

Morphing Wing Integrated Safety Approach and Results

Maurizio Verrastro and Sylvain Metge

Abstract SARISTU morphing wing is mainly based on three devices: enhanced adaptive droop nose (EADN), adaptive trailing edge device (ATED) and winglet active trailing edge (WATE). All these devices are used together to improve the overall wing efficiency and to reduce the aerodynamic noise. The safety activities described in this paper were performed to verify whether this concept can comply with the standard civil flight safety regulations and airworthiness requirements. The safety analysis was performed in two steps: a functional hazard assessment (FHA) and a system safety assessment (SSA). Both analyses were performed at wing integration level (IS12) and at single morphing wing devices level. A complete mapping between these two levels of analysis was structured from the beginning of the process, starting from the aircraft functional definition, to integrate and harmonize both FHA and fault trees results. FHA was used to assess the severity of the identified Failure Conditions and then allocate safety requirements. Fault tree modelling technique was used to verify the compliance of the system architectures to the quantitative safety requirements resulting from the FHAs. The paper sets out the hypotheses and common data used by the fault trees. A complete but simple example illustrates the safety approach all through the different steps of the safety methodology. Other safety activities commonly performed in the aeronautical field such as the particular risk analysis (PRA), common mode analysis (CMA) and zonal safety analysis (ZSA) were identified in the frame of SARISTU project. This paper concludes with a summary highlighting the main results of these safety activities with some lessons learned from the safety approach adapted to SARISTU context.

M. Verrastro (✉)

Alenia Aermacchi S.p.A. Military Aircraft Safety, 10072 Caselle, Italy
e-mail: maurizio.verrastro@alenia.it

S. Metge

Airbus Operations S.A.S., Toulouse, France
e-mail: sylvain.metge@airbus.com

Nomenclature

A/C	Aircraft
AOA	Angle of attack
ATE(D)	Adaptive trailing edge (device)
AS0x	Application Scenario x
CAT	CATASTROPHIC
CCA	Common cause analyses
CMA	Common mode analyses
DAL	Design assurance level
EADN	Enhanced adaptive droop nose
EASA	European aviation safety agency
EMC	Electro magnetic compatibility
EMI	Electro magnetic interference
FC	Failure Condition
FCS	Flight control system
FDAL	Functional development assurance level
FH	Flight hour(s)
FHA	Functional hazard analysis/assessment
FOD	Foreign object damage
FT	Fault tree
FTA	Fault tree analysis
HAZ	HAZARDOUS
HIRF	High-intensity radiated fields
HW	Hardware
IS12	Integration Scenario 12
LND	Landing
MAJ	MAJOR
MCS	Minimal cut set
MIN	MINOR
MoC	Means of compliance
MT	Maintenance time
NSE	No safety effects
PFHA	Preliminary FHA
PRA	Particular risk analysis
PSSA	Preliminary system safety assessment
REQ	Requirement
SSA	System safety assessment
SW	Software
T/O	Take-off
WATE	Winglet active trailing edge
ZSA	Zonal safety analysis

1 Introduction

The goal of SARISTU project is to design a smart wing with morphing devices aimed to improve the overall aircraft (A/C) aerodynamic efficiency and to reduce the aerodynamic noise. A wing model will be realized to perform wind tunnel testing activity. This activity is required to validate theoretical calculation performed to evaluate the morphing wing advantages. A safety analysis following standard civil flight safety regulations is not required to validate the wind tunnel model and results. Nevertheless, the safety analysis was performed to verify whether SARISTU concept can comply with the applicable airworthiness code requirements, in particular with EASA CS-25 Ref. [1].

SARISTU morphing wing concept is mainly based on three devices working together. Every device is associated with an “Application Scenario” (AS0x) and the integration is provided as separate work package:

AS01—Enhanced Adaptive Droop Nose (EADN): It is a movable leading edge with a morphing skin. The aim of this device is to reduce drag and noise by optimizing the laminar flow in a range of angle of attack (AOAs). In the wing tunnel test model, the EADN will be used only as “high-lift device”. However in the following functional hazard analysis (FHA), the drag optimization function during climb/descent/cruise phases has also been taken into account (Fig. 1).

AS02—Adaptive Trailing Edge Device (ATED): It is a morphing skin trailing edge device, with the aim to optimize the wing shape in order to reduce drag. This device has the capability to be also used for the wing load alleviation/control function (not implemented in SARISTU). This device will be used during cruise and landing flight phases, only (Fig. 2).

AS03—Winglet Active Trailing Edge (WATE): It is a winglet movable trailing edge with a morphing skin part. Its aim is to optimize/reduce wing drag and structural loads (fatigue and vibrations loads control, turbulence, gusts and manoeuvre load alleviation, and wing load protection) (Fig. 3).

IS12—Wing Integration Verification and Validation: this work package consists in integrating the complete morphing wing. The three previously mentioned devices will be integrated in a dedicated wing box, with a proper interface necessary to perform the wing tunnel measurements.

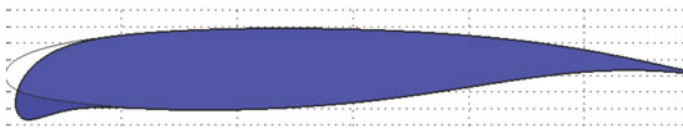
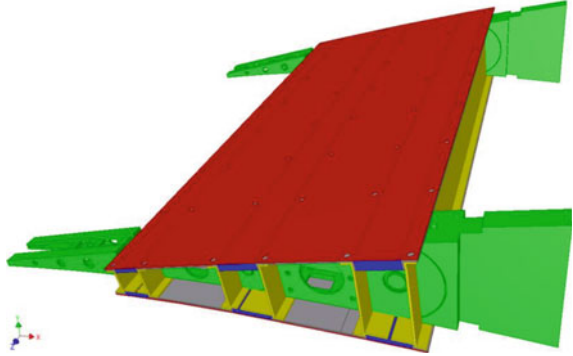
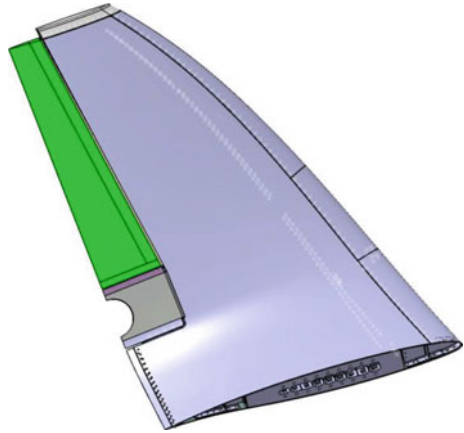


Fig. 1 Wing profile with lowered EADN

Fig. 2 ATED 3D view**Fig. 3** WATE 3D view

2 Safety Analysis Approach Overview

This section shows the approach used to achieve a SARISTU system safety assessment. Main drivers are the already-mentioned CS-25 regulations as well as the Aerospace Recommended Practices SAE ARP 4754a Ref. [3] and SAE ARP 4761 Ref. [4]. In fact, the SARISTU morphing wing concept can be analysed following the currently available rules and practices. Figure 4 shows a general safety assessment process overview as required by the CS-25 safety regulation. The dotted rectangle highlights the boundary of the process used for SARISTU project.

Activities included in the SARISTU safety assessment boundaries are “*System FHAs*”, “*Analyses*” and “*System Safety Assessment*”. The system level is identified in the complete morphing wing, and therefore it is under IS12 work package responsibility. A preliminary functional hazard assessment (PFHA) at SARISTU level is then the starting point for this process. “*Analyses*” boxes are the functional hazard assessment (FHA) and the fault tree analyses (FTAs) performed by the three Application Scenarios (AS01, AS02 and AS03) leaders. The system safety

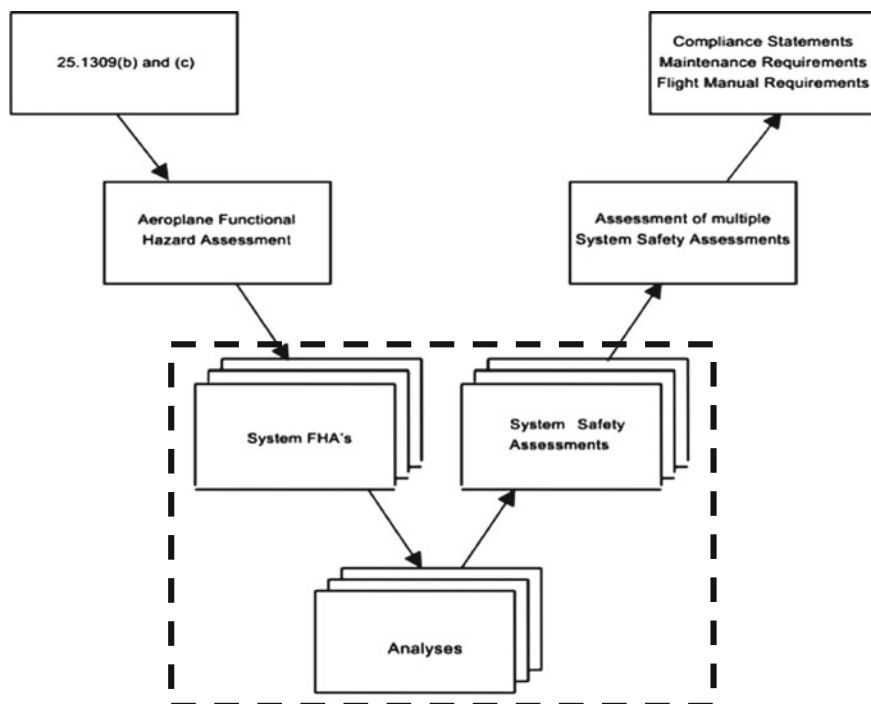


Fig. 4 CS-25 safety assessment process overview

assessment (SSA) is mainly composed of a consolidated FHA and the fault tree analysis at morphing wing level (IS12).

3 Functional Approach Definition

Generic aircraft safety analyses are based on a functional approach. Aircraft and system-level functions are first identified, and then, their failure modes are analysed to identify the end effects (i.e. safety consequences on the aircraft and its occupants). A complete aircraft-level analysis is not the target of this project, but it is clear that SARISTU functional failure repercussions are expected at aircraft level. It is evident from Fig. 4 that System FHAs are connected to the complete airplane functional hazard assessment. In particular for SARISTU project, a reference aircraft has been defined as reported in the deliverable number A_DEU_121_1_R2 Ref. [6] and depicted in Fig. 5. The reference aircraft is a twin-fuselage-mounted engine medium-range type. In the previously mentioned SARISTU deliverable, a morphing wing functional description has been reported, but from the aircraft-level point of view, only major geometrical and system design information have been provided (the goal of this document is an aeromechanical and performance

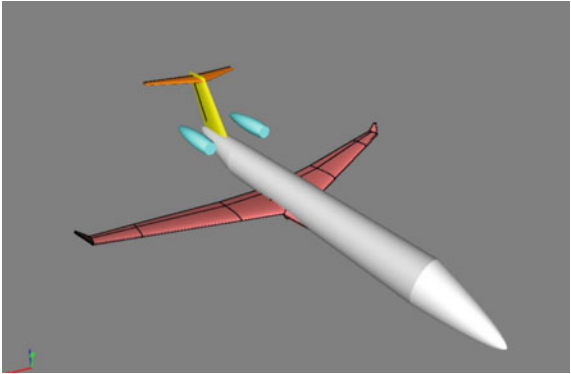


Fig. 5 Reference aircraft overview

assessment). A very generic A/C functional overview is listed in a paper titled “Framework for the Application of System Engineering in the Commercial Aircraft Domain” Ref. [9]. This document collects the results of a working group with people affiliated with several organizations as AIAA, SAE, IEEE, and specialists of many manufacturer’s companies in the aerospace (e.g. Boeing, Rockwell, Honeywell, Airbus-Aeromatra). For SARISTU project, a subset of aircraft-level functions was selected to evaluate high-level SARISTU functional failure effects. A very high-level generic aircraft functional overview is depicted in Fig. 6. The high-level functions potentially impacted by SARISTU are circled. The selected functions are mainly related to the A/C aerodynamic configuration control and forces generation. The structural behaviour has also been considered for the load alleviation/control functions.

SARISTU functions extracted from project deliverable Ref. [6] are the following: drag minimization, lift adaptation, turbulence/gust load alleviation, manoeuvres load alleviation, vibration and fatigue control, and A/C load protection. Following the morphing wing-level functional definition, the detailed selected aircraft functions are reported in Table 1.

SARISTU and relevant aircraft-level functions need to be linked in order to make easier the assessment of the functional failure end effect. This connection is reported in Table 2. This information is also useful to make clear the link between

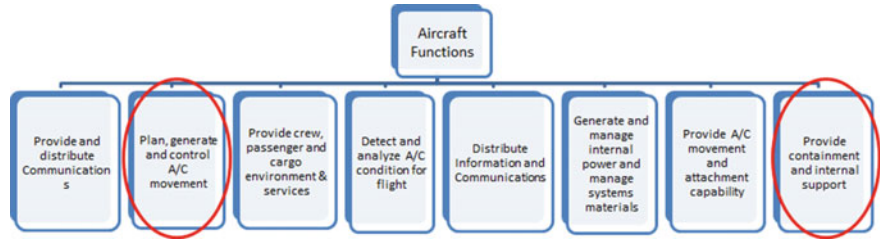


Fig. 6 High-level generic aircraft functional overview

Table 1 Aircraft-level functions selected for SARISTU

Aircraft functions
2. Plan, generate and control A/C movement
2.2 Generate and control aircraft movement
2.2.5 Control A/C aerodynamics configuration
2.2.5.1 Control lift and drag
2.2.6 Protect aerodynamic control
2.2.6.1 To provide protection against turbulence effects
2.2.6.2 To provide protection against stall load
2.2.7 Provide aerodynamic control forces
2.2.8 Support supplemental flight control
2.2.8.1 To provide overload protection and A/C load protection
2.2.8.2 To provide protection against manoeuvres effects
2.2.13 Generate lift
2.2.14 Provide aerodynamic stability
8. Provide containment and internal support
8.1 Provide containment
8.1.2 Provide structural integrity and load distribution
8.1.2.1 To provide fatigue protection

the SARISTU (and IS12)-level FHA and the Application Scenario detailed analyses. Application Scenarios can be easily linked with SARISTU functions. In this way, a complete mapping between Application Scenarios and SARISTU (IS12) aircraft-level functions is traced. This latest connection is reported in Table 3. Drag minimization and lift adaptation cannot be considered as fully independent functions. In fact a modification of the wing profile/shape leads to a wing pressure

Table 2 Link between aircraft and morphing wing functions

Morphing system functions	Aircraft-level functions	
Drag minimization function	2. Plan, generate and control A/C movement	2.2.5.1 Control lift and drag 2.2.7 Provide aerodynamic control forces
Lift adaptation function	2. Plan, generate and control A/C movement	2.2.5.1 Control lift and drag 2.2.7 Provide aerodynamic control forces 2.2.13 Generate lift 2.2.14 Provide aerodynamic stability
Turbulence/gust load alleviation	2. Plan, generate and control A/C movement	2.2.6.1 To provide protection against turbulence effects
Manoeuvres load alleviation	2. Plan, generate and control A/C movement	2.2.8.2 To provide protection against manoeuvres effects
Vibration and fatigue control	8. Provide containment and internal support	8.1.2.1 To provide fatigue protection
A/C load protection	2. Plan, generate and control A/C movement	2.2.6.2 To provide protection against stall load 2.2.8.1 To provide overload protection and A/C load protection

Table 3 Link between morphing wing functions and SARISTU subsystems (Application Scenarios)

Morphing system functions	Involved subsystem	Way to operate	SARISTU FHA Function
Drag minimization function	EADN	Continuous/quasi-static operation	Wing shape optimization control function “Drag minimization” and “lift adaptation” cannot be modified independently (i.e. a modification of the aerodynamic profile in order to increase lift also cause a drag coefficient change). The EADN will be used also as “high-lift device”, during take-off and landing phases
	ATED	Continuous/quasi-static operation	
	WATE	Continuous/quasi-static operation	
Lift adaptation function	EADN	Continuous/quasi-static operation	
	ATED	Continuous/quasi-static operation	
	WATE	Continuous/quasi-static operation	
Turbulence/gust load alleviation	WATE	Occasional/dynamic operation	Turbulence/gust load alleviation function
Manoeuvres load alleviation	WATE	Occasional/dynamic operation	Manoeuvres load alleviation function
Vibration and fatigue control	WATE	Continuous/fast-dynamic operation	Wing vibration and fatigue control function
A/C load protection	WATE	Occasional/dynamic operation	Wing loads protection function

distribution change, which simultaneously affects both lift and drag levels. Due to this consideration, at IS12 FHA level, these two functions will be merged in a single function called “wing shape optimization control”. The EADN works in conjunction with ATED and WATE to optimize the wing shape, but during take-off and landing phase, it acts as a “high-lift” device. In this case, the EADN contribution to the A/C flight safety is heavier with respect to the other devices. This is why it can be traced as “stand-alone” effect on lift adaptation function.

Load alleviation/protection/control functions, and vibrations/fatigue loads control will be implemented using the WATE device only, at least for this testing phase and for this SARISTU concept. The ATED has also the capability to perform this task thanks to its fast actuation speed, but in the frame of SARISTU, it will be used for the wing shape optimization only. As a general consideration, the WATE alone cannot perform all the possible wing load alleviation/protection and control functions. For example, to perform stall load protection, aerodynamic surfaces, which greatly modify the lift generation in a more direct way, are required (e.g. ATED, aileron, and spoilers). In the SARISTU project FHA, only the WATE device will be considered for wing loads alleviation/protection/control functions (including vibrations control).

4 Dual-Level Safety Assessment: IS12 and AS0x FHAs and FTAs

4.1 Functional Hazard Assessment General Overview

Functional hazard assessment is a safety analysis focused at system/aircraft functional level. As reported on the already-mentioned SAE ARP 4754a, the FHA *“examines aircraft and system functions to identify potential functional failures and classifies the hazards associated with specific Failure Conditions. The FHA is developed early in the development process and is updated as new functions or Failure Conditions are identified. Thus, the FHA is a living document throughout the design development cycle”*.

Functional failures are identified with the associated severity. Then, qualitative requirements are set in this analysis (redundancy, functional design assurance level (FDAL), specific monitoring, etc.). In the IS12 FHA, SARISTU-level functional failures are considered. The following failure scenarios are analysed for every morphing system function:

- Total loss of function,
- Partial loss of function,
- Erroneous provision of function, and
- Inadvertent provision of function

Failure Condition's classification is provided in accordance with CS-25 regulations based on the severity of their effect:

NO SAFETY EFFECT (NSE) *“Failure Conditions that would have no effect on safety; for example, Failure Conditions that would not affect the operational capability of the aeroplane or increase crew workload”*.

MINOR (MIN) *“Failure Conditions which would not significantly reduce aeroplane safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew”*.

MAJOR (MAJ) *“Failure Conditions which would reduce the capability of the aeroplane or the ability of the crew 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 workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries”*.

HAZARDOUS (HAZ) *“Failure Conditions, which would reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating, conditions to the extent that there would be: (i) A large reduction in safety margins or functional capabilities; (ii) Physical distress or excessive workload such that the*

Effect on Aeroplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	<---Probable--->	<----Remote---->	Extremely <-----> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:	No Probability Requirement	<-----> <10 ⁻³ Note 1	<-----> <10 ⁻⁵	<-----> <10 ⁻⁷	<10 ⁻⁹
Classification of Failure Conditions	No Safety Effect	<----Minor----->	<----Major----->	<--Hazardous-->	Catastrophic
Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category aeroplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.					

Fig. 7 Required probability figures versus safety classification

flight crew cannot be relied upon to perform their tasks accurately or completely; or (iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew”.

CATASTROPHIC (CAT) *“Failure Conditions, which would result in multiple fatalities, usually with the loss of the aeroplane. (Note: A “Catastrophic” Failure Condition was defined in previous versions of the rule and the advisory material as a Failure Condition which would prevent continued safe flight and landing.)”.*

Figure 7 shows these requirements and the expected effects on flight crew, passengers, and on the aeroplane for every identified severity.

4.2 SARISTU Functional Hazard Assessment Peculiarity

SARISTU-level FHA table provides the following information: (1) a failure mode identification number, (2) failure mode brief description, (3) flight phase during which the failure mode can occur, (4) severity classification according to CS-25

MoC, (5) average failure probability per flight hour according to safety objectives expressed in the CS-25 MoC, (6) Failure Condition identification with reference to involved subsystems and relevant failure modes, (7) detailed description of the A/C-level effects, (8) detection means (if detection is possible), (9) flight crew reaction after failure detection (if detection is possible) and (10) possible requirements coming from safety considerations (e.g. redundancy requirements and inspections), (11) external events involved in the hazard (if applicable) and (12) justification for safety categorization following CS-25 regulations.

In SARISTU project, the Application Scenarios FHA's format was not imposed, but the technical information to be provided was agreed with IS12 leader. In the Scenarios Application FHAs, the following data are reported: (1) A failure mode identification, (2) failure mode title, (3) failure mode description, (4) aircraft-level effects, (5) Failure Condition identification/title, (6) safety classification, (7) justification for safety classification, (8) flight phase during which the failure mode can occur, (9) detection means, (10) flight crew action, (11) associated requirements and (12) link with the impacted IS12 functions (optional).

The morphing wing FHAs are performed following a standard approach. The peculiarity of SARISTU safety analysis is the work packages assignment. In fact, every Application Scenario is a single morphing wing device that shall be integrated in the complete wing. This picture is very close to a "real-life" application: an aircraft manufacturer (in SARISTU, it is represented by IS12 work package) will assemble devices from different suppliers (in this case represented by Application Scenarios AS01, AS02 and AS03). So every SARISTU Application Scenario is analysed as a "stand-alone" device, but the failure mode effects are evaluated at A/C level, merged and properly combined at IS12 (wing integration) level.

Since the above-mentioned safety analyses are performed at different levels, two different approaches have been used to achieve the FHAs:

- **IS12 FHA:** it is a high-level functional safety assessment. A/C-level functions impacted by wing morphing system (see Sect. 3) with the relevant functional failures is the starting point of this analysis.
- **AS0x FHAs:** these analyses are low-level functional hazard assessments. The starting points are the device function failure modes, with the target at IS12-level Failure Conditions (FCs).

The most demanding aspect of this "dual-level approach" is to guarantee consistency between the previously mentioned analyses. The Failure Conditions identified at AS0x level should always be linked with a higher level entry found in the IS12 scenario analysis. For example, the criticality of a FC identified at AS0x level shall be lower or equal to the safety classification of the target FC at IS12 level. A complete mapping between the two levels is required to guarantee that every possible failure is taken into account. The main driver of this mapping activity is provided by the functional approach definition described in the previous section.

Only after the FHA's mapping phase conclusion, the SSAs can be performed starting from devices level. The IS12 FTA is obtained by the proper combination of

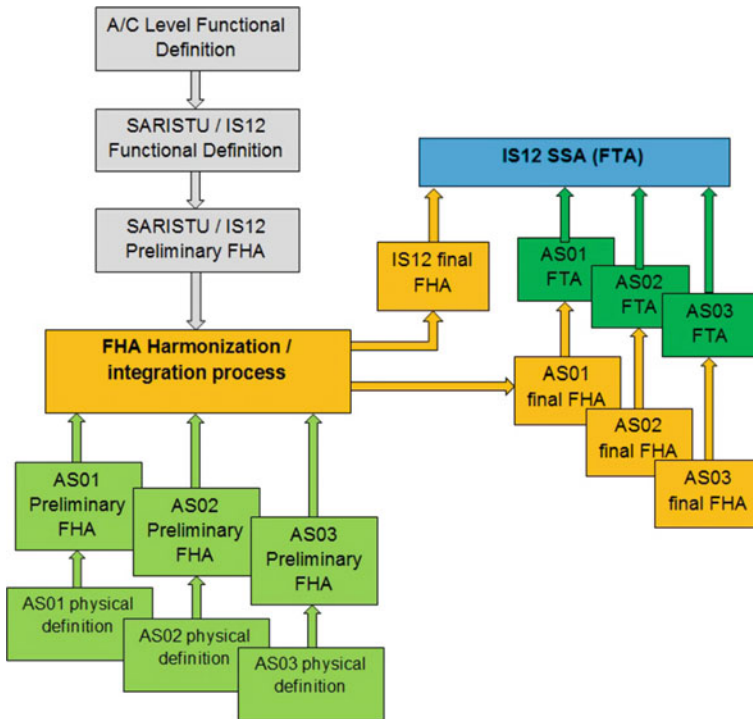


Fig. 8 “Dual-level” approach for SARISTU safety activities

the AS0x fault trees (FTs). This combination is based on the previously mentioned mapping. A flow diagram of the SARISTU safety process is shown in Fig. 8.

Failure scenario classification is always associated with the aircraft-level consequences in terms of pilot workload, safety margin, occupant comfort and health status. In addition, failure scenarios and conditions are associated with the proper flight phases. In the SARISTU safety analyses, only take-off, cruise (including climb and initial descent) and landing were considered. Ground flight phases are out of SARISTU scope.

There are some differences between Scenarios Application and wing integration-level FHAs. For each Scenario Application, a “total loss of function” can be easily identified (i.e. jamming, loss of actuator). At IS12 level, the same Failure Condition is a combination of AS0x-identified failures.

The wing shape optimization (mainly associated to drag minimization) is obtained by the simultaneous actuation of all SARISU devices. The total loss of this IS12 function (i.e. Failure Condition FC 2.2.5.1-01) was classified as MAJOR. The linked system Failure Conditions are as follows: AS01 FC5 “Reduced performances”—MAJ and AS03—FC2 “Jam of both tabs/electromechanic actuators”—MAJ. Both FCs are classified with the same severity and their safety classification is in accordance with the concerned IS12 FC. So the “Total loss of wing shape

optimization” is considered as the WATE (AS03) *OR* EADN (AS01) loss of function *OR* the loss of ATED (AS02) in conjunction with WATE or EADN (the ATED FC is AS02—FC01 “Loss of ATED control”—MIN). FC01 from ATED is combined with the other previously mentioned Application Scenario FCs because it has been estimated having a very minor impact on the drag and lift generation as an isolated failure.

Partial loss scenario can be split in two main cases at both safety analysis levels: symmetric partial loss (e.g. loss of performance) or asymmetric partial loss (in this case, “partial” is referring to the loss of wing shape optimization on one wing only). At IS12 level, asymmetric Failure Conditions are combined with proper external events or other system failures (single engine loss, strong crosswind at take-off or landing) to consider worst-case scenarios. Similar considerations are applicable in case of erroneous or inadvertent provision of SARISTU function.

The EADN is designed to be mainly used as “high-lift device” during take-off and landing. For this reason, at IS12 level, some Failure Conditions are also caused by this device only, associated with lift adaptation function. A clear example is the IS12 FC 2.2.13-01, which takes only into account the contribution of AS01 FC 2.1 “Inability to control aircraft during take-off (T/O) and the Landing phase (LND)”.

For structural load-related functions, the CS-25 regulations impose to consider by design the additional stresses caused by the failure of a load control device. In particular, CS-25.301 paragraph states “*For aeroplanes equipped with systems that affect structural performance, either directly or as a result of a failure or malfunction, the influence of these systems and their Failure Conditions must be taken into account*”. The consequence is that the structure will be able to withstand the additional load caused by a failed device without safety relevant damages by design. A physical discomfort for the passengers can be experienced at worst; this is why the safety classification of these events is always MINOR.

The main criticalities emerged from the Application Scenarios FHAs are mainly due to EADN and WATE devices. EADN will be used as a “high-lift” device during take-off and landing. During these flight phases, an erroneous position of morphing droop nose (due to the “loss” or “erroneous” EADN function provision) could cause an aircraft stall (symmetric or asymmetric) which can be unrecoverable if the flight level is too low (see AS01—FC 2.1 “Inability to control aircraft during T/O/LND” classified as CAT). In fact, in such a case, the pilots have a very short lapse of time to start a recovery action. The consequence is that a high functional integrity level is necessary to make this device airworthy. A FDAL A is then required for EADN (or a dual independent DAL B design is also accepted). No single failure shall lead to this Failure Condition.

For the WATE device, a CATASTROPHIC Failure Condition is identified in case of winglet trailing edge-forced oscillations or free float causing a possible flutter, identified as AS03—FC1 “destruction of whole wing”. The higher level consequence can be the aircraft loss. In addition, for this scenario, no single failure shall cause such a Failure Condition. A fail safe design is a requirement for this device. For example, to prevent surface free float, a dual load path is necessary for

the actuator connection, and an independent control/monitor architecture shall be implemented (dual-duplex actuator control unit).

The IS12 Analysis highlighted that SARISTU Failure Conditions can mainly cause passenger discomfort and an increase of pilot workload (conservatively classified as MAJOR assuming a significant increase of workload at worst). The main criticality emerged from this safety analysis is related to possible asymmetric configuration due to SARISTU failures in conjunction with external additional asymmetry effects (flight control system failures are excluded due to the low probability level expected considering the combination of SARISTU failures with flight control system failures). Two additional asymmetry circumstances have been considered: a single engine loss and strong crosswind at take-off or landing.

Asymmetric SARISTU configuration combined with a single engine loss (IS12 FC 2.2.7-02) has been classified HAZARDOUS (HAZ) since the reference A/C is designed with fuselage-mounted engines. This configuration causes a limited thrust asymmetry since both engines are very close to the A/C longitudinal centreline.

Asymmetric SARISTU configuration combined with strong crosswind at T/O or landing (IS12 FC 2.2.7-03, see Sect. 5 for details) has been classified CATASTROPHIC (CAT). Since it is not possible to evaluate the asymmetry level caused by this FC, a conservative approach has been used for the previously mentioned classification.

4.3 SARISTU Functional Hazard Assessment ***Harmonization and FTA Basis***

As already stated, the peculiarity of the SARISTU approach is that A/C-level functions and safety impact have been included in the IS12 Integration-level analysis, performed in parallel with AS0x devices level analyses. These latest analyses are linked with the Integration Scenario according to an iterative harmonization process, in order to achieve a consolidated FHA at both levels. Taking into account the multi-level functional link explained in Sect. 3, the main problem was how to highlight it in the FHA tables. A traceability table was built starting from IS12 FHA (see Tables 4 and 5).

Each row is a failure scenario identified at IS12 level, and three columns are dedicated to each device to identify the associated lower-level Failure Condition, with its reference and severity. In this way, it is possible to easily check the coherence of the safety classification and the completeness of the analysis. In addition, this table provides a basic structure for the IS12-level fault trees (see Sect. 4.3 for details). Safety requirements and means of compliance have been added into this table, as well.

4.4 System Safety Assessment—Fault Tree Analysis

This section reminds the basic principle of the fault tree technique used by SARISTU partners in their preliminary system safety assessment activity (PSSA). Fault tree analysis (FTA) was used to check that the qualitative and quantitative requirements associated to each Failure Condition and expressed in the FHAs have been met. FCs classified as NSE (NO SAFETY EFFECT) and MIN (MINOR) do no need to be modelled by a fault tree (FT), according to the CS25 book 2 (Means Of Compliance—Ref. [2]).

A detailed description of the FTA technique can be found in the appendix D of the “*Guidelines and methods for conducting the safety assessment process on civil airborne system and equipment*”—ARP 4761 (see Ref. [4]). A fault tree analysis (FTA) is a deductive failure analysis, which focuses on one particular undesired event (Failure Condition). A FTA is a top-down safety analysis technique that is applied as part of the PSSA to determine what single failures or combinations of failures at the lower levels (basic events) may cause or contribute to each Failure Condition. A fault tree analysis uses Boolean logic gates to show the relationship of failure effects to failure modes. A basic event is defined as an event which for one reason or another has not been further developed (the event does not need to be broken down to a finer level of detail in order to show that the system under analysis complies with applicable safety requirements). A basic event may be internal (system failure) or external (e.g. icing condition, fire) to the system under analysis and can be attributed to hardware failures/errors or software errors. Probability of individual failures is only assigned to the hardware (HW). The occurrence of software (SW) errors are probabilistic but not in the same sense as hardware failures. Unlike hardware failures, these probabilities cannot be qualified. No SW failures were thus considered in the FT built by the SARISTU scenario leaders.

The FT calculation produces the minimal cut sets (MCS), i.e. the shortest *logic And* combination of independent basic failures that lead to the Failure Condition. The *order* of the MCS is the number of elements found in the MCS. Failure Conditions that have been classified as CAT shall comply with the fail safe criteria. This means that no single failure shall lead to the occurrence of a CAT Failure Condition. Therefore, MCS of order equal to 1 are not acceptable for CAT Failure Conditions.

The hypotheses and common data used by the fault trees by the SARISTU partners are briefly described in this section.

One individual FT was built for each Failure Condition coming from the FHAs whose safety classification is equal or more than MAJOR. The FC is the top event of the fault tree as shown in the example depicted in Fig. 9. Its average probability of occurrence per flight hour (FH) is deduced from the quantification of all MCS generated by the calculation of the fault tree.

If a system FC is classified as MINOR at AS0x level, but contributes to a MAJOR or worst safety severity FC at IS12 level, then the FT was built at AS0x

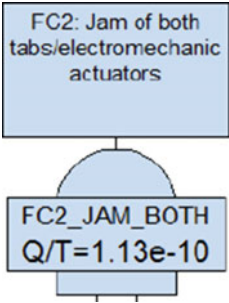


Fig. 9 Top event of a fault showing the title of the FC and its estimated probability

level in order to evaluate its contribution to the IS12 fault trees. An illustration of this specific case is given below. Figure 10 depicts a simplified FT at IS12 level. The top event is the IS12 Failure Condition FC 2.2.5.1-02 “Erroneous provision of wing shape optimization”, which was classified MAJ.

The FT from Fig. 10 shows that one contributor to the top event (IS12 Failure Condition ref. 2.2.5.1-02) is the Failure Conditions ref. FC08 from WATE system. FC08 has a MINOR effect, only. But since this system Failure Condition contributes to the occurrence of the IS12 Failure Condition at wing integration level, the AS03 scenario leader had to build a FT dedicated to FC08 despite the low level of safety. Notations used in the SARISTU fault trees are explained in Sect. 5.

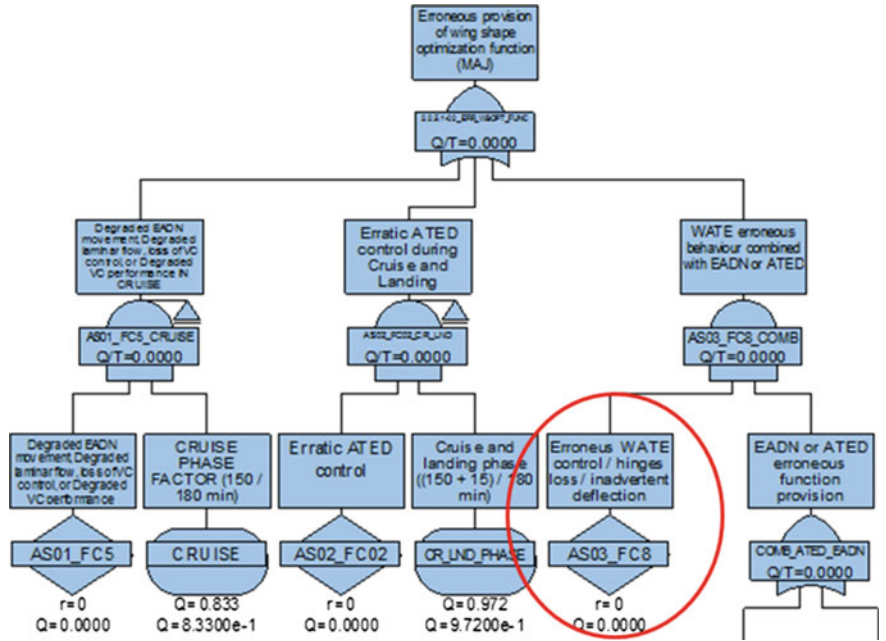


Fig. 10 System-level FC08 from WATE is classified as MIN but contributes to a MAJ IS12 FC

The traceability table reported in Sect. 4.3 provides the guidance for the FT's integration at IS12 level. The FCs at Application Scenario level are based on component-level failure modes. This level of detail is typical for a “bottom-up” approach. On the contrary, as per FHA case, The FTs at IS12 level are obtained with a “top-down” approach. At IS12 level, every FCs at AS0x is traced as “undeveloped” event. In this way, the higher level FTs can be easily obtained by a proper combination of lower level FCs, with the introduction of the required “exposure factors” or external events where necessary. A concrete example of this dual-level approach for the FTA is described in Sect. 5.

4.4.1 Assumptions—Principles

The following assumptions and principles were followed and applied by SARISTU partners in charge of the FTA.

External events in the FTA: The fault trees must consider the combination of system failures with external events (e.g. wind or icing condition) whenever relevant. The following table shows an example of probabilities for external events that are commonly used in FTA. These figures were used by the SARISTU scenario leaders (see Fig. 11).

4.4.2 Active Versus Hidden Failures—Time Parameters

Both active and hidden failures have been considered in the SARISTU fault trees. Active failures are failures that can be detected by the flight crew when they occur during the current flight. For active failures, a mean flight time, T_0 , must be used in the calculation of the FC. SARISTU partners agreed to use a mean flight time equal to 3 h (mission time used for an A330 aircraft) that has been considered as an appropriate value for SARISTU. However, for some specific scenarios, a proper “exposure” time can be used in case a Failure Condition is expected to occur only in a specific flight phase.

Hidden failures (named also latent/passive/dormant failures) are failures not detected by the flight crew or detected but not reported. Such failures shall be checked at a certain moment of the aircraft life, according to airworthiness

Fig. 11 Environmental conditions events and associated probabilities

ENVIRONMENTAL CONDITIONS EVENTS & ASSOCIATED PROBABILITIES

ENVIRONMENTAL CONDITION EVENT	PROBABILITY
Strong Head wind (> 25 kts)	8×10^{-3} (per cycle)
Strong Tail wind (> 10 kts)	8×10^{-3} (per cycle)
Strong Cross wind (> 18 kts)	1×10^{-2} (per cycle)
Icing conditions	1

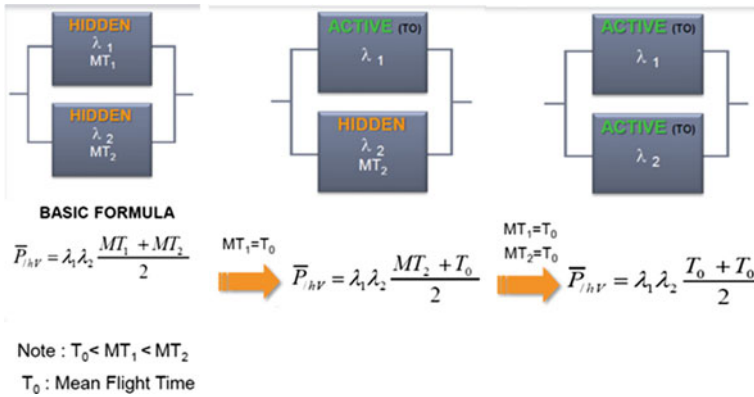


Fig. 12 Example of calculation of a dual system involving active and hidden failures

requirement during periodic inspections for maintenance purpose. Safety check intervals or maintenance time (MT) must be considered in the calculation of the FC involving hidden failures. The MT value is set based on the usual checks (periodic inspections) of the aircraft. The standard safety check intervals (A checks, B checks ...) have been considered in the quantification of the FTs.

In Scenario Application AS03 on WATE system, an interval of 8000 flight hours was considered between maintenance checks, i.e. disassembly and inspection of all hinges for detection and elimination of all dormant failures. For equipments that are never inspected, we use the aircraft lifetime. This value comes from “Fatigue Loads design criteria”. SARISTU partners agreed on a MT of “60,000 h” as a standard value but a calculation with a more conservative value of 87,600 h. This maintenance interval was used by the AS03 scenario leader for disassembly and inspection of WATE device that are only required every D-check.

The figure below shows a simple example of calculation for a simple redundant system highlighting the difference of formulae depending on the type of failures: two active failures, one active failure and hidden failure, and two hidden failures (Fig. 12).

4.4.3 On Safety Factor

The structural damage tolerance and loads are out of the PSSA scope. Such specific safety issues are addressed by structure specialists in separated documents. However what is requested is to identify the systems that may exert loads on structural parts when failures occur as explained in the CS25.303 section “Factor of safety”: “...Unless otherwise specified, a factor of safety of 1.5 must be applied to the prescribed limit load which are considered external loads on the structure” (Fig. 13).

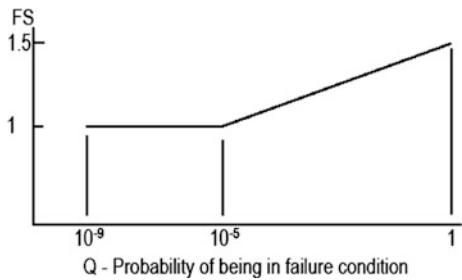


Fig. 13 Computation of the safety factor (FS)

AS03 scenario leader used this principle to quantify the structural damage of the WATE system. The Failure Condition FC5 “Degraded WATE performance” was classified MIN considering the safety repercussions on the occupants of the aircraft. However, the aircraft structure must be seized for jam in worst-case load position, in compliance to CS25.303. This is why, as a result of the FHA made on the WATE system required, the following safety requirement ref. REQ5 asked “*To check ultimate loads and safety factors of the whole aircraft structure for occurrence of failure and continuation of flight loads*”. A fault tree was thus generated and calculated to compute the ultimate loads for degraded WATE performance (see details in paper Ref. [7] titled “*Design, Manufacturing, and Testing of the Wingtip Active Trailing Edge*” from Wildschek and Storm).

5 Catastrophic Failure Condition: Example of Integrated Safety Analysis

A CATASTROPHIC Failure Condition at IS12 has been identified considering an asymmetric SARISTU devices configuration in combination with strong crosswind at T/O or landing.

This FC is labelled “FC 2.2.7-03—Partial loss of wing shape control capability (Asymmetric) combined with strong crosswind at take-off or landing”. This FC is summarized in Fig. 14. This figure allows the identification of the main “actors” of

ID Failure Mode	Title	AC Flight phase(s)	Safety requirement			FT req FT / R / OE	Failure Causes / Involved Subsys	TRACEABILITY				REQUIREMENTS / COMMENTS	REQUIREMENTS IMPLEMENTATION / DEMONSTRATION
			Severity	Rationale	Objective			WAGE	ATE	EAEN	External event or condition		
2.2.7-03 FC5 CATASTROPHIC CS25.303	Partial loss of wing shape control capability (Asymmetric) combined with strong crosswind at take off or landing	Take off and landing	CAT	Multiple cause on percentage stability Possible AC loss	AC 25.303	Y	AC 25.303 Loss of SARISTU wing shape control on one wing only (with asymmetric lateral balance) combined with strong crosswind (loss of WATE, strong crosswind, asymmetric down wing, AED) and/or loss of lateral control wing (AED) (Bad weather condition)	FC5	NAU	FC02	CAT	Strong crosswind at take off or landing REQ5: To check ultimate loads and safety factors of the whole aircraft structure for occurrence of failure and continuation of flight loads REQ6: A SARISTU wing shape optimization (see Fig. 14) must be able to generate control law variation. Lightning control system is required. A an asymmetric configuration, the SARISTU FC5 can be investigated. The automatically compare the asymmetry	FT design solution

Fig. 14 FC 2.2.7-03 extracted from traceability table

this Failure Condition: The AS02 FC labelled “*FC07—Partial loss of ATED (Asymmetric) combined with strong crosswind at landing*”, the AS03 FC labelled “*FC4—controllability degradation, asymmetric configuration due to one jammed WATE*”, and the external event “Strong Crosswind”. In addition, also the exposure factor is presented in this table: take-off and landing.

The system FCs (from WATE and ATED Application Scenarios) are reported as “undeveloped events” on the IS12 fault tree. These undeveloped events are depicted as diamonds by the FT tool. The details of these Failure Conditions are reported in the Application Scenario analyses. The undeveloped events probability have been extracted from Application Scenarios FTs.

Flight phases (e.g. landing) and external events (e.g. strong crosswind) are depicted by an elliptical shape in the FTA tool. In the FT reported in Fig. 15, the following “conditional events”¹ have been used:

- I. Landing-phase exposure time, labelled “*LND_PHASE*”. This phase is estimated to be about 15 min long over 180 min (the 3 flight hours used as reference flight time). The exposure factor is then $15/180 = 0.08333$. This exposure factor is applied on the ATED Failure Condition.
- II. Take-off- plus landing-phase exposure times, labelled “*TO_LND_PHASE*”. This exposure factor is based on the take-off duration estimation (2.5 min) plus the landing duration (15 min as before). The exposure factor is then $(2.5 + 15)/180 = 0.09722$.
- III. Strong crosswind external event, labelled “*WIND_TO_LND*”. The probability value is $1e-02$ *per cycle* as already reported in Fig. 11 depicted on previous section.

The two Application Scenario undeveloped FCs and the external event are connected by a logic *AND* gate, which means that both FCs and the strong crosswind shall simultaneously occur to cause the identified hazard. The main requirement coming from this hazard is that a symmetry check of SARISTU devices is required to reduce the probability of occurrence of this failure scenario. This requirement is comparable with classic aircraft secondary flight controls (e.g. FLAPS). This hazard does not necessitate demanding architectures to comply with required safety figure. In fact, the exposure factors and the FC’s combinations allow SARISTU system to comply with the top event requirement of $1e-9/FH$ also with Application Scenario figures with an order of magnitude of $1e-3/FH$.

¹Conditional event is a wording used with fault tree + tool.

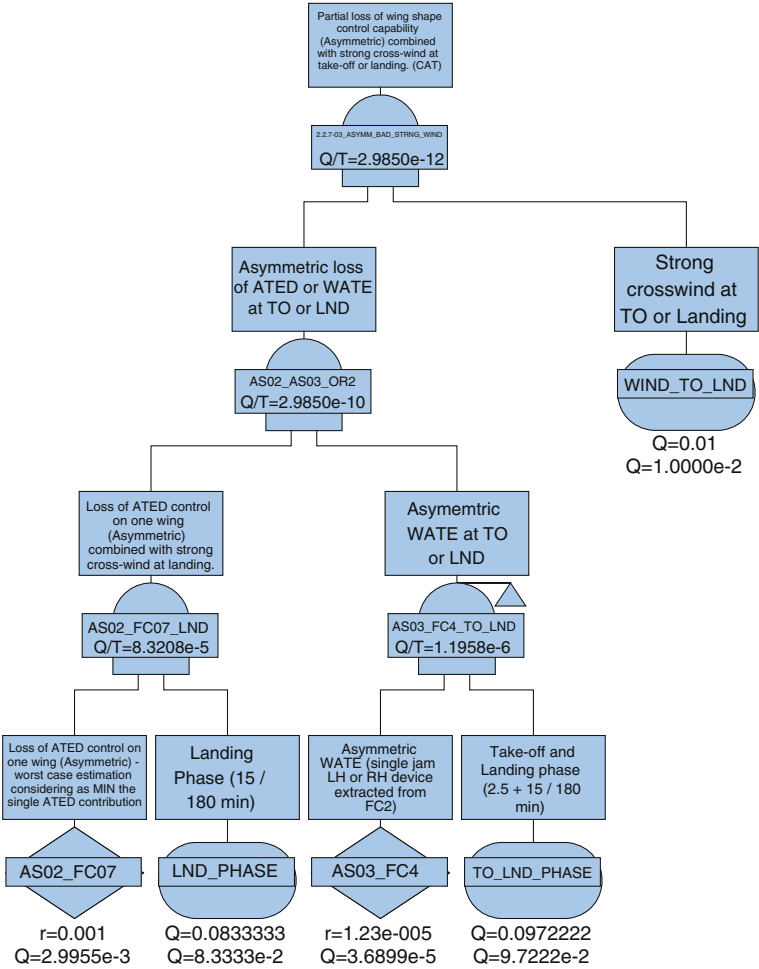


Fig. 15 IS12 fault tree for FC 2.2.7-03

6 Common Cause Analyses (PRA, ZSA, CMA)

In addition to the FHA and PSSA, other safety activities commonly performed in the aeronautical field like common causes analyses (CCA) were identified during the safety assessment of SARISTU. CCA consist of three different but complementary activities:

- A zonal safety analysis (ZSA) to ensure that equipment installation in the aircraft meets the safety requirements and minimize the potential common modes due to this installation. It contributes to the verification of the segregation requirement application from the FHA and PSSA.

- A particular risk analysis (PRA), consisting of systematic studies of all the external and intrinsic hazards such as fire, burst, lightning strike, bird strike and leaking fluids. whose repercussions largely exceed system design perimeter, having effects on structures, system installation, impacting multiple system at the same time and/or affecting different sections of the aircraft.
- A common mode analysis (CMA), which is a qualitative analytical assessment of all potential common causes that can affect a number of elements otherwise considered to be independent and which can lead to CATASTROPHIC Failure Conditions. The CMA contributes to the verification of independence criteria (fail safe criteria) used in the fault trees. In the frame of SARISTU safety assessment, a complete CMA activity was not performed. For the wind tunnel demonstration, there was no real need to do it but absolutely required for a real implementation. However, CATASTROPHIC Failure Conditions expressed in the FHAs were assigned a fail safe requirement (“*no single failure shall lead to a CAT FC*” as stated in the CS25 book 2—Means Of Compliance, Ref. [2]).

At this stage of SARISTU R&T project, the CCA activity has mainly consisted in providing a list of PRA requirements. Alenia Aermacchi as safety leader at system integration level (IS12) involved specialists on PRA to produce a first list of applicable PRA requirements relevant for SARISTU with the support of Airbus based on the several standard documents (e.g. EASA Regulation Ref. [1], in particular CS25.581 on lightning Protection, CS25.631 on Bird strike damage, CS25.867 on Fire protection and CS25.899 on Electric bonding and protection against static electricity, DO-160 for EMI, HIRF applicable requirements Ref. [5]).

Most of the particular risk analyses (PRAs) are strictly related to the whole aircraft design. For a demonstrator, it has no sense to perform such type of analysis. Nevertheless, it is important to consider, for example, that the leading edge design has implemented in SARISTU should be able to withstand a bird impact. Moreover, all the subsystems shall be designed considering the currently available norms regarding the electromagnetic compatibility (EMC), lightning strike. PRAs that are of interest for SARISTU are the following ones:

- Lighting strike protection
- Bird strike/FOD behaviour due to leading edge requirements
- Electromagnetic hazards (lightning strike, EMI, HIRF)
- Flailing shaft (slats and flaps)
- Wiring hazard (failure in wire bundle).

The following picture shows foreseen protections against PRA risks coming from AS01 concept. Particular risks were considered in the SARISTU design (AS01) as depicted in Fig. 16.

Design requirements to protect against aforementioned particular risks were expressed in Sect. 5.3 related to design constraints of SARISTU D123.1 deliverable titled “Wing Demonstrator design principles” Ref. [8].

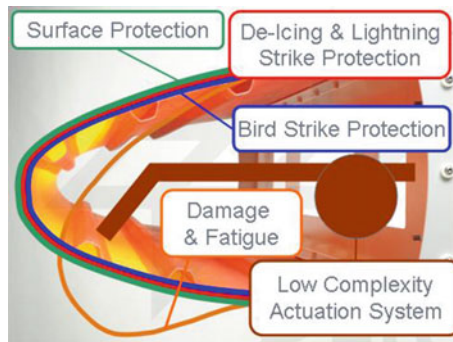


Fig. 16 Protections against PRA risks

ZSA is not required for the SARISTU demonstrator. This is why in the frame of SARISTU project there is no need to verify whether the installed equipment is subjected to these particular risks. This will be done in a real implementation.

7 Conclusion

Even if SARISTU project does not require a safety analysis to perform wind tunnel model validation, this activity was performed in order to provide a clear status on the maturity of the concept regarding safety considerations. Both wing integration- and Application Scenario-level FHAs were performed using standard techniques. However, the approach was tailored for SARISTU project: the morphing wing system analysis was performed starting from a generic aircraft-level functional breakdown and then becoming the target for the Application Scenario safety analyses.

Several lessons have been learnt from the safety activity performed on SARISTU all along the duration of the project. First of all, it is worth reminding that an appropriate methodology was elaborated at the beginning of the project to address the safety of SARITU concept in an original and very efficient way. Alenia Aermacchi as leading the wing integration activity focused on the A/C-level safety assessment. Each scenario leader concentrated his effort on assessing the safety of their own systems. An iterative harmonization process with a simple but effective traceability form was used to make the safety analyses (both FHAs and FTAs) coherent.

The safety methodology applied in the frame of SARISTU can be easily used in a “real-life” application, making easy to exchange information between the “integration-level” industry and the subsystems suppliers. This methodology shows some advantages also for the detailed quantitative analysis: the lower level FTs can be developed by the subsystem owner, while the Integration Scenario leader can develop high-level FTs, verifying in a very fast and effective way the compliance

with the safety requirements. The safety approach applied in the frame of SARISTU can also be followed for a deeper analysis level, not accounted in SARISTU project.

The support of Airbus in all safety activities, as a major civil aircraft manufacturer, provided a real added-value to the project. Thanks to the organization of safety and airworthiness sessions the first year of the project, Airbus made sure that all contributors had the same level of knowledge on safety; this support from Airbus enabled them to perform the expected safety activity in a well-matched way. Several workshops were managed by Airbus in order to coordinate the safety activities and assure that the SARISTU partners progressed well on their own safety tasks while exchanging their results with the other partners, especially Alenia Aermacchi having the wing integration leadership. Regular technical and progress meetings were organized between Airbus and Alenia Aermacchi in order to reinforce the effectiveness of the safety management of SARISTU. Even if SARISTU is an R&T project that does not require the same level of rigor as an industrial product, all the safety activities were performed in compliance with the airworthiness regulations.

The results of the wind tunnel tests will probably impact some safety feedback like, for example, the pilot workload assumptions made during the FHAs. Lastly, the safety methodology has shown that a limited and optimized effort put on the safety assessment all along the life of the project permitted to provide good, trusted and reusable results. In the near future if such a new wing integration concept is implemented on a new generation of aircraft or on existing aircraft, the safety results from SARISTU can be partly reused.

Acknowledgments The research leading to these results has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under Grant Agreement No 284562.

References

Standard regulations and practices

1. EASA CS-25 (2014) Book 1, European Aviation Safety Agency—Certification specifications for large aeroplanes CS-25 amendment 15, 21 July 2014
2. EASA CS-25 (2014) Book 2, European Aviation Safety Agency—Acceptable means of compliance for large aeroplanes CS-25 amendment 15, 21 July 2014
3. SAE ARP 4754a (2010) US SAE international, guidelines for development of civil aircraft and systems, Revised Dec 2010
4. SAE ARP 4761 (1996) US SAE international, guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, Dec 1996
5. RTCA DO-160, Environmental conditions and test procedures for airborne electronic/electrical equipment and instruments from EUROCAE

SARISTU project documents

6. Baldassin E, Di Gifico M, Gemma R, Carossa GM, Russo S, Ricci S, De Gaspari A, Peter F. Deliverable A_DEU_121_1_R2, Reference baseline wing and morphing wing aeromechanical requirements
7. Wildschek A, Storm S. SARISTU AS03 Final Paper, Design, manufacturing, and testing of the wingtip active trailing edge
8. Apicella A, Russo S, Ricciardelli C. Deliverable A_DEU_ D123_1_R1, Wing demonstrator design principles

Other documents/papers

9. Working group document, Framework for the application of system engineering in the commercial aircraft domain

Smart Intelligent Aircraft Structures (SARISTU)
Proceedings of the Final Project Conference
Wölcken, P.C.; Papadopoulos, M. (Eds.)
2016, XXVIII, 1039 p. 865 illus., 774 illus. in color.,
Hardcover
ISBN: 978-3-319-22412-1