 THE RESEARCH LEADING TO THESE RESULTS HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S SEVENTH FRAMEWORK PROGRAM (FP7/2007-2013) FOR CRYSTAL – CRITICAL SYSTEM ENGINEERING ACCELERATION JOINT UNDERTAKING UNDER GRANT AGREEMENT N° 332830 AND FROM SPECIFIC NATIONAL PROGRAMS AND / OR FUNDING AUTHORITIES.

CRitical S**YST**em Engineering **A**cce**L**eration

Use – Case Definition Simulation for PRA

D210.010

DOCUMENT INFORMATION

Project	CRYSTAL
Grant Agreement No.	ARTEMIS-2012-1-332830
Deliverable Title	Simulation for PRA
Deliverable No.	D210.010
Dissemination Level	CO
Nature	R
Document Version	V01.02
Date	2014-01-29
Contact	Odile Laurent
Organization	A-F
Phone	+ 33 5 61 18 12 76
E-Mail	Odile.laurent@airbus.com

AUTHORS TABLE

Name	Company	E-Mail
Odile Laurent	A-F	odile.laurent@airbus.com
Hélène Moutier	A-F	helene.moutier@airbus.com

REVIEW TABLE

Version	Date	Reviewer
V01.00	2013-12-20	Hélène Moutier
V01.01	2014-01-13	Jean-Luc Johnson
V01.01	2014-01-20	Ralf Bogusch

CHANGE HISTORY

Version	Date	Reason for Change	Pages Affected
V01.00	2013-12-16	Initial version	
V01.01	2013-12-20	Internal review	13,14,15,18,31,38
V01.02	2014-01-22	External reviews	

CONTENT

Content of Figures

1 Introduction

1.1 Role of deliverable

This document will describe the Airbus use case and its interaction with the other work packages. It provides an overview of the scenario and the tools chain envisaged to support this activity.

This document has the following major purposes:

- Define of the overall use case, including a detailed description of the underlying development processes and the set of involved process activities and engineering methods
- Provide input to WP601 (IOS Development) required to derive specific IOS-related requirements
- Provide input to WP602 (Platform Builder) required to derive adequate meta models
- Define the technology baseline with respect to the use-case, and the expected progress beyond (existing functionalities vs. functionalities that are expected to be developed in CRYSTAL)

1.2 Relationship to other CRYSTAL Documents

The PRA use case is tightly linked with the fuel use case led by Airbus UK. Indeed, the Particular Risk analysis which is conducted in the frame of the current use case relies partially on the fuel system.

It is pointed out that more detailed information about the fuel system is available in the fuel use case description document D211.010.

1.3 Structure of this document

In this document, first we describe the Particular Risk Analysis (PRA) process used within Airbus, second we depict the tools and tools chain supporting this PRA process, then the systems that will be used to assess the tools chain developed in the frame of CRYSTAL are described and finally, the PRA engineering methods are highlighted. Some of them are detailed in annex 1.

The engineering methods that are not refined in this document will be detailed in a next version of the document.

2 Use Case Description

2.1 Use case overview and objectives

The use case described in this document deals with the Particular Risk Analysis (PRA) process and activities.
Particular risk analysis aim at assessing all aspects of events that can cause severe damage to the aircraft or its systems and jeopardise a continued safe flight and landing.
Most of the PRA are required by airworthiness regulations or derived from in-service experience.
More than 20 PRA are requested today. We can classify them in 4 categories:

- Burst/projectile type hazard
  - Uncontained Engine Rotor Failure (UERF)
  - Propeller Blade Release (PBR, when applicable)
  - Uncontained APU Rotor Failure (UARF)
  - Wheel & Tyre Failure (W&TF)
  - RAT Blade Release (RBR)
  - Bird Strike (BS)
  - Hydraulic Accumulator Burst (HAB)
  - Oxygen Cylinder Burst
  - Battle damage (for A400M)
- Vibration type hazard
  - Fan Blade Off / Sustained Engine Imbalance (FBO / SEI, since A340-500/600)
  - Nose Wheel Imbalance (NWI)
- Fire/explosion type hazard
  - Fire / Explosion / Smoke Risk (FESR)
  - Fuel Tank Explosion Risk (FTER)
  - System Fire Protection in Class E Cargo Compartments (for freighter versions)
- Miscellaneous
  - Thermal Risks (TR)
  - Bleed Air Duct Rupture (BADR)
  - Crashworthiness (including Wheels Up Landing)
  - Survivability of Systems (SoS, part of CRI D12 on A380)
  - Failure in Wire Bundle (FWB, functional assessment part of CRI F33 on A380)
  - Electro Magnetic Hazards (EMH : Lightning Strike, HIRF, EMI, ESD)
  - Flailing Shaft (FS)
  - Aft Pressure Bulkhead Rupture (APBR)
  - Rapid Decompression
  - Tail Strike (TS)
  - Data Security

The current PRA process is time consuming because the analysis made are mainly based on engineer judgment and most of the engineering activities are conducted manually. It is thus crucial to find a way to introduce new tools and tools chain for supporting the Airbus PRA process.
In particular, due to the large number of stakeholders involved in the PRA activities, a lot of information must be collected from different sources prior to the analysis. Then, the manipulation of heterogeneous data

coming from the structure and system worlds is necessary to conduct the safety analysis resulting from a dedicated PRA type.
These data are generally stored and managed by specific environments that do not interoperate. One key objective of the current use case is to find a way to automate as far as possible the data extraction and exchange to be used by the different stakeholders all along the PRA process. For this purpose, it makes sense to rely on the CRYSTAL interoperability concept, developed by the WP601.

Another key issue is the existence of common data used by different domains (e.g. thermal, safety, structure, system, …) , but that are identified differently by each domain and duplicated in each domain environment. This situation leads to the necessity to ensure consistency between this distributed common information. The ontology notion specified in the WP209 may help to solve this crucial concern.

Finally, the use case also has the ambition to automate some current manual PRA activities with new tools (e.g. use some simulations to analyse the consequences of multiple failures on a system function). Tools developed or enhanced in the frame of SP6 could be good candidates for this purpose.

The set of systems on which the PRA will be conducted are:

- The fuel system,
- The warning and display cockpit system,
- The primary flight control system,
- The electrical system.

It is pointed out that only some functions of the systems listed in the previous paragraph will be part of the CRYSTAL use case.

The PRA that is chosen for this study is the engine burst, named “Uncontained Engine Rotor Failure (UERF)” by aviation regulations. The choice of the PRA does not affect the engineering process. So, another PRA might be chosen if it is considered more appropriate in the course of the project.

In this chapter, we describe the PRA process, then we present the systems on which the PRA process will be applied.

2.2 Overview of the current PRA engineering process

2.2.1 Particular risk analysis objectives

A particular risk (e.g. engine burst) is an event that can cause severe damage to an aircraft or its systems and jeopardise a continued safe flight and landing.

Aeronautic regulations (e.g. CS 25.903 for engine burst) require that the aeroplane must be designed to ensure capability of continued safe flight and landing after the occurrence of an event caused by a particular risk (e.g. system damaged by a debris after engine explosion).

Particular risk analyses are performed to:

- Identify the risk area at an early stage of the aircraft development,
- Provide guidance material to perform aircraft architecture (system, structure and system installation),
- Contribute to the design process by providing design directives to ensure safety requirements are taken into account,
- Minimize the risk
- Evaluate the remaining risk after practical design precautions have been taken.

In order to meet these above objectives, the development of the aircraft design is supported by preliminary analysis. Identification of vulnerable safety-critical components/systems must be performed so that the particular risk damage can be either avoided or minimised by:

- Segregation,

- Removal from potential trajectories
- Protection,
- Appropriate local design principles,
- Adequate structure and system architecture.

These analyses must be carried out as early as possible in the design stage to avoid late and expensive redesign.

Particular risk policy documents describing the main assumptions to be used in the analyses, the identification of the interfaces with other particular risk analyses, the previous experiences and the specific tools to be used (e.g. identification of affected equipment using digital mock up, simulation) are set up.

The particular risk analysis is performed in 4 major phases:

- Phase 1: Preparation of the PR requirements and recommendations
- Phase 2: Design and validation process
- Phase 3: Verification process
- Phase 4: Preparation of Final Compliance Demonstration

2.2.2 Description of the particular risk analysis phases

2.2.2.1 Global overview of PR activities

The following figure depicts the different phases and activities of a PRA.

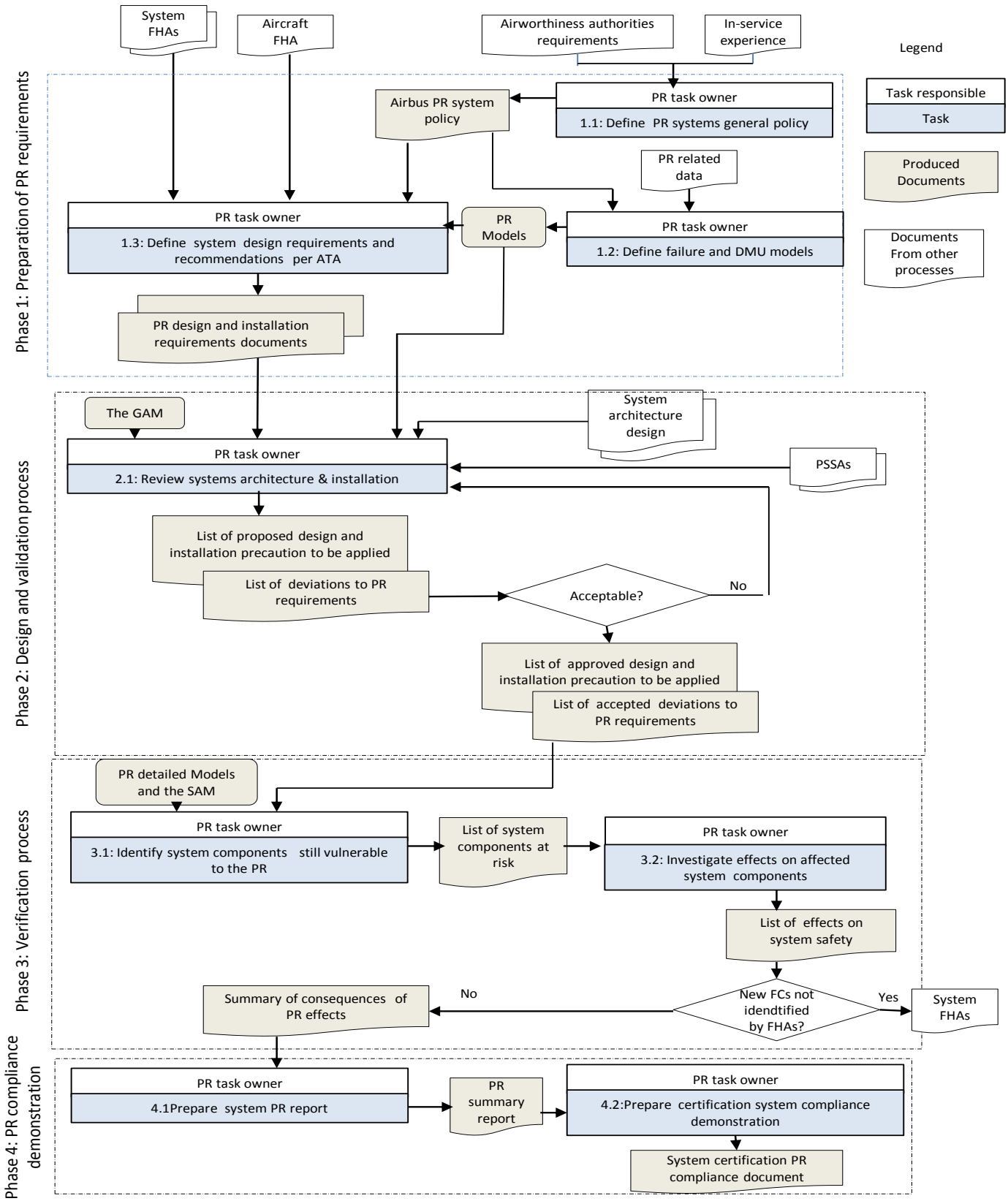


Figure 1: PR process

2.2.2.2 Description of Phase 1: Preparation of the PR requirements

This phase is made of 3 tasks:

- Definition of the PR systems general policy
- Definition of failure and Digital Mock-Up models
- Definition of system design requirements and recommendations per ATA

2.2.2.2.1 Task 1.1 - Define PR systems general policy

Objectives:

- Define the inputs for the PRA:
  - general directives and assumptions,
  - failure model types,
  - general design guidelines.

Responsible:

- PR Task Owner with support from:
  - systems design specialists,
  - installation teams,
  - aircraft specialists (handling quality teams, aircraft performances teams, ...)
  - Aircraft DMU specialists.

Inputs:

- Airworthiness Authorities requirements (e.g. CS 25.903 for engine burst)
- In-service experience data

Task Description:

Based on the above input, the PR task owner mainly defines the following data:

- high level PR model (e.g. for a bird strike: size, weight, speed, energy of the bird, impact angles, altitude, …)
- which kind of operation the A/C is supposed to be able to perform after the considered PR occurs
- The status of the A/C systems to be considered in the frame of the analysis: MMEL (Master Minimum Equipment List) conditions, combinations with other events or failures, …
- type of component misbehaviour to be considered in case of damage by the considered PR (“loss” for computer – “jammed” or “broken” for mechanical part)

Deliverable:

PR Systems policy covering all above aspects

Used tools:

No specific tool. Only WORD documents.

2.2.2.2.2 Task 1.2 – Define failure and DMU models

Objectives:

- Define the models that are required for the PR analysis:
  - DMU models and other models specific to each kind of PRA (e.g. fragments characteristics for engine burst)
  - affected aircraft zones (e.g. drawings of the aircraft rotor burst risk areas for engine burst)
  - depending on the PR, possible guidelines for installation (e.g. for engine burst: guidelines for engines location and position)

Responsible:

- PR Task Owner.

Inputs:

- PR system policy

- all relevant data (e.g. for engine burst: engine location data, engine manufacturer data, A/C general arrangement)

Task Description:
Based on the above input, the PR task owner identifies the consequences of the PR on the aircraft components and zones.

Deliverables:
- DMU models which are necessary to conduct the PR analysis
- PR failure model report (description of the affected aircraft zones, systems hit list affected by the PR, first installation requirements…)

Used tools:
Catia for the DMU models, specific Airbus Catia modules for dedicated PR (e.g. ARIAS for engine burst)

2.2.2.2.3 Task 1.3 – Define system design requirements and recommendations

Objectives:

Provide systems design and systems installation design requirements in order to avoid that the PR could cause Catastrophic or Hazardous Failure Conditions.

Responsible:

PR Task Owner with support from:
- systems design specialists,
- structure teams,
- safety specialists,
- installation teams.

Inputs:

- PR policy document,
- Systems architecture
- A/C FHA and Systems FHAs,
- PR failure model report.

Task Description:

- Identify catastrophic and hazardous Failure Conditions that are relevant in the frame of the considered PR including conditions that could result from combination of structure damages (including their possible effects on systems) and damages on other systems.
- Define design and installation requirements related to the considered PR

Deliverables:

- PR design and installation requirement documents

Used tools:

The activity is mainly based on an engineer judgment.

2.2.2.3 Description of Phase 2: Design and validation process

This phase is made of one task: review of systems architecture and installation.

2.2.2.3.1 Task 2.1: Review systems architecture and installation

Objectives:

- To confirm that the PR design and installation requirements are correctly understood and implemented
- To identify necessary deviations to the PR requirements

Responsible:

PR Task Owner with support from:

- design and systems design specialists,
- safety specialists,
- installation teams,
- systems physical architects.

Inputs:

- PR design and installation requirements document
- The 3D system physical architecture; the Global Architecture mock-up (GAM)
- PR models
- Systems architecture design

Task Description:

- to hold system installation and architecture reviews for each affected A/C section or affected systems, in order to:
- list and assess the proposed design solutions
- list deviations to PR requirements
- check against interference with other PRs & ZSA (design solutions should be compatible with those implemented for other PR and ZSA requirements)

Deliverables:

- list of approved design and installation precaution to be applied,
- list of accepted deviations to PR requirements

Used tools:

The activity is based on an engineer judgment

2.2.2.4 Description of Phase 3: Verification process

This phase is composed of two tasks:

- the identification of the system components still vulnerable to the PR and the verification of the systems detailed 3D mock-up; the SAM (Space Allocation Mock-up),
- the analysis of the effects on systems components affected by the PR

2.2.2.4.1 Task 3.1: Identify systems components still vulnerable to the PR

Objectives:

To identify all combinations of components likely to be damaged by the consequences of a PR in non-protected areas.

Responsible:

PR Task Owner with support from:

- systems design specialists,
- structure teams,
- safety specialists,
- systems physical architects,
- installation teams.

Inputs:

- List of approved design solution and design installation to be applied,
- List of accepted deviations,
- The systems detailed 3D mock-up (SAM),
- PR detailed models.

Task Description:

For system installations not protected by structure, the PR responsible with support from the relevant teams

shall perform the analysis (through DMU reviews, design and installation documents, …) of the PR effects in order to identify all combinations of components likely to be damaged.(e.g. for engine burst: systems components that are on the trajectories of the engine debris).

Deliverables:

- List of systems components at risk.

Used tools:
Catia for DMU models and dedicated modules depending on the PR.

2.2.2.4.2 Task 3.2 : Investigate effects on affected systems components.

Objectives:

To assess at aircraft level the capability to perform continued safe flight and landing when systems are damaged by the considered PR.

Responsible:

PR Task Owner with support from:
- systems design specialists,
- structure teams,
- safety specialists,
- installation teams.

Inputs:

- List of system components at risk,
- PR detailed models.

Task Description:

Based on the list of system components still at risk, the PR responsible shall:

- Analyse damages on affected systems components
- Identify the effect at aircraft level on system safety,
- Ensure that new FCs are incorporated into the A/C and systems FHAs, if necessary,
- Ensure that the relevant systems design requirements documents are updated accordingly.

Deliverables:

- Requirements for A/C and system FHAs, if necessary,
- Summary of consequences of PR effects.

Used tools:

The activity is mainly based on an engineer judgment combined with dedicated performance and handling quality in-house tools.

2.2.2.5 Description of Phase 4: PR compliance demonstration

This phase is made of two tasks:

- the preparation of the system PR report,
- the preparation of the certification system compliance demonstration.

2.2.2.5.1 Task 4.1: Prepare systems PR report.

Objectives:

Produce specific system PR document

Responsible:

PR task owner with support from all involved actors in the PRA.

Inputs:

- List of approved design solutions,
- List of accepted deviations,

- Summary of consequences of PR effects,
- Installation and structure description,

- architecture system description.

Task Description:

The PR task owner will summarise all the reports on the subject in order to get a unique report at aircraft level which will demonstrate the compliance with the concerned PR System policy.

Part of this report may be used as support for certification document against systems bird strike analysis.

Deliverables:

PR summary report

Used tools:

No specific tools (WORD documents).

2.2.2.5.2 Task 4.2 : Prepare certification system PR compliance demonstration

Objectives:

Produce Certification system PR compliance demonstration

Responsible:

PR task owner with support from all involved actors in the PRA.

Inputs:

PRA summary report

Task Description:

Upon request, based on the PRA summary report, the Task Owner shall support the “Systems” DCS to prepare the certification document.

Deliverables:

System Certification Systems PR compliance documents.

Used tools:

No specific tools (WORD documents).

2.3 Focus on the PRA engineering tasks in the frame of CRYSTAL

In the frame of CRYSTAL, the objective is to:

- reinforce the use of models in the PRA process, more specifically to go forward a Model Based System Analysis (MBSA) approach,
- automate as far as possible the data exchange between the different tools that will be introduced to support the MBSA activities.

The tools description is not part of this section. The tools chain used to conduct the engineering tasks described in this paragraph are depicted in chapter 3.

The following figure describes the engineering activities including MBSA that are linked to the Airbus Use Case.

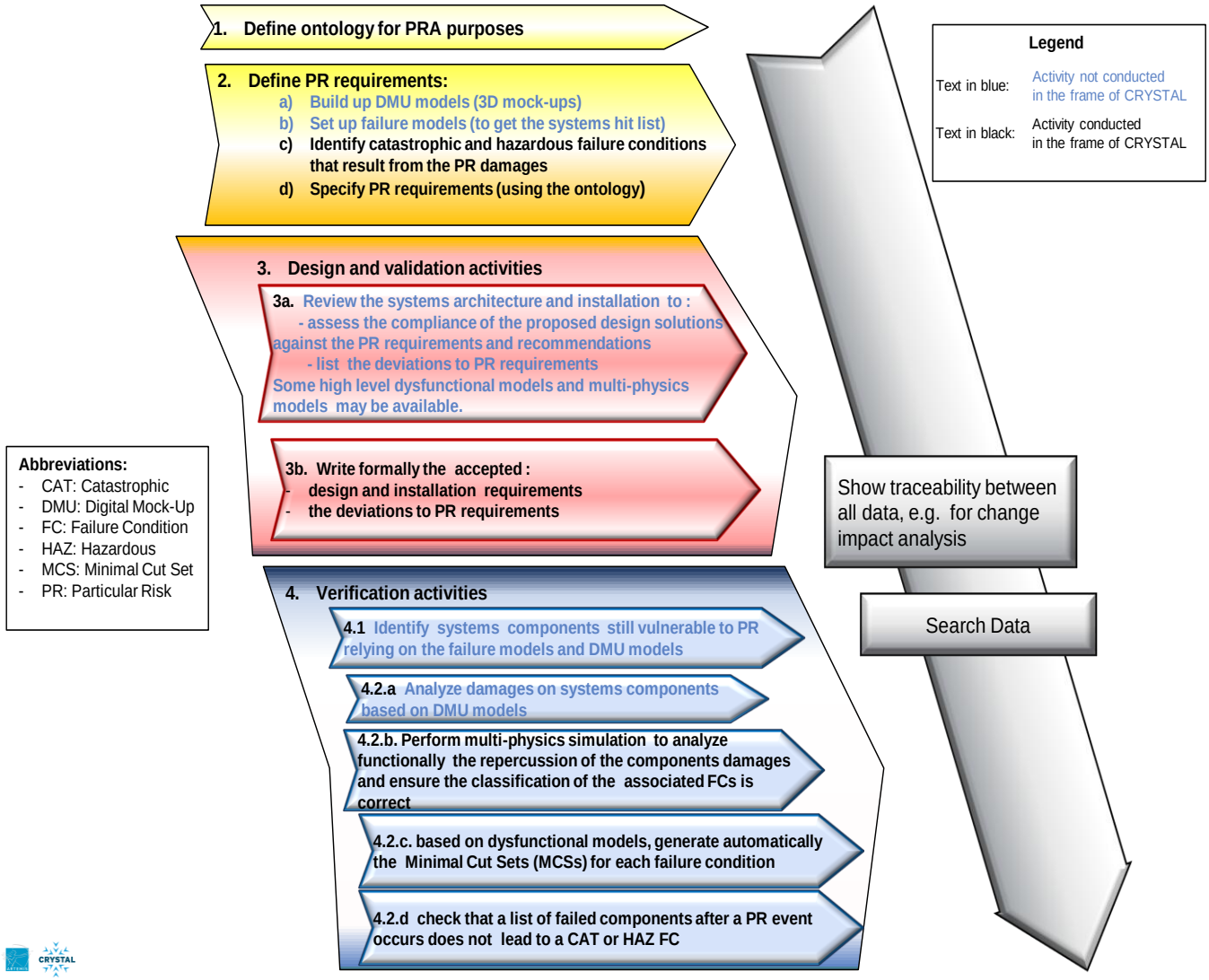


Figure 2 PRA MBSA activities

The engineering tasks that will be conducted in the frame of the PRA use case cover partially the phases 1, 2 and 3 of the PRA process described in the section 2.2 of this document.
The phase 4 “preparation of Final Compliance Demonstration” of the PRA process is out of the scope of the current PRA use case.

The mapping between the PRA process depicted in figure 1 and the steps shown on the figure above can be represented by the following table:

Name of the PRA process phase (figure 1)	Name of the PRA engineering steps (figure 2)

Preparation of the PR requirements	• define ontology for PRA purposes • define RR requirements
design and validation process	design and validation activities
Verification process	Verification activities
PR compliance demonstration	Out of the scope of the PRA use case

2.3.1 Step 1: Define ontology for the PRA purposes:

The objective of this engineering step is to define the concepts manipulated all along the PRA process. The concepts will be defined by a lexical name, a set of attributes and rules that characterize the objects described. A common definition, agreed by the PRA stakeholders, of all the information needed to support the PRA is essential to improve the current way of working. Such a PRA dictionary will ease the data sharing between the PRA actors and will allow to automate the data exchange, when needed.

Typical PRA concepts that will be defined are:

- Failure condition,
- Minimal cut Set,
- System function,
- Fault tree.

This list is not exhaustive. The concepts to be specified will be those necessary to implement the PRA use case. The idea is not to define a complete PRA ontology, but to assess the relevance of the use of such an ontology in the PRA process relying on a MBSA approach.

2.3.2 Step 2: define PR requirements:

At this stage of the PRA process the catastrophic and hazardous failure conditions are identified.

For the fuel system, an example of a catastrophic failure condition is:

total inability to supply fuel to both engines in flight.

Then, the PR requirements are derived from the identified failure conditions. An example of an engine burst requirement leading to the catastrophic failure condition described above is:
total loss of fuel supply to the unaffected engine shall not be possible in the event of an UERF.

The failure conditions and the PR requirements will be formalized using the ontology concepts.

Classes of PR requirements will be identified in order to ease requirements formalization. These classes of requirements will be described using “requirements patterns”.

An example of pattern could be:

Total loss of <object identified in the ontology> to <object identified in the ontology> <verb listed in the ontology> in the event of an <PR identified in the ontology>

Where < > is replaced by the adequate value for each instance of a requirement fulfilling the pattern characteristics.

It is pointed out that the generation of hit list and the 3D mock-up construction are not part of the PRA use case.

2.3.3 Step 3: Design and validation activities:

At this stage of the PRA process, the PR requirements are identified and formalized as described in step 2. The main added value of a requirements formalization based on a common vocabulary between the stakeholders of the PRA process is to facilitate the design and validation activities avoiding misunderstanding and ambiguity.

The system design is still under definition and can evolve depending on constraints specified by different disciplines. So, the PR requirements can challenge some of the design solutions. The purpose of the design and validation activities in the PRA process conducted by the system designer and the PRA specialist, is to check whether the PR requirements are met. This system design and installation review relies on engineer judgment that can be based on system analysis coming from models simulation and 3D mock-up. These modelling and simulation activities are not part of the CRYSTAL PRA use case.

Following this PRA review an adjustment of the PR requirements may be made. The new formulation of the PR requirements will rely on the same approach as the one described in step2.

2.3.4 Step 4: Verification activities:

The two first verification activities of the PRA process which consist in:

- Identifying systems components still vulnerable to PR relying on the failure models and the aircraft Digital Mock-Up (DMU),
- Analysing the damages on the systems components of the aircraft DMU

are not part of the current PRA use case.

In the frame of the CRYSTAL PRA use case, assuming that:

- the identification of the combinations of components (hit list) that are damaged by the PR impacts are available,
- the system detailed design and installation choices are made,

the verification activities that will be conducted are:

1. firstly, multi-physics models are developed or reused in order to check the functional repercussions at aircraft level of the failed components due to the PR are in line with the initial safety classification (catastrophic, hazardous, major, minor),
2. secondly, dysfunctional models are developed or reused from which the fault trees and minimal cut sets are automatically generated,
3. thirdly, based on the hit list and the minimal cut sets list, the failure conditions reached are identified either automatically or manually. Then, it is checked the classification of the failure conditions identified is neither catastrophic, nor hazardous. If it is the case, a new design and installation loop is necessary to find a solution that allow avoiding such safety events classifications.

2.3.5 Transversal activities:

In parallel to the different steps described above, traceability activities are performed. The PRA artefacts are linked together in order to able to make impact analysis when a modification occurs at any stage of the PRA process.

The traceability links between the following artefacts will be set up:

- Requirement/failure conditions,
- Requirement/ model
- Hit list/3D mock-up
- Hit list/failure condition
- Fault trees/dysfunctional model/failure condition
- Hit list/dysfunctional model

Other traceability links might be useful to support the PRA process.

Moreover, particular risk analysis tasks require a lot of information to manipulate in different environments. The capability to search easily heterogeneous information is crucial to make the PRA process leaner and more efficient. So, efficient search engine shall be available to retrieve easily the adequate data to perform the PRA tasks.

These transverse capabilities will be part of a “PLM like” environment.

2.4 Stakeholders & Roles

The following tables described the stakeholders and roles involved in the PRA process.

Stakeholders	**Role**
Requirement engineer	Write the requirements
Particular Risk Analysis specialist	conduct the Particular risk analysis tasks
System safety analysis specialist	In charge of system safety analysis tasks
Aircraft Safety analysis specialist	In charge of multi-systems analysis tasks
System modelling engineer. There are different kinds of system modelling engineers: as many as domains (thermal, functional, mechanical, …)	Build up the appropriate models.
System design engineer (or designer)	Specify the system design
System installation engineer	Specify the system installation
3D modelling engineer	Build up the 3D mock-up

3 Tools chain description

This chapter describes the tools and tools chain that will be used to conduct the PRA activities described in the previous chapter.

3.1 PRA tools chain

The following drawing depicts the tools that will be used and the interoperability links that are necessary to build up a consistent tools chain in order to automate as far as possible the PRA tasks conducted in the frame of this PRA use case.

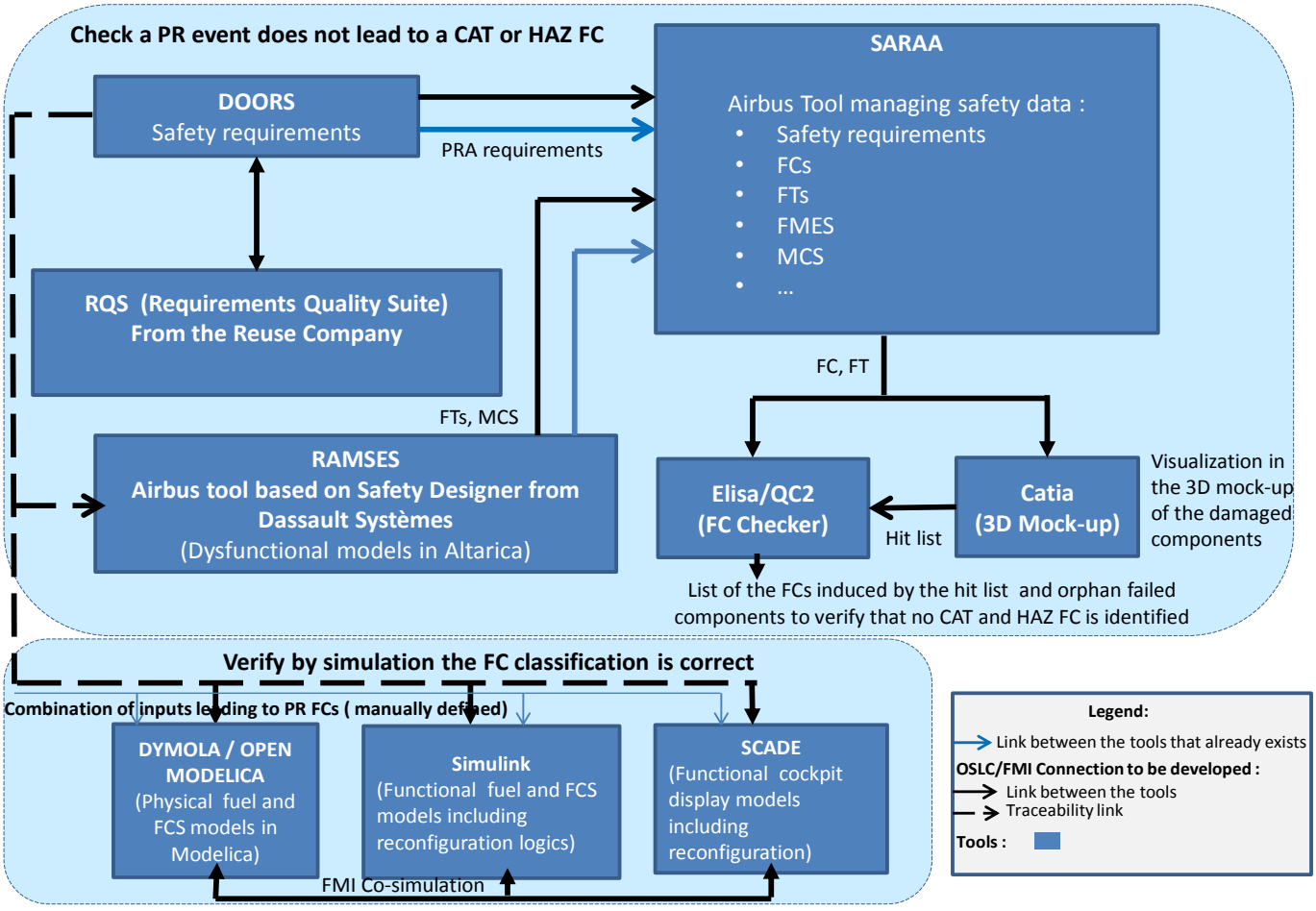


Figure 3 Overview of the PRA tools chain

The table defined below shows the mapping between the PRA activities conducted in the frame of CRYSTAL described in figure 3 and the tools chain supporting them:

PRA activity number from figure3	PRA activity description	Tools chain
1	define ontology for the PRA purposes	RQS
2	**define PR requirements**	RQS-DOORS-SARAA-Catia
3	**Design and validation activities**	RQS-DOORS-SARAA-Catia
4	**Verification activities**	
4.2.b	• Perform multi-physics co-simulation	DYMOLA-Simulink-SCADE
4.2.c	• Generate the MCs	RAMSES-SARAA
4.2.d	• Check a PR event does not lead to a CAT or HAZ failure condition	SARAA-Catia-ELISA/QC2

The interoperability OSLC connectors shown on the previous figure are expected to be developed in the frame of CRYSTAL. Nevertheless, priorities shall be set up if the effort to develop all of them is too high against the available resources.

3.2 Brief tools description

3.2.1 DOORS

DOORS is a well-known commercial tool sold by IBM whose aim is to support requirements based engineering activities. The DOORS offers the following features:

- requirements capture,
- traceability by linking requirements to design items, test plans, test cases and other requirements,
- requirements management in a centralized location for better team collaboration.

At Airbus, since the A380 programme, DOORS is used to manage aircraft requirements, whatever their types.

3.2.2 RQS

The Requirements Quality Suite (RQS) commercialized by the Reuse Company is a set of tools aiming to customize, manage and improve the quality of a set of requirements.

It is composed of 3 modules:

- RAT (Requirements Authoring Tool) that allows authoring requirements. Based on requirements patterns, RAT assists the user in the requirements capturing and writing,
- RQA (Requirements Quality Analyzer) RQA that supports the definition, measurement, improvement, analysis and management of the quality of requirements specifications in systems and software projects,
- kM (knowledgeMANAGER) that provides an ontology management system allowing to define and manage the semantics of the systems development data, as well as the concepts and relationships that describe application knowledge.

RQS was assessed within Airbus, but is not operationally used today.

3.2.3 SARAA

SARAA (Safety And Reliability Analysis for Aircraft) is an Airbus tool supporting safety and reliability analysis for new aircraft designs in accordance with the standards agreed with the certification authorities (DGAC, FAA). The tool covers the development and documentation of Functional Hazard Analysis (FHA), Preliminary System Safety Analysis (PSSA), System Safety Analysis (SSA) and Common Mode Analysis (CMA). This includes both system level development of the safety case and aircraft level analysis and synthesis.

The tool organises safety analysis according to Aircraft and ATA chapter. The primary view is of a series of chapters in Microsoft Word supported by an information database. Most of the safety information is entered through a forms-based editor supported by navigation and browsing capabilities.

The reliability model includes calculation of dependency diagrams and fault-trees. This is accessed using graphic editors linked to the information model in the rest of the tool. Fault trees can be imported from the FaultTree+ tool (version 10) as well as entered through the graphic editor.

SARAA is a daily tool for safety teams.

3.2.4 Catia

Catia V5 is commercialized by Dassault Systèmes. The aim of Catia is to provide 3D Digital Mock Up and Product Lifecycle Management (PLM) solutions.

Since the A340 programme, all the Airbus aircrafts are designed using a 3D mock-up built up in Catia.

Catia is a key tool for the PRA process.

3.2.5 DYMOLA

Dymola is a design, modelling, and simulation solution for complex systems, based on the Modelica language. Dymola enables the definition and optimization of dynamic behaviour and complex interactions thanks to a simple and practical model creation interface, using a symbolic digital solver for complex models.

The tool is sold by Dassault Systèmes. It was assessed by Airbus but it is not operationally used.

3.2.6 RAMSES

RAMSES is an Airbus tool relying on Safety Designer from Dassault Systèmes. RAMSES is an Integrated Development Environment for the development and the analysis of safety models of systems, based on the AltaRica formal language. With RAMSES, one can create models and libraries of reusable components, observe the propagation of faults by raising events in a dedicated step-by-step simulator, and perform several calculations to assess the modeled systems.

The main RAMSES capabilities are:

- Graphical model editor: Edit AltaRica models through drag & drop, tables or text editor; organize models in libraries for future re-use.
- Step-by-step simulator: Simulate the propagation of faults on AltaRica models, by specifying initial configurations and raising events at will.
- Compiler to fault trees: Automatically generate fault trees from AltaRica models, specifying top events and initial configurations.
- Critical scenario generator: Automatically generate sequences of events that can occur on an AltaRica model, leading to a specified critical state.

- FMEA assistant: Automatically generate drafts of FMEA.
- Report generator: Generate reports in the DocBook, RTF, XML file formats.

RAMSES is not used operationally yet, but is a key enabler for safety R&T projects.

3.2.7 ELISA/QC2

ELISA (Enhanced Aircraft System Lean Installation Safety Assessment) is an innovative approach that provides the safety specialists a methodology and toolsets that facilitate safety assessments (PRA, segregation verification), by making the bridge between safety databases storing Failure Conditions (Fault Trees, Dependence Diagrams) and geometrical databases storing Aircraft Systems Installation (DMUs at all stage of the program) using Functional Identifiers. ELISA also offers the capability to identify a set of failure conditions from a hit list generated during a PRA analysis.
The ELISA prototype is available and used in R&T projects.

QC2 (Quality Control 2) is an Airbus Catia macro whose aim is to detect the non-compliance of the design with technical design rules.

QC2 ensures the aircraft DMU (Digital Mock-up) is conformed to:

- the Aircraft Architecture and Requirements conformity,
- the Design and Manufacturing Technical Rules of Installation,
- the Safety Rules,
- the target Aircraft Configuration.

The 2 tools are envisaged to check a PR event does not lead to a catastrophic or hazardous Failure Conditions. An analysis has to be done before choosing one of these two tools before integration in the PRA tools chain.

3.2.8 Simulink

Simulink from MathWorks is a world-wide used block diagram environment for multi-domains simulation and Model-Based Design. It supports simulation, automatic code generation, and continuous test and verification of embedded systems. Simulink provides a graphical editor, customizable block libraries, and solvers for modelling and simulating dynamic systems.

MatLab/Simulink is widely used in the systems domain within Airbus.

3.2.9 SCADE

SCADE Ansys covers the full development cycle of critical embedded software from specifications to the generation of correct by-construction production code in C and Ada.
It supports both data flow and control logic type of applications.
It is the only commercial automatic code generation tool qualified to the strictest level of the civilian avionics standard RTCA DO-178B, Level A.

SCADE is used to implement the detailed design of Airbus critical avionics systems (e.g. flight Control system and flight warning system).

4 Systems description

The set of systems on which the engine burst analysis will be done is made of:

- The fuel system,
- The cockpit control, alert and display system,
- The electrical system,
- The communication system,
- The flight control system

In this paragraph, the systems components and the systems functionalities of the above systems are briefly depicted and the sub-set of the systems that will be part of the PRA use case are highlighted.

4.1 The fuel system

4.1.1 Brief description

The primarily purpose of the fuel system is to ensure the required fuel feed supply to the engines. In addition to the Engine Feed function, other systems functions are needed to ensure a suitable fuel system management, including fuel quantity measurement and fuel distribution.

The A350 XWB aircraft is fitted with three fuel tanks, which provide fuel to two engines and the APU.

Fuel is stored in three fuel tanks, one in each wing (Wing tanks) and one spanning the wings inboard ribs including the centre fuselage section (centre tank). Each tank vents to atmosphere through surge tanks that are located outboard of the wing tanks. The wing tanks vent to the adjacent vent surge tank and the centre tank vents through the left wing vent surge tank. The system ensures that fuel is not spilled or siphoned overboard during normal ground and flight manoeuvres.

4.1.2 Fuel system architecture

The Fuel System stores the fuel in a series of tanks allocated in the wings, horizontal stabilizer and/or fuselage. The fuel is redistributed between the tanks to ensure engine feed and other functions as lateral and longitudinal CG position modification.

In-tank equipment as sensor and fuel probes are provided for fuel quantity management and monitoring. The data is acquired and sent to the control computer via the fuel tank data concentrator, which provides control commands to in-tank valves and pumps to perform engine feed, fuel transfer, jettison and to provide alerts and indications to the flight crew. The fuel control computer consists in two segregated and independent computers (one of them is in control while the second one is stand-by, available in case of failure).

The following picture represents a simplified typical civil aircraft Fuel System layout:

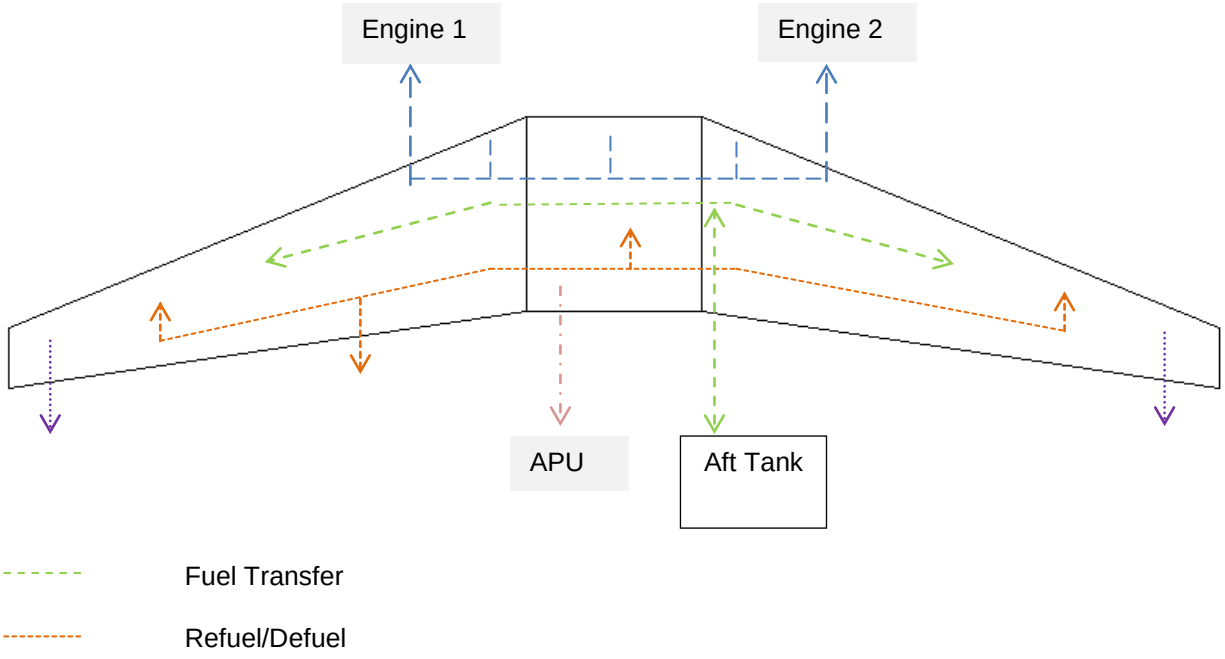


Figure 4: fuel system layout

4.1.3 Fuel system functions and components

Fuel System Function	description	Involved component
Supply Fuel to the Engines: .	To control delivery of fuel to the engine interface. This includes fuel shut-off when required	• Engine Feed Pumps • LP Valves. • Crossfeed Valves • Thermal Relief Valves • Air Release Valves • Pressure Holding Valves • Clack Valves (collector cells). • Non Return Valves
Supply Fuel to the APU .	To control delivery of fuel to the APU interface. This includes fuel shut-off when required	• Engine Feed Pumps • APU Pump • APU LP Valve • APU Isolation Valve • APU Drain and Vent Valve
Control Tank Pressures	To limit the differential pressure between the tank and atmosphere.	• Vent Line Fuel Drain Valves. • Overpressure Protectors. • NACA Inlets/Outlets.

Fuel System Function	description	Involved component
Manage fuel distribution, (including refuel, containment, distribution, defuel and jettison)	To manage the movement of fuel	• Transfer Valves • Crossfeed Valves • Tank Inlet Valves • APU Valve • Refuel Valve • Jettison Valves • Transfer Pumps • Jet Pumps
Indicate fuel state, (including quantity and temperature)	To provide information to the ground and flight crew on the fuel state of the aircraft(e.g. gross weight and centre of gravity)	• Fuel Probes • Temperature Sensors • Fuel Characteristics Sensors
Provide indication and support for maintenance activities.	To provide system equipment health monitoring & maintenance data feedback to operators	All equipment except the ones involved Fuel Containment and Venting

Where the components are defined as follow:

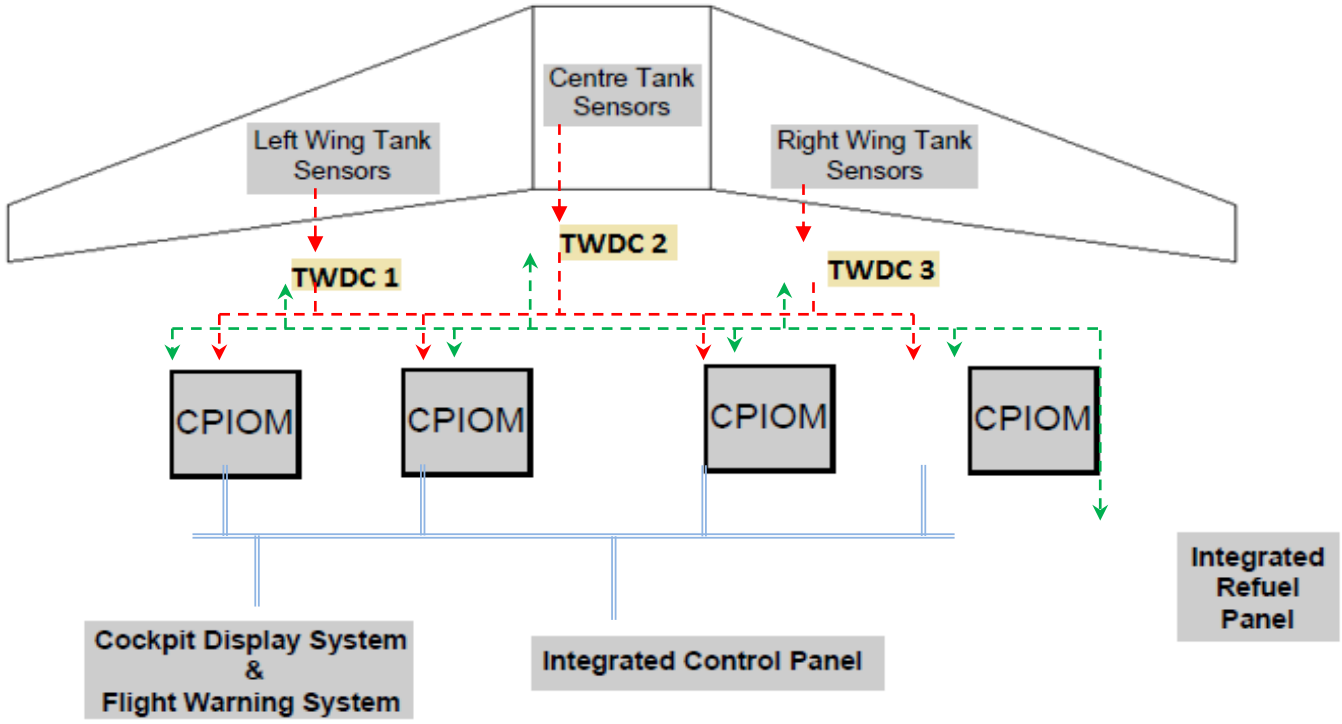
Component Type	Description
Electrically actuated valves	
Transfer Valves	Controls fuel flow in the transfer gallery to re-distribute fuel between tanks.
Cross-feed Valves	Allows either the engines and APU can be fed from any fuel tank.
LP Valves	Stops fuel flow to the engines from fuel system when required
Tank Inlet Valves	Controls fuel flow into the tanks.
APU Valve	Stops fuel flow to the APU when required
Refuel Valve	Controls fuel flow between the fuel gallery ground refuelling / defueling Equipment.
Jettison Valves	Allows discharge of fuel from all tanks overboard to reduce the fuel load and hence the aircraft weight
Probes and sensors	
Fuel Probes	Provided for fuel quantity measurement.
Temperature Sensors	Measures fuel temperature.
Fuel Characteristics Sensors	Measures fuel properties as density, permittivity and temperature.
Fuel Pumps	
Transfer Pumps	Pump fuel from one tank to the fuel transfer gallery.
Engine Feed Pumps	Pumps fuel from the engine feed tanks (collector cell) to the engine feed gallery.
APU Pump	Pumps fuel to the APU feed line.

Component Type	Description
Mechanical & fluid actuated equipment	
Jet Pumps	Provided for fuel and/or water scavenge in the fuel tanks.
Non-return Valves	Ensures fuel flow in only one direction, provide the means to prevent fuel path backwards.
Surge Relief Valves	Provided to minimize surge pressure produced when a shut-off valve closes.
Thermal Relief Valves	Provided to limit the fuel gallery pressure generated from thermal expansion of fuel in a closed section.
Air Release Valves	Allows air to escape from the fuel gallery to prevent air being fed to the engines or APU.
Water Drain Valves	Typically installed at the low points of the tanks, allows the water to be removed by manual operation of the valve.

4.1.4 Focusing on the fuel quantity management system

In the frame of the PRA use case, we focus on the Fuel Quantity Management System (FQMS) which is comprised of in-tank equipment, external Tank Wall Data Concentrators (TWDCs) -which process data from the in-tank equipment and to be transmitted to the Core Processing Input/Output Modules (CPIOMs), an Integrated Refuel Panel (IRP), plus Control and Display System (CDS) and Integrated Control Panel (ICP) interfaces.

Each tank has a dedicated TWDC which acquires analogue data from the in-tank components and converts it into digital signal to be sent to the CPIOMs (via CAN and discrete links). The FQMS consists of two identical sides (each side uses 2 CPIOMs) in order to support the required fuel system reliability requirements, providing redundancy in the event of relevant FQMS failures. The CPIOMs communication with the interfaces systems is achieved via the Avionics Full Duplex Switched Ethernet Network (ADFX).



Discrete Link
CAN link
AFDX

Figure 5 : FQMS architecture

4.2 The cockpit control, alert and display system

4.2.1 ARCAD functions:

ARCAD encompasses Control, Alert and Display functions of the cockpit.
ARCAD manages the information from the aircraft systems to be displayed on the different Display Units (DU) providing the flight crew with operational assistance for both normal and abnormal situations (system failure or dangerous aircraft configuration). It also manages the keyboards and the Integrated Control Panels (on the cockpit ceiling) that allows the pilots to control the aircraft.
For the new aircrafts generation, ARCAD intends to gather the functions provided by flight warning system and the control display system of the Airbus family.

Another innovation of ARCAD is the introduction of tactile display.

The following figure shows the keyboards, displays and control panels of an A350 cockpit.

Figure 6 : A350 cockpit

4.2.2 ARCAD architecture

ARCAD shall be seen as an HMI resource for new generation aircraft systems. The following picture gives an architecture overview of this resource highlighting the components roles (display, open world, control, processing):

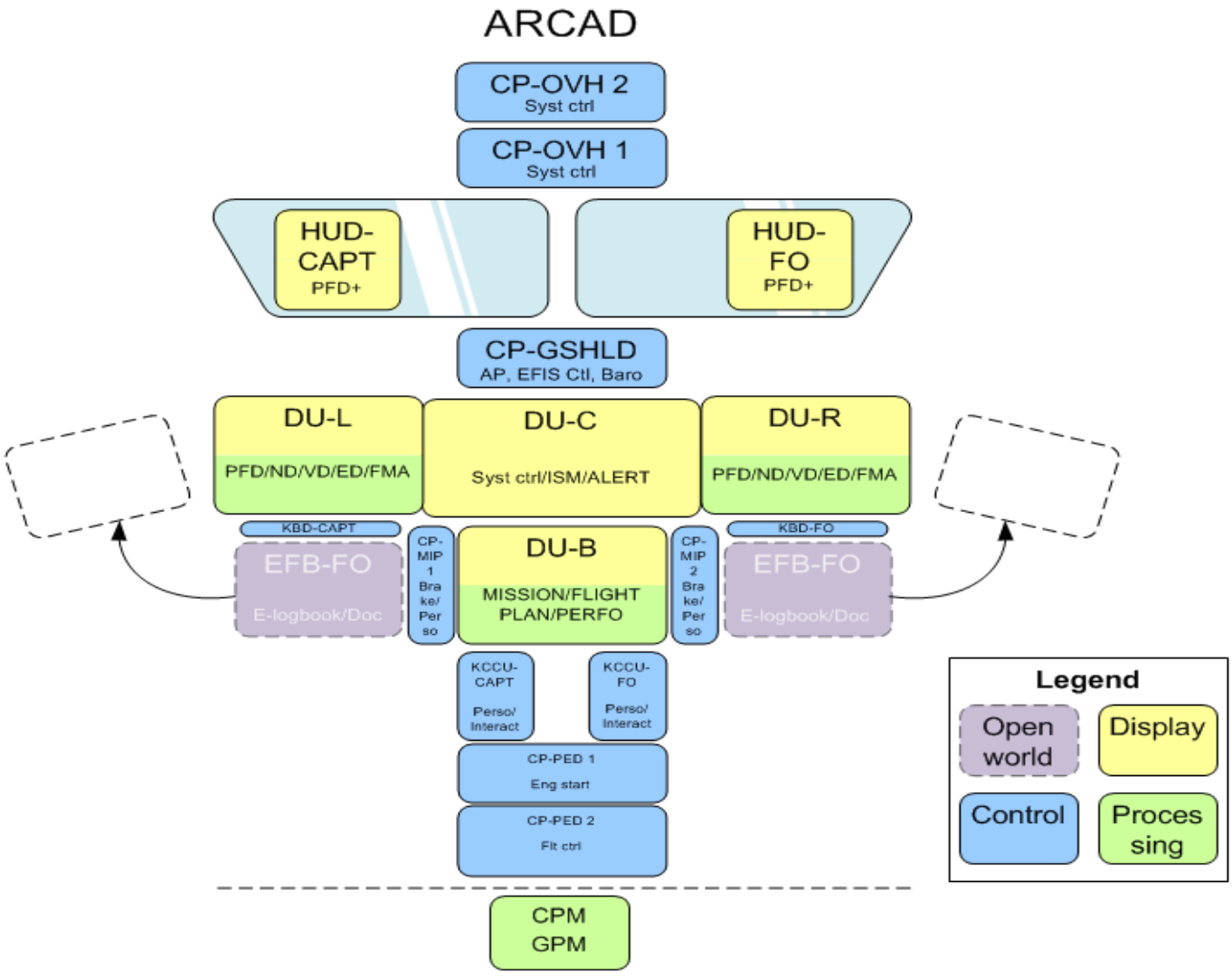


Figure 7: ARCAD components

Where :
DU-C: Display Unit Central
DU-L: Display Unit Left
DU-R: Display Unit Right
DU-B: Display Unit Back-Up
HUD: Head Up Display
FO: First Officer
CAPT: Captain
PFD: Primary Flight control, on which the key aircraft parameters are displayed (attitude, airspeed, altitude, Vertical speed, heading, ..)
ND: Navigation Display
VD: Vertical Display on which the weather radar information, terrain information and vertical trajectory are displayed
ED: Engine Display
KCCU: Keyboard Control Command unit

FMA: Flight Management
EFB: Electronic Flight Bag; a dedicated platform managed by the airlines and that hosts operational applications
CP: Control Panel

4.2.3 ARCAD operating modes

ARCAD is divided into 2 segregated and dissimilar subsystems:

- ARCAD MAIN (specific LRUs) that is the main instrument used in nominal mode,
- ARCAD AUXI (hosted on IMA) which ensures two main functions:
  - Auxiliary nominal mode instrument,
  - Back-up mode instrument.

In nominal mode:

- All Display Units are managed by ARCAD MAIN.
- The DU-Center (DU-C) display is computed by DU-Bottom (DU-B) and sent via video link. The displays of both Head-Up Displays are managed by ARCAD MAIN: the HUD CAPT (resp. HUD F/O) display is computed by DU-R (resp. DU-L) and then sent via video link.
- Alert and Control functions are provided by ARCAD MAIN.

In back-up mode (total loss of ARCAD MAIN resources), ARCAD AUXI provides back-up capabilities for Display, Control and Alert functions. In addition, ARCAD AUXI manages the display of DU-C: a core processing module and a graphical module compute the display and send it to DU-C via video link.

4.2.4 ARCAD communication resources

The following picture illustrates the two types of ARCAD internal communication: A818 video links and CAN bus.

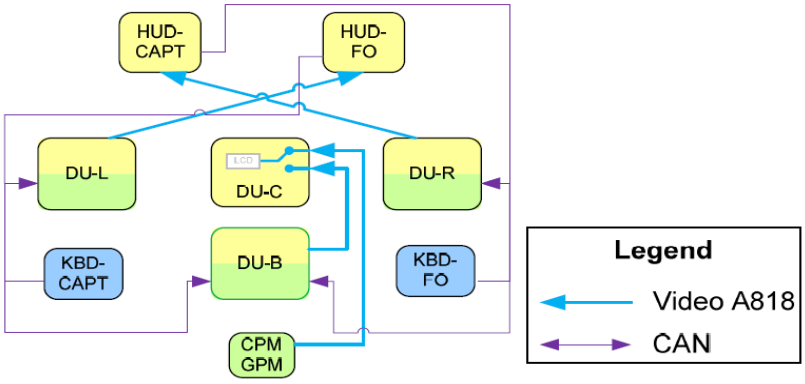


Figure 8: ARCAD internal communication means

The A818 video links are used to transmit the computed displays to the dumb elements:

- Smart DU-B (or CPM/GPM if DU-B is failed) computes the display of DU-C.
- Smart DU-L (resp. DU-R) computes the display of HUD F/O (resp. HUD CAPT).

The CAN bus is used:

- Between the keyboards and the smart DUs for data transmission (keys pressed, touchpad information, healthy status...).
- Between the HUDs and the smart DUs for specific data (healthy status,...) and not for display.

As depicted in figure 3, the other links between ARCAD resources and with A/C systems are:

- AFDX network, used for nominal communication (healthy status...) between smart DUs, CPM/GPM and CPs (which are connected to AFDX through µ-switches) and for external communication with other A/C systems.

- A818 video links: links used between the CMV and the smart DUs.
- EreBus network, composed of five EreBus stars:
  _ Smart DUs are connected to the 5 EreBus stars for external communication with other A/C systems and for internal communication when the nominal internal network (AFDX) is lost.
  _ Dumb DU-C is connected to the EreBus star Fuel&L/G, for communication with smart DUs or with CPM (tactile acquisition).
  _ CPM and GPM are connected to 2 EreBus stars: Fuel&L/G and ECS, for communication with other A/C systems.

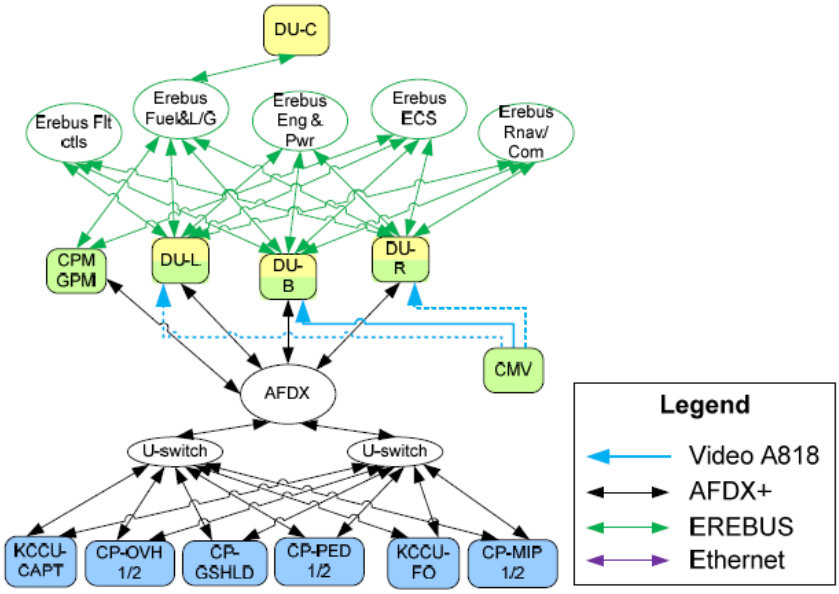


Figure 9 : ARCAD communication features

Note: The H/W controls depicted in previous figures are not the only control means. There are software controls, displayed on the DUs, with which the pilots can control A/C. In case of failure of some H/W controls, a reconfiguration occurs in order to have these controls as software controls.

4.3 The electrical system

4.3.1 Electrical system functions:

Basic core functions of the Electrical System are:

- To generate the electrical power required by the aircraft electrical loads (electrical generation system) with the required power quality and in all the aircraft configurations.
- To distribute the electrical power to all of the systems that required electrical power supply (electrical distribution system).

Another function of the electrical system is the exchange of information:

- Communication intra- and inter-system to perform electrical system functions
- Information to the cockpit/cabin crews (warning, maintenance and electrical system status)

4.3.2 Electrical system components

The electrical system (See Figure 10 for the schematic representation) is composed of:

- A 230 VAC normal network with variable frequency. It can be supplied by:
  - four (4) generators of 100 kVA with variable frequency called Variable Frequency Generator (2 VFG by engine)
  - one (1) auxiliary generator of 100 kVA in flight with constant frequency called APU Gen
  - up to two (2) ground plugs for Ground cards able to provide 90kVA.

- A 115 VAC normal network, supplied by 4 Auto Transformer Unit (ATU) of 60kVA.

- A 28 VDC normal network without power interruption (No Break Power Transfer). It is supplied by two Transformer Rectifier Units (TRU1 and TRU2) and 2 Ni-Cd batteries (BAT1 and BAT2).

- An emergency network 230VAC, 115VAC and 28VDC segregated from the normal network and with dissimilar technologies compared to the normal network.
  - The emergency 230VAC network is supplied by the normal AC network (if available) or by an electrical RAT up to 50 KVA (depending of aircraft speed and DPL) with variable frequency.
  - The emergency 115VAC network is supplied by the 2 ATU from the 230 VAC emergency network, or by the 1 static inverter from the EMER battery 1 (during RAT extension, specific shedding on RAT configuration and after landing in electrical emergency configuration).
  - The emergency DC network is supplied by the 2 TRU from the AC emergency network, or by the EMER batteries 1 and 2 (during RAT extension, specific shedding on RAT configuration and after landing in electrical emergency configuration).

4.3.3 Electrical system architecture

The complete electrical network follows those principles:

1/ Segregation between Normal and Emergency network: at least 2 separate circuits, with dissimilar technologies.
2/ For installation aspects, there is a segregation between electrical side 1 and electrical side 2: Normal (side 1 and 2) and Emergency (side 1 and 2) networks are divided in 2 separate sides.
3/ Primary and secondary distribution are in the same centre.

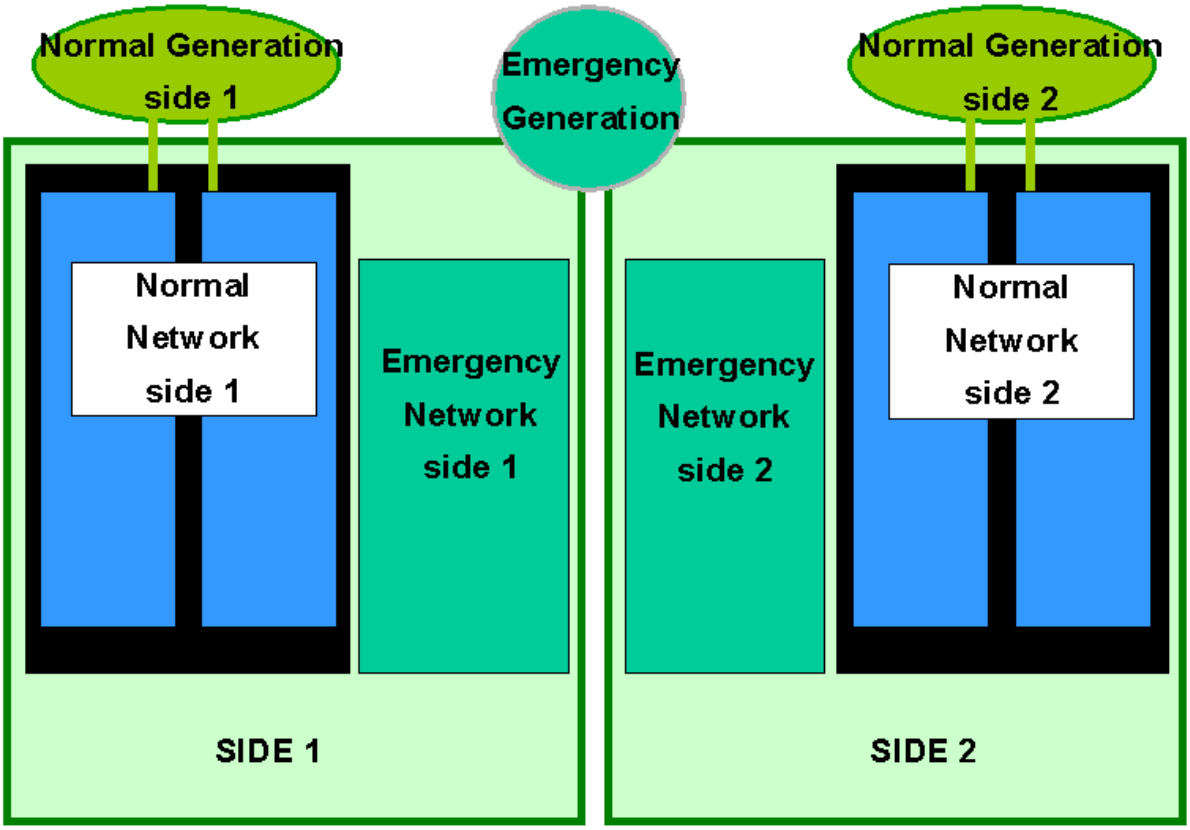


Figure 11: Electrical system architecture

4.4 The communication system

4.4.1 AFDX network:

The purpose of AFDX Network is to provide a high-rate data communication capability usable by the aircraft systems for both operational and non-operational (maintenance, data loading) data communication.

The AFDX Network performs a common service of data communication that can be defined by the following functional breakdown:

- **To switch AFDX frames**: it is the main role of the AFDX Network ensured by the switches
- **To acquire/transmit AFDX frames**: this function is supported by the End System of each AFDX Network subscriber
- **To provide Network BITE Function:** the NBF fulfills the BITE of the AFDX Network
- **To provide AFDX Network alerts**: this function enables to detect any AFDX Network failure

If the topology of the AFDX network is necessary to conduct the PRA use case, it will be provided to the relevant partners.

4.4.2 IMA (Integrated Modular Avionics) principles

The general purpose of the IMA is to provide a generic computing and data communication capability usable by aircraft systems in order to implement their functions. The IMA is made of CPIOMs and CRDCs. CPIOMs are providing computing resources to applications, CRDCs are used as remote communication gateway. The complete set of the IMA components is connected to the AFDX Network.

The IMA is composed of 2 types of components:

- **Core Processing and Input/Output Module (CPIOM)**: offers both a computation capability for software applications running on it and I/O capability (AFDX, ARINC429 and/or discrete and/or analog and/or CAN). There are 12 CPIOMs H and 9 (and 1 optional) CPIOMs J. Both CPIOM types are very similar, apart from the variety of available interfaces: CPIOMs J only are able to generate audio signals, while CPIOMs H are generating a wider variety of signals (discretes, switches, etc).
- **Common Remote Data Concentrator (CRDC)**: is used to data concentrate analogue and discrete I/O remotely and communicates serial data to/from computer processing resources on the aircraft. The CRDC also performs simple conditional logic on I/O enabling a small amount of autonomous behavior. In addition to the data concentration function the CRDC acts as an AFDX gateway from CAN and ARINC 429.

4.5 The flight control system

The primary flight control system is in charge to control the aircraft in roll, yaw and pitch axes with flight envelope protection. They generate orders from pilot interfaces or from automatic flight guidance (FG function) to control actuators. Actuators move the following surfaces :

- Ailerons (inboard and outboard), which are involved in :
  - Roll control in manual (from side sticks) or Auto Pilot (AP) (from FG) mode,
  - Gust Load Alleviation Function (GLA)
  - Manoeuvre Load Alleviation (MLA)
  - Lift augmenting
- One rudder, which allows mainly performing the yaw control and the Dutch Roll Damping. In addition, it is used to control the aircraft on the ground.
- elevators and a Trimmable Horizontal Stabilizer (THS), which allow the pitch control.
- Spoilers are used in the following functions :
  - Roll control,
  - Manoeuvre Load Alleviation Function,
  - Speed brake and ground spoiler functions,
  - Advanced Drooped Hinge Flap (ADHF)

The following generic aircraft shows the aircraft movable surfaces.

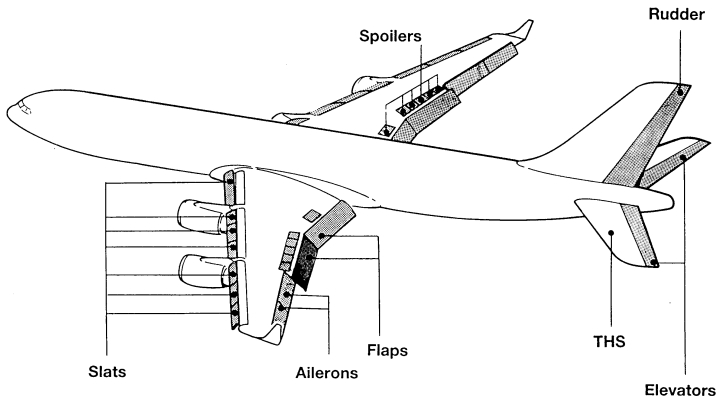


Figure 12 : Aircraft movable surfaces

Depending on the part of the flight control system that will be part of the PRA use case, some more information on the system architecture will be provided.

5 Identification of Engineering Methods

This chapter specifies the engineering Methods that of PRA interest. It is reminded that an engineering method describes how an activity can be conducted using guidelines, tools and languages which interoperate with each other.

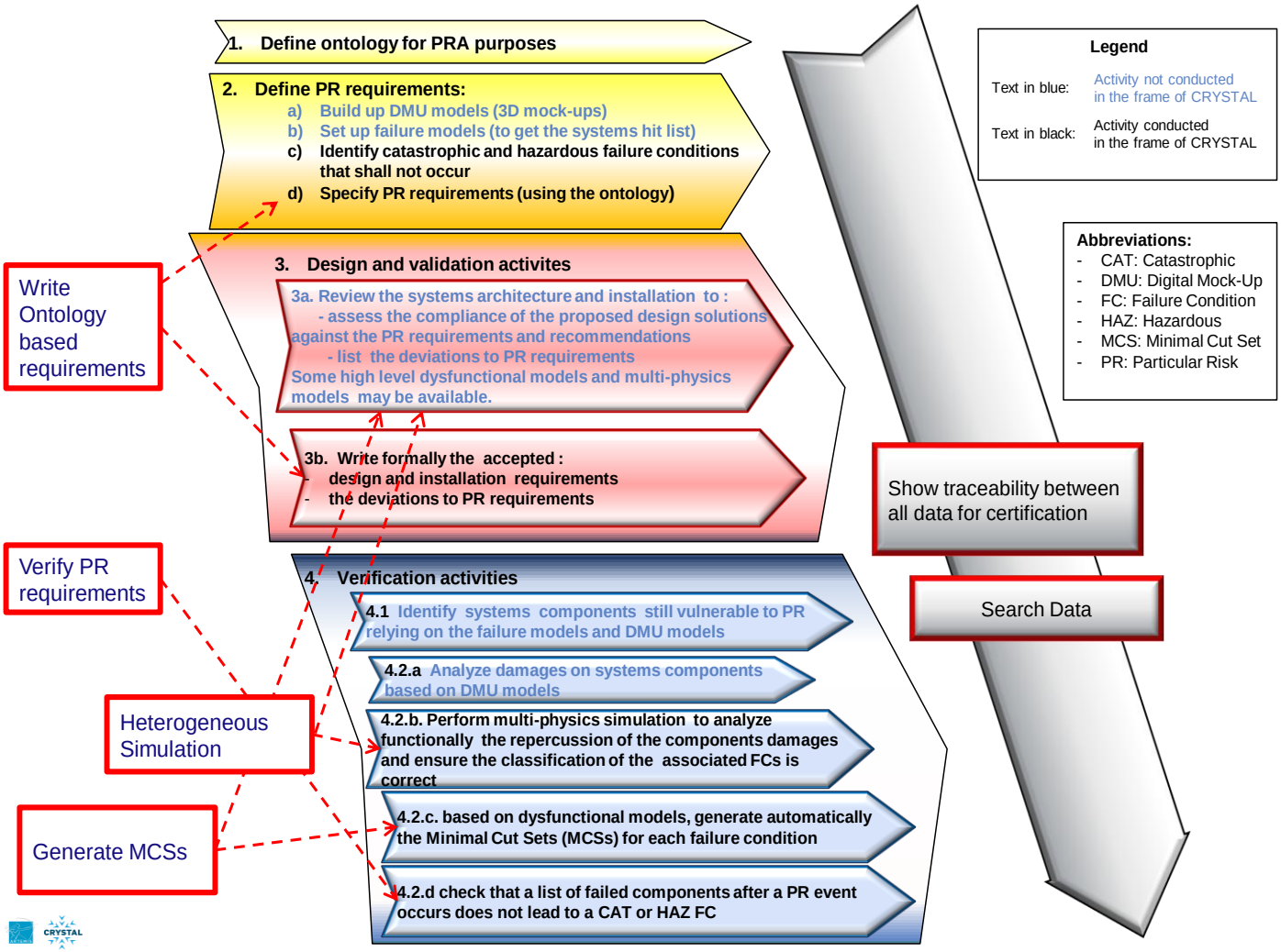


Figure 13: PRA engineering methods

As shown on the figure above, in the frame of the PRA use case, 6 engineering methods have been identified:

- Write ontology based requirements,
- Generate Minimal Cut Set (MCS),

- Verify PR requirement
- Run heterogeneous simulation
- Show traceability between all data for certification
- Search data.

5.1 Write ontology based requirements

The objective of this engineering method is to specify particular risk requirements relying on patterns and ontology, then to store the requirements in DOORS and to transfer them in SARAA.

The inputs of this engineering method are:

- The ontology in RQS
- The PR requirements patterns in RQS
- The textual regulations requirements and a high level system design

The outputs of this engineering method are:

PR requirements based ontology requirements.

The steps of the engineering methods are:

- The PR requirements are written in RAT,
- The requirements are checked in RQA,
- When the requirements are correct, they are transferred to DOORS.

The detailed description of this engineering method will be part of the next version of the use case.

5.2 Generate Minimal Cut Set

The objective of this engineering method is to generate automatically minimal cut sets from dysfunctional models and failure conditions.

The inputs of this engineering method are:

Dysfunctional models in Altarica in the RAMSES environment

List of failure conditions

The outputs of this engineering method are:

Per FC, a list of MCSs

The steps of the engineering methods are:

Get the relevant Altarica models in RAMSES,

For each FC, In RAMSES add the relevant observer

Per FC, generate the MCSs.

A detailed description of this engineering method is done in annex 1, with the reference “UC201b _Generate MCSs_002”.

5.3 Verify PR requirement

The objective of this engineering method is to check no PR event can lead to a CAT or HAZ failure condition.

The inputs of this engineering method are:

The Failure conditions relevant to the PRA and their associated MCs

PRA hit list from the Airbus Catia impact tool

The outputs of this engineering method are:

A compliance PRA report highlighting there is neither HAZ or CAT failure conditions induced by any PR event.

The steps of the engineering methods are:

- Select the Particular Risk requirements from DOORS
- Select the Failures Conditions that are relevant for this PR from SSA in SARAA
- For each Failure Condition, identify all the Minimal CutSets
- Select PRA Hit List that results from the Airbus impact tool simulation
- Compare Hit List and MCSs
- Generate the Failure Condition report that identify Failure Conditions that occur after the PR event
- Assess compliance
- Iterate after any installation modification that may have an impact on the compliance assessment.

A detailed description of this engineering method is made in annex 1, the reference is "UC201b _Verify PR requirement_001".

5.4 Run heterogeneous simulation

The objective of this method is to launch co-simulations in different simulation tools in order to analyse the functional repercussions of damaged components caused by PR events.

The inputs of this engineering method are:

The models in the appropriate languages. In our case in MODELICA, SCADE and Simulink.

The outputs of this engineering method are:

The PRA simulation results

The steps of the engineering methods are:

Select the appropriate models in DYMOLA

Select the appropriate models in SCADE and send the list to DYMOLA

Select the appropriate models in Simulink and send the list to DYMOLA

Run combined simulation in DYMOLA. The simulation models run in the different tools when it is needed. For that purpose, a request is sent by DYMOLA either to Simulink or SCADE using the FMI standard.

The detailed description of this engineering method will be part of the next version of the use case.

5.5 Show traceability between all data for certification

The objective of this engineering method is to trace all the artefacts needed to manage PRA activities.

The inputs of this engineering method are:

All the PRA data stored in the different tools

The outputs of this engineering method are:

Capability to navigate between all the artefacts and to perform impact analysis when a modification is made.

The steps of the engineering methods are:

- Select the initial data
- Select the destination data
- Set a link between the two data
- Repeat this sequence as many times as required
- Select a data
- Visualize the traceability chain

The detailed description of this engineering method will be part of the next version of the use case.

5.6 Search data

This engineering method supports search request in order to get PRA data whatever the tool in which they are stored. In order to meet this objective, a search engine has to be provided.

The inputs of this engineering method are:

All the PRA data

The outputs of this engineering method are:

The data corresponding to the search request

The steps of the engineering methods are:

- Write the appropriate search request in the search engine
- Send the request to all the tools
- Receive the data from the tools
- Provide the list of searched data to the user.

The detailed description of this engineering method will be part of the next version of the use case.

6 Terms, Abbreviations and Definitions

AA	Airworthiness Authorities
A/C	Aircraft
AMC	Acceptable Mean of Compliance
ATA	Air Transport Association of America
CPO	Central Program Office
CG	Centre of Gravity
DCS	Designated Certification Specialist
DMU	Digital Mock-Up
FC	Failure Condition
FQMS	Fuel Quantity Management System
FHA	Functional Hazard Analysis
GAM	Global Aircraft Mock-up
MMEL	Master Minimum Equipment List
PDD	Process Description Document
PR	Particular Risk
PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
RAT	Ram Air Turbine
SAM	Space Allocation Mock-up
SR	Safety Representative
SSFP	Site Safety Focal Points
TO	Task Owner
UERF	Uncontained Engine Rotor Failure
ZSA	Zonal Safety Analysis

7 Annex I: Detailed Description of the Engineering Methods

Engineering Method: UC201b _Generate MCSs_002					
Purpose: For each identified FC, generate MCSs (Minimal Cut Set) from dysfunctional models					
Comments:					
Pre-Condition		**Engineering Activities (made of steps)**		**Post-Condition**	
* dysfunctional Altarica models are available in RAMSES (customized environment of Safety Designer provided by Dassault Ssystème) * the failure conditions and the associated RAMSES models references are stored in the Airbus safety tool called SARAA * an o		1. in the orchestration tool, launch service "get list of Failure conditions" 2. Request is forwarded to SARAA 3. SARAA sends back the list of requested failure conditions 4. in the orchestration tool, launch service "get MCSs list corresponding to the li		* MCSs are generated and stored in SARAA	
Notes:				Notes:	
Artefacts Required as inputs of the Activities		**Artefacts used internally within the Activities (optional)**		**Artefacts Provided as outputs of the Activities**	
Name	Failure condition	Name		Name	Minimal Cut Set (MCS)
Generic Type: (Tool or language independend type)	Safety data	Type:		Generic Type: (Tool or language independend type)	Safety data
Required Properties: (Information required in interactions between steps)	Failure condition number	Properties:		Provided Properties: (Information provided in interactions between steps)	Version List of components
Description & Interoperability Additional Constraints:		Description:		Description & Interoperability Additional Constraints:	
Name	Dysfunctional models	Name		Name	
Generic Type: (Tool or language independend type)	Altarica models	Type:		Generic Type: (Tool or language independend type)	
Required Properties: (Information required in interactions between steps)	Model version Model name	Properties:		Provided Properties: (Information provided in interactions between steps)	
Description & Interoperability Additional Constraints:		Description:		Description & Interoperability Additional Constraints:	

Engineering Method: UC201b _Verify PR requirement_001					
Purpose: the safety designer would like to check that a list of failed components after a PR (particular Risk) event occurs does not lead to a catastrophic(CAT) or hazardous(HAZ) Failure Condition (FC)					
Comments:					
Pre-Condition		**Engineering Activities (made of steps)**		**Post-Condition**	
* the PR requirements are stored in an Airbus tool called MV2 * the DMU models are available in the Catia environment * the failure conditions and the associated minimal cut sets (MCS) are stored in the Airbus safety tool called SARAA * the failure model		1. in the PR checker, launch service "get list of PR requirements" 2. Request is forwarded to MV2 (that manages the PR requirements) 3. MV2 sends back to the PR checker the list of PR requirements 4. in the PR checker, launch service "get the PR hit list"		* PR report document highlighting: * the HAZ and CAT FCs, * the discrepancies between the hit list and the MCSs * Visualization in the DMU models of the MCSs associated to CAT and HAZ FCs	
Notes:		Notes:		Notes:	
Artefacts Required as inputs of the Activities		**Artefacts used internally within the Activities (optional)**		**Artefacts Provided as outputs of the Activities**	
Name	Failure condition	Name		Name	Failure condition
Generic Type: (Tool or language independend type)	Safety data	Type:		Generic Type: (Tool or language independend type)	Safety data
Required Properties: (Information required in interactions between steps)	Failure condition number	Properties:		Provided Properties: (Information provided in interactions between steps)	Failure condition number
Description & Interoperability Additional Constraints:		Description:		Description & Interoperability Additional Constraints:	
Name	Minimal Cut Set (MCS)	Name		Name	DMU models
Generic Type: (Tool or language independend type)	Safety data	Type:		Generic Type: (Tool or language independend type)	3D model
Required Properties: (Information required in interactions between steps)	Version List of components	Properties:		Provided Properties: (Information provided in interactions between steps)	Model name Model version
Description & Interoperability Additional Constraints:		Description:		Description & Interoperability Additional Constraints:	
Name	DMU and failure models	Name		Name	
Generic Type: (Tool or language independend type)	3D models	Type:		Generic Type: (Tool or language independend type)	
Required Properties: (Information required in interactions between steps)	Model version Model name	Properties:		Provided Properties: (Information provided in interactions between steps)	
Description & Interoperability Additional Constraints:		Description:		Description & Interoperability Additional Constraints:	
Name	Requirements	Name		Name	
Generic Type: (Tool or language independend type)	Natural language requirement	Type:		Generic Type: (Tool or language independend type)	
Required Properties: (Information required in interactions between steps)	Requirement ID Requirement version Requirement statement	Properties:		Provided Properties: (Information provided in interactions between steps)	
Description & Interoperability Additional Constraints:		Description:		Description & Interoperability Additional Constraints:	