failure determines in the end what the allowed time period of operating with a failed system will need to be. This strongly relates to the required reliability of the system (mean time between failure).

Detected failures in the technical domain

Hazard TD.1: LOC or LSA condition occurs while the AARS is flagged as unavailable: in this case the pilot has to return to a manual recovery strategy. Assuming that the pilot is still properly trained to perform such recovery (see TD.1), there will still be a reasonable probability that the recovery is successful, albeit at significantly increased workload.

Therefore, hazard TD.1 is considered hazardous, in case the LOC or LSA condition is present.

Hazard TD.2: AARS fails during a recovery procedure in progress, and provides an annunciation to the pilot of its failure: this hazard relates to the required continuity of function. In case this hazard occurs, the severity of the hazard depends on where in the recovery process the failure occurs. If the failure occurs near completion of the recovery, it is possible that the pilot may take over successfully. However in worst case it is unlikely that the pilot is able to take over and perform a successful manual recovery.

Therefore, hazard TD.2 is (conservatively) considered catastrophic.

Detected failures in the operational domain

Detected failures in the operational domain relate to the ability and effectiveness of pilots to operate with a failed AARS.

Hazard OD.1: Pilot unable to perform a manual recovery in case AARS is unavailable. This hazard occurs when the pilot recovery training is not effective, and therefore the pilot training is not able to mitigate the consequences of the failed AARS (see also hazard TD.1). Due to this hazard the severity of hazard TD.1 increases.

Therefore, hazard OD.1 is considered catastrophic, in case the condition of TD.1 does exist.

Detected failures in the ATM domain

It is not likely that information concerning the unavailability of AARS will be shared with Air Traffic Control (just like unavailability of TCAS and EGPWS are not shared). Therefore, in this particular case detected failures are not relevant in the ATM domain. It is also hard to imagine what action ATC would have to take, if such information would be available. Therefore, a detected failure of AARS is irrelevant in the ATM domain.

7.4.4 Undetected failures

An undetected failure concerns the situation that the system is not (or partially) functional and that this state is not known to the flight crew. In this case the pilot will engage the system, in case conditions require. However the system will fail to perform its intended function.

Undetected failures in the technical domain

Hazard TU.1: AARS unable to initiate and perform recovery manoeuvre when LOC or LSA conditions occur: In this case the flight crew has recognised the LOC/LSA condition and has established that criteria for engagement of AARS have been met. However, after pilot initiation the AARS fails to perform the recovery manoeuvre. When the flight crew is not aware of the failure they will lose valuable time trying to diagnose the aircraft systems whilst they rely on the AARS to restore stable flight. It is unlikely that the crew is able to recognize the failure of AARS to perform the recovery procedure, and therefore it is also unlikely that the crew will be able to successfully intervene under such critical conditions.

Therefore, hazard TU.1 is considered catastrophic.

Hazard TU.2: AARS unable to terminate the recovery manoeuvre, after successful recovery: It is assumed that failure of the termination function can occur separately from the other functions. In that case the undetected failure of this secondary function will lead to inability of the flight crew to switch of the AARS. In such a situation it will not be possible for the flight crew to take over control of the aircraft though the aircraft is in a stable flight condition. This may potentially (in some cases) lead to conflict with terrain or with other traffic. It may however be assumed that the stable flight condition is easily recognised by the crew, and that the crew is able to disengage the system by alternative means (e.g. pulling the circuit braker). So, the consequence is mainly a delay in time for returning to normal control, while the flight condition itself is safe.

Therefore hazard TU.2 is considered: minor.

Undetected failures in the operational domain

Undetected failures in the operational domain refers to the capability of pilots, by means of appropriate procedures or training, to cope with the consequences of the AARS failing to perform its intended function, under conditions where it is expected to operate. This relates to the question, what kind of procedures or training would be suitable to provide pilots with this capability. It may be possible to train pilots to recognize when AARS fails to perform the recovery manoeuvre correctly. However, it would be hard to imagine how pilots could intervene successfully, given the fact that due to the LOC or LSA situation the AARS has been engaged by the same pilot as a last resort. Therefore, it has to be assumed that undetected failures are not resolvable by any procedure or training. Therefore, the hazard severity of TU.1 cannot be further reduced by actions in the operational domain. Further assessment of undetected failures in the operational domain is therefore irrelevant.

Undetected failures in the ATM domain

AU.1: Failure to communicate with ATC that recovery is in progress: in case communication with ATC fails, it will be difficult for ATC to recognize that the aircraft has initiated the recovery manoeuvre, and consequently is unable to respond to any ATC instructions. This may lead separation infringement and some delay in the capability to solve this situation, as the aircraft causing the infringement cannot be controlled. Nevertheless it may be assumed that ATC is able to restore separation by proper instructions to the surrounding traffic. However, due to mentioned delay, the actual separation infringement might be more severe and workload might increase significantly. This hazard severity is similar to hazard AS.1b.

Therefore hazard AU.1 is considered: hazardous.

7.4.5 Erroneous operation

Erroneous operation of the system relates to errors introduced by the implementation of the function, which may lead incorrect commands to one or more of the flight control surfaces or to the engine controls. Since the AARS has full authority, in order to be able to perform the recovery procedure, there is no protection outside the AARS to prevent this. The erroneous operation, as defined here, manifests itself only in the technical domain, as it is related to the technical implementation of the intended function.

Erroneous operation in the technical domain

TE.1: AARS is self-engaged, without appropriate pilot input: in this case the AARS is engaged erroneously. There is no pilot command requiring engagement, and no LOC or LSA condition exist that would warrant engagement. If the AARS functions properly, it will bring the aircraft to a stable condition, that may deviate from the initial condition in which it was employed. Since, due to AARS engagement, other systems and manual control inputs from the pilot are overridden the situation can be very confusing to the pilot, despite the fact that the aircraft remains in a stable and safe condition. Nevertheless, this may lead to substantial confusion and increased workload.

Therefore hazard TE.1 is considered: major

TE.2: The AARS drives one or more control surfaces or engine controls to the limit, at maximum rate (hard-over): A hard-over at maximum deflection rate causes a fatal manoeuvre of the aircraft. The flight crew is not likely to recognize the situation and take over control.

Therefore hazard TE.2 is considered: catastrophic

TE.3: The AARS drives one or more control surfaces or engine controls to an incorrect position: The output commands show realistic values to steer the aircraft but the values are incorrect with respect to the intended function. This hazard has the same effect as the undetected failure of the AARS, see TU.1.

Therefore hazard TE.3 is considered: catastrophic.

7.4.6 Overview of the identified hazards and severities

Table 7-2 gives an overview of the identified hazards and their severities.

Table 7-2: Summary results FHA

Nr	Hazard	Hazard type	Hazard Domain	Severity
TS.1	TCAS alert during recovery manoeuvre	System generated	Technical	major
TS.2	EGPWS alert during recovery manoeuvre	System generated	Technical	hazardous
OS.1	Pilot follows TCAS alert during recovery manoeuvre	System generated	Operational	catastrophic
OS.2	Pilot follows EGPWS alert during recovery manoeuvre	System generated	Operational	catastrophic
OS.3	Pilot does not recognize LOC or LSA condition properly and fails to engage AARS.	System generated	Operational	hazardous
AS.1	During recovery manoeuvre the aircraft deviates significantly from the assigned ATM clearance (laterally or vertically)	System generated	ATM	major

Nr	Hazard	Hazard type	Hazard Domain	Severity
TD.1	LOC or LSA condition occurs while the AARS is flagged as unavailable	Detected failure	Technical	hazardous
TD.2	AARS fails during a recovery procedure in progress, and provides an annunciation to the pilot of its failure	Detected failure	Technical	catastrophic
OD.1	Pilot unable to perform a manual recovery in case AARS is unavailable.	Detected failure	Operational	catastrophic
TU.1	AARS unable to initiate and perform recovery manoeuvre when LOC or LSA conditions occur	Undetected failure	Technical	catastrophic
TU.2	AARS unable to terminate the recovery manoeuvre, after successful recovery	Undetected failure	Technical	minor
AU.1	Failure to communicate with ATC that recovery is in progress	Undetected failure	ATM	hazardous
TE.1	AARS is self-engaged, without appropriate pilot input	Erroneous operation	Technical	major
TE.2	The AARS drives one or more control surfaces or engine controls to the limit, at maximum rate (hard-over)	Erroneous operation	Technical	catastrophic
TE.3	The AARS drives one or more control surfaces or engine controls to an incorrect position, during recovery	Erroneous operation	Technical	catastrophic

7.5 Safety objectives

The high level safety requirements are derived from the results of the Functional Hazard Analysis. From the severity of the hazards, that are associated with the introduction of the system functions (and corresponding functional failures), the safety requirements for each of the functions can be derived. In order to achieve acceptable safety the probability of occurrence of a functional failure shall be inversely related to the corresponding severity.

The system design should be compliant with this basic requirement. It is evident that the correlation between the criticality level of the function and the functional failure probability should be defined, in order to set the high level system safety requirements. For system certification (in the technical domain) the requirements of CS25.1309 apply. CS25.1309 defines failure condition probability in qualitative and quantitative terms, as given in the following table.

Table 7-3: CS15.1309 definition of probability terms

Failure probability term	Qualitative probability	Quantitative probability per flight hour
Probable	to occur one or more times during the entire operational life of each aeroplane.	10^{-5} < probability
Remote	unlikely to occur to each aeroplane during its total life, but which may occur several times when considering the total operational life of a number of aeroplanes of the type	10^{-7} < probability < 10^{-5}
Extremely remote	not anticipated to occur to each aeroplane during its total life but which may occur a few times when considering the total operational life of all aeroplanes of the type	10^{-9} < probability < 10^{-7}
Extremely improbable	so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type	probability < 10^{-9}

The safety objective for each function is directly derived from the criticality level of the function and the acceptable probability of occurrence. According to CS25.1309 the safety objectives are defined as follows:

> *a logical and acceptable inverse relationship must exist between the Average Probability per Flight Hour and the severity of Failure Condition effects such that:*
>
> *(1) Failure Conditions with No Safety Effect have no probability requirement.*
> *(2) Minor Failure Conditions may be Probable.*
> *(3) Major Failure Conditions must be no more frequent than Remote.*
> *(4) Hazardous Failure Conditions must be no more frequent than Extremely Remote.*
> *(5) Catastrophic Failure Conditions must be Extremely Improbable.*

Based on these safety objectives, for each of the AARS functions the required failure probability can be established, using the results of Table 7-2.

A number of important observations have to be made here. First of all the AARS is designed to be used as a “safety net” for rarely occurring situations. This means that let’s say the AARS will only be employed once per 100,000 flight hours. Yet, the failure of AARS to perform its intended function may be catastrophic. In that sense it’s function is flight critical. According to the safety objectives, catastrophic failure conditions must be extremely improbable (<10^{-9}). The question is whether the system must comply with this safety objective, once the conditions for engagement do exist (thus probability of LOC is 1), or is it allowed to take into account that the probability of the initiating condition is 10^{-5}. Based on experience with a similar (safety net) system, like the windshear detection & guidance systems, it is known that it is acceptable for certifying authorities to consider for the hazard assessment that windshear is present (probability 1), but in defining the safety objectives the actual probability of a windshear encounter can be taken into account. Thus the safety objective for catastrophic failure conditions can be divided by the probability of windshear encounter. Therefore, given the probability of windshear encounter of 10^{-5}/FH, the failure of the windshear detection function shall be $10^{-9}/10^{-5}=10^{-4}$/FH. This is the reason that non-redundant implementation of windshear detection systems is acceptable. It is expected that this reasoning equally applies for the AARS, and that the system design may take this into account.

A second observation is that safety objectives have been defined here in the technical domain. It is questionable whether in the other domains (operational and ATM) the same definitions, in terms of hazard severity and acceptable level of probability do apply. While in the technical system domain the probability of catastrophic failure shall be $< 10^{-9}$, in the ATM domain the overall contribution to catastrophic failure shall be $<1.35*10^{-8}$ [ESARR4]. Because the AARS contribution to unsafety in the ATM may only use a small part of the total budget, it can be envisioned that introduction of AARS may not contribute to more than (in the order of) 1% of the total ATM budget for unsafety. In that case, a catastrophic failure of AARS in the ATM domain shall be in the order of 10^{-10}. This illustrates that definition of safety objectives in different domains may lead to different probability requirements for similar hazard categories. This should be well realised, when using the same certification methodology over different domains.

8 Stage 5: Design

8.1 Objective

As explained in ASCOS D1.3, the objective of stage 5 is to demonstrate that Claim 2 of the generic safety argument is met, namely that the logical design of the AARS has the functionality and behavioural and performance attributes necessary to satisfy the functional specification considered in Claim 1. This claim considers all normal, abnormal, degraded and emergency conditions of the operational environment. In addition, this claim considers all the possible hazardous failure modes of the logical design and sets mitigations and assurance requirements such that the system is acceptably safe in the presence of these failures.

In this context, logical design is a high-level architectural representation, independent from the physical implementation. As such it considers the functions provided by the system elements (i.e. human roles and tasks and machine-based functions), but not the equipment, personnel or procedures which provide these functions.

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. Requirements derived during this stage are set without necessarily prejudging how that design should be physically implemented. However, the assessment also needs to consider the achievability of any requirements and therefore must consider whether the requirements can be met (at least in principle) by the preliminary design. This broadly aligns with the preliminary system safety assessment PSSA process, as described in SAE ARP4761 [31].

The briefing document for stage 5, ref [24], identified the following steps:

1. Identify the logical elements and interfaces within the design

2. Assess how the elements work together to satisfy the intended safety functions[7]

    - by exploring the interfaces and using the scenarios from stage 4.

3. Assess what could fail within each of the logical elements and interfaces

    - by exploring the causes of the functional failures of stage 4 and identify mitigations for these failures.

4. Assess the levels of development assurance

    - needed to ensure that the mitigating requirements are successful in making the system sufficiently safe.

[7] The title of step 2 has been slightly modified with respect to the title for step 2 in the stage 5 briefing document from Ebeni: "Assess how the elements work together to satisfy the high level safety requirements". The high level safety requirements resulting from stage 4 are considered to be intended functions of the AARS.

5. Confirm that the system as designed will meet the requirements, including the required level of safety performance.

The main output of the safety assessment is as follows:

- Design Safety Requirements for each element of the logical architecture, as necessary to provide the functionality and performance specified in the specification stage;
- Safety Assurance Requirements for each element of the logical architecture, as necessary to satisfy the level of assurance specified in the specification stage;
- Additional Design Safety Requirements (or assumptions, where appropriate) to capture any internal means of mitigating the causes of the hazards arising from failure of the system.

8.2 Identify the logical elements and interfaces within the design

For the assessment of stage 5 the following logical elements shown in this figure are considered:

- Aircraft manufacture and certification domain:
    - AARS processing
    - AARS Sensors
    - CMD/CTL and display unit
    - Flight and engine control systems (actuators)
- Aircraft operational domain
    - Flight crew ownship
    - Other air traffic
- ATM/ANS equipment domain
    - ATM/ANS equipment
- ANSP domain
    - Air Traffic Controller

Figure 8-1 shows the logical elements and the interfaces for the AARS design. Interfaces between other domains are not shown (e.g. ATCO communication with other aircraft).

Figure 8-1: Logical elements and interfaces for the AARS design

The AARS logical design resembles the functional breakdown from the stage 1. From discussions with Ebeni it was concluded that this design should be kept as abstract as possible and without considering physical implementations. In an aircraft PSSA process phase the designers identify multiple candidate architecture solutions taking into account performance requirements and economic constraints. These candidate solutions are assessed to what extent they can meet the safety objectives, possibly including redundant solutions.

8.2.1 Candidate design solutions

In this section four candidate technical design solutions in the aircraft manufacture and certification domain are introduced which will be discussed. From these four candidates one technical design solution will be chosen for assessment of the logical design.

8.2.1.1 *AARS as fully stand-alone system*

The AARS is implemented as a separate unit that does not share any functionality with other systems in the aircraft.

Interfacing

- Flight crew: The AARS interfaces with the flight crew by means of a separate command/control/display unit in the cockpit.
- Flight control system: The AARS interfaces with the flight controls by generating command inputs directly to the flight control actuators on same abstraction level where the automatic and/or primary flight control system (APFCS) provides this. When the AARS is active in recovery mode the system will have full authority over the actuators. This means that command inputs from the APFCS are ignored and are replaced by command inputs from the AARS.
- Engine control system: The AARS interfaces with the engines by generating command inputs directly to the engine control system on the same abstraction level where the automatic and/or primary power control system provides this. When the AARS is active in recovery mode the system will have full authority over the engine control system. This means that command inputs from automatic and/or primary power control system are ignored and are replaced by command inputs from the AARS.
- Sensors: The AARS uses its own set of sensors which will deliver flight parameters independently from the existing sensors that are used by other systems in the aircraft. Sensor transduction functions are implemented in the AARS unit.
- ATC: ATC alerting is possible using several existing systems in the aircraft, such as: ADSB-transponder, radio telephony (COM) and (in the future) datalink. The appropriate system is initiated and controlled by means of the AARS unit.

Health monitoring

Health monitoring functions are performed within the AARS unit and are part of the required functionality.

8.2.1.2 *AARS functionality is integrated in the primary flight control system*

The AARS functionality is largely implemented in the hardware and software of the APFCS. This design solution of course will only be available for fly-by-wire aircraft. Since in this design solution the AARS shares hardware and software resources with the APFCS it might be more vulnerable for failures in the APFCS.

Interfacing

- Flight crew: To initiate and terminate the recovery action a separate command/control/ unit in the cockpit is necessary. Annunciating to the flight crew is possible by means of the display and annunciating systems that are used by the APFCS.
- Flight control system: The AARS interfaces with the flight controls by generating flight commands within the APFCS on the same abstraction level where the APFCS generates flight commands. When the AARS is active in recovery mode the APFCS will give full authority to the AARS and translate the AARS flight commands into commands to the flight control actuators.
- Engine control system: The AARS interfaces with the engines by generating power setting commands within the APFCS on the same abstraction level where the APFCS generates flight commands. When the AARS is active in recovery mode the APFCS will give full authority to the AARS and translate the AARS power setting commands into commands to the engine control system.
- Sensors: The AARS uses its own set of sensors but the sensor transduction functions are implemented in the software of the APFCS. The APFCS interfaces with the sensor units using the same hw/sw interface systems as for its own sensors.
- ATC: ATC alerting is possible using several existing systems in the aircraft, such as: ADSB-transponder, radio telephony (COM) and (in the future) datalink. In all cases the alerting function is implemented in the software of the APFCS, from where the appropriate system is initiated and controlled.

Health monitoring

APFCS is a flight critical system and health monitoring is an integral part of it. APFCS can facilitate health monitoring functionality for the AARS. So health monitoring of the AARS is also to be implemented in the hardware and software of the APFCS.

8.2.1.3 *AARS functionality is implemented in avionics*

The AARS functionality is largely implemented in the hardware and software of an avionics system, like FMS or EGPWS. Since in this design solution the AARS shares hardware and software resources with the concerned avionics system it might be more vulnerable for failures in that avionics system.

Interfacing

- Flight crew: To initiate and terminate the recovery action a separate command/control/ unit in the cockpit is necessary. Annunciating to the flight crew is possible by means of the display and annunciating systems whereto the concerned avionics system has access. However it should be guaranteed then that in all cases that the AARS needs to annunciate the access indeed is provided with the appropriate priority. If that cannot be guaranteed there should be chosen for a solution with a separate command/control/display unit in the cockpit.

- Flight control system: The AARS interfaces with the flight controls by generating flight commands within the avionics system. The avionics system acts in commanded mode. That means that the commands are passed through to the auto flight system which has the right criticality to translate these flight commands into steering commands and interface with the flight control actuators.
- Engine control system: The AARS interfaces with the engines by generating power setting commands within the avionics system. The avionics system acts in commanded mode. That means that the commands are passed through to the auto flight system which has the right criticality to translate these power setting commands into commands to the engine control system.
- Sensors: The AARS uses its own set of sensors but the sensor transduction functions are implemented in the software of the avionics system. The avionics system interfaces with the sensor units using the same hw/sw interface systems as for its own sensors.
- ATC: ATC alerting is possible using several existing systems in the aircraft, such as: ADSB-transponder, radio telephony (COM) and (in the future) datalink. In all cases the alerting function is implemented in the software of the avionics system, from where the appropriate system is initiated and controlled.

Health monitoring

The avionics system is not a flight critical system, but it may contain some form of health monitoring functionality, which can also be made available for health monitoring of the AARS. The proper avionics system should be chosen such that it can sufficiently facilitate health monitoring functionality for the AARS. So health monitoring of the AARS is also to be implemented in the hardware and software of the Avionics system.

8.2.1.4 *AARS functionality integrated in the auto flight system*

The AARS functionality is largely implemented in the hardware and software of the auto flight system. Since in this design solution the AARS shares hardware and software resources with the auto flight system it might be more vulnerable for failures in the auto flight system.

Interfacing

- Flight crew: To initiate and terminate the recovery action a separate command/control/ unit in the cockpit is necessary. Annunciating to the flight crew is possible by means of the display and annunciating systems whereto the auto flight system has access. However it should be guaranteed then that in all cases that the AARS needs to annunciate the access indeed is provided with the appropriate priority. If that cannot be guaranteed there should be chosen for a solution with a separate command/control/display unit in the cockpit.

- Flight control system: The AARS interfaces with the flight controls by generating flight commands within the auto flight system. The auto flight system has the right criticality to translate these flight commands directly into steering commands and interface with the flight control actuators.
- Engine control system: The AARS interfaces with the engines by generating power setting commands within the auto flight system. The auto flight system has the right criticality to translate these power setting commands directly into commands to the engine control system.
- Sensors: The AARS uses its own set of sensors but the sensor transduction functions are implemented in the software of the auto flight system. The auto flight system interfaces with the sensor units using the same hw/sw interface systems as for its own sensors.
- ATC: ATC alerting is possible using several existing systems in the aircraft, such as: ADSB-transponder, radio telephony (COM) and (in the future) datalink. In all cases the alerting function is implemented in the software of the auto flight system, from where the appropriate system is initiated and controlled.

Health monitoring

Part of the auto flight system is flight critical and health monitoring is an integral part of the auto flight system. It can facilitate health monitoring functionality for the AARS. So health monitoring of the AARS is also to be implemented in the hardware and software of the APFCS.

8.2.1.5 *Evaluations of candidate systems*

The four candidate design solutions that have been introduced in the previous sections are evaluated in this section.

1. The AARS as fully stand-alone system is the only solution that has the advantage that it can be applied in all aircraft types that make use of a flight control system and an engine control system because it does not share any functionality with other systems in the aircraft. This of course means that the unit must contain all necessary functionality including (if necessary) redundancy and health monitoring.
2. The implementation of the AARS functionality integrated in the primary flight control system has as advantage that the system can operate at a high level. The APFCS itself is primary intended to control the aircraft and thus provides all necessary functionality for that including all fault tolerance and heath monitoring that it needs as flight critical system. The AARS then only has to deliver flight commands to the APFCS. A disadvantage is that failures in the APFCS could influence the functionality of the AARS. In such a (very rare) situation a LOC caused by a failure in the APFCS could possibly not be resolved by the AARS. The greatest disadvantage of this solution of course is that it can only be applied in aircraft that are equipped with fly-by-wire, and therefore it will be more difficult to offer the system as a retro-fit system to existing aircraft.
3. The implementation of the AARS functionality largely integrated in the in the hardware and software of an avionics system, like FMS or EGPWS has as advantage that it is a relatively cheap solution. Also health monitoring functions are facilitated from within the avionics system. A disadvantage might be that the avionics system is not flight critical and possibly is too vulnerable for system errors that can cause

erroneous behaviour of the AARS which given the fact that the AARS should have full authority might have fatal effect.

4. The implementation of the AARS functionality largely integrated in the hardware and software of the auto flight system has as advantage that health monitoring functions are facilitated from within the auto flight system. Also compared with an avionics system, like FMS or EGPWS, the auto flight system has a higher integrity and is less vulnerable for system errors that can cause erroneous behaviour of the AARS. This has as a disadvantage it is relatively less cheap to integrate the AARS functionality.

8.2.2 Selection of preferred candidate design solution from an economical point of view

From these four candidate design systems solution 1: AARS as fully stand-alone system, has been chosen for further analysis based on engineering judgement. It can be applied in almost each type of aircraft and the required integrity for the AARS functionality is not restricted by the safety characteristics of the hosting avionics system.

8.3 Assess how the elements work together to satisfy the intended safety functions

In step 2 the logical elements identified in step 1 and their interfaces is assessed for the two scenarios. The two scenarios identified in stage 4 are explored using a sequence diagram.

The two scenarios have many similarities, so for the sake of brevity they are combined into a single sequence diagram as shown in Figure 8-2. The sequence diagram has been based on the sequence diagrams as part of the Systems Engineering Unified Modelling Language (UML). For practical reasons the UML drawing conventions were not strictly adhered to. The diagram is used primarily to show the interactions between logical elements in a sequential order that those interactions occur. Time progresses from top to bottom in the diagram. Arrows indicate conveyance of information between logical elements. Stars are used to indicate that information is continuously conveyed.

Figure 8-2: sequence diagram for LoC-I scenario with successful recovery

In the Aircraft manufacture domain the system continuously reads inputs from its own sensor suite and calculates the required outputs to the flight control system (FCS) and engine control system (ECS). Upon initiation by the flight crew by means of the command and control (CMD/CTL) and display unit these outputs are passed through to the FCS and the ECS. Simultaneously information is shown on the CMD/CTL and display unit to inform the flight crew about the recovery status. Depending on the chosen option ATC is alerted about the recovery manoeuvre by means of a signal that is automatic generated by the AARS or by an emergency call of the flight crew (not shown in Figure 8-2). When the recovery manoeuvre is completed successfully, this is annunciated to the flight crew on the CMD/CTL and display unit and the flight crew can terminate the recovery action by means of the CMD/CTL and display unit. After termination of the recovery action the crew restores normal communication with ATC.

In the Aircraft operational domain introduction of the AARS is associated with the generation of dedicated flight procedures which are laid down in the operators Operation Manual and Aircraft Flight Manual. These procedures relate to the recognition of LOC and or LSA situations and how to react in such a situation, when to decide to initiate the AARS and how to proceed after initiation of AARS. These procedures need to be trained and it is likely that dedicated flight simulations are necessary. These training aspects are to be described in the operators Training manual.

In the ANSP and ATM/ANS equipment domain the introduction of the AARS will lead to the extension of certain ATC procedures. These extensions relate to the behaviour of the air traffic controller after an alert about a recovery manoeuvre from an aeroplane under his/her control has been received. This is comparable with the way ATC procedures have been extended after introduction of TCAS in the recent past.

During the construction of the sequence diagram the following observations were made:

- The diagram construction forces the authors to carefully consider all the functions and when/how they are activated. For example, the AARS display unit, for instance, must be actively displaying the AARS status throughout the flight, whether the AARS is engaged or not.
- The AARS processing element is modelled to be “hot standby”; it must already be active when the AARS is engaged.
- The ATM/ANS equipment is required to forward the aircraft AARS activation to the Air Traffic Controller; currently it is not shown how this should be done, but this observation should lead to a discussion on the right solution for this. It could be limited to voice communication, or automated by means of an automatic downlink message. Attention should be given in this respect to identified future hazards from FAST (AoC_95: *Proliferation of caution and warning systems and alerts may overwhelm the controllers in periods of heavy workload*)
- It is not shown how the flight crew detects the Loss of Control, as it is difficult to identify a single logical element for this. It was decided not to model this aspect.

8.4 Assess what could fail within each of the logical elements and interfaces

In this section possible failures in the design of logical elements and interfaces are identified and associated with the hazards identified during stage 4. The effect of the failures is analysed and safety requirements (in the form of safety objectives) are established.

8.4.1 Aircraft manufacture domain

MF.1: One or more functions in the AARS HW/SW unit fail.

No detailing has yet taken place in the architecture of the AARS HW/SW unit, so it is considered on the same abstraction level as in the FHA. That means that the effects of failing functionality are those that are described in the FHA. These are: TU.1, TU.2, TD.1, TD.2, TE.1, TE.2 and TE.3. Worst case is catastrophic.

MF.2: The display functionality of the CMD/CTL display unit fails.

1. No "AARS unavailable" can be displayed.
   This failure causes that the detection of a failure and therefore the unavailability of the AARS functionality cannot be communicated to the flight crew. This corresponds with hazard TU.1 (catastrophic) of the FHA.
2. No "recovery completed" can be displayed.
   This failure corresponds with hazard TU.2 (minor) of the FHA.

The most stringent requirement severity of these two hazards is: catastrophic. So the safety objective of the display functionality of the CMD/CTL display unit is: extremely improbable.

MF.3: The recovery initiation functionality of the CMD/CTL display unit fails

1. The recovery cannot be initiated.
   This failure corresponds with Hazards TD.1 (hazardous), TD.2 (catastrophic) and TU.1 (catastrophic) of the FHA. So the criticality of failure MF.3 depends on the probability that the failure has been detected by the system and also by the probability of a successful annunciation to the flight crew that the failure occurred. The safety design requirement of the recovery initiation functionality of the CMD/CTL display unit can be determined making use of fault trees.

MF.4: The recovery termination functionality of the CMD/CTL display unit fails.

1. The recovery action cannot be terminated in the "normal way".
   This failure corresponds with Hazard TU.2 (minor) of the FHA. Though TU.2 is an undetected failure the influence of the fact that the failure has been detected or not seem negligible on the severity of the hazard (in all cases there is some increased workload) so the severity is minor. So the safety objective of the recovery termination functionality of the CMD/CTL display unit is: probable.

MF.5: One or more of the AARS dedicated sensors fail.

1. Given the fact that all sensors are necessary to perform and complete the recovery manoeuvre in the correct and save way it is assumed that the AARS cannot perform its intended function after failure of one or more sensors. So failure MF.5 can lead to the detected failure of the recovery function. That corresponds with Hazards TD.1 (hazardous), TD.2 (catastrophic) and OD.1 (catastrophic) of the FHA. Furthermore failure of one or more sensors may lead to an erroneous operation of the AARS. That corresponds with Hazards TE.2 (catastrophic), TE.3 (catastrophic) of the FHA. So the criticality of failure MF.5 depends on the probability that the failure has been detected by the system and also by the probability of a successful annunciation to the flight crew that the failure occurred. The safety objective of the sensor system can be determined by making use of fault trees. However since only one of these hazards has a severity other than catastrophic the safety objective for failure of the sensor system is: extremely improbable.

MF.6: The automatic electronic interface between AARS HW/SW unit and ATC fails.

1. ATC cannot be alerted that the aeroplane in in a recovery following a LOC or LSA situation, other than by the flight crew.
   It is assumed that when the AARS is equipped with an automatic generated electronic alert towards ATC the flight crew will not bother to make an emergency call with radio telephony. This failure corresponds with Hazard AU.1 (hazardous) of the FHA. So the safety objective of the electronic interface between AARS HW/SW unit and ATC is: extremely remote.

MF.7: The interface between sensor(s) and AARS fails.

1. Failure of interface causes that the sensor output(s) cannot be used by the AARS and consequently that the AARS cannot perform its intended function.
   This failure has the same consequences as failure MF.5. So the safety objective of the interface between sensor(s) and AARS is: extremely improbable.

MF.8: The interface between the AARS HW/SW unit and the CMD/CTL display unit fails.

Failure of the interface can cause that:

1. The recovery cannot be initiated.
   This failure has the same consequences as failure MF.3.
2. The recovery cannot be terminated.
   This failure has the same consequences as failure MF.4.
3. No “AARS unavailable” can be displayed.
   This failure has the same consequences as failure MF.2-1
4. No “recovery completed” can be displayed.
   This failure has the same consequences as failure MF.2-2
5. Any combination of these 4 effects can occur.

At least one of these consequences corresponds with a hazard of the FHA that has a severity: catastrophic. That is MF.8-3 that has the same consequences as failure MF.2-1. The safety objective of that failure is based on hazard TU.1 (catastrophic) of the FHA. That means that the safety objective of the interface between the AARS HW/SW unit and the CMD/CTL display unit is: extremely improbable.

MF.9: The interface between AARS HW/SW unit and the flight control system (FCS) fails

1. The AARS will be unable to control the flight controls and therefore the AARS cannot perform its intended function or the failed interface causes an erroneous input of the actuator of the flight control system.
   The failure corresponds with Hazards TD.1 (hazardous), TD.2 (catastrophic), OD.1 (catastrophic), TU.1 (catastrophic), TE.2 (catastrophic) and TE.3 (catastrophic) of the FHA. The safety objective of the interface can be determined by making use of fault trees. However since only one of these hazards has a severity other than catastrophic the safety objective of the interface between AARS HW/SW unit and the flight control system (FCS) is: extremely improbable.

MF.10: The interface between AARS HW/SW unit and the engine control system (FCS) fails

1. The AARS will be unable to control the engine and therefore the AARS cannot perform its intended function or the failed interface causes an erroneous input of the engine control system.
   As in MF.9 the failure corresponds with Hazards TD.1 (hazardous), TD.2 (catastrophic), OD.1 (catastrophic), TU.1 (catastrophic), TE.2 (catastrophic) and TE.3 (catastrophic) of the FHA. So the safety objective of the interface between AARS HW/SW unit and the flight control system (FCS) is: extremely improbable.

8.4.2 Aircraft Operational domain

OF.1: The flight crew fails (timely) to initiate the recovery action upon reaching a LOC or LSA situation.

2. This failure corresponds with Hazard OS.3 (hazardous) of the FHA. So the safety objective of the flight crew initiation of the recovery action upon reaching a LOC or LSA situation is: extremely remote.

OF.2: The flight crew fails (timely) to inform ATC that the aeroplane is in recovery action.

1. This failure corresponds with Hazard AS.1b (hazardous) of the FHA. So the safety objective of the flight crew action to inform ATC that the aeroplane is in recovery action is: extremely remote.

OF.3: The flight crew fails (timely) to inform ATC that a recovery action is terminated and controllability is regained.

1. ATC will be unaware for some time that the crew has regained (full or limited) control of the aeroplane. However, ATC will continue to keep environmental traffic separated from the aeroplane. However, after some time normal communication with the flight crew will be restored, possibly initiated by ATC. So it is assumed that this failure has no extra consequences.

8.4.3 ANSP and ATM/ANS equipment domain

AF.1: ATC fails to recognise the automatic generated electronic alert that an aeroplane is in recovery action.

1. It is assumed that when the AARS is equipped with an automatic generated electronic alert towards ATC the flight crew will not find it necessary to make an emergency call with radio telephony. This ATC failure corresponds with Hazard AS.1b (hazardous) of the FHA. So the safety objective for the communication link between the flight crew and ATC to inform ATC that the aeroplane is in recovery action is: extremely remote.

AF.2: ATC fails to recognise the emergency call by radio telephony that an aeroplane is in recovery action.

1. It is assumed that the AARS is not equipped with an automatic generated electronic alert towards ATC. This failure corresponds with Hazard AS.1b (hazardous) of the FHA. So the safety objective of the flight crew action to inform ATC that the aeroplane is in recovery action is: extremely remote.

8.5 Assess the levels of development assurance

In this section the levels of development assurance (DALs) must be determined to ensure that the mitigating requirements are successful in making the system sufficiently safe.

In the Aircraft Manufacture Domain, ED-79A, ref [32], provides a specific FDAL assignment schedule for functions that protect the aircraft against external events, which is applicable to the AARS, see Figure 8-3. Note that only CAT and HAZ top level failures are considered. Functions with lower level failures are not assigned with a DAL.

Figure 8-3: Protection function FDAL assignment as a function of probability of an external even (ref ED79A)

The conditional probability of a LoC-I or LSA event is assumed to be less than 10^{-5} per flight hour.

Observation:
The ATM equipment, ANSP and Aircraft operational domain currently lack the process for assignment of system level DALs. Therefore no DALs could be assigned logical elements in these domains. For the level of software used in the ATM domain the EUROCAE document ED-153, ref [33], describes a process to assign Software Assurance Levels SWALS, but this is beyond the scope of this case study.

Table 8-1 provides for number of logical elements the assigned DAL. For the sake of brevity not all hazards have been addressed.

Table 8-1: AARS related functional failures and DAL assignments

Fail. ID	Description	Logical element(s)	Domain(s)	Severity	(F)DAL
MF.1	One or more functions in the AARS HW/SW unit fail.	AARS processing	A/C manuf.	CAT	B
MF.2	The display functionality of the CMD/CTL display unit fails.	AARS CMD/CTL & display unit	A/C manuf.	CAT	B
MF.3	The recovery initiation functionality of the CMD/CTL display unit fails	AARS CMD/CTL & display unit	A/C manuf.	CAT	B
MF.4	The recovery termination functionality of the CMD/CTL display unit fails.	AARS CMD/CTL & display unit	A/C manuf.	MIN	n/a
…					
OF.1	The flight crew fails (timely) to initiate the recovery action upon reaching a LOC or LSA situation	Flight crew	Aircraft operational	HAZ	?
…					
AF.1	The communication link between the flight crew and ATC (to inform ATC that the aeroplane is in recovery action) fails	AARS processing ATM equipment	A/C manuf. ATM equipmnt	HAZ HAZ	C ?
…					

8.6 Confirm that the system as designed will meet the requirements, including the required level of safety performance.

Relevant hazards have been identified and the specifications (safety objectives) guarantee that when the system performs as designed, all identified hazards are mitigated sufficiently, both in the absence of (self) failure) and in the event of (self)failure of the AARS.

8.7 Other requirements

In document Stage 4 it is argued that the flight crew might utilize the AARS in any event where they lose faith in a safe and comfortable outcome. Such an event is estimated to occur with a probability of 1x10-5 per flight hour which on average corresponds with once in 100,000 flight hours. The most critical failures of the AARS are “undetected failure of the main intended function” and “initiation of the AARS” which have a TLS of 1x10-4 per flight hour. This corresponds with a MTBF of 10,000 flight hours.

From this it follows that the average time laps between utilization of the AARS is 10 times higher than the MTBF of the AARS most critical functions. This means that it is probable that the AARS is already failed before the system must come into action. To prevent this implementation of the AARS functionality should be such that the system is equipped to perform health monitor functions such as a self/availability test, what together with a dedicated maintenance program should guarantee the availability of the AARS functions.

9 Conclusions and recommendations

In this report the (initial) development of a hypothetical Automatic Aircraft Recovery System, intended to reduce the number of Loss of Control accidents, has been subject to the new certification process as developed within the ASCOS project (see Deliverable D1.3 [14]). The main novelties of the new approach concern:

- A (partial) transition from compliance based to performance based certification; where traditionally certification is performed by defining a certification basis and showing compliance with the associated certification specifications, the new approach is based on an argument structure consisting of a collection of claims that together ensure that introduction of the item to be certified is acceptably safe and remains acceptably safe over its life cycle. It can be said that the collection of claims represent a new manifestation of the certification basis. The argument structure may contain in itself prescriptive elements as in a traditional certification basis (hence the notion of *partial* transition), but the new approach is primarily focused on explicitly proving that an acceptable (target) level of safety is met, instead of proving that all requirements of an agreed certification basis are satisfied (which is only implicit proof that acceptable safety is achieved).
- Taking into account from the start that the item to be certified may affect safety in any element of the Total Aviation System. This forces to devote sufficient attention to the interfaces between the various domains (such as technical, flight operational, ATM, airports, etc.) within the TAS. This may prevent that safety improvements by introduction of new systems in one domain may contribute in an unexpected way to hazards in another domain.

The question addressed in this report is how an innovative system, like AARS, may be certified according to the new approach; what are the potential benefits and shortcomings of this approach? It is emphasized that the design of the AARS has been developed only to the level required to assess the new approach. In this report several observations were made concerning the application of the new approach to the certification of the AARS. Based on these observations the following conclusion and recommendations are provided.

1. Application of the Areas of Change from FAST to identify potential future hazards can be useful in the design and certification process. Due to the large number of defined AoCs –in a seemingly rather unstructured way- it is however cumbersome to ensure that all possible applicable future hazards are properly identified.
2. The risk assessment tool, as developed within the ASCOS project, has limited value as a safety assessment tool within for instance the Preliminary System Safety Assessment process (as part of stage 5 of the approach). The main benefit would be in the area of definition of relevant accident scenarios. On the other hand, in stage 1 of the approach, the tool may be helpful to estimate the potential effectiveness of the system and as such may contribute to the proper definition of the intended change.
3. The application of an argument structure, as an alternative for a traditional certification basis, seems attractive from a theoretical viewpoint and provides a logic structure for the certification process. However, the development of a consistent argument structure that in a logical way builds up a collection

of claims and sub-claims to prove that the top level claim is satisfied is a difficult task. The role of the argument architect is difficult, and it is recommended that persons that fulfil this task would have to be specifically trained and qualified.

4. The top-level claim of the argument structure is by definition that the "*the operation of … system achieves acceptable safety across the TAS*". By definition the specification of the acceptable level of safety is the responsibility of the certifying authority. However, it is unclear how the acceptable level of safety can be set by the authority across the TAS, as there is not a single competent authority. It raises the question which authority is responsible for safety across the TAS and in fact who is the certifying authority in this respect?
   It is recommended that the possible introduction of the ASCOS approach will be accompanied with organisational adaptations in the certifying organisations to ensure that responsibilities and tasks are clearly and consistently arranged across the TAS.
5. Within the ASCOS approach it is unclear whether the top-level safety claim is satisfied if there are safety benefits in one domain while there are safety reductions in another domain.
   It is recommended that within the description of the ASCOS approach guidelines are incorporated to address this issue, and how the net safety result is determined.
6. In the context of the introduction of AARS –being a non-mandatory safety improving device- it is unclear how the top-level safety claim ("acceptably safe") should be interpreted, as the TAS is already acceptably safe without the system. It appears that the top-level claim purely focuses on safety, and not on a requirement that any new system shall also perform its intended function.
   It is recommended that the top-level claim is adapted to reflect this requirement.
7. In the description of the approach (D1.3) it is stated that Stage 4 broadly aligns with a FHA, and Stage 5 with a PSSA. However, the FHA and PSSA are standard elements of existing design and certification processes and it somewhat unclear how these processes can be consistently incorporated in the argument structure. The argument structure (at lower levels) may formulate sub-claims that are inherently addressed by FHA and PSSA processes. Interfacing the FHA and PSSA with the argument structure may therefore be cumbersome, although it is shown in this report that – with some effort – it is possible.
8. In the description of the methodology (D1.3) it is stated that Stage 4 focuses on the behaviour of the changed system in the absence of failure. At the same time it is stated that this stage broadly aligns with the FHA process. These two statements appear to be incompatible, as a functional hazard assessment process cannot be conducted without addressing functional failures of the system.
   It is recommended that the description in D1.3 is updated to reflect the characteristics of the FHA.
9. It is recommended that in Stage 4 sub-claims are specifically directed to hazards in the various domains across the TAS (e.g. flight technical, flight operational and ATM), such that responsibilities for mitigating these hazards can be clearly assigned to specific stakeholder and authorities.
10. It is recommended that the ASCOS approach provides guidance concerning the consistent application of safety objectives over the various domains of the Total Aviation System. It is not a-priori evident that failure conditions with a given severity level are equally acceptable (in terms of frequency) within the various domains.

Finally, as was mentioned in the introduction, the AARS use case was intended to highlight potential efficiency and safety gains of using the ASCOS approach when applied to a novel aircraft system.
The question remains whether the ASCOS approach may indeed lead to such improvements. Although more insight is gained by this use case a definitive conclusion cannot be drawn in this respect.
As shown, safety benefits may be anticipated by using an approach that takes into account the Total Aviation System. It leads to early identification of potential negative safety consequences in other domains (such as ATM in this case) which can thus be mitigated as part of the basic design. Therefore, surprises may be avoided, leading to safety and efficiency benefits. However, these benefits will be achieved at some costs, namely early involvement of all stakeholders and authorities from all aviation domains. This will add complexity to the initial design and certification process and requires an increased management and communication burden. Most likely also organisational adaptations are required to ensure that responsibilities are properly distributed.

Whether the transition from a traditional compliance based certification to a more performance based approach may contribute to safety and efficiency benefits is difficult to answer, based on the results of this case study. The current certification methodologies for aircraft systems are well established. Although the AARS is a novel system, sufficient experience and guidance exist (see for instance ED-79A/ARP 4754A, ref [32]) to efficiently certify such system. Moreover, essential stages (4. Specification and 5. Design) of the new approach broadly align with existing FHA and PSSA methods, and therefore are not expected to provide substantial improvement. The set-up of the logical argument structure may help to provide a foundation for the certification basis. However, the set-up of the argument structure itself is not without difficulties. In particular to define a consistent set of claims to an appropriate level and full coverage of all hazards is a laborious and complex task. Argument architects need to be specifically trained for such task. It is expected that a proper argument structure might be – in theory – beneficial from a safety viewpoint, as it explicitly addresses the required safety level, as opposed to current certification approaches that are more implicit. However, it is questionable if this benefit will materialize for a practical case, such as AARS, and if it is worth the additional effort.

References

#	Title, Authors(s), Year
[1]	COMMISSION REGULATION (EU) No 965/2012 of 5 October 2012, laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:296:0001:0148:EN:PDF
[2]	Commission Regulation (EU) No 800/2013 of 14 August 2013 amending Regulation (EU) No 965/2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council Text with EEA relevance http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:227:0001:0074:EN:PDF
[3]	Commission Regulation (EU) No 71/2014 of 27 January 2014 amending Regulation (EU) No 965/2012 laying down technical requirements and administrative procedures related to Air Operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council Text with EEA relevance http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2014:023:0027:0030:EN:PDF
[4]	European Aviation Safety Agency, Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Part-CAT, Initial issue 25 October 2012, Annex to ED Decision 2012/018/R, http://easa.europa.eu/agency-measures/docs/agency-decisions/2012/2012-018-R/Annex%20to%20ED%20Decision%202012-018-R.pdf
[5]	European Aviation Safety Agency Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Part-ORO, Consolidated version including Amendment 2, 23 August 2013 Supplementary document to ED Decision 2013/019/R http://www.easa.europa.eu/agency-measures/docs/agency-decisions/2013/2013-019-R/04%20Part-ORO%20(AMC-GM)_Amdt2-Supplementary%20document%20to%20ED%20Decision%202013-019-R.pdf
[6]	JSAT Loss of Control, CAST Approved Final Report, Results and Analysis, Paul Russel & Jay Pardee, December 15, 2000
[7]	ACARE; European Aeronautics Vision for 2020: Meeting society's needs and winning global leadership, Report of the Group of Personalities, ISBN 92-894-0559-7, 2001.
[8]	ACARE; The Strategic Research Agendas SRA-1, SRA-2 and the 2008 Addendum to the Strategic Research Agenda, 2008.
[9]	European Commission; Aeronautics and Air Transport: Beyond Vision 2020 (towards 2050), Background Document from ACARE, 2010.
[10]	European Commission; Flightpath 2050: Europe's Vision for Aviation, Report of the High Level Group on Aviation Research, ISBN 978-92-79-19724-6, 2011.
[11]	ASCOS Website; http://www.ascos-project.eu , 2014.
[12]	ASCOS D1.1, Analysis of existing regulations and certification processes, B. Pauly, T. Longhurst, A. Iwaniuk, M. Idzikowski, B. Dziugiel, v1.3, 20-08-2013.
[13]	ASCOS D1.2: Definition and evaluation of innovative certification approaches, U. Dees, P. van der Geest, A. Simpson, S. Bull, P. Blagden, T. Longhurst, A. Eaton, G. Temme, B. Pauly, v1.3, 20-08-2013.
[14]	ASCOS D1.3: Outline proposed certification approach, A. Simpson, S. Bull, T. Longhurst, v1.2, 18-12-2013.
[15]	ASCOS D3.1: Total aviation system safety assessment methodology, J.P. Magny (JPM), A.L.C. Roelen (NLR), J.J. Scholte (NLR), T. Longhurst (CAAi), A. Iwaniuk (IoA), v1.6, 30-12-2013.
[16]	EASA; European Aviation Safety Programme Manual, TE.GEN.00400-001, 2011.
[17]	EASA; European Aviation Safety Plan 2011-2014, E.T004-02, 2011.
[18]	EASA; Annual Safety Review 2010, ISBN 978-92-9210-097-1, 2011.
[19]	EUROCONTROL SRC; Annual Safety Report 2010, SRC Document 47, Ed. 1.0, 2011

[20] ASCOS Annex I. - “Description of Work”, Part B, 10 July 2012

[21] Final report on the accident on 1th June 2009 to the Airbus A330-203, registered F-GZCP operated by Air France flight AF447 Rio de Janeiro - Paris

[22] Crashed during approach, Boeing 737-800, near Amsterdam Schiphol Airport, 25 February 2009

[23] EASA Certification Specifications for Large Aeroplanes, CS-25 Amendment 14

[24] ASCOS Briefing on Stage 5 Assessment Process for WP4.2, P12011.42.1.4

[25] ASCOS D3.3, Tool for risk assessment and user manual

[26] ASCOS D2.4, Tools for Continuous Safety Monitoring

[27] ASCOS D3.2, Risk models and accident scenarios

[28] ASCOS D3.4, Overall Safety Impact Results and User Manual

[29] ASCOS D3.6, WP3 Final Report Safety Risk Management

[30] List of Areas of Change, In: Ongoing and Future Phenomena and Hazards Affecting Aviation compiled by Brian Smith, NASA Ames Research Center November 15, 2013, http://www.nlr-atsi.nl/fast/FAST_AoCs_20131115.pdf

[31] SAE ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996-12-01

[32] EUROCAE ED-79A, SAE ARP4754A Guidelines For Development Of Civil Aircraft And Systems, December 2010

[33] EUROCAE ED-153, Guidelines For Ans Software Safety Assurance, Augustus 2009