FIRST APPLICATION AND FEEDBACK ON PRELIMINARY AIRCRAFT SAFETY ASSESSMENT

Stephane DEPORT & Stephane BAILLY
Airbus Helicopters
Aéroport Marseille Provence 13700 Marignane
France

1 ABSTRACT

The X4 is the future Airbus Helicopters modern rotorcraft. It will embed the most modern technologies, including Integrated Modular Avionic (IMA).
This creates interdependencies between systems, as functions are no longer supported by a single system. This was already the case for Airbus Helicopters' previous development, and the need for an efficient methodology appears obvious with the growth in complexity of X4.
Therefore, the work in progress in the frame of ARP4761a/ED135a appears to be an opportunity to improve the process. Airbus Helicopters see foremost in the new activity of Preliminary Aircraft Safety Assessment a powerful way to enhance the management of helicopter systems interdependencies.
In the frame of its new medium class helicopter certification, Airbus Helicopters will perform this new activity. In spite of the fact that the development of ARP4761a/ED135a is still in progress, Airbus Helicopters decided to apply this methodology believing that safety benefit can be found.
By performing a PASA and allocating safety objectives to each system safety analysis, interdependencies are no longer a risk but are anticipated and under control. The functional interdependency diagrams capitalize on knowledge of system functionality. As an umbrella analysis, the PASA process ensures higher consistency between systems safety analysis throughout the helicopter development.
The PASA is an iterative process. The PASA should start early in the development. Nevertheless, the proposed helicopter architectures shall have sufficient maturity to reduce iterations. By contrast, starting the analysis late will decrease PASA benefits.
PASA will be re-applied on future developments, it has been identified that appropriate tools can help to save time and improve efficiency.

2 ACRONYMES

Acronyms	Signification
CAT	CATASTROPHIC according to CS29-§1309 risk classification
CCA	Common Cause analysis
CMA	Common Mode analysis
Coffe	Combined Functional Failure Effects Analysis
DF	Dependent Failure
FC	Failure Condition
FHA	Functional Hazard Assessment
HAZ	HAZARDOUS according to CS29-§1309 risk classification
H/C	Helicopter
IMA	Integrated Modular Avionic
IR	Independence requirement
MAJ	MAJOR according to CS29-§1309 risk classification
PASA	Preliminary Aircraft Safety Assessment
PSSA	Preliminary System Safety Assessment
REQ	Requirement

3 PASA MAIN OBJECTIVES

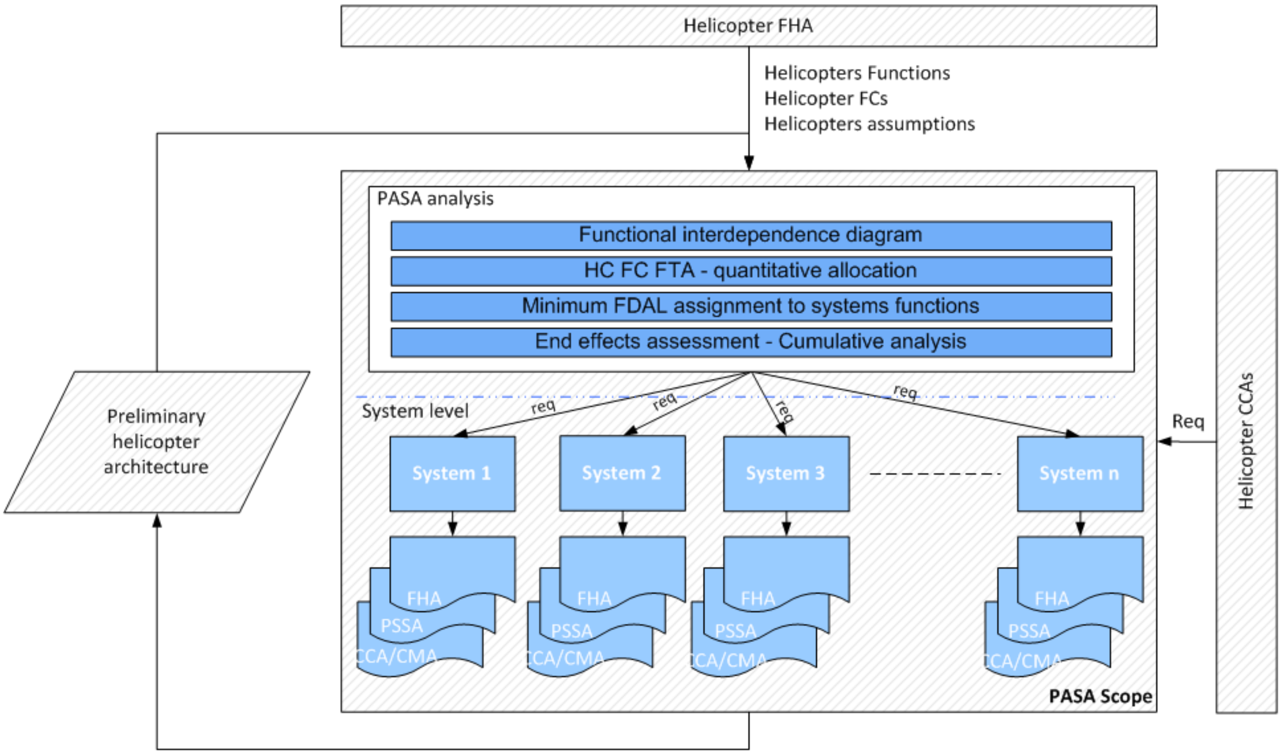
The complex integration of aircraft systems creates additional failure combinations at helicopter level that might otherwise not be present when helicopter functions are implemented by stand-alone or federated systems.

For example, helicopter digital networks and data multiplexing establish new sources of common mode failures. Many signals and data are shared extensively through various systems creating upon failures complex cumulative effects at helicopter level.

The PASA top down approach is particularly important in order not to miss system interdependencies with potential critical effects in case of failure, whether induced by common resources, by helicopter architecture choices, external events or shared signals and information.

The PASA enhances the identification and the traceability of system interdependencies by allocating helicopter safety requirements to each system.

4 AIRBUS HELICOPTERS METHODOLOGY



Helicopter FHA
Helicopters Functions
Helicopter FCs
Helicopters assumptions
PASA analysis
Functional interdependence diagram
HC FC FTA - quantitative allocation
Minimum FDAL assignment to systems functions
End effects assessment - Cumulative analysis
Preliminary helicopter architecture
System level
req
req
req
req
Req
Helicopter CCAs
System 1
System 2
System 3
System n
FHA
PSSA
CCA/CMA
PASA Scope

Figure 1: Preliminary Aircraft Safety Assessment scope

The PASA begins early in development process, immediately after establishing the list of Helicopter failure conditions in the H/C Functional Hazard Assessment. In order to manage this challenge successfully, the PASA conducted by Airbus Helicopters is drawn up through four main steps:

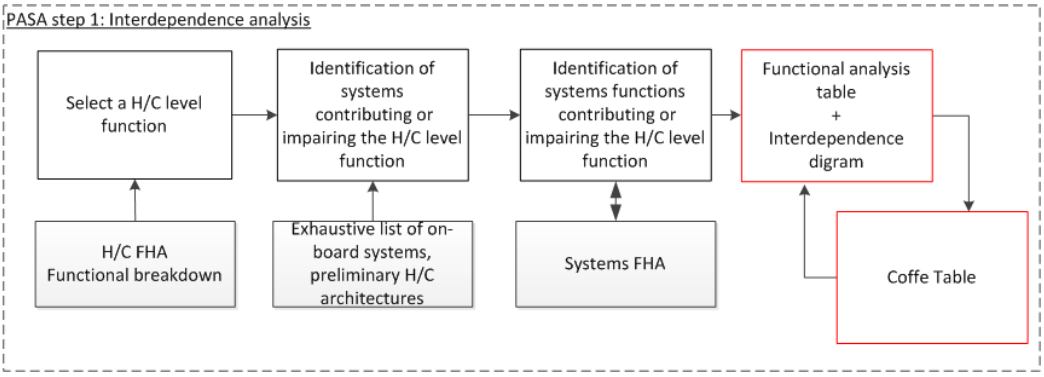
1) The first step consists of identifying the relationships between systems and their functions that contribute or may impair the aircraft-level functions through interdependence diagrams.
2) The objective of the PASA's second step is to allocate responsibilities regarding the Helicopter level Failure Conditions to be demonstrated within the relevant System Safety Assessment. A system is selected to support the demonstration for each H/C level Failure Condition, collecting contributions from other systems. A fault tree model based on the step 1 data outputs is built for each H/C Failure Condition in order to highlight system contributions, logics and interactions. Quantitative allocation is given to each system contributor so as to achieve H/C level's requirements.
3) The third step of the PASA defines the minimum Function Development Assurance Level (FDAL) required for system functions and independence requirements based on FDAL reduction.

4) In the last PASA step, a cumulative analysis after failure is performed for shared transversal signal/data such as main rotor speed, collective position, weight on wheel, etc., or common resources such as hydraulic, electrical generation, etc., to address the whole effect at H/C level and ensure that appropriate design or safety nets are provided to cope with the event, failure or fault. Additionally, operational situation upon adverse operating conditions is studied to ensure that the crew could land safely at a suitable site.

The PASA conducted by Airbus Helicopters is a continuous iterative process, starting from a top level of preliminary aircraft architecture down to a detailed analysis at system level.

4.1 PASA first step: interdependence analysis

The first step defines a clear scope for each aircraft-level function and describes the aircraft architectures in order to understand how systems work together to perform the helicopter functions. Crew awareness or environmental conditions are considered with the most severe plausible effects in this analysis.


PASA step 1: Interdependence analysis

Select a H/C level function

Identification of systems contributing or impairing the H/C level function

Identification of systems functions contributing or impairing the H/C level function

Functional analysis table + Interdependence digram

H/C FHA Functional breakdown

Exhaustive list of on-board systems, preliminary H/C architectures

Systems FHA

Coffe Table

Figure 2: Process for interdependence analysis

4.1.1 Functional analysis table

Hereafter is shown one of the key outputs of the first step of the PASA. The function analysis table manages cross links between helicopter and system functions.

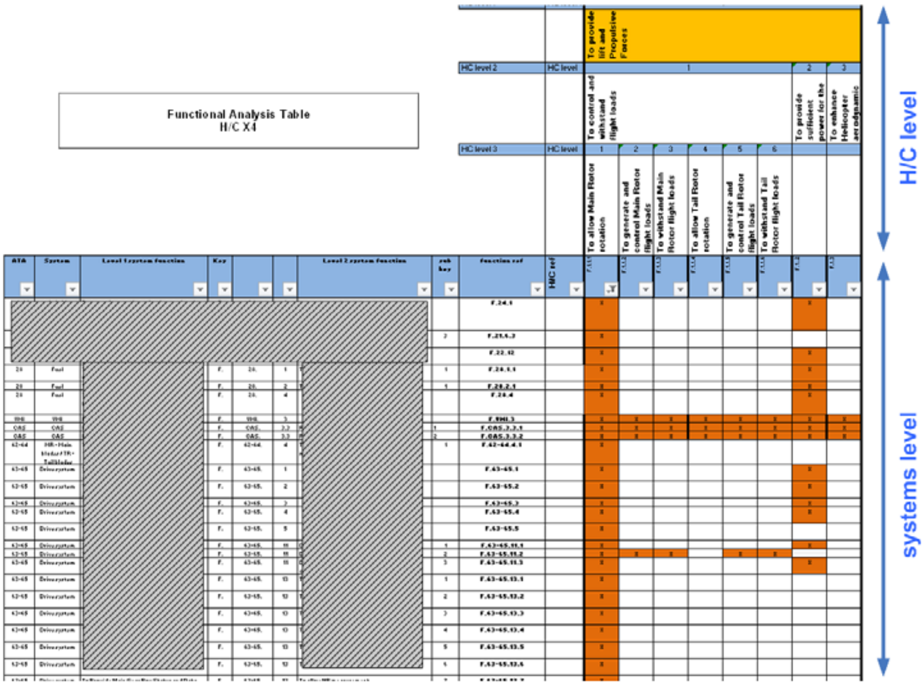

Functional Analysis Table
H/C X4
To provide lift and Propulsive Forces
HC level 2
HC level 3
To control and withstand flight loads
To provide sufficient power for the Helicopter
To enhance aerodynamic
To allow Main Rotor rotation
To generate and control Main Rotor flight loads
To withstand Main Rotor flight loads
To allow Tail Rotor rotation
To generate and control Tail Rotor flight loads
To withstand Tail Rotor flight loads
ATA
System
Level 1 system function
Key
Level 2 system function
sub key
Function ref
H/C ref
H/C level
systems level

Figure 3: Functional analysis table extracted from PASA

4.1.2 *Interdependence functional diagram*

Hereafter is provided an example of the mapping that could have been performed during the independence analysis:

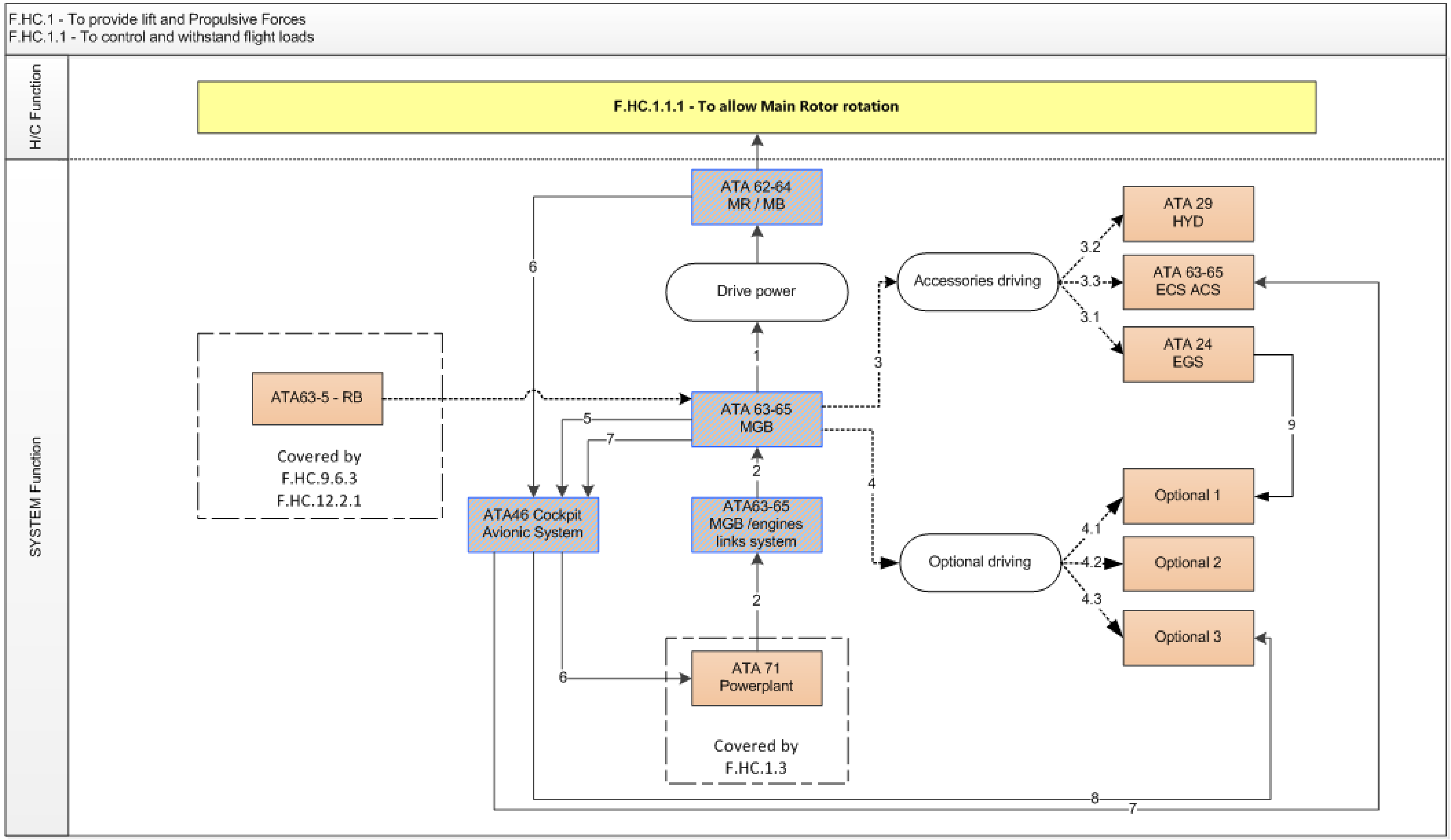
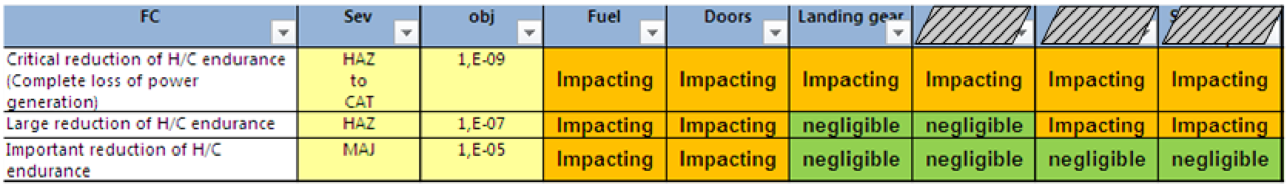


Figure 4: Interdependence analysis for Helicopter function F.HC.1.1.1

Note: The function consists in the transmission of the mechanical power (speed and torque) from the outputs of the power generation sources to the Main Rotor through the drive systems allowing the main rotor rotation at a commanded rotor speed. This function also provides to the main rotor a free rotation capability to ensure auto rotation flight phase. Additionally, a part of the power is used to drive accessories and optional devices.

4.1.3 *“Combined Functional Failure Effects Analysis”*

Despite the “coffe” as described in the future ARP4761a/ED135a is not being an exhaustive process, it has been used sparingly for specific failure conditions to assess the influence of different systems in H/C failure condition and address independence requirements. The failure and the combined failures of each system function and their impact on a given helicopter failure condition are determined in this analysis. An example is provided below:



FC	Sev	obj	Fuel	Doors	Landing gear	▨	▨	S▨
Critical reduction of H/C endurance (Complete loss of power generation)	HAZ to CAT	1,E-09	Impacting	Impacting	Impacting	Impacting	Impacting	Impacting
Large reduction of H/C endurance	HAZ	1,E-07	Impacting	Impacting	negligible	negligible	Impacting	Impacting
Important reduction of H/C endurance	MAJ	1,E-05	Impacting	Impacting	negligible	negligible	negligible	negligible

Figure 5: “coffe table”

4.2 PASA second step: quantitative objective allocation to system

The main objective of the second step of PASA is to build a fault tree analysis for each HC failure condition allocating a probability to each System functional failure:

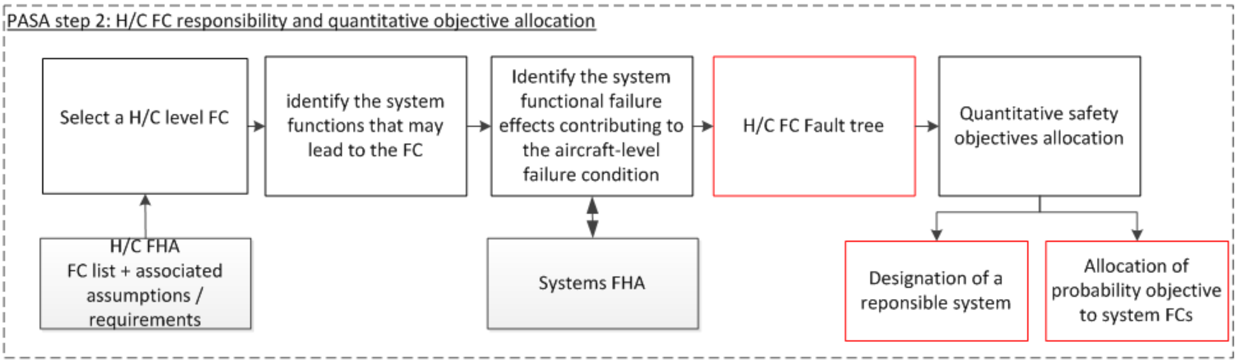

PASA step 2: H/C FC responsibility and quantitative objective allocation
Select a H/C level FC
identify the system functions that may lead to the FC
Identify the system functional failure effects contributing to the aircraft-level failure condition
H/C FC Fault tree
Quantitative safety objectives allocation
H/C FHA FC list + associated assumptions / requirements
Systems FHA
Designation of a reponsible system
Allocation of probability objective to system FCs

Figure 6: Process for H/C FC evaluation - H/C FCs contribution / responsibility and quantitative requirements

4.2.1 *H/C FTA*

A fault tree model is built for each helicopter failure condition. The basic logic and event symbols used in the FaultTree+ tool are detailed below:

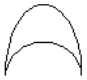
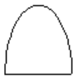
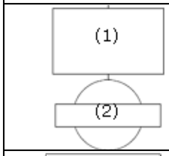
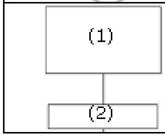
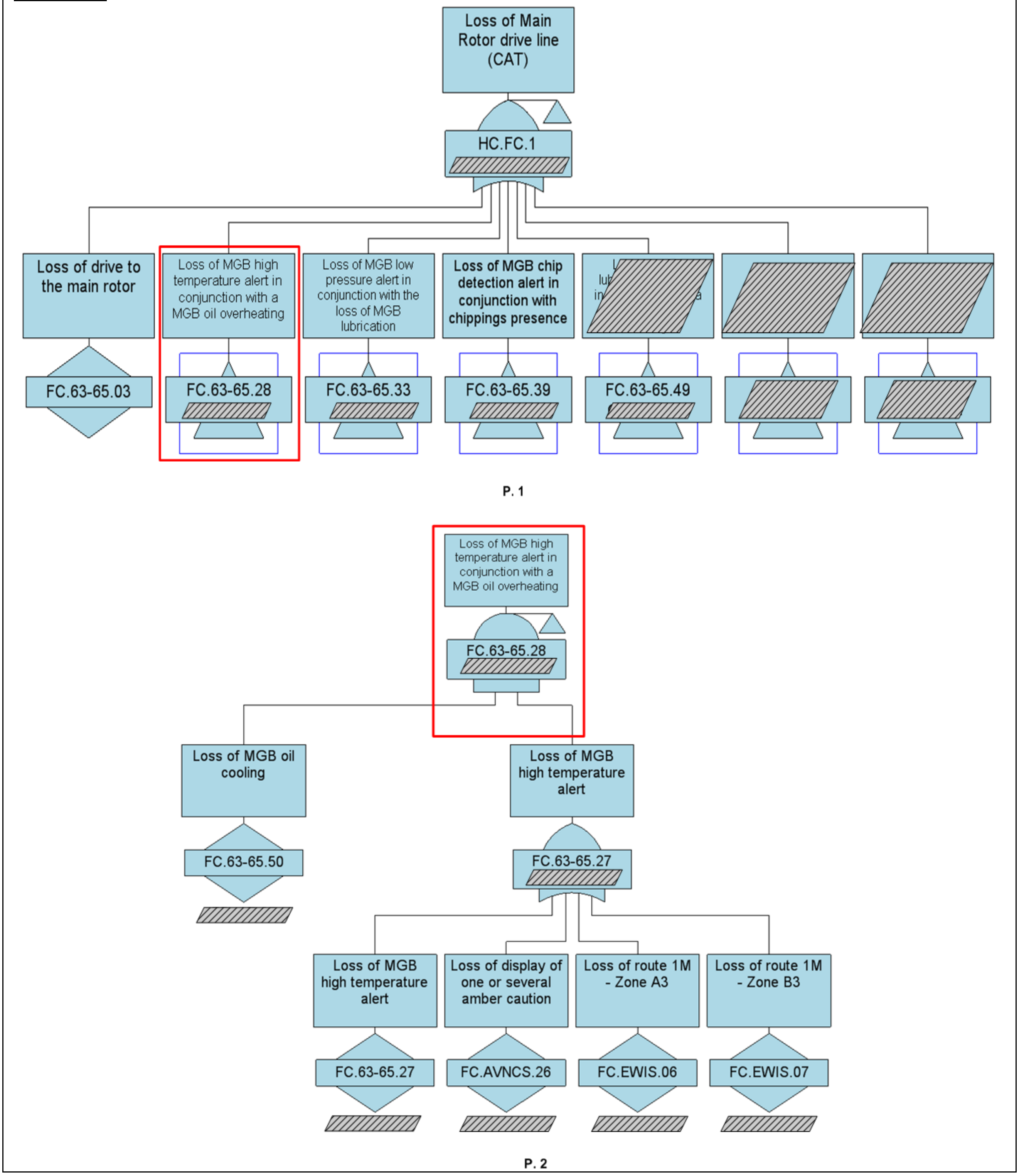
	**OR gate**: Boolean logic gate – output event occurs if any one of the input events occurs
	**AND gate**: Boolean logic gate – output event occurs if all input events occur together
	**EVENT box**: represents system FCs (1) Title of the FC (2) Reference of the FC
	**TOP EVENT box**: represents H/C FCs, (1) Title of the FC (2) Reference of the FC

Table 1: Supporting material for fault tree building

FAILURE CONDITION SUPPORTING MATERIAL				
Reference :	Title :	**Loss of Main Rotor drive line**	Class. :	Responsible:
FC.HC.1			**CAT**	**Drive system**

Fault tree:

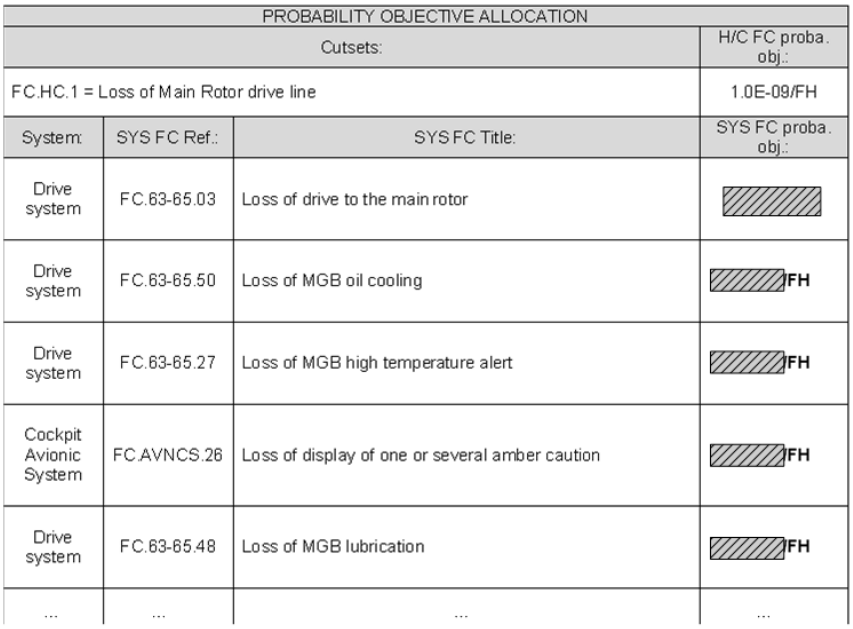


Loss of Main Rotor drive line (CAT)
HC.FC.1
Loss of drive to the main rotor
FC.63-65.03
Loss of MGB high temperature alert in conjunction with a MGB oil overheating
FC.63-65.28
Loss of MGB low pressure alert in conjunction with the loss of MGB lubrication
FC.63-65.33
Loss of MGB chip detection alert in conjunction with chippings presence
FC.63-65.39
FC.63-65.49
P. 1
Loss of MGB high temperature alert in conjunction with a MGB oil overheating
FC.63-65.28
Loss of MGB oil cooling
FC.63-65.50
Loss of MGB high temperature alert
FC.63-65.27
Loss of MGB high temperature alert
FC.63-65.27
Loss of display of one or several amber caution
FC.AVNCS.26
Loss of route 1M - Zone A3
FC.EWIS.06
Loss of route 1M - Zone B3
FC.EWIS.07
P. 2

Figure 7: “FC.HC.1 FTA”

4.2.2 *Probability objective allocation*

Compliance with quantitative requirements for H/C level objectives is performed by allocating probability to each system FC and checking through computation of the fault tree that the objective may be achieved.
It is not necessary to divide equally the quantitative contributions among the multiple system FCs involved in the H/C FC. Some objectives could be sampled by taking into account Airbus Helicopters experience on previous programs, industrial objectives or industrial constraints.



PROBABILITY OBJECTIVE ALLOCATION			
Cutsets:			H/C FC proba. obj.:
FC.HC.1 = Loss of Main Rotor drive line			1.0E-09/FH
System:	SYS FC Ref.:	SYS FC Title:	SYS FC proba. obj.:
Drive system	FC.63-65.03	Loss of drive to the main rotor	[redacted]
Drive system	FC.63-65.50	Loss of MGB oil cooling	[redacted]FH
Drive system	FC.63-65.27	Loss of MGB high temperature alert	[redacted]FH
Cockpit Avionic System	FC.AVNCS.26	Loss of display of one or several amber caution	[redacted]FH
Drive system	FC.63-65.48	Loss of MGB lubrication	[redacted]FH
...	...	...	...

Figure 8: Example of probability allocation synthesis

4.2.3 *H/C FC responsibility allocation*

For each H/C level FC, a system is designated to ensure the H/C level assessment taking into account possible contributions from other systems. This is done pending the importance of their contributions in the function:

- Mono-system Failure Condition: the responsibility of H/C level Failure Condition assessment is given to the concerned system.

- Multi-system failure conditions (associated in **AND/OR**): this situation arises when the contribution of several systems is involved to create the Failure Condition (AND/OR association). For this case of H/C level Failure Condition, the responsibility of H/C level Failure Condition assessment is given to one of the involved systems only based on criteria such as:

    - Obviously larger quantitative contributor
    - System directly linked to the FC (other system contributors have an indirect effect on the H/C level, the effect is seen through the responsible system)
    - etc

The Responsible System takes overall responsibility for the H/C level Failure Condition; including contribution from other systems, therefore this responsibility includes all necessary link/coordination with the other contributing. The role of the **Contributors Systems** is to demonstrate compliance with any safety requirements received from the Responsible System relevant to the given Failure Condition.

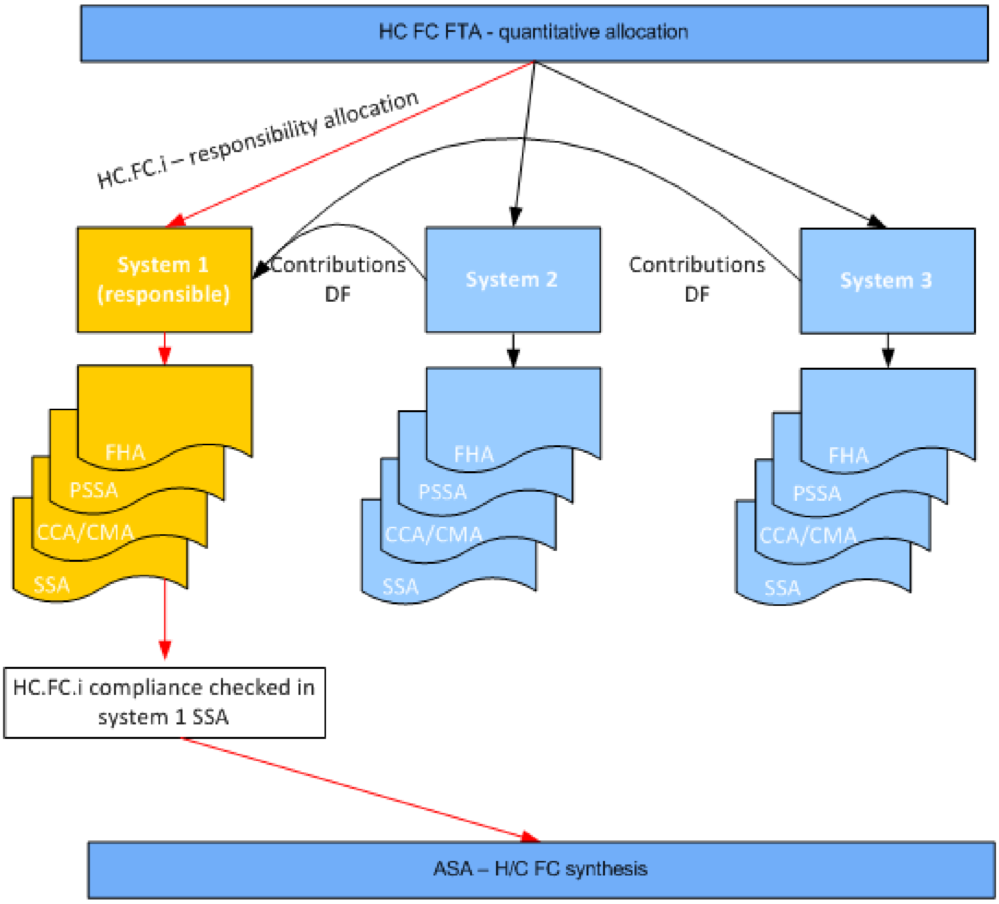


Figure 9: Responsibility allocation process

4.3 PASA third step: Minimum FDAL required and intersystem independence principles allocation

FDAL reduction according to rules defined by ARP4754a/ED79a is possible at H/C level. For such cases, the objective of the third step of PASA is to define the Minimum FDAL required by system functions and associated independence requirements.

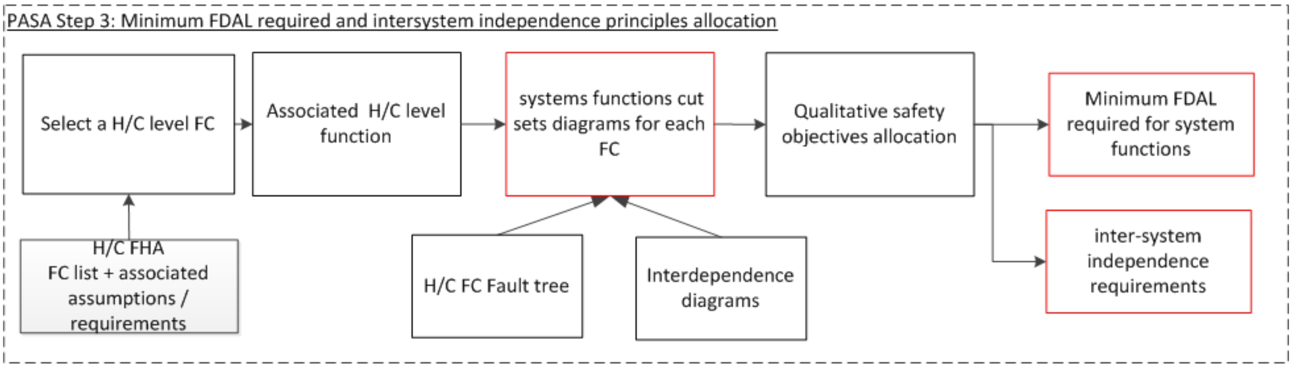
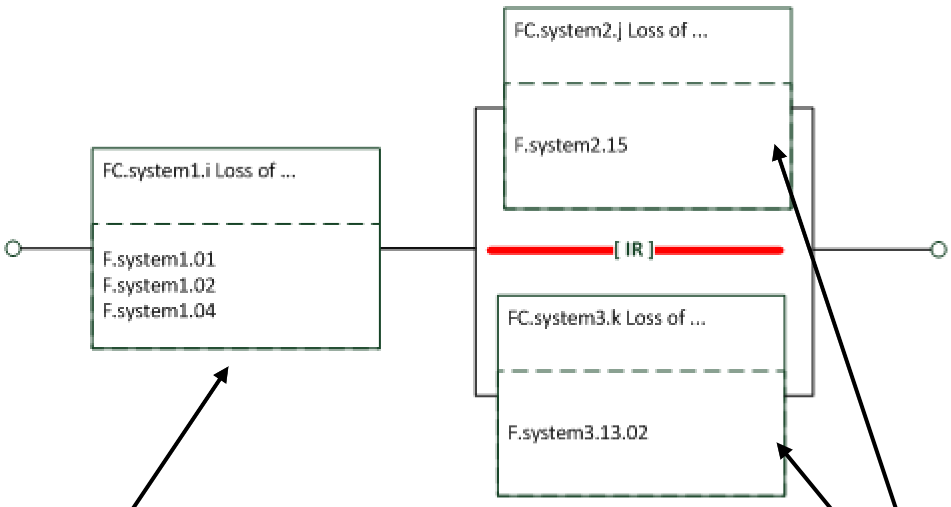

PASA Step 3: Minimum FDAL required and intersystem independence principles allocation
Select a H/C level FC
Associated H/C level function
systems functions cut sets diagrams for each FC
Qualitative safety objectives allocation
Minimum FDAL required for system functions
inter-system independence requirements
H/C FHA FC list + associated assumptions / requirements
H/C FC Fault tree
Interdependence diagrams

Figure 10: Quantitative requirements allocation

The FDAL is allocated to a system function taking into account the severity of the helicopter failure conditions and contribution of other functions, in line with ARP4754a FDAL allocation rules.

The following chart logic is used in cut sets diagrams:

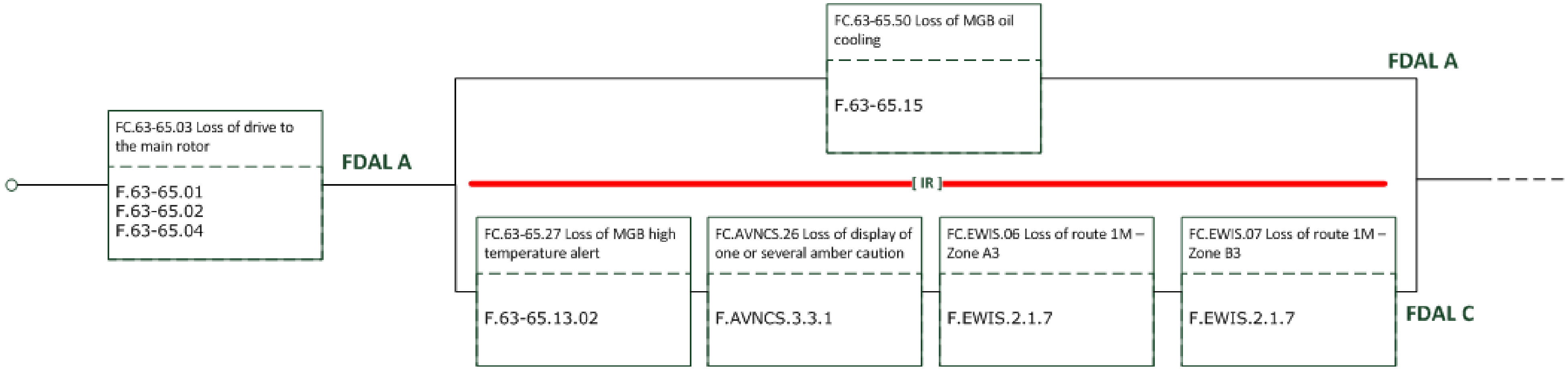
BLOCK DIAGRAM SUPPORTING MATERIAL				
Reference: **FC.HC.xx**	Title:	**Loss of .....**	Classification:	**CAT**
H/C fct F.HC.		**To provide....**	FDAL required:	**A**
Block diagram: 				
Comment(s):				

System 1 failure condition “i” leads to the H/C FC as a single driver. System functions FDAL supporting this FC “i” shall be equal to the FDAL level required at H/C level

System 2 failure condition “j” **AND** System 3 failure condition “k” lead in combination to the H/C FC.
FDAL levels required for System functions supporting FC “j” and “k” will be allocated following ARP4754 A / ED79A.

Figure 11: chart of Cut-sets diagram

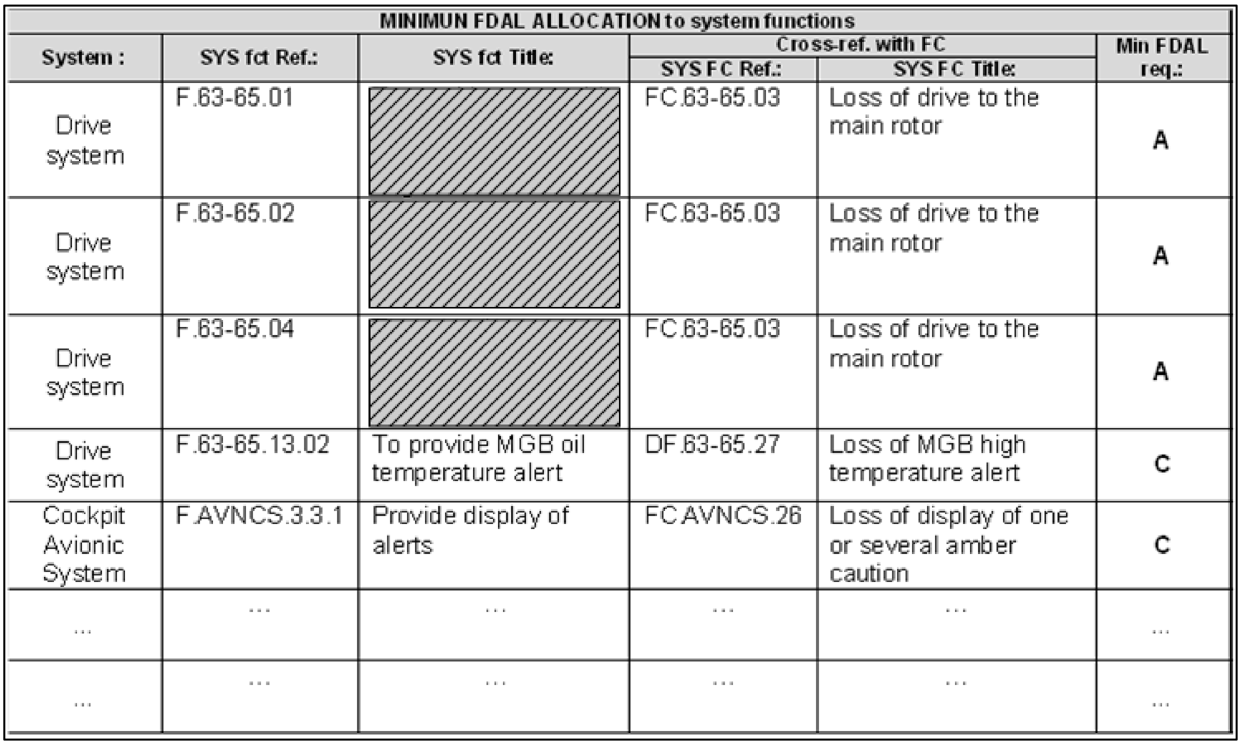
When a FDAL reduction has been used, an “Independence requirement” is captured. No more FDAL reduction is allowed at system level.
An example of FDAL allocation to system function is provided on the next page.

CUT SETS BLOCK DIAGRAM SUPPORTING MATERIAL			
Reference: **H/C.FC.1**	Title: **Loss of Main Rotor drive line**	Classification:	**CAT**
H/C fct **F.HC.1.1.1**:	**To allow Main Rotor rotation**	FDAL required:	**A**
Block diagram:: 			

FC.63-65.03 Loss of drive to the main rotor
F.63-65.01
F.63-65.02
F.63-65.04
FDAL A
FC.63-65.50 Loss of MGB oil cooling
F.63-65.15
FDAL A
[IR]
FC.63-65.27 Loss of MGB high temperature alert
F.63-65.13.02
FC.AVNCS.26 Loss of display of one or several amber caution
F.AVNCS.3.3.1
FC.EWIS.06 Loss of route 1M – Zone A3
F.EWIS.2.1.7
FC.EWIS.07 Loss of route 1M – Zone B3
F.EWIS.2.1.7
FDAL C

Figure 12: Example of Cut-sets diagram

Hereafter is presented an extract of the outputs issue from the previous diagram. The FDAL required for each system function which has an influence on the studied H/C level FC is given:



MINIMUN FDAL ALLOCATION to system functions					
System :	SYS fct Ref.:	SYS fct Title:	Cross-ref. with FC		Min FDAL req.:
			SYS FC Ref.:	SYS FC Title:	
Drive system	F.63-65.01	[redacted]	FC.63-65.03	Loss of drive to the main rotor	A
Drive system	F.63-65.02	[redacted]	FC.63-65.03	Loss of drive to the main rotor	A
Drive system	F.63-65.04	[redacted]	FC.63-65.03	Loss of drive to the main rotor	A
Drive system	F.63-65.13.02	To provide MGB oil temperature alert	DF.63-65.27	Loss of MGB high temperature alert	C
Cockpit Avionic System	F.AVNCS.3.3.1	Provide display of alerts	FC.AVNCS.26	Loss of display of one or several amber caution	C
...	...	...	...	...	...
...	...	...	...	...	...

Table 2: FDAL synthesis table

Resulting from FDAL reduction, independence is provided in the following table:

INTER SYSTEMS INDEPENDENCE PRINCIPLE(S) ALLOCATION										
ref	Req	SYS fct Ref.:	SYS fct Title:		System :		SYS fct Ref.:	SYS fct Title:		System :
IR1	*No common mode shall lead to*	FC.AVNCS.26	Loss of display of one or several amber caution	*by*	CAS	*and*	FC.63-65.50	Loss of MGB oil cooling	*by*	MGB
IR2	*No common mode shall lead to*	FC.63-65.27	Loss of MGB high temperature alert	*by*	MGB	*and*	FC.63-65.50	Loss of MGB oil cooling	*by*	MGB
…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…

Table 3: independence principles table

This analysis is performed for each helicopter Failure Condition.
A system function might be highlighted as a driver of several helicopter failure conditions and thus several FDAL may be requested. The highest FDAL is retained as explained in the next figure:.

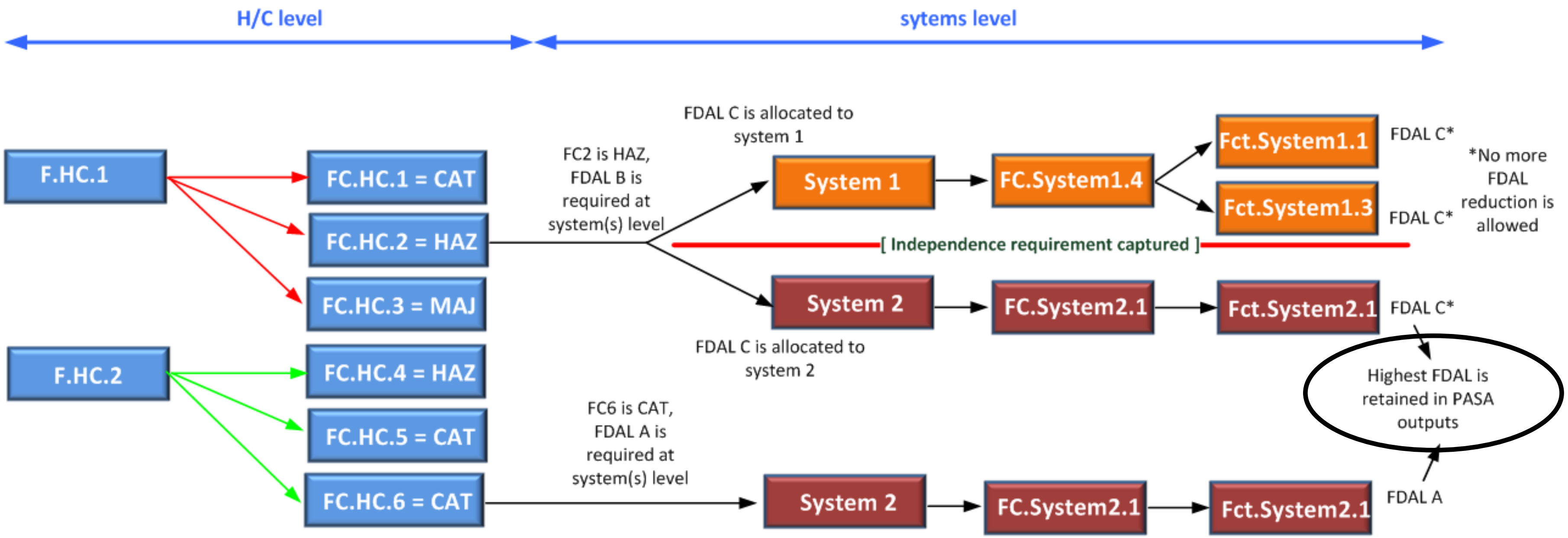

H/C level
sytems level
F.HC.1
FC.HC.1 = CAT
FC.HC.2 = HAZ
FC.HC.3 = MAJ
F.HC.2
FC.HC.4 = HAZ
FC.HC.5 = CAT
FC.HC.6 = CAT
FC2 is HAZ, FDAL B is required at system(s) level
FDAL C is allocated to system 1
System 1
FC.System1.4
Fct.System1.1
Fct.System1.3
FDAL C*
FDAL C*
*No more FDAL reduction is allowed
[Independence requirement captured]
System 2
FC.System2.1
Fct.System2.1
FDAL C*
FDAL C is allocated to system 2
Highest FDAL is retained in PASA outputs
FC6 is CAT, FDAL A is required at system(s) level
System 2
FC.System2.1
Fct.System2.1
FDAL A

Figure 13: FDAL allocation process

4.4 PASA fourth step: End effect assessment

4.4.1 *Common resources and shared signal cumulative analysis*

Shared transverse signal/data such as present position, stick position, weight on wheel, etc., or common resources such as hydraulic, electrical generation, etc. might be a root cause for common modes upon failure. The aim of the cumulative analysis is to assess the effect of an initiating failure on each system and determine if the “cascade effect” at helicopter level is limited to an acceptable level in term of H/C controllability and crew workload or if a redesign is necessary.

4.4.2 *Operational situation during adverse operating conditions*

This analysis highlights the required functions to cope with an adverse event which may be encountered.
In the first instance, based on Airbus Helicopters flight test crew recommendations and certification requirements, the minimum helicopter function list is established to ensure that the rotorcraft can be operated safely by the crew whatever the adverse event.
Secondly, in case of aggravating circumstances which are deemed extremely improbable, the analysis should demonstrate that all necessary helicopter capabilities are available for the flight crew to cope with these extreme cases.

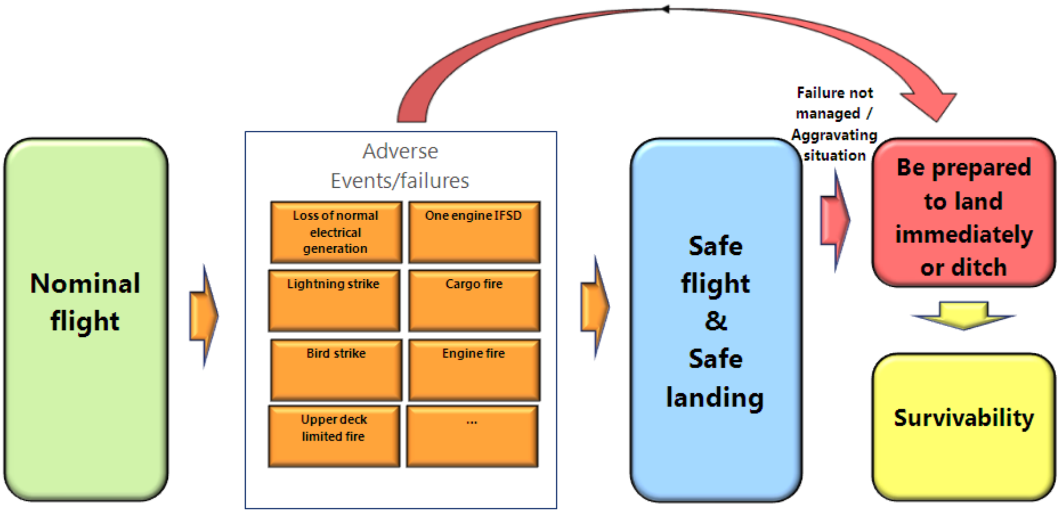

Nominal flight
Adverse Events/failures
Loss of normal electrical generation
One engine IFSD
Lightning strike
Cargo fire
Bird strike
Engine fire
Upper deck limited fire
...
Safe flight & Safe landing
Failure not managed / Aggravating situation
Be prepared to land immediately or ditch
Survivability

Figure 14: Adverse operating condition

5 PASA FEEDBACK

By performing a PASA and allocating safety objectives to each system safety analysis, interdependencies are no longer a risk but are anticipated and under control. The functional interdependencies diagrams capitalize on knowledge of systems functionality. As an umbrella analysis, the PASA process ensures higher consistency between systems safety analysis throughout the helicopter development.

Several risks have been identified and experience has been capitalized on to decrease the number of iterations and enhances the PASA processes. Hereafter the main issues are highlighted:

- At the PASA elaboration step, the helicopter architecture is not frozen and several configurations exist. To minimize the number of iterations, the PASA should start with a “light process” leading progressively to the detailed one described in this document. A focus on novel technology and complex function is recommended.

- As an optional system list is not established, sufficient margins should be taken into account during quantitative allocation. These margins shall be carefully defined to master development cost.

- Specific systems or functions may be introduced later in the development. It should be also considered in the quantitative and qualitative allocation.

- FDAL allocation is a complex process as several options are possible.

6 CONCLUSION

Despite it is a very demanding process, the PASA allows a more exhaustive analysis. Therefore it contributes to secure new helicopter developments by reducing risk discovering system interactions late in the development process. Finally, this high level activity is beneficial for the helicopter safety; more particularly we consider the complex aspects of new helicopters.

7 BIBLIOGRAPHY

CS29	Certification Specification for large Rotorcraft
ED79A / ARP4754A	Certification Considerations for Highly-Integrated or Complex Aircraft Systems. Society of Automotive Engineers (SAE) International, Aerospace Recommended Practice ARP4754, 1996-12.
ARP 4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. Society of Automotive Engineers (SAE) International, Aerospace Recommended Practice ARP4761, 1996-12.
AC29-2C chg 3	Advisory Circular for Certification of Transport Category Rotorcraft.

COPYRIGHT STATEMENT