L-1.1 Consistency Process of Systems Engineering (SE) and Safety Analysis (SA) activities

DATE: 07/2021

Summary

The objective of this document is to describe the exchange process between systems engineers and safety analysts, and to recommend what should be done in terms of traceability, reviews, etc to ensure the consistency of this process.

Author(s)	*Function(s) & name(s)*	*Researcher*	*H.Fadiaw* *A.Dubois* *A.Awadid* *R. Demachy*
Approver	*Function & name*	*Project leader IRT Saint Exupéry*	*F. Lacrampe*
		Project Manager IRT SystemX	*A. Dubois*

Table of Contents

Evolutions

Version	Date	Modified §	Modification summary	Modified by
V1	July 2021	All	Creation	Afef Awadid, Anouk Dubois

1 Introduction

1.1 Objective of the document

As mentioned earlier, this document aims to describe the exchange process between systems engineers and safety analysists teams that ensures overall consistency and maintains it over time. For the sake of simplicity, this we designate this process as Systems Engineering (SE)/ Safety Analysis (SA) process is called SE/SA in the rest of the document.

This document has been produced in the context of the WP1 of the S2C project, which aims at defining such an SE/SA exchange process by explaining how the data are exchanged between Systems Engineering and Safety Analysis disciplines. Moreover, this objective is to recommend what should be done in terms of traceability, reviews, and so on, to ensure the consistency of such a process. In this its first version, this document presents 2 types of results:

- An experience feedback from S2C project partners on existing SE/SA processes and their limitations
- A graphical representation of some aspects of the SE/SA process.

In a next version, process recommendations to support SE/SA consistency will be detailed.

1.2 Organisation of the document

The document is organised as follows:

- Section 1 gives bibliography linked to this document and acronyms explanation.
- Section 2 “ARP Process” quotes how ARP4754A and ARP4761 mention consistency, review or traceability items, since these guidelines are the basics of the process to be constructed. More particularly, it focuses on safety analyses and the ARP point of view.
- Section 3 " SE/SA Process: S2C partners practices” presents a feedback of S2C partners internal practices in terms of SE/SA process: different project partners have been interviewed with involvement of System and Safety engineers or Experts to catch current process and areas of improvement.
- Section 4 presents a first graphical representation of the SE/SA process. This representation will be completed and improved in a future version of this document.
- Section 5 is an overall conclusion of this document, along with some perspectives.

1.3 Documentation and terminology

1.3.1 Related Documentation

- ARP 4754A
- ARP4761

1.3.2 Terminology

WP	Work Package
AFHA	Aircraft Functional Hazard Analysis
ASA	Aircraft Safety Assessment
FC	Failure Condition
PASA	Preliminary Aircraft Safety Analysis
PSSA	Preliminary System Safety Assessment
SA	Safety Analysis
SE	System Engineering
SFHA	System Functional Hazard Assessment
SSA	System Safety Assessment

2 ARP Process

This SE/SA exchange process is carried out in an aeronautical context that is framed by a set of guidelines including ARP4754A and ARP4761. These guidelines outline the analyses and activities to be carried out to design an aircraft. Thus, our work on SE/SA exchange process is strongly framed by the process described in ARP4754A, which is presented below.

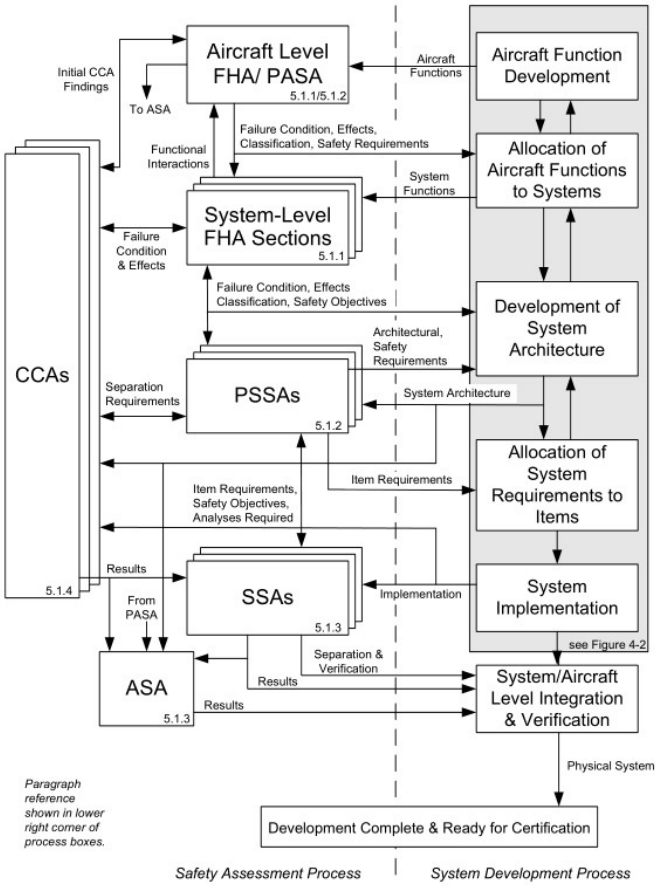


Figure 1 – ARP Model of SE/SA Exchange Process (cf. ARP 4754A)

Figure 2 summarizes safety analyses (left) and system engineering activities (right), along with the data exchanged between them.

The ARP process presented above constitutes the basis of our study. For that reason, we first investigated how ARP4754A and ARP4761 deal with consistency by:

- Quoting all mentions to “consistency”, “review” or “traceability terms. These terms are indeed key concepts for consistency process.
- Focusing then more precisely on Safety analyses and SE/SA process specificities.

The following section describes thereby the starting point for the SE/SA consistency process.

2.1 Consistency

The main ways that are mentioned by the ARP4754A to establish consistency is to use requirement development plan (to support requirement consistency), and to encourage communication between development teams (cf. Section 5.3 in ARP4754A).

The ARP puts a particular emphasis on the consistency across the requirement set. Indeed, it advocates two ways to ensure this consistency: (1) the development of review plans (cf. Figure 2 in ARP4754A) and (2) the establishment of requirement development plans and standards (cf. Section 5. 3).

2.2 Traceability

Development plan is closely linked to the term “traceability” that is often mentioned in ARP.

The traceability is defined by the ARP4754A as the recorded relationship between two or more elements of the development process. For example, between a requirement and its source or between a verification method and its requirement (§2.2 section Definitions in ARP4754A). Indeed, the ARP4754A highlights the traceability links between the derived requirements (those emerging from the function requirements allocation process) and the associated Failure condition classification. The goal is to determine the impact of these derived requirements on safety analysis (see ARP4754A page 26). Another traceability links that are considered in the ARP4754A are those between requirements and software architecture, and between requirements and hardware architecture. These links aim to ensure that derived requirements are captured and that all function requirements are achieved in the implementation (see ARP4754A – Page 30). Moreover, according to the ARP4754A, if the FHA is constructed in system-oriented sections, traceability of hazards and Failure Conditions between the aircraft-level and system-level is necessary (cf. Section 5.1.1).
In summary, the ARP4754A presents the traceability as requirements validation methods. Indeed, Traceability is defined as an essential component of validation of the aircraft, systems and items requirements (Bi-directional flow of requirements). The requirement should either be traceable to a parent requirement, or by identification of the specific design decision or data from which the requirement was derived (cf. Section 4.5.6 Validation methods).

Traceability by itself may be sufficient to demonstrate that a lower level requirement satisfies a higher level requirement with regards to completeness. However, where additional value has been added through design decisions or detail, additional rationale should be captured. This rationale should document how the lower level requirement(s) satisfy the parent requirement. Some lower level requirements may not be traceable to a parent requirement (i.e. derived requirements); these requirements should have rationale to document their validity (cf. Section 4.5.6 Validation methods).

2.3 Review

Besides traceability, engineering review is introduced in the ARP4754A as another requirements validation method. Against this background, the engineering review is advocated in the case of untraced requirements

(derived requirements). In fact, untraced requirements should be reviewed to determine whether they are (cf. ARP4754A page 62):

- derived as part of the development process, or;
- developed from a missing parent requirement that may be added, or;
- assumptions that need to be managed.

Furthermore, derived requirements should be examined to determine which aircraft-level function (or functions) they support so that the appropriate Failure Condition classification can be assigned and the requirement validated. While derived requirements will not impact the higher-level requirements, some may have implications at higher levels. Derived requirements should be reviewed from a safety perspective (i.e. impact on safety analyses) until it is determined that no further impact is propagated (cf. ARP4754A, page 53).
To assist the engineering review activity, the ARP4754A advocates the use of templates and checklists. As a matter of fact, according to the ARP, checklists may be used by reviewers for completeness checks of a set of requirements. The checklist should cover all areas that have a primary interest in the system and their applicable interfaces to insure that their needs and expectations will be satisfied. In this vein, the ARP4754A provides the following guidelines to assist in developing checklist questions for assessing the completeness at each hierarchical level of requirements. This list should be tailored for the specific application (cf. ARP4754A , page 60):

a. Is it apparent from the traceability and supporting rationale that the requirement(s) will satisfy the parent requirement?
b. Are all owners of interfacing systems or processes represented in the systems requirements set?
    (1) All Higher level functions allocated to this system fully covered.
    (2) Safety requirements represented
    (3) Regulatory standards and guidance represented
    (4) Industry and company design standards represented
    (5) Flight operations and maintenance scenarios represented
c. Are all interfaces to other systems, people and processes identified?
d. Are the constraints (e.g. protocol, mounting configuration, and timing) associated with each interface defined in sufficient detail for the interface to be realized?
e. Are the system, people or process behaviors that result from an interface, agreed to and captured as requirements on both sides of the interface? For example an engine system may provide data to a flight display system. How that data is used in the flight display system and how the crew interface requirement with the engine control system owner. Another example is the flight crews input to the throttles input to the engine which results in engine thrust behavior. The expected thrust behavior should be agreed to and captured as requirements with the flight crew or those that represent flight crews in general.
f. For a required behavior, should there be an associated prohibited behavior defined and if yes, is the prohibited behavior defined?
g. Is the functional requirements set fully allocated and traced to the system architecture?
h. Does the functional allocation clearly allocate between electronic hardware and software in the system architecture?
i. Are assumptions adequately defined and addressed?

In the following subsections, we focus on the safety analyses specificities regarding the SE/SA process.
We sorted SE and SA elements of ARP Process into tables that sum up:

- The inputs and outputs of the Safety analyses
- The roles and responsibilities described in the ARPs
- Recommendations of the ARP regarding tools
- The transition criteria (activity stopping conditions),
- Recommendation of the ARP regarding traceability or review practices.

Below are all the tables that have been produced as a result of this work.

2.4 AFHA Aircraft Functional Hazard Assessment

Activity	AFHA
Description	Examines aircraft functions to identify potential functional failures and classifies the hazards associated with specific failure conditions. The FHA is made early in the development process and is updated as new functions or Failure Conditions are identified. Thus, the FHA is a living document throughout the design development cycle.
Input(s)	- The list of the aircraft functions (e.g., lift, thrust, etc.) - Operational conditions: crew awareness, Flight phases, operational events, environmental events & conditions
Output(s)	- Safety requirements which are composed of • Aircraft-associated failure condition list • Classification of each Failure Condition based on the assessment of FC effects: FDAL • Safety Objectives (quantitative objectives of FCs) - List of hypotheses that have an impact on the FC list and to be verified later in the development (allows the emergence of new safety/test/qualification requirements ...)
Organisation: Roles and responsibilities	What does the ARP say: 5.2 Aircraft Level FHA and PASA A team led by the Aircraft Safety Group is responsible for developing the Aircraft Level FHA and for ensuring that all system level FHAs are consistent with other system FHAs and with the aircraft FHA. This team will also be responsible for preparing a Preliminary Aircraft level Safety Assessment (PASA) based on the aircraft FHA, with refinement over the course of the development program. This team will assess the effects of individual and combined system failures on aircraft level functions. From this activity, safety requirements (for example functional separation requirements to ensure that combinations of system failures do not compromise continued safe flight and landing) can be generated and submitted into the requirement database with appropriate compliance owner and affected owners. The team will have the responsibility to track the functional hazard status to closure. The Aircraft level FHA is complete when all functional hazards have been identified and addressed. Organization / Roles and Responsibilities Aircraft Safety Group / Develop and document Aircraft Level FHA Design / Provide input and review of Aircraft Level FHA 5.2.1 Continued Safe Flight and Landing Functions List: The Aircraft Safety Group will provide the program with the list of functions that are required for Continued Safe Flight and Landing. This list is used to help determine the architectural layout of the aircraft. Organization / Roles and Responsibilities Aircraft Safety Group / Develop Continued Safety Flight and Landing functions list Design / Review and concur with the list and use to determine architecture and capabilities As a conclusion: Leader of AFHA is safety aircraft department, which supervises overall works, but the safety analyses re in general co-written by both safety analyst and system engineer
Tools/methodology	Referring to the ARP 4761, to the Aircraft level FHA is associated the Fault Tree, and hence the fault tree construction and analysis tools.
Traceability	What does the ARPs say :

	A.4 FHA OUTPUTS: A.4.1 Documentation: The results of the FHA process should be documented so that there is traceability of the steps taken in developing the FHA report. The following information should be documented during the FHA process. •
Review	Linked to FTA usage, ARP mentions following needs : FTA usage includes: a. Facilitation of technical/certification authority assessments and reviews. (The completed fault tree displays only the failure events which could individually or collectively lead to the occurrence of the undesired top event.)

2.5 *PASA – Preliminary Aircraft Safety Assessment*

Activity	PASA
Description	Establish the aircraft or specific system or item safety requirements and provide a preliminary indication that the anticipated aircraft or system architectures can meet those safety requirements. The PASA is updated throughout the system development process ultimately resulting in the Aircraft Safety Assessment (ASA).
Input(s)	List of FCs from the AFHA Aircraft architecture (allocation of aircraft functions to systems) Operational conditions
Output(s)	Evaluation of FCs: quantitative and qualitative requirements (failure conditions for systems, DAL requirements, independence requirements, design requirements (monitoring, prohibition of DAL reduction, ...)
Organisation: Roles and responsibilities	What does the ARPs say: 5.2 Aircraft Level FHA and PASA A team led by the Aircraft Safety Group is responsible for developing the Aircraft Level FHA and for ensuring that all system level FHAs are consistent with other system FHAs and with the aircraft FHA. This team will also be responsible for preparing a Preliminary Aircraft level Safety Assessment (PASA) based on the aircraft FHA, with refinement over the course of the development program. This team will assess the effects of individual and combined system failures on aircraft level functions. From this activity, safety requirements (for example functional separation requirements to ensure that combinations of system failures do not compromise continued safe flight and landing) can be generated and submitted into the requirement database with appropriate compliance owner and affected owners. The team will have the responsibility to track the functional hazard status to closure. The Aircraft level FHA is complete when all functional hazards have been identified and addressed. Organization / Roles and Responsibilities Aircraft Safety Group / Develop and document Aircraft Level FHA Design / Provide input and review of Aircraft Level FHA 5.2.1 Continued Safe Flight and Landing Functions List: The Aircraft Safety Group will provide the program with the list of functions that are required for Continued Safe Flight and Landing. This list is used to help determine the architectural layout of the aircraft. Organization / Roles and Responsibilities Aircraft Safety Group / Develop Continued Safety Flight and Landing functions list Design / Review and concur with the list and use to determine architecture and capabilities

Tool(s)/Methodology	No information in the ARPs
Traceability	Recommended by the ARPs: • With AFHA (SA/SA)
Review	No information is available in this regard.

2.6 SFHA – System Functional Hazard Assessment

Activity	SFHA
Description	Examines system functions to identify potential functional failures and classifies the hazards associated with specific failure conditions. The FHA is developed early in the development process and is updated as new functions or Failure Conditions are identified. Thus, the FHA is a living document throughout the design development cycle.
Input(s)	Failure Conditions, effects, classification and Safety requirements from AFHA System functions from the activity of allocation of aircraft functions to systems
Output(s)	Safety requirements which are composed of: 1. System-associated fault configuration list consisting of: a. Failure Condition(s). b. effects of the Failure Condition(s). c. Classification of each Failure Condition based on the identified 2. List of hypotheses that have an impact on the configuration list of faults to be checked in the further developments
Organisation: Role and responsabilites	What does the ARPs say Organization / Roles and Responsibilities Aircraft Safety Group / Ensure the System Level FHAs are performed in accordance with FHA Manual Design / Prepare the System Level FHAs
Tool(s)/Methodology	Referring to the ARP 4761, to the FHA is associated the Fault Tree, and hence the fault tree construction and analysis tools.
Traceability	What does the ARPs say : A.4 FHA OUTPUTS: A.4.1 Documentation: The results of the FHA process should be documented so that there is traceability of the steps taken in developing the FHA report. The following information should be documented during the FHA process.
Review	Linked to FTA usage, ARP mentions following needs :

	FTA usage includes: a. Facilitation of technical/certification authority assessments and reviews. (The completed fault tree displays only the failure events which could individually or collectively lead to the occurrence of the undesired top event.)
Consistency	5.3.1 FHA Manual: Safety should prepare a Functional Hazard Assessment Manual to aid the designers in accomplishing the task. This will help to ensure consistency in the FHA results

2.7 PSSA – Preliminary System Safety Assessment

Activity	PSSA
Description	Establish the aircraft or specific system or item safety requirements and provide a preliminary indication that the anticipated aircraft or system architectures can meet those safety requirements. The PASA and PSSA are updated throughout the system development process ultimately resulting in the Aircraft Safety Assessment and System Safety Assessments. It is a systematic examination of a proposed architecture(s) to determine how failures could cause the Failure Conditions identified by the FHA. The objectives of the PASA and PSSA are to complete the safety requirements of an aircraft, system or item and validate that the proposed architecture can reasonably be expected to meet the safety requirements.
Input(s)	"safety" rules from the aircraft manufacturer SFHA (FC list) System architecture
Output(s)	Safety requirements for system architecture Safety requirements for Item level Safety requirements for interfaces Information to be traced back to the aircraft level (impacts)
Organisation: roles and responsibilities	What does the ARP say: Aircraft Safety Group: ensures the application of model methods and data consistency Design: Perform PSSA and implement changes required.
Tool(s) / methodology	No information in ARP on specific tools but ARP recommend Fault tree Analysis
Traceability	Recommended by the ARPs: • With SFHA (SA/SA) (extract from ARP4761: Traceability should be demonstrated between requirements established in the FHA/PSSA) • With the activity Development of system architecture (SA/SE)
Review	ARP4754A recommends a review according to the DAL

2.8 SSA - System Safety Assessment

Activity	SSA
Description	Collects, analyses, and documents verification that the aircraft and systems, as implemented, meet the safety requirements established by the PSSA.
Input(s)	a. System architecture b. Systems interfaces List of FCs c. Results of verification data which include: Common Cause Analyses results and reliability data of subsystems and interface failure probabilities (quantitative system data), maintenance intervals associated with hidden failures ...
Output(s)	Determination of compliance with regulatory safety requirements: • FCs list with severity and probability of occurrence • Justification of software and hardware DALs in relation to FCs • Justification of independence for systems with independence requirements • establishing compliance with the requirements allocated to systems by internal processes
Organisation: roles and responsibilities	What does the ARPs say: • Design Create the SSA. • Aircraft Safety Group Participates in the SSA. Program Engineering Review and approve the SSA. **Organization** / **Roles and Responsibilities** Design / Create the SSA. Aircraft Safety Group / Participates in the SSA. Program Engineering / Review and approve the SSA. **Organization** / **Roles and Responsibilities** Design / Create the SSA. Aircraft Safety Group / Participates in the SSA. Program Engineering / Review and approve the SSA.
Tool(s)/Methodology	No information is available in the ARPs
Traceability	Traceability • with the output requirements of FHA (SA/SA) • With system architecture (SE/SA) (be sure that the system architecture doesn't introduce new FCs)
Review	No specific information is available in the ARPs

3 SE/SA Process: our partners practices

3.1 Overview of the conducted interviews

The interviews carried out with our industrial partners aims to capture the SE/SA exchange process from the practical standpoint. An overview of the conducted interviews is given in Figure 3.

Figure 2- Overview of the interview dates and participants

In line with what has been mentioned previously, the main objective of the interviews is to understand the internal practices of each industrial partner regarding exchanges between SE and SA teams. This aims to provide a clear picture of how SE and SA teams collaborate and exchange their complementary expertise. To do so, many questions have been raised during the interviews conducted with the different industrial partners. Below, we provide an overview of these questions:

- Do you have a formalized process for exchanges between your SE and SA teams?
- In your opinion, what prerequisites are necessary to carry out these exchanges? System engineers with sufficient knowledge of safety? Co-engineering approach (separate responsibilities but frequent exchanges between the system and safety teams)? Others?

- What are the key roles in the SE/SA process?
- Are traceability activities a priority? How do you manage traceability? By what means? What artifacts are involved?
- How do you manage consistency in the SE/SA process?
- How do you perform SE/SA Reviews?
- What elements/ activities/ artifacts need to be consistent?
- What do you think of the idea of implementing a checklist mechanism to avoid the potential loss of knowledge?

3.2 Dassault Aviation feedback

3.2.1 Existence of SE/SA exchange process

An SE/SA exchange process has recently defined by Dassault Aviation in order to support one of their programs. However, it is not yet rigorously applied. Indeed, its formalized activities are sometimes seen as time consuming or less priority, especially when they are not carried out at the right time. Nevertheless, it is

worth noting that the design/system teams' representatives of Dassault Aviation express their need for a shared process with their industrial partners (viz., the system suppliers).

SE/SA exchanges are present at Dassault Aviation but are more characterized by physical and relational co-engineering between SE and SA teams than by formal links or activities between them. This co-engineering is characterized by frequent iterations between the SE and SA teams, with safety practices knowledge on the side of the SE manager. Indeed, the latter has the safety knowledge that allows him/her to understand the safety issues and impacts on his/her SE perimeter. For example, he adjusts the functional decomposition taking into account the safety issues and objectives (DAL), the objective being to propose a decomposition that allows the safety objectives to be grouped together and avoids all functions being DAL A.

3.2.2 Roles in the SE/SA exchange process

A key role in the SE/SA exchange process, in Dassault Aviation, is the Technical Officer (Technical Coordinator). The latter does not validate the design and safety documents. Instead, he is the responsible for their production. These documents are then reviewed and validated by the technical design and safety business referents. One of the objectives is to take into account and identify safety issues, as early as possible, in the design process, while involving different disciplines (technical, safety and other experts).

3.2.3 Aircraft manufacturer/ system supplier interaction

At Dassault Aviation, the contractual relationship is based on the use of a non-compliance matrix to trace the functions and requirements to which the system supplier is not committed and which may require a reallocation to another system. This means that the non-compliance matrix is fulfilled by the supplier, where he notes which functions he can't handle. The aircraft manufacturer should then revise the allocation. Once these reallocations have been made, the system specifications are updated.

The interactions between the aircraft manufacturer and the system supplier are characterized by co-engineering efforts. For the preliminary design phase, these interactions rely on physical workspaces, which bring together all the teams: design and safety representatives of both aircraft manufacturer and system supplier. The goal of using physical workspaces is to facilitate interactions and alignment of the preliminary design definitions. These workspaces are a strong vector of consistency in development.

3.2.4 Activities in the SE/SA exchange process

SFHA

A scenario-based approach is used to carry out the SFHA, in line with classic operational and functional analysis practices in systems engineering. The Failures Conditions described in the SFHA are based on the functions failures identified during the functional analysis (Hazard Table). The SFHA are completed by PFSS (Post Failure Situation Sheet) which describe the main system failure scenarios leading to these hazardous events and the effects on the aircraft, the crew and the passengers. Finally, it is worthwhile to remember that SFHAs are all produced by Dassault Aviation.

Review

After the Preliminary Design Review, each system supplier continues its detailed design on its own. Agile co-engineering is replaced by formal Aircraft manufacturer /Systems suppliers reviews to validate a first baseline of the system specification, and then to validate each update delivery. Once the critical design review has been completed (the baseline is frozen), all modifications are made through a change request process. Beyond these formal reviews, there is a regular dialogue between the different design/ safety teams of both aircraft manufacturer and systems providers.

These formal reviews between the aircraft manufacturer and the system suppliers are accompanied by the uploading of the system specification and its functional and logical architecture (system functional analysis) into the aircraft manufacturer's IS tool. This enables the aircraft manufacturer based on the performed analysis to check the consistency of the aircraft manufacturer/system requirements and, in particular, to justify the non-impact of the refined/derived requirements of the system manufacturer on the aircraft level safety objectives. Thus, the functional decomposition of the system at ranks 1 and 2 (as well as the interface elements with the other systems) are recovered in the DA work environment. This retrieval is limited to a notion of re-import, and does not consist in an integration of the data in the aircraft manufacturer's environment. The consistency between the detailed definition data and the global definition data is however ensured by reviews.

Note that at Dassault Aviation, the SE/ SA co-engineering is punctuated by peer reviews with experts, organized throughout the development process at the main project milestones, to verify/validate the overall consistency and that nothing has been forgotten. The results of these reviews are necessary to declare the design valid.

Traceability

Safety requirements are managed in the same way as System requirements. As a result, at Dassault Aviation there is no need for a formal traceability link between the safety requirement and the system requirement, as both are in the same document. Today, the Rational of the safety requirement can be used to notify the analysis that allowed the identification of this requirement ("PSSA", "SFHA" ...). Moreover, the safety requirements are treated, in a similar way as all the other types of requirements, in terms of refinement.

It should be noted that the Dassault Aviation IS tool is the 3DExperience platform of Dassault Systèmes. This platform integrates (according to the RFL principle):

- The aircraft level requirements base
- The system level requirements base
- The package level requirement base (to manage the supplier's solution).
- Functional modeling: functions, interfaces, functional breakdown structure (FBS) refinement
- Traceability links between requirements and functions
- Logical modeling with formal function/component traceability/ allocation links

Based on this, the traceability is performed using the 3DX platform. Three types of traceability links can be considered:

- Requirements/ Requirements: a traceability link between two different levels of requirements (R/R link).
- Requirements/ Models: a traceability link between requirements and functions (R/F link). By a model, we refer to the formalization of the functional analysis by a model. An important point to note, here, is that the two first traceability links (viz., R/R and R/F links) are supported by the 3DX platform.
- Models/ Models: a traceability link between a functional model and a logical model (F/ L link). In this context, it is worth mentioning that no tool links to date with the Tree or SA model in Cecilia.

3.3 Thales feedback

3.3.1 Existence of SE/SA exchange process

There is no official process at Thales that formalizes SE/SA exchanges, and even less so at the level of the Thales group, as each entity of the group may have some leeway. Coordination between these two disciplines occurs rather naturally, and can fluctuate according to Thales entities and teams. Due to differences in culture between entities, different possible interpretations, of what the safety process should be may exist. Moreover, there are differences in safety needs according to systems to be designed.

Nevertheless, elements of the framework for operational safety are present (in addition to the ARP) in the business and operating processes management system, defined in the Thales process repository called "Chorus 2.0". Chorus is a set of processes dedicated to the engineering domain in the broadest sense of the term, and applied in all Thales business units Chorus defines the roles and responsibilities of these roles, without focusing on the "how". However, it gives references to practices or tools to deal with them. "Architect" and Project Design Authority (PDA) are examples of roles defined in Chorus. These roles are decisive in the exchanges between the system supplier and the aircraft manufacturer.

3.3.2 Roles in the SE/SA exchange process

At Thales, the SE/SA roles are as follows:

- The SE architect: drives/performs system engineering work
- The SA analyst: pilots/performs the safety work
- The PDA: validates the SE specifications by ensuring the compatibility of the work with Safety requirements.

The role of the PDA may vary according to the size of the project: on small projects and small teams, the PDA is only responsible for the architecture. On larger projects, the architect is responsible of both SE and SA.

The interviewees indicate that the systems engineer must have a fairly extensive operating safety culture, enabling him to ensure that the design of a system meets the safety objective (in fact, knowing the hazardous events and criticality can lead to constraints on the duplication of organic components). This dual competence is mentioned in the Chorus: the roles "architect" and "PDA" must have competence in "operational safety".

These roles are part of a co-engineering context between SE and SA teams: separate responsibilities but frequent exchanges. The SE and SA teams interact in the description of the types of failures, in the way these failures propagate, and in the re-reading of the fault trees from PSSA/SSA. In general, it is the SE entity that verifies the trees/results of the SA entity, because it is less easy for the safety engineer to read an architecture, and as he participates in the project in a more punctual way.

3.3.3 Aircraft manufacturer/ system supplier interaction

Today, the relationship between the aircraft manufacturer and Thales is a usual contractual relationship characterized by:

- The aircraft manufacturer providing the aircraft level specification elements.
- Reviews are carried out at project milestones to share the aircraft manufacturer's needs or requirements and verify Thales' response to the aircraft manufacturer's needs.

However, this contractual relationship is accompanied by co-engineering approaches with collaborative work in plateau mode, depending on the project phases.

It should be noted that Thales TRT is considering to define an interaction contract, the objective being to define the right level of visibility between the aircraft manufacturer and the system supplier, and to provide (and contract) the right level of abstraction in the specifications.

3.3.4 Activities in the SE/SA exchange process

SFHA

Thales indicates that the SFHA analysis is not necessarily done by the system supplier, as it depends on the type/importance/issue of the system. Generally, there are two cases depending on whether the system is specific or more generic, interchangeable and reusable, and where certification can then simplify the reuse process:

- The case where the system does not have its own certification: in this case, the SFHA analysis is not carried out on the system supplier side, but on the aircraft manufacturer side. In this case, Thales directly recovers the FHA (Failure Condition) results and implements the PSSA analysis. As the SFHA is linked to the proposed architecture, a feedback is provided between the aircraft manufacturer and Thales, via formal reviews or informal meetings.
- The case where the system has its own certification: the SFHA analysis is necessary for certification and the analysis is carried out on the system supplier's side. These are cases of generic, interchangeable, reusable systems, or in the case of product lines of avionics systems, where a certification can be performed upstream. In this case, the system supplier certifies his system Technical Standard Order (TSO) process, and the implementation of the SFHA analysis at system level is necessary.

Thales points out that the SFHA exercise asks to specify the hazardous events and the criticalities (definition in a generic way). On the APs (Automatic Pilots), oscillating and slower failures (...) are known, but the criticality may depend on the machine. Thus, the definition of "criticality" is not easy and may require the experience of the pilots.

SE/SA Review

Thales conducts internal reviews at the time of milestones, which involve the various SE and SA experts. However, the discussions take place mainly before the milestones, the objective is to avoid discovering scoops during the review. These prior exchanges are not formalized, as the process is not clearly defined. During these reviews, the focus is mainly on the safety analysis of new technologies.

The use of the checklist, which aims to verify by asking questions at the right level of abstraction that nothing important has been forgotten, is not ritualized for the moment, but Thales sees it as a necessary contribution. Indeed, safety at Thales is currently based on the expertise of engineers who have been in place in the company for many years, but the trend towards shorter development cycles advocates a tool-based, rigorous and formalized methodology.

To verify consistency, Thales starts with the SSA analysis and then works its way up the entire chain. Apart from the definition validation reviews carried out at milestones between the SE/SA teams and with the experts, there is no additional mechanism implemented to guarantee consistency.

Traceability

To date, there is no clearly established traceability process at Thales. Thales' vision is that it is not possible to have a single traceability model because each project has its own specificities. Thales recommends defining the traceability model at the start of any program, in order to define the source and target artifacts for which

traceability is deemed necessary, and the types of links to be put in place. This implies the use of tools with the ability to define traceability models with a certain flexibility.

In the absence of a traceability pattern, Thales insists on the need to establish the principles of traceability, which according to Thales must include or address the following points:

- The need to implement traceability between hazardous events and functional chains, in order to guarantee the robustness and safety of the data displayed on the HMIs. Indeed, these data are the result of complex functional chains and the safety must be verified for each of these chains (make the safety data oriented).
- Should Failure Conditions be represented on the SE side?
- Need to trace the link between FCs and the failure modes of the items. How to proceed?

It is to be noted that the system and safety requirements belong to the same requirements repository at Thales.

3.4 Liebherr feedback

3.4.1 Existence of SE/SA exchange process

Liebherr Toulouse (LTS) indicates that there is currently no formalized process detailing the exchanges between their system and safety teams. Nevertheless, an operating process with a high level of abstraction exists. Furthermore, LTS development plans / working methods can give elements of operating modes on these SE/SA exchanges, but without guarantee of consistency. Indeed, LTS relies on a requirements management guide which explains what data safety analyses generates, how to archive/store them what formal links are to be traced (in DOORS) with the different specification artifacts.

The presence of system and safety engineers on the same site, and in close proximity, allows frequent discussions between them, without the need for a dedicated collaborative workspace. However, workspace discussions are still possible, but the safety engineers are not systematically present. Indeed, the safety engineers have a punctual expertise activity and can intervene on different projects in parallel. Their participation in the collaborative workspace is difficult to implement, unlike the SE engineer, who is often dedicated to the project due to the volume of his activities.

3.4.2 Roles in the SE/SA exchange process

An SE/SA exchange process involves three roles at Liebherr:

- The systems engineer
- The safety engineer
- The chief engineer

The systems engineer and the safety engineer: these two roles are played by different people. The SA engineer checks how the safety requirements are taken into account in the system specification. However, he is not required to review all the system requirements.

The role of the chief engineer is to validate the design, taking into account the safety point of view, with his dual role of "systems engineer" and "safety analyst". In fact, he carries out, among other things, a systematic

validation of the requirements derived from the safety analysis, and establishes the link between the system specification and the corresponding safety elements.

3.4.3 Team training

SE/SA exchanges require a strong knowledge of safety analysis from the systems engineers. This is the reason why systems engineer receive two levels of training in safety.

3.4.4 Aircraft manufacturer/ system supplier interaction

The aircraft manufacturer provides the system specification (all its requirements), as well as the results of the SFHA analysis to the system manufacturer (LTS). The latter re-appropriates and refines the specification received. The system specification (DOORS base) are sent to the aircraft manufacturer for approval.

Note: LTS is not in favor of directly reinjecting its specification elements into the 3DX platform of the aircraft manufacturer (DA) to avoid liability problems.

Exchanges between LTS and aircraft manufacturers may differ depending on the aircraft manufacturer (Airbus/ Dassault Aviation/ Bombardier/Embraer...):

- Direct exchanges between LTS's SA experts and their aircraft manufacturer counterparts, with participation of the systems engineer.
- The systems engineers handle all the exchanges and study the aircraft manufacturer's documents. They only call on the safety engineers when necessary.
- LTS/Bombardier case: it is based on discussions between LTS (SE & SA) and the Design Approval Designee (DAD), who represents the authority at Bombardier by ensuring that the system and the associated safety concept will be acceptable to the authority (Transport Canada Civil Aviation - TCCA).

Some Key elements shared between LTS and the aircraft manufacturer include:

- The assumptions of the safety analysis taken into account
- The flight procedures, and associated cockpit messages, which size the scenarios based on the existence of manual reconfigurations.
- The means of verification that will be necessary to complete the SSA (e.g. smoke evacuation flight test, to confirm that the failures modelled in the trees do indeed produce the effects considered on the smoke evacuation function).
- External failures (i.e. interfacing systems) that influence the safety analysis.
- Periodic inspections (scheduled maintenance), which are part of the ALS "Airworthiness Limitation Section" of the aircraft maintenance manual prepared by the aircraft manufacturer, and necessary for the type certification of the aircraft.

3.4.5 Activities in the SE/SA exchange process

SFHA

LTS indicates that it does not carry out SFHA activities internally (because it is not a certification holder). Indeed, at this stage, LTS does not have a complete vision of the operational context, the installation constraints... that it is necessary to know in order to carry out an SFHA. LTS receives the SFHA analysis carried

out by the aircraft manufacturer, but exchanges between LTS and the aircraft manufacturer can enrich this analysis.

The question arises as to the interest of this approach: should we work by scenario in the manner of the V&V (to verify that the safety analyses are consistent with what they should do and how they should do it) ? At this stage, LTS cannot guarantee that the operational scenarios are well taken into account in the PSSA.

Moreover, these scenarios would have to be approved by the aircraft manufacturer because they are ultimately conditioned by the SFHA assumptions that LTS does not control. Furthermore, it was argued by the interviewees that the scenario-based approach will be more natural/easy to implement with MBSA.

Review

At LTS, 2 to 3 major reviews are generally organized at key stages of development (PDR, CDR and Certification). The review consists of the systems engineer re-reading the fault trees. In his review, the systems engineer is accompanied/guided by his "safety" counterpart. In this respect, LTS underlines the interest of the MBSE and MBSA approaches to allow a simple and quick review. It is worth noting that no checklist is used for the review. It is guided by the expertise of the safety analyst. However, in the context of reviews with some aircraft manufacturers, these are guided by checklists.

Traceability

At LTS, a formal traceability (strong links) is realized by the safety engineer between the safety requirements and the system requirements (stored in DOORS). Note that the links can be traced at a certain level of granularity and between sets.

- The failure rates of each failure mode contributing to a fault tree (several hundred requirements)
- Failure detections associated with failures considered in the fault trees (several dozen requirements)
- System reconfigurations associated with failures taken into account in the fault trees (several dozen requirements)
- The minimum performance and/or technical characteristics, geometrical characteristics conditioning certain combinations of failures (several dozen requirements)
- The development levels of functions and items (Function Development Assurance Level (FDAL)/ Item Development Assurance Level (IDAL)) (several dozen requirements).

Concerning the Safety hypotheses, which are essential to the analyses and to the SE/SA coherence, LTS indicates that some hypotheses are formalized and traced, but not all. In particular, the "system performance" hypotheses (e.g. pressurization) are traced, because the associated failure scenarios are not obvious to deal with, and are subject to greater processing rigor. In general, LTS indicates that the "vertical links" between safety analyses re well traced, via DOORS and other document reference management tools.

Consistency

LTS encountered few cases of inconsistency that led to serious problems. However, the failure rate is not at the expected level and can lead to impacts on certification. Today, the failure rate is controlled via the requirements.

3.5 Airbus / Apsys feedback

3.5.1 Existence of SE/SA exchange process

There is not really a formalized SE/ SA exchange process. Nevertheless, the processes are anchored in Airbus practices. In fact, SE/SA interactions occur naturally, based on their experience. Moreover, these interactions are guided by the ARP, which is a guideline for exchanges between the Design and Safety teams. An important point to make here, is that safety documents are co-written and co-signed by both teams.

When it comes to SE/ SA interactions, Design (systems engineering) and Safety analyses can be managed by the same team (depending on the size of the project), but more often design and safety entities are independent.

The rituals and modes of Design/Safety interactions depend on the project:

- Regular workshops (once a week or several / week) between design and safety to discuss/converge/work. In addition, there are email exchanges.
- Operation in integrated plateau mode, and according to an agile method on innovative concepts (case of new flight control concept)
- Or due to lack of time and ignorance of the fact that the earlier the "Safety" entity intervenes, the more time is saved, the development can be carried out only on the design side, without interaction with the "Safety" entity. The latter is solicited a posteriori, at the end, to produce the necessary "Safety" analyses/documentation => Risk of questioning DAL associated to the FCs.

The state of the discussion is formalized in the deliverables (for example the "Functional Requirement Document" (FRD) which traces and justifies the design choices).

3.5.2 Roles in the SE/SA exchange process

Airbus relies on the principle of Design/ Safety independence of the ARP. In fact, Design and Safety are two different entities, right up to the hierarchy (engineering manager). The program director is the only one to wear both hats (design and safety). However, the safety documents (FHA, SSA) are co-written and co-signed by both entities. Therefore, an FHA (resp. SSA) is, in fact, controlled by the design team as it is also the author of the document. The double check Design/ Safety is at level 1 "authors", and at level 2 "validation".

There is another important role in the SE/SA exchange process: the CVE (Compliance Validation Engineering). The CVE Safety validates the safety part, while the CVE design validates the design part.

- The CVE has an independent role, which is to validate all the analyses. The CVE intervenes at the end of the process ("safeguard" of the good realization of the product);
- At Airbus, the CVE corresponds to the role of Designated Certification Specialist (DCS), in charge of the certification file, and responsible for the product certification. The DCS can be involved in the different phases of the development lifecycle (follow-up and validation of the development, or only documentary validation in fine, in anticipation of the certification).

It is interesting to mention that the different roles are defined by the authorities. Airbus follows the recommendations.

In general, the safety team conducts the analyses, and the systems engineering team checks for validation. However, for some analyses, the involvement of the SE side is stronger. This is the case for the SSA, where the systems engineer carries out the fault tree (as he has a better understanding of the organic/material view), under the instruction of the Safety engineer who focuses on the method and verifies that the rules of the ARP

are respected. The result of the analysis remains, in all cases, in charge of "Safety". Nevertheless, the documents are co-signed by the "Design" and "Safety" entities.

It should be noted that for known systems, the systems engineer, due to his experience, is free to take into account the safety constraints in his design. Whereas, for new innovative systems or major changes in operating principles (e.g., navigation system), the safety contact person accompanies the SE contact person in his design.

3.5.3 Team training

At Airbus, it was essential to raise awareness of "Safety" training throughout the systems engineering department. Moreover, different levels of training, more or less detailed, can be proposed, depending on the needs. Concerning the development of engineer profiles with dual safety / system skills, the transition from "Design" to "Safety" skills is not a common practice.

3.5.4 Aircraft manufacturer/ system supplier interaction

The system designer/aircraft operator discussions are systematically managed by the "Design" team. The "Safety" constraints/requirements have been included in the system specification. The "Design" contact person, who knows the ARP process, then manages the exchanges. This is due to the fact that the "Design" contact is the owner of the system.

- There are no particularly exchanges between the "Safety" entity on the Airbus side and the "Safety" entity on the system owner's side.

- The aircraft manufacturer must ensure that all the demonstrations of the functions are done, and manage the cases of multi-systems. The Airbus SA team does not recover the supplier specifications (system manufacturers), nor the intermediate analysis results. On the other hand, the final results of the SSA (documentation verification, FMEA, fault tree...), as well as the document that traces the systems' response to the requirements, can be recovered by the Airbus safety team. It is worthwhile mentioning, here, that the only case where Airbus recovers the specification elements/analysis results from the supplier is the engine. Airbus is, then, integrator and needs it to get certified.

The aircraft SE team recovers all supplier documents. It can also ask the SA team to check/validate the safety part of the supplier documents.

This specific case is due to the fact that the engine manufacturer certifies directly its engine and Airbus certifies the engine integration (nacelle, FADEC, and engine control in the cockpit).

3.5.5 Activities in the SE/SA exchange process

SE/ SA Review

In addition to the Design/Safety meetings and working discussions, formal reviews at the different milestones of the project exist. These reviews are of different levels of granularity and aim to verify:

- Design Maturity

- Safety Maturity: the "Safety" feasibility is requested very early, in the form of a risk analysis.

The organization of work and reviews is done by failure scenario. Thus, for each function with its description, a failure scenario is defined, then mitigation measures are proposed. The work is based, among other things, on the System Description Document (SDD), which describes the functional scope. The verification activities performed by the Safety analyst to ensure that the safety requirements have been taken into account on the "design" side, are carried out over time via discussions and workshops.

Traceability

At Airbus, the Design/Safety traceability is done at the requirements level, and not at the model level. The "Safety" specification is integrated as a paragraph in the "System" specification. The "Design" team must ensure, via the compliance matrix that the "Safety" requirements allocated to the sub-systems are taken into account.

3.5.6 Use of models

A few key points have been pointed out concerning the use of models:

- The case of ATA27 (flight control) with the use of MBSE "SCADE" type models required a real, time-consuming job of translating the "SCADE" models into ppt to be able to more easily discuss/exchange around the models. Ideally, the "Safety" team should be familiar with the "SCADE" suite. However, in practice, very few "Design" people know the "Safety" tools, and vice versa. Thus, there is a great need to identify a solution to facilitate the reading of the models in order to save time.
- A MBSE/MBSA gateway has been tested in the framework of a research project (3DX model, MBSA coupling).
- The interest to study how to generate automatically the FTA from the MBSE, to save time, the fault tree being currently systematically built manually.

3.5.7 MBSA

The MBSA approach is in the research stage at Airbus. It should be noted that as long as this approach is not recognized as a means of demonstration by the ARPs, any MBSA modeling must be revalidated by the classic "Safety" approach (FTA / dependency diagram / ...).

Consistency

At Airbus, the risks of inconsistency are strongly limited by:

- The intervention of experts in the definition
- The "over-design" (over-dimensioning which allows the system to be robust, but at a higher cost).
- The "integrated" operation between the Design/Safety teams

For Airbus, the problems of consistency come mainly from possible misunderstandings at the Customer/Supplier interfaces. The legal constraints around “execution of contracts” impose reasoning in the form of textual specifications, which leads to difficulties in understanding the overall system, when it is complex. However, there can be problems of documentary consistency.

- The case of an old program to be realigned with a new certification. Demonstrations are difficult to carry out, because the history is difficult to trace. Thus, a problem of consistency can arise when the basis of the certification is changed.

- The case of product evolution over time: the technical facts management phase may involve other parties than those who contributed to the development. Possible problems of consistency, of documentary alignment, on the "Design" or "Safety" side.

Note that maintaining consistency over time is well handled for critical systems, but can be a problem for non-critical systems. The challenge is to see how to simplify the current operation / save time, while ensuring the right level of consistency.

3.6 LGM feedback

3.6.1 Existence of SE/SA exchange process

LGM representative indicates that it is not aware, through its various experiences, of any clearly established process detailing the exchanges between their system and safety teams. In the absence of a process that "structures" the SE/SA exchanges, the sharing of documentation and discussions during technical meetings make it possible to gather the information necessary for the Safety work. Nevertheless, some process parts exist. Moreover, ARP4754A provides process elements by recommending to carry out formal tripartite reviews, involving the SE contact person, the SA contact person and the certification contact person (DAD), to validate and verify the requirements.

3.6.2 Team training

LGM recommends or even requires training to align the Safety and System vocabularies. This is necessary to carry out SE/SA exchanges. However, it should be noted that the LGM representative believes that the need for training in the aeronautics industry is less since all the players are familiar with and follow the Easy Access Rules for Large Aeroplanes (CS-25), the upstream alignment vector.

3.6.3 Documents validation and roles

The LGM representative distinguishes between two types of validation: formal validation and informal validation. In the case of a formal validation, a formal review is required.

Some Safety deliverables are co-signed by the SE and SA entities. This co-signature assumes that the system engineer understands the content of these deliverables.

In the Bombardier case, the validation involves different roles: the system architect (the integration engineer), the Safety peers, the Safety manager, and the test pilot. The program manager is not involved.

Note: at the time, Safety depended on quality and the documentary validation also went through a quality manager. Today, the Safety department is considered more as a technical job (like the SE). In terms of independence of views (advocated by the ARP and also by other standards such as EN61508 recommends validation by independent teams), the attachment of safety to quality was of interest.

It should be noted that our LGM contact, in the context of one of his missions, had a validation activity for derived requirements (requirements not attached to a high level) but did not validate the part of the perimeter marked out by the SI processes on the quality side.

3.6.4 Activities in the SE/SA exchange process

SFHA

The SFHA analysis is done at the aircraft manufacturer level. It should be noted that ARP4754A has clarified the FHA. Indeed, the interviewees distinguish:

- AFHA: Analysis of level 1 to 3 functions (at aircraft level)
- SFHA: Analysis of functions from level 4 to 7 (system level)

The SFHA can in theory be done by the aircraft manufacturer or the system supplier. But as the aircraft manufacturer is the one who specifies the needs, it is often him who carries out the SFHA. Indeed, if the system designer does the SFHA analysis, he must make/imagine hypotheses on the aircraft behavior, the pilot reaction, as well as the impact of the hazardous event on the aircraft. In all cases, the aircraft manufacturer is the one who validates and carries the SFHA (because it carries the certification of the aircraft with the authorities). It should be noted in this context that Bombardier always carried out the SFHA itself. The SFHA is carried out in a team, involving the system architect (the SFHA starts from the list of functions and their descriptions), and the certification teams (to validate the FCs).

Note: the only elements certified according to CS-25 are the aircraft and the engine. But TSOs (Technical Standard Orders) allow certification of other systems, such as equipment (seat, radio, etc.). The SFHA analysis is required by CS-25 for the aircraft and the engine.

Since the SFHA can be performed collaboratively by the aircraft manufacturer and the system supplier, the responsibility in case of a problem is not clear. Contractual clauses may provide some answers.

Review

Safety requirements are verified by peer reviews, particularly in terms of quality (compliance with the rules for writing requirements). However, LGM does not have experience with systematic SA/SE reviews.

Concerning the use of checklists in support of SE/SA design, checklists are used at Bombardier, but more to deal with the quality of requirements. LGM cites a few elements that can be assimilated to the notion of a checklist: the safety plan (high level) which explains the process to be implemented, as well as application notes which explain what to do during certain reviews. However, this is not systematized. For example, there is no procedure for reviewing derived requirements. Moreover, the CMA, which is a subject that is not very well defined by the ARPs, is the subject of an implementation procedure.

Traceability

Feedback from an aircraft manufacturer updating a legacy design revealed the following points:

- The aircraft specification was a very commercial requirement specification. Thus, the link between the requirement and the system specs was particularly difficult to make, and therefore not realized.
- The traceability links were made between the functions and the high level specification.
- As safety is based on the list of functions as input data, the FHAs are by nature linked to the functions (CF identified by function), but not to the requirements specification (too commercial).

LGM mentions that Doors is a good tool to ensure traceability. However, in the absence of such a tool, a less equipped traceability was practiced and was nevertheless satisfactory.

MBSA

The use of the MBSA model has been practiced in advance design because there were no certification constraints. The first experiences of certification by the MBSA (flight control) should encourage this practice.

Consistency

According to the LGM representative, the consistency problems come mainly from the evolution of the system. In theory, all system modifications are tracked by change management tools. But not all of them are analyzed by the safety team, because some changes are considered (sometimes wrongly) to have no safety impact.

A difficulty is also reported on the evolution of evolutions: Case of a 1st evolution which was the subject of a first definition, and which is the subject of new iterations of modification...

In spite of everything, LGM believes that there is no real problem of consistency with serious impacts. Of course, we cannot control everything, but through discussions, problems are identified and corrected, but perhaps belatedly.

3.7 Airbus Defense and Space feedback

To come

3.8 MBDA feedback

To come

3.9 Synthesis of the partners practices

3.9.1 Existence of SE/SA exchange process

		Industrial partners					Directions of improvement
		Dassault Aviation	Thales	Liebherr	Airbus	LGM	
Existence of SE/SA exchange process	No formalized process exists		X	X	X	X	Modeling a shared process formalizing the SE/ SA exchanges
	A formalized process exists, but not applied	X					
	Existing practices regarding SE/SA exchange	SE/SA exchanges characterized by physical and relational co-engineering	Internal business plan (Chorus) + ARP	An operating process with a high level of abstraction + development plans / work methods	SE/SA interactions occur naturally based on experience + ARP	Sharing of documentation + Discussions during technical meetings	

In the following, we present the concepts process, and process modeling as defined in literature. It is apparent that multiple definitions of a "process" exist. Yet, they are all similar in that their focus is on the what and why of this notion. Typically, the "what" aspect sheds light on the activities of the process. Whereas the "why" aspect sets emphasis on the goal of the process. In line with this, [Scheer and Nüttgens, 2000] describe a process as "a procedure relevant for adding value to an organization". In the same vein, a process is defined as "the combination of a set of activities within an enterprise with a structure describing their logical order and dependence whose objective is to produce a desired result" [Aguilar-Saven, 2004].

The term process modeling is used to characterize the identification and (typically rather informal) specification of the processes at hand [van der Aalst et al, 2003]. One of the key benefits of process modeling is that it facilitates a group to share their understanding of the process by using a common process representation, which helps human understanding and communication [Aldin and De Cesare, 2009]. This is, indeed, our main objective of the modeling of the SE/ SA exchange process.

3.9.2 SE/ SA Reviews

			Industrial partners					Directions of improvement
			Dassault Aviation	Thales	Liebherr	Airbus	LGM	
SE/ SA consistency	Means for SE/ SA consistency	Frequent discussions	X			X	X	A checklist – based approach to assist the conduct of a system/safety review
		Systematic SE/ SA review	X	X	X	X		
		Non-systematic SE/ SA reviews					X	
	Existing practices regarding SE/ SA consistency		Peer reviews with experts, organized throughout the development process at the main project milestones	Internal reviews at the time of milestones, involving various SE and SA experts	2 to 3 major reviews are organized at key stages of development (PDR, CDR and Certification)	SE/SA meetings and working discussion + formal reviews at the different milestones of the project	Peer review of Safety Reqs in terms of quality, but not in a systematic way	

As (1) reviews rely mostly on the expertise of safety engineers, and (2) there is no clearly defined review process, a checklist-based approach could be useful to assist a system/safety review. In this vein, it is worth noting that the ARP4754A advocates the use of templates and checklists to the assist the review activity (see section 3.3).

Furthermore, we give below some thoughts/recommendations that were discussed with some industrial partners on how to improve SE/SA consistency:

- The system engineer needs to take ownership of the fault tree, so that he can think about events that could have led to additional FCs.

Improve the traceability of certain assumptions. In fact, Assumptions needs better formalization and then traceability. A classification of the criticality of these assumptions to prioritize and reduce overwork cost. For example, the assumptions made for the PSSA analysis, which are essential because they can cause inconsistencies (incompleteness), or certain functional assumptions. These assumptions are not all translated into requirements, and therefore difficult to trace.

- Maintaining consistency over time. Indeed, the focus is often put on consistency at the moment T. However, it is the maintenance of consistency over time that is more problematic. It should be noted, in this respect, that the change management process is not sufficient because confusion between safety acceptability and safety impact is frequently made by systems engineers: they filter the technical facts to be treated on the safety side

by having a bad analysis of the safety impact. A good practice would be that 100% of the list of "change requests" is analysed by the safety analyst (time consuming, and less involvement of safety engineers once the critical milestones are passed).

- Fault trees can move away from the system definition (by tunnel effect), and therefore be a source of inconsistency.

- Distinguish between non-conscious inconsistency, and acceptable conscious inconsistency: the case where the inconsistency is known but where the choice is deliberately made not to be consistent, either because of the lack of gain in reliability analyses, or because of the need for simplification (no additional information).

- Interest in having a behavioral model on the SE side and using formal methods to help with safety analysis.

3.9.3 Traceability

		Industrial partners					Directions of improvement
		Dassault Aviation	Thales	Liebherr	Airbus	LGM	
Traceability in the SE/SA exchange process	R/R traceability	X		X	X		A general conceptual model of traceability, with associated instantiation rules (what artifacts to trace, why, and when) ➔ Objective: definition of "customized" traceability models ➔ Starting point: existing industrial traceability plans
	R/M traceability	X				X	
	No clearly established traceability process		X				
	Existing practices regarding SE/SA exchange	Traceability using 3DX platform + R/R links (two # levels of reqs) + R/F links	To date, no clearly established traceability process at Thales ? Traceability according to the specific needs of the project	A formal traceability (strong link) at a certain level of granularity between safety reqs and system reqs	System/safety traceability at the req level + compliance matrix to ensure that the safety reqs allocated to the sub-systems are taken into account	The traceability links are made between the functions and the high level specification	

3.9.4 Components of the SE/SA exchange process

		Industrial partners					Directions of improvement
		Dassault Aviation	Thales	Liebherr	Airbus	LGM	
Components of the SE/SA exchange process	Different roles	X	X	X	X	X	Multi-view modeling of the SE/SA exchange process to deal with its complexity
	SFHA activity	X	X	X	X	X	
	SE/SA review activity	X	X	X	X	X	
	Traceability activity	X	X	X	X	X	
	Shared documents	X	X	X	X	X	
	Other elements	X	X	X	X	X	
General	The SE/ SA exchange process is a complex process as: (1) It is composed of many elements of different types (roles, activities, data, etc.) (2) It is composed of complex activities such as the SFHA and the SE/SA review activities. By a complex activity, we refer to an activity that contains sub-activities, and hence that can be described by an independent process.						

Multi-view modeling is defined in a straightforward manner by [Reineke and Tripakis, 2014] as "a methodology where different aspects of the system are captured by different models or views". Following the same direction, [Bork et al, 2015] define multi-view modeling as a "particular approach for coping with the complexity of the system by decomposing its overarching model into several views". However, these views are not independent from each other. Indeed, [Persson et al, 2013] defines three types of view relationships: precedence relationships, dependency relationships and co-dependency relationships. The first reposes on the idea that a given view should exist before another without sharing data. The second type means that a view should exist before another- with the second view involves data coming from the first one. Lastly, the third type takes place when two views share data mutually. As the views are overlapping, consistency between them should be taken into account. The aforementioned author used the term consistency to denote the absence of any contradiction in the information contained in the created views.

From this synthesis, we identify the following improvement axis:

- Modeling a shared process formalizing the SE/ SA exchanges
- A checklist –based approach to assist the conduct of a system/safety review

- A general conceptual model of traceability, with associated instantiation rules (what artifacts to trace, why, and when). Objective: definition of "customized" traceability models / Starting point: existing industrial traceability plans
- Multi-view modeling of the SE/SA exchange process to deal with its complexity

From these axis, we propose to focus on the following points in the next steps of our study:

- Consolidate the proposed change scenario-based approach for ensuring consistency between system and safety teams.
- Develop a checklist –based approach to assist the conduct of a system/safety review.
- Develop a general conceptual model of traceability, with associated instantiation rules (guidelines: what artifacts to trace, why, and when).

4 A graphical representation of SE/SA consistency process

In this section, we propose a graphical representation of the SE/SA exchange process, based on 6 views in line with previous recommendations on multi-view modelling:

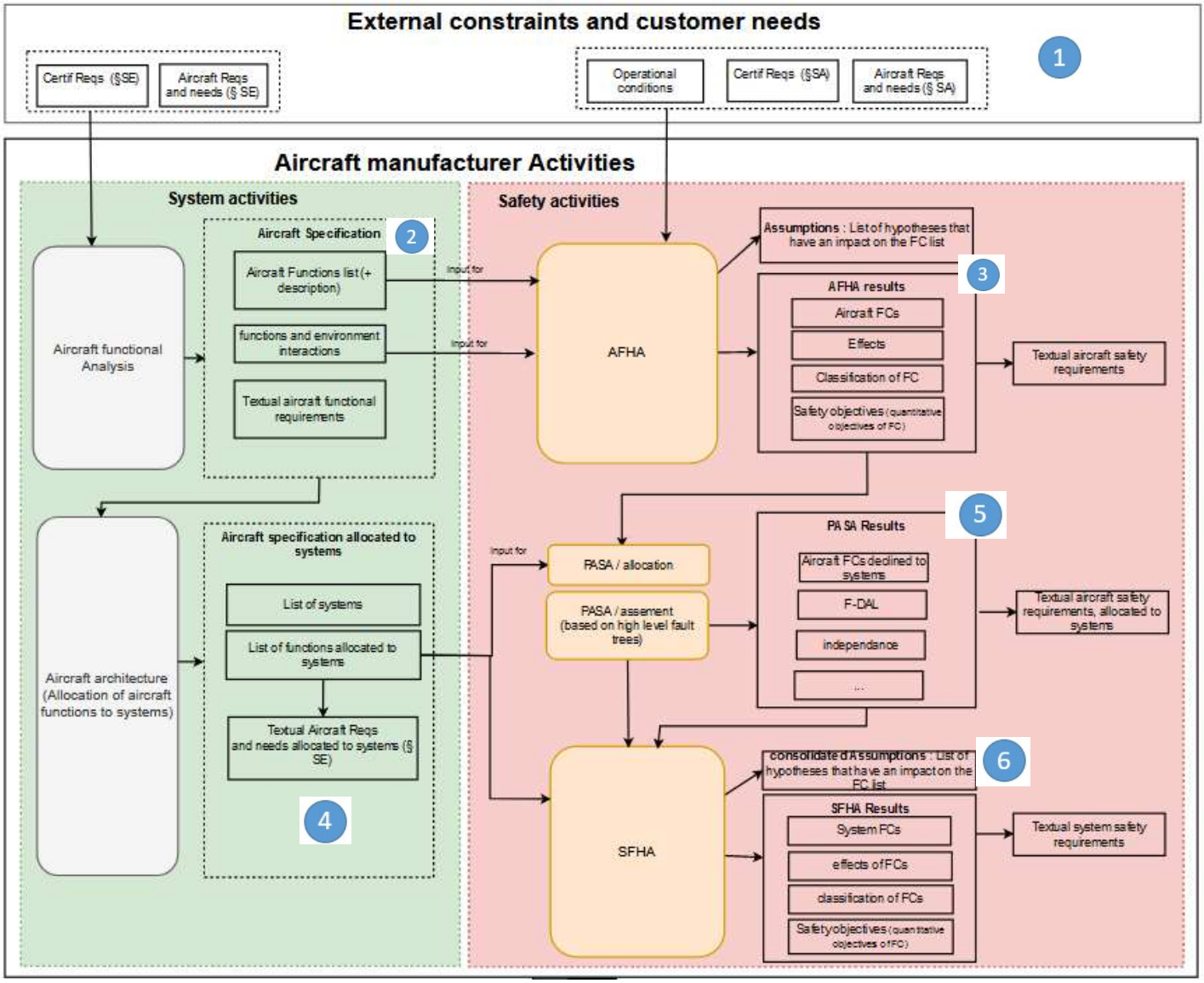
- Aircraft Manufacturer view which presents Design activities (conception) and corresponding Safety analysis at aircraft level.
- System Provider view which presents Design activities (conception) and corresponding Safety analysis at system level. The focus is made here on the activities led by the system provider, on a contract basis
- Verification / Validation view
- "Aircraft Manufacturer / System Provider interaction" view which details the interface between these two actors
- a traceability view : to be completed in a further version
- a review view

This representation is a first proposal made to our partners that is still to be discussed and validated. It has been built on the basis of interviews with the partners. A particular point concerns the SFHA activity, which can be carried out either on the aircraft manufacturer's side or on the system supplier's side, depending on who is responsible for the certification of the system.

For the two first views which describes SE/SA activities and the data exchange between them, examples are given on the basis of our AIDA study case.

4.1 Aircraft Manufacturer view

Following pictures represent SE and SA activities led by the aircraft manufacturer.



If AFHA and PASA are led by the aircraft manufacturer, SFHA is also from Aircraft maker responsibility as it is required for Aircraft certification. But Engine makers or Systems providers can sometimes manage such SFHA analysis when they have to carry out certification of their systems.

Thus, the aircraft manufacturer manages aircraft level considerations (aircraft functional analysis, AFHA, PASA) but also system level considerations linked to the allocation activities (system allocation, SFHA).

The following table describes major activities of the process above and examples are given based on our AIDA study case.

1

External constraints and customer needs :

At each aircraft development program pre-exist external constraints of different types : Certification requirements applying for SE or SA activities, the customer requirements and needs about aircraft, or operational conditions

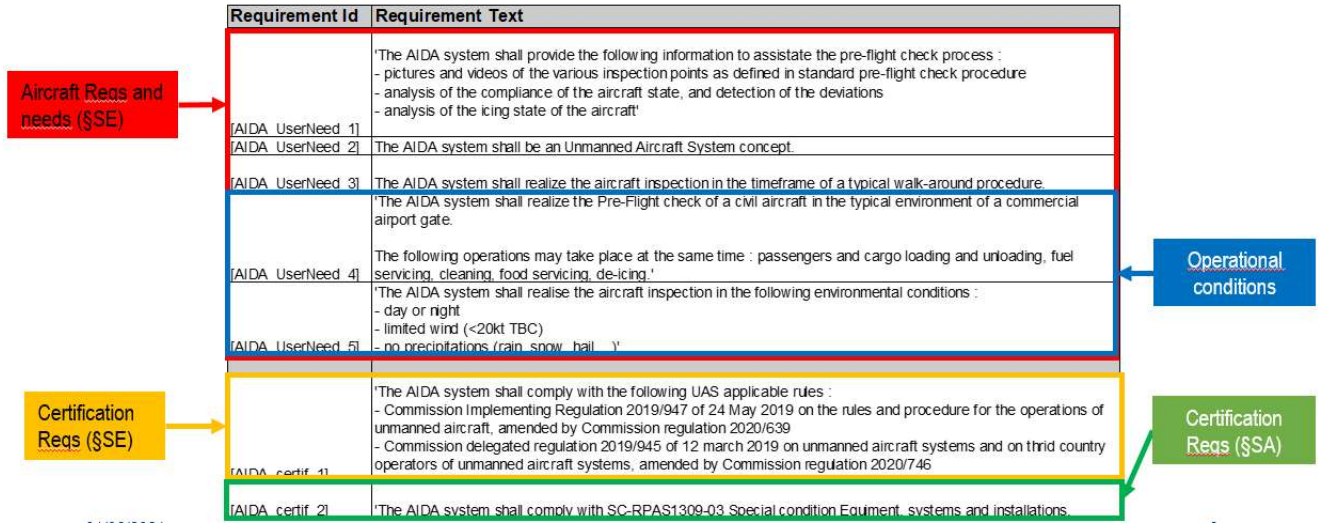


Figure 3 - Example of high level requirements and needs

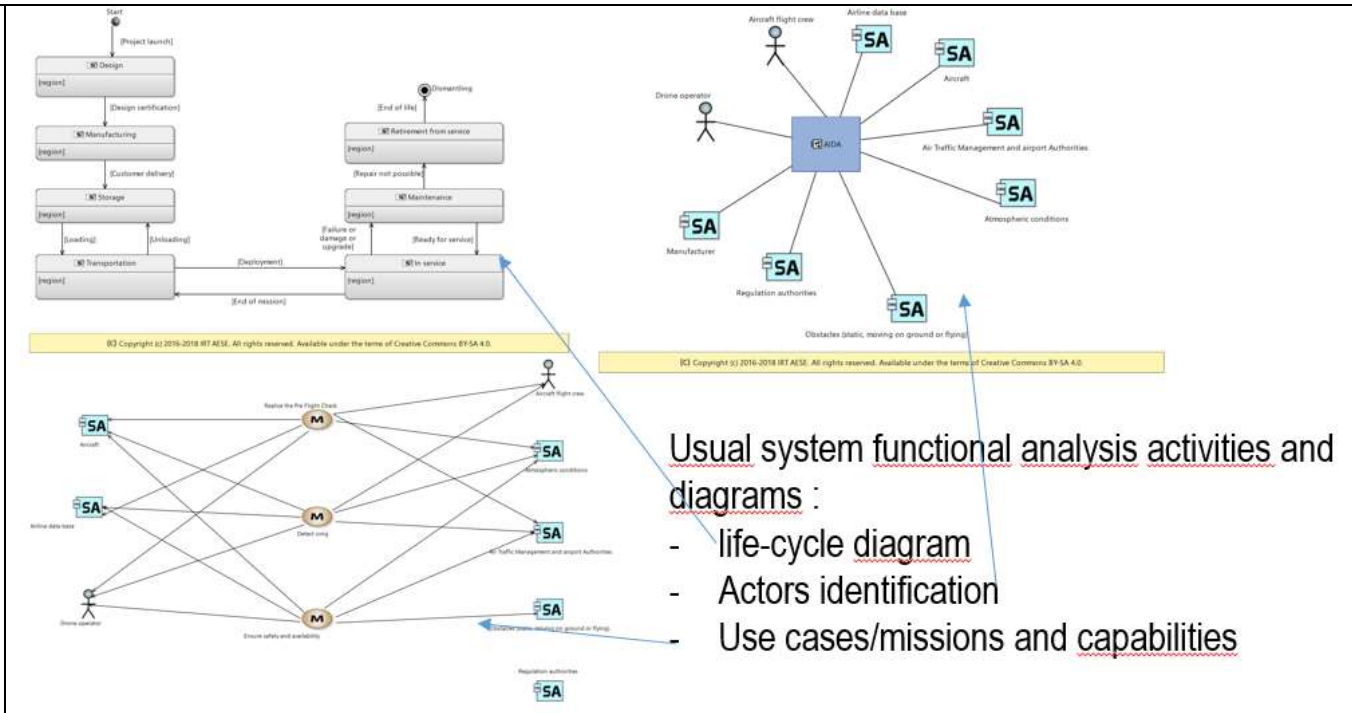
2

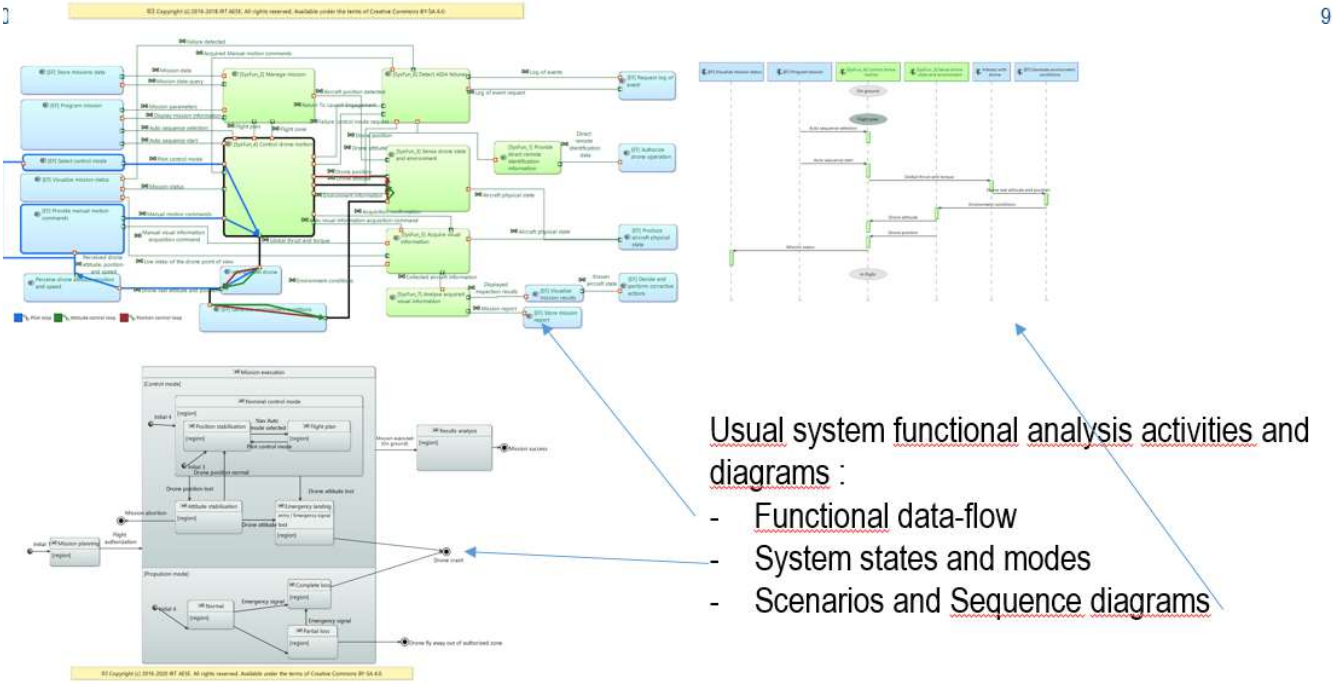
Aircraft functional Analysis / Aircraft specification :

The aircraft manufacturer activities start with the "Aircraft functional analysis", led by the system engineer (SE), which consists in defining Aircraft functions (at aircraft level). In order to do that, the system architect has to define aircraft life-cycle, actors that interact with the aircraft, and use cases/missions and capabilities that the aircraft has to satisfy.

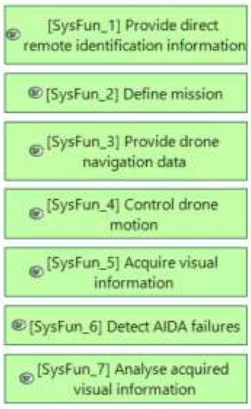
This activity is based on external inputs / constraints induced by certification or aircraft customer.

Aircraft functional requirements are also produced that are used to contracting and traceability aspects.





High level functions :



Functional architecture :

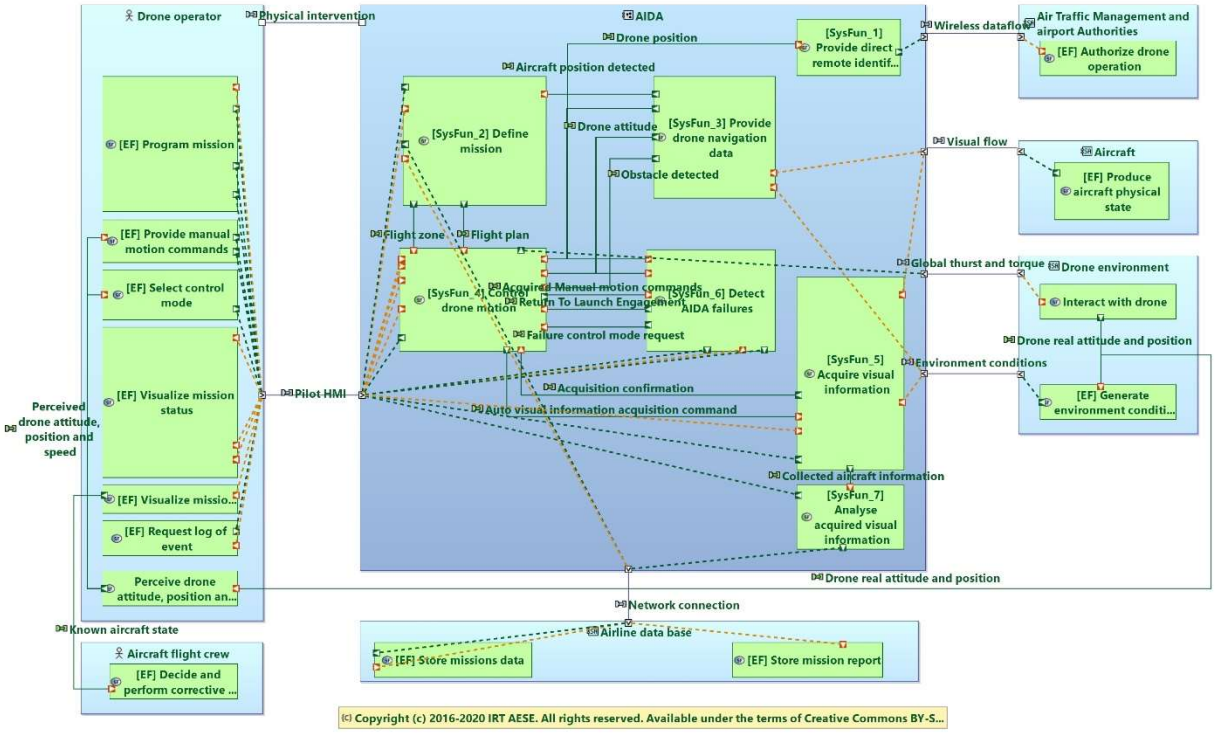


Figure 4 - Example of function analysis

Example of textual aircraft functional requirements : they specifies the expected functions, the associated behaviour and performances (etc …)

Requirement Id	Requirement Text
[AIDA_Fun_1]	**SF1 - Provide direct remote identification information :** When the drone is in operation, the AIDA system shall broadcast a direct remote identification that: - allows the upload of the UAS operator registration number in accordance with Article 14 of Implementing Regulation (EU) 2019/947 and exclusively following the process provided by the registration system| - ensures, in real time during the whole duration of the flight, the direct periodic broadcast from the UA using an open and documented transmission protocol, of the following data, in a way that they can be received directly by existing mobile devices within the broadcasting range: i the UAS operator registration number| ii the unique physical serial number of the UA compliant with standard ANSI/CTA-2063| iii the geographical position of the UA and its height above the surface or take-off point| iv the route course measured clockwise from true north and ground speed of the UA| and V the geographical position of the remote pilot or, if not available, the take-off point| -ensures that the user cannot modify the data mentioned under points ii, iii, iv and v'
[AIDA_Fun_2]	**SF2 - Define mission :** The AIDA system shall compute the authorized flight zone and the flight plan based on mission parameters provided by the pilot and mission data retrieved from the airline database.
[AIDA_Fun_3]	**SF3 - Provide drone navigation data :** In the Mission execution mode, the AIDA system shall compute the drone attitude and angular rate with the following performances : -roll : range +/-90°| accuracy 0.1° | resolution 0.01° -pitch : range +/-90°| accuracy 0.1° | resolution 0.01° -heading : range +/-180°| accuracy 0.1° | resolution 0.01° -angular rate : range +/- 360°/s | accuracy 0.1°/s | resolution 0.01°/s'
[AIDA_Fun_4]	**SF3 - Provide drone navigation data :** In the Mission execution mode, the AIDA system shall compute the drone position and speed with the following accuracy : -position : 1m -speed : 0.1m/s'
[AIDA_Fun_5]	**SF4 - Control drone motion :** The AIDA system shall provide the following control modes : - Flight plan : the drone execute automatically the selected sequence (flight plan defined by the operator, or one of the pre-defined sequence : take-off, aircraft detection, landing, Return-To-Home) - Speed consign : the drone keeps its current position, and moves when required by the pilot (pilot commands are interpreted as speed commands) - Manual modes : the drone stabilizes its attitude (null pitch and roll, current heading), and moves when required by the pilot (pilot commands are interpreted as yaw rate, pitch and roll commands)
[AIDA_Fun_6]	**SF4 - Control drone motion** : In Flight plan mode, the AIDA system shall execute automatically the flight plan defined by the operator.
[AIDA_Fun_7]	**SF4 - Control drone motion :** In position stabilisation mode, the AIDA system shall maintain the drone in its current position, and move the drone when required by the pilot (manual motion commands are interpreted as speed commands).
[AIDA_Fun_8]	**SF4 - Control drone motion :** In manual mode, the AIDA system shall stabilize the drone attitude (null pitch and roll, current heading), and move the drone when required by the pilot (manual motion commands are interpreted as yaw rate, pitch and roll commands).
[AIDA_Fun_9]	**SF5 - Acquire visual information :** The AIDA system shall acquire pictures or videos when the pilot commands an acquisition or when required for the flight plan execution.
[AIDA_Fun_10]	**SF6 - Detect AIDA failures :** The AIDA system shall detect the attitude measurement failures, and cut off the power supply to the motors when a failure is detected.
[AIDA_Fun_11]	**SF6 - Detect AIDA failures :** The AIDA system shall detect the altitude measurement failures, and cut off the power supply to the motors when a failure is detected.
[AIDA_Fun_12]	**SF6 - Detection AIDA failures :** The AIDA system shall detect the drone control failures, and cut off the power supply to the motors when a failure is detected.
[AIDA_Fun_13]	**SF6 - Detection AIDA failures :** The AIDA system shall detect the motor failures, and cut off the power supply to the failed motor when a failure is detected.
[AIDA_Fun_14]	**SF7 - Analyse acquired visual information :** The AIDA system shall analyse the collected pictures and videos to detect aircraft abnormal state and icing.

3

AFHA Analysis :

The AFHA allows to identify safety potential hazards related to aircraft, the functional failure conditions, how these functions can fail, and the severity of failure condition effects.

From the Aircraft functional analysis, the "Aircraft function list" and its description of each function is used as input data to manage “AFHA”, in addition to certification requirements, Aircraft safety requirements and needs of the aircraft level (see external constraints and customer needs).

The AFHA gives as output:

- the "list of hypotheses that have an impact on FC list". These hypothesis must be validated with the system engineer.

- and a set of data (AFHA results) composed of FCs, effects of FCs, classification of FCs (Catastrophic, Severe-Major/Hazardous, Major, Minor and No safety effect.), Safety objectives (quantitative objectives of FC). These information are then transformed in textual "Safety requirements";

These AFHA results are inputs data for the next safety analysis “PASA”.

Example of list of hypotheses that have an impact on FC list

Hyp. 1 : the drone is operated on the airport perimeter, inside an authorized flight zone around the inspected aircraft, in which the ATC ensure the absence of any other flying object (aircraft or drone).

Hyp. 2 : the drone operator always have direct line of sight on the drone

Hyp. 3 : normal inspection operations are always conducted in Flight Plan auto mode. The manual mode is a back-up mode, when the automatic control is not possible

Example of AFHA result :

Function ID	Function name	Function failure ID	Functions failures	S/R repercussion Immediate effect of failure on Drone, operator, people around	Detection means warnings/hidden?	High level effect	Failure condition	Classification operability/ reliability
SF1	Control drone propulsion	Fm1.1	Loss of thrust	Complete loss of drone thrust. Loss of drone uncontrolled in authorized area. Potentially crash on inspected aircraft.	Detected visually by the pilot	Crash in authorized area	FC02 : Uncontrolled drone in an authorized area	HAZ
		Fm1.2	Erroneous thrust	Erroneous drone control. Potentially flight in unauthorized zone leading at worst to fatalities.	Detected by the Monitoring function	Potentially flight in unauthorized zone leading at worst to fatalities.	FC01 : Uncontrolled drone (drone fly away) in an unauthorized area	CAT
SF2	Control drone attitude and position	Fm2.1	Erroneous or loss of drone attitude and position control	Control loss is detected by the monitoring function. Motors are depowered. Loss of drone uncontrolled in authorized area. Potentially crash on inspected aircraft.	Detected by the monitoring function	Crash in authorized area	FC02 : Uncontrolled drone in an authorized area	HAZ
		Fm2.2	Erroneous or loss of drone attitude and position control combined with loss of protection function	Control loss, not detected by the monitoring function. Potentially flight in unauthorized zone leading at worst to fatalities.	Detected visually by the pilot	Potentially flight in unauthorized zone leading at worst to fatalities.	FC01 : Uncontrolled drone (drone fly away) in an unauthorized area	CAT
		Fm2.3	Erroneous or loss of drone attitude and position control, combined with incapacity to control the drone in manual mode	Drone operator cannot control the drone manual mode. In worst case, erroneous position control leads the drone out of the authorized area.	Detected visually by the pilot	Potentially flight in unauthorized zone leading at worst to fatalities.	FC01 : Uncontrolled drone (drone fly away) in an unauthorized area	CAT
		Fm2.4	Partial erroneous or loss of drone attitude and position control	No effect in Manual Mode. In auto mode operator switches to Manual mode, increased workload and end of mission.	Detected visually by the pilot	Mission abortion	FC03 : Loss of drone capability leading to mission abortion	MAJ
		Fm2.5	Partial erroneous or loss of drone attitude and position control combined with incapacity to control the drone in manual mode	Loss of drone uncontrolled in authorized area. Operator cannot control the drone in manual mode. The drone stays more or less in the same position until the battery runs out of power.	Detected visually by the pilot	Loss of drone uncontrolled in authorized area. Potentially crash on inspected aircraft.	FC02 : Uncontrolled drone in an authorized area	HAZ

Figure 5 - Example of AFHA Results

The AIDA function list corresponds to the first columns of the AFHA and frames the display of results. In that example, Failure condition (FC) are derived from "Function failures" and are considered as an unsafe system behaviour induced by the function failure or failure mode, but other examples present failure condition as "function failure". See following Table 4.1-1 from ARP4761

1 Function	2 Failure Condition (Hazard Description)	3 Phase	4 Effect of Failure Condition on Aircraft/Crew	5 Classification	6 Reference to Supporting Material	7 Verification
Decelerate Aircraft using Wheel Braking	Total loss of wheel braking	Landing or RTO	See Below			
	a. Unannunciated loss of wheel braking	Landing or RTO	The crew detects the failure when the brakes are operated. The crew uses spoilers and thrust reversers maximum extent possible. This may result in a runway overrun.	Hazardous		S18 Aircraft FTA
	b. Annunciated loss of wheel braking	Landing	Crew selects a more suitable airport, notifies emergency ground support, and prepares occupants for landing overrun. Crew uses spoilers and thrust reversers to the maximum extent possible.	Hazardous	Crew procedures for loss of normal and reserve modes	S18 Aircraft FTA
	Partial Symmetrical loss of wheel braking	Landing or RTO	See below			

In following example (extracted from **Aircraft System Safety.** http://dx.doi.org/10.1016/B978-0-08-100889-8.00003-9, Copyright © 2017 Duane Kritzinger. Published by Elsevier Ltd. All rights reserved), no distinction is made between failure condition and failure mode. Effects of FC is thereby considered to explain the unsafe system behaviour induced by the function failure

ID	Function	Failure condition/ mode (hazard description)	Phase	Effect of failure condition[a]	Consequence[b]	Severity	Justification	Qualitative objective	Predicted failure probability	Verification planned/ achieved
4.1.a	Display Aircraft Altitude	Loss of all barometric Altitude Display (annunciated)	IFR conditions	Pilots immediately aware of malfunction (either through failure flag or totally 'off-line') and will need to contact ATC ASAP in order to maintain altitude	Failure conditions which would prevent Continued Safe Flight and Landing	Catastrophic	Further substantiated by AC25-11B Table 4.3 and CS25 [Amm17] AMC Appendices Chapter 3 Table 5	Extremely improbable	TBD	Conduct FTA (#4.1A) to show that loss of all Altitude displays has $p < 1 \times 10^{-9}$ per flight hour Prove Development Assurance Level A
4.1.b	Display Aircraft Altitude	Loss of all barometric Altitude Display (unannunciated)	IFR conditions	See 4.1A above	Failure conditions which would prevent Continued Safe Flight and Landing	Catastrophic	Further substantiated by AC25-11B Table 4.3 and CS25 [Amm17] AMC Appendices Chapter 3 Table 5	Extremely improbable	TBD	As per 4.1.1.a above, no further verification planned, as this will never be a passive (i.e. unannunciated) failure condition) Prove Development Assurance Level A

These different examples point out how important it is (for consistency) to share same understanding of Function Failure / Failure Mode / Failure Condition… even more when different stakeholders interact altogether (aircraft manufacturer, systems providers)

Example of textual aircraft safety requirements :

Requirement Id	Requirement Text
[AIDA_Safety_01]	The AIDA system shall be designed so that the Failure Condition « Uncontrolled drone, leading the drone to an unauthorized area, identified as Catastrophic, has a failure rate lower than 10-8/Fh and does not result from a single failure.
[AIDA_Safety_02]	The AIDA system shall be designed so that the Failure Condition «Uncontrolled drone in authorized area », identified as Hazardous, has a failure rate lower than 10-6/fh.
[AIDA_Safety_03]	The AIDA system shall be designed so that the Failure Condition «Loss of drone capability leading to mission abortion », identified as Major, has a failure rate lower than 10-4/fh.
[AIDA_Safety_04]	The AIDA system shall be designed so that the Failure Condition «Loss of drone protection », identified as Major, has a failure rate lower than 10-5/fh.

Figure 6 - Example of textual aircraft safety requirements

4

Aircraft Architecture Activity :

On SE side, System activities go on with the activity "Aircraft architecture. Indeed, The system engineer has now a complete set of requirements to be fulfilled by its system (here the aircraft), and an architecture model that represents the « black box » view of its system (high level functions and external interfaces). He starts designing the architecture of the system :

- Functions decomposition => Functional Breakdown Structure
- Identification of systems that constitute the aircraft => Product Breakdown Structure
- Allocation of functions to systems
- Identification of requirements sets for each system

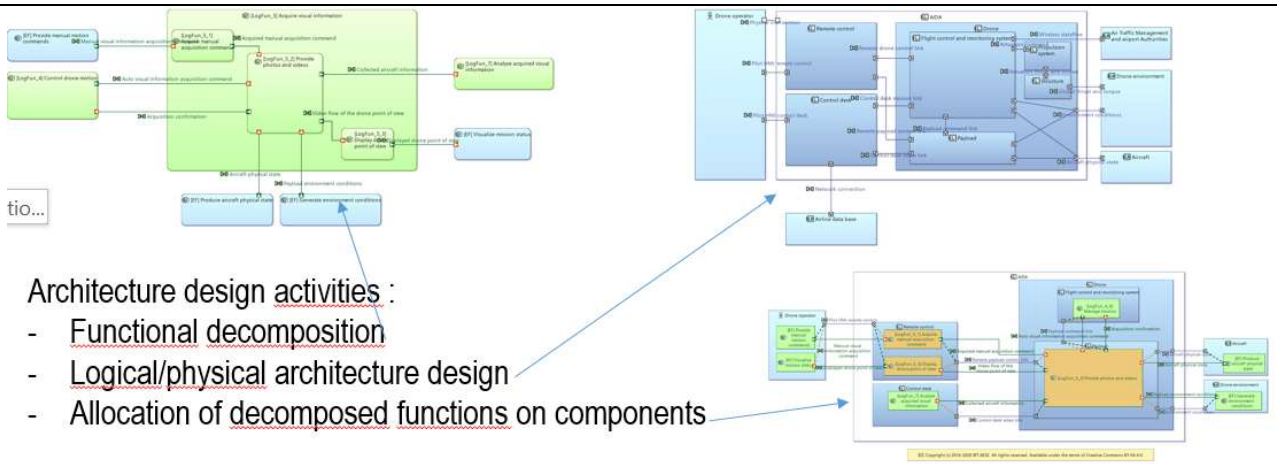


Figure 7 - Example of architecture design

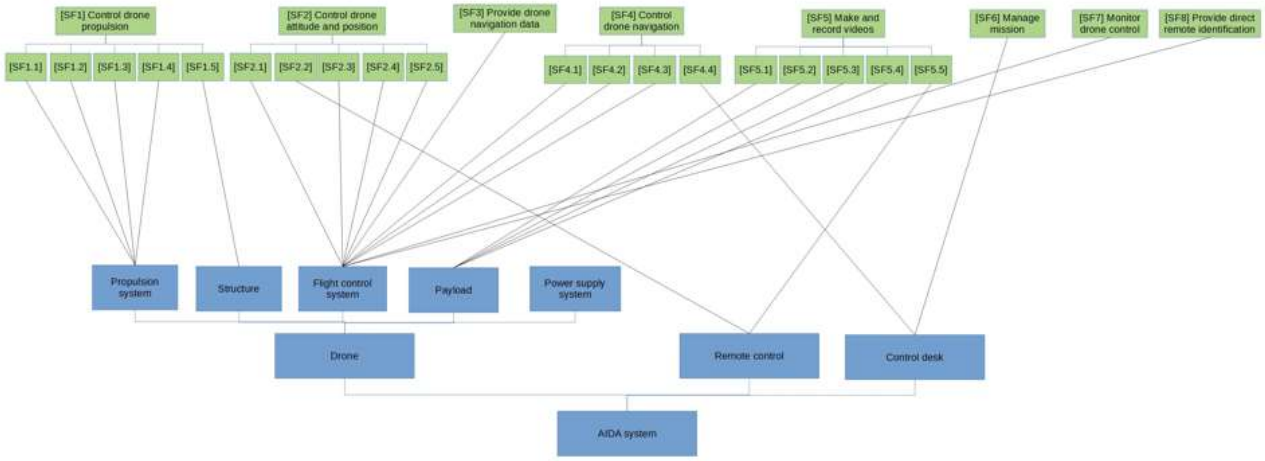


Figure 8 - Example of allocated functions allocated to systems

Example of textual aircraft Requirements allocated to systems; 2 cases are possible.

- Case 1: A/C level function is directly allocated to system. AIDA_fun_2 (SF6 – Define Mission – the AIDA system shall compute the authorized flight zone and the flight plan based on mission parameters provided by the data retrieved from the airline database) is directly allocated to the control desk (Control desk_0001)

Requirement Id	Requirement ID
Control desk_0001	**SF6 - manage mission** The control desk shall compute the authorized flight zone and the flight plan based on mission parameters provided by the pilot and mission data retrieved from the airline database.

- Case 2: A/C level function are refined for allocation to systems. AIDA_fun_9 (SF5 – Acquire visual information – The AIDA system shall acquire pictures or videos when the pilot commands an acquisition or when required for the flight plan execution) is refined into requirements for the remote control and for the payload

Requirement Id	Requirement text
Remote control_0005	**SF5.5 - Acquire manul payload control** The remote control shall acquire the manual payload control information from the operator and send it to the payload.

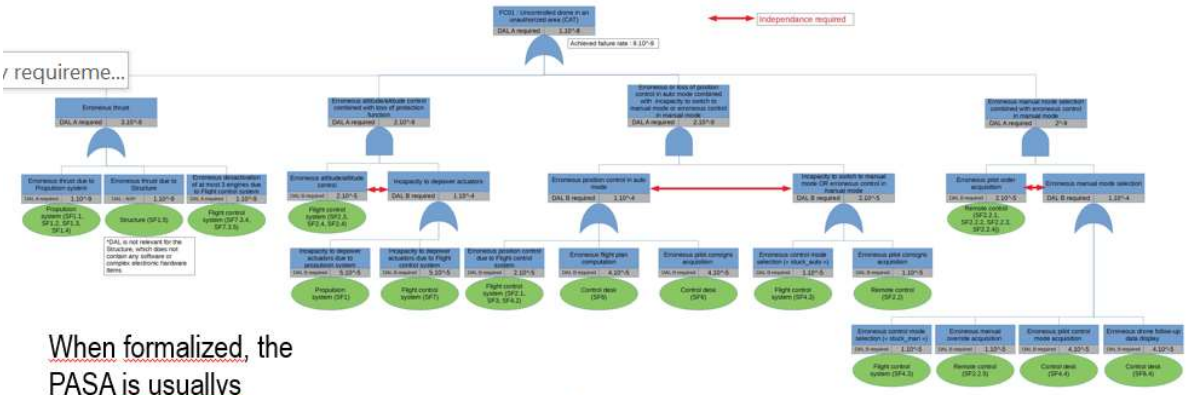
Requirement Id	Requirement text
Payload_0001	**SF5.1 - Select camera control** The payload shall compute the camera position consign, the photo and video acquisition command and the file storage format, from the manual payload control provided by the remote control and the automatic payload control information provided by the flight controller.
Payload_0002	**SF5.2 - Control camera orientation** The payload shall set the camera to the computed camera position consign.
Payload_0003	**SF5.3 Make photos and videos** The payload shall acquire photos and video when triggered by the payload control function.
Payload_0004	**SF5.4 Digitise photos and videos** The payload shall digitise photos and videos in the required format and send them to the control desk.

5

PASA Analysis :

The PASA identifies the interactions and dependencies between the different systems constituting the aircraft. It assesses how these interactions can lead to the aircraft FC, and aims at producing "aircraft safety requirements allocated to systems" in response to the previous "aircraft safety requirements" from AFHA. For this activity, Safety analyst uses the "list of allocated functions to systems" and realizes an interdependence analysis and an assessment of how these systems contributes the aircraft failure condition (failure condition evaluation). FTA (Fault Tree Analysis) can been used to clarify and assess the interactions between systems.

"PASA" then produces safety requirements which are necessarily the aircraft safety requirements declined to systems, with for each system: F-DAL mention, safety objectives allocated to systems, independence requirements, ...



When formalized, the PASA is usuallys based on high level fault trees.
FC and DAL requirements for systems are identified

Requirement Id	Requirement text
[PropSys_0003]	'The Propulsion system shall be designed so that the following Failure Conditions : - "Erroneous thrust due to Propulsion system" has failure rate lower than 1.10^-9 and does not result from a single failure. - "Incapacity to depower actuators due to propulsion system" has failure rate lower than 5.10^-5.'
[PropSys_0004]	'The Desing Assurance Level associated to the functions of the Propulsion system shall be as follows : - Control Propeller 1 : FDAL A - Control Propeller 2 : FDAL A - Control Propeller 3 : FDAL A - Control Propeller 4 : FDAL A

Figure 9 - Example of PASA Results and textual aircraft safety requirements allocated to systems

It can be noted that there are no standard recommendations for the display of PASA results. Upwards was a graphical representation based on Fault Tree. But a more tabular representation can also been used, based on an interdependence matrix, as below. This display flexibility can be problematic when consistency relies on data display control

Example from ARP 4761 Rev A (Marko Jim) of interdependence matrix :

			System	Wheel Brake System				...	Flight Control System							Engine		...
Aircraft Function	Aircraft Failure Cond #	Aircraft Failure Condition	System Function [illegible]	Control normal brake	Control emergency brake	Provide anti-skid	Provide auto-brake	...	Control ailerons	Control spoilers	Control rudder	Control elevator	Control stabilizer	Control flaps	Control slats	Control Thrust Direction	Control Throttle	...
Decelerate aircraft on ground	3.2.3.L1	Inability to stop the aircraft within the available runway		X	X	X	X	...		X				X	X	X	X	...
Decelerate aircraft on ground	#	Inadvertent activation of deceleration function on the ground		X	X	...	X	...	...	X	...	...	...	...	...	X		...

6

SFHA Analysis :

Then aircraft manufacturer leads SFHA, based on PASA results and on the “list of allocated functions to systems” from SE Side. Textual system safety requirements are produced.

The SFHA process is similar to the AFHA process, only the assessment is performed at system level, taking into account the functions allocated to each system.

Example of SFHA results (rights), based on propulsion system functions (links) :

Function ID	Functional BreakDown		Function failure ID	Functions failures	S/R repercussion Immediate effect of failure on Drone, operator, people around	Detection means warnings/hidden?	System Failure condition	Classification operability/ reliability
1	Control drone propulsion							
1.X		Control propeller X	Fm 1.1.1	Loss of one propeller control	Loss of one thrust on one propeller. Detected visually by the operator. Operator switches to Manual mode to land the drone. Controllability with 3 propellers is not sufficient to ensure that the drone will not go out of authorized area. Potentially flight in unauthorized zone leading at worst to fatalities.	Visually detected by operator	Erroneous thrust due to propulsion system	CAT
			Fm 1.1.3	Total loss of propellers control	Total loss of thrust. Crash in authorized area, potentially on inspected aircraft.	Visually detected by operator	Complete loss of thrust due to propulsion system	HAZ
			Fm 1.1.4	Erroneous thurst and torque provided by the propeller	Erroneous control of one propeller. Potentially flight in unauthorized zone leading at worst to fatalities.	Visually detected by operator	Erroneous thrust due to propulsion system	CAT
			Fm.1.1.5	Erroneous control of one propeller	Erroneous control of one propeller is detected by both the monitoring function and the operator. One motor is depowered. Operator switches to Manual mode to land the drone. Controllability with 3 propellers is not sufficient to ensure that the drone will not go out of authorized area. Potentially flight in unauthorized zone leading at worst to fatalities.	Visually detected by operator	Erroneous thrust due to propulsion system	CAT
			Fm1.1.6	Loss of actuators depower capability	No effect as long as the actuators depower is not requested by the monitoring function.	Hidden	Incapacity to depower actuators due to Propulsion system	HAZ

[SF1.1] Control propeller 1

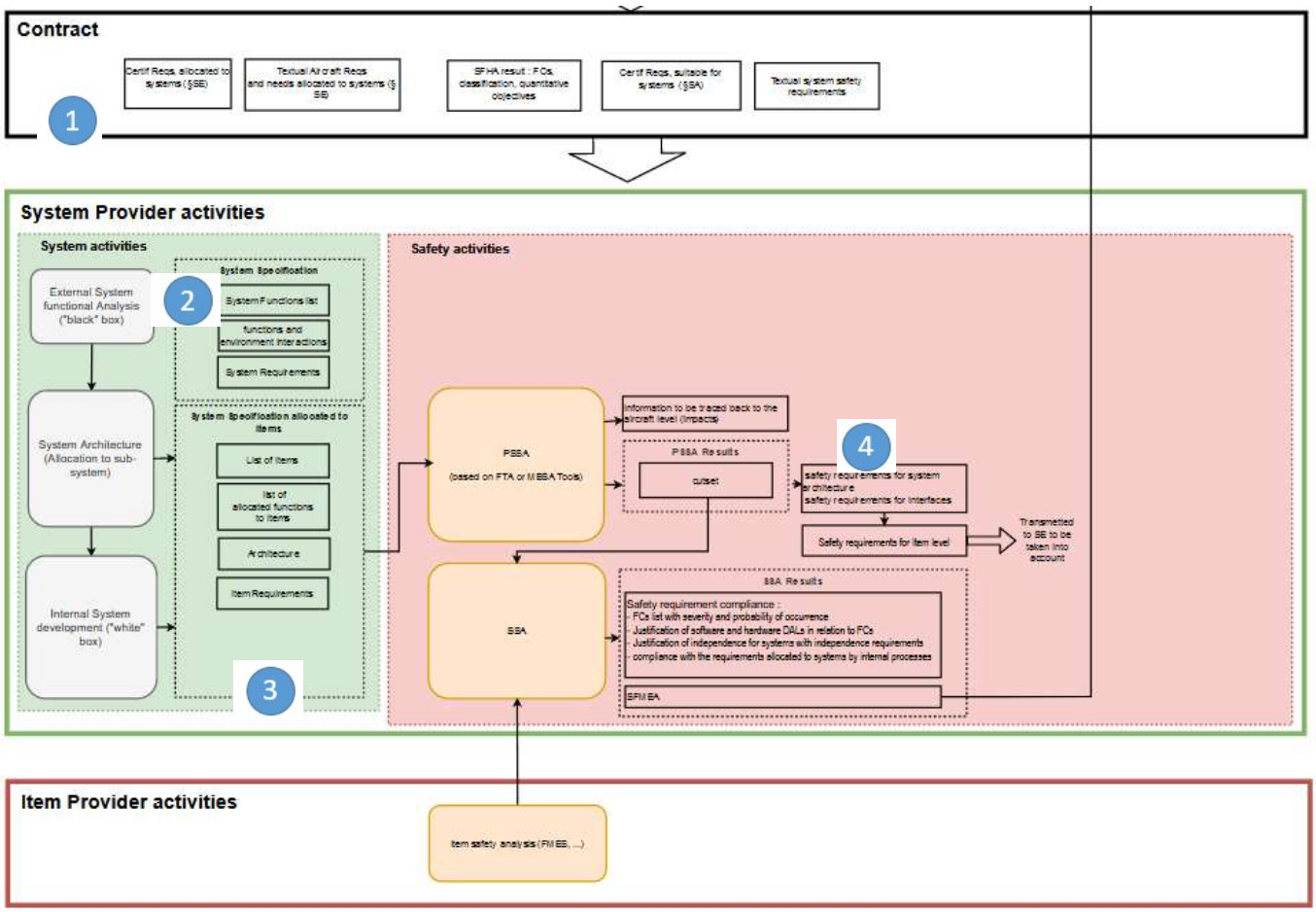
[SF1.2] Control propeller 2

[SF1.3] Control propeller 3

[SF1.4] Control propeller 4

List of Failure Conditions	FC title	Criticity	Failure rate objective
FC_prop_01	Erroneous thrust due to Propulsion system	CAT	1.10^-9
FC_prop_02	Incapacity to depower actuators due to Propulsion system	HAZ	1.10^-4
FC_prop_03	Complete loss of thrust due to Propulsion system	HAZ	1.10^-7

4.2 System supplier Activities



1	**Contract :** Aircraft manufacturer works with system providers on the basis of contracts that gather all information and requirements or needs that the systems providers have to satisfy. Thus, the first activity led by the System engineer or the safety analyst is to appropriate the content of the system and safety requirements from aircraft level. Such requirements are contractual data between the aircraft manufacturer and the system representatives, and they have to be well understood by system representatives to make sure that the developed system meet the requirements of aircraft manufacturer. For that reason, a data review is essential on both SE and SA sides to allow a common understanding of the aircraft manufacturer's needs and requirements. Following documents are contractual inputs for System layer analyses and illustrated on AIDA study case : Certification requirements allocated to system: no examples in AIDA. For an aircraft, we can find some items of the CS25 to be applicable directly to systems. Ex : CS25-903.a is allocated to the engine :

CS 25.903 Engines
(See AMC 25.903)

(a) *Engine type certification.*

(1) *reserved*

(2) Any engine not certificated to CS-E must be shown to comply with CS-E 790 and CS-E 800 or be shown to have a foreign object ingestion service history in similar installation locations which has not resulted in any unsafe condition.

(3) Any engine not certificated to CS-E must be shown to comply with CS-E 780 or be shown to have an ice accumulation service history in similar installation locations which has not resulted in any unsafe conditions.

Textual aircraft reqs and needs allocated to systems: they are the same as above (see § 5.1 n° 4).
Other example for the propulsion system

Requirement Id	Requirement text
[PropSys_0001]	The Propulsion system shall be composed of 4 identical propulsion units.
[PropSys_0002]	'The Propulsion system shall ensure the following functions : - Control propeller 1 - Control propeller 2 - Control propeller 3 - Control propeller 4'

SFHA results : (example for the propulsion system of AIDA)

List of Failure Conditions	FC title	Criticity	Failure rate objective
FC_prop_01	Erroneous thrust due to Propulsion system	CAT	1.10^-9
FC_prop_02	Incapacity to depower actuators due to Propulsion system	HAZ	1.10^-4
FC_prop_03	Complete loss of thrust due to Propulsion system	HAZ	1.10^-7

Certif reqs allocated to system (§SA): no examples in AIDA.

Textual system safety requirements :

Requirement Id	Requirement text
[PropSys_0003]	The Propulsion system shall be designed so that the following Failure Conditions : - "Erroneous thrust due to Propulsion system" has failure rate lower than 1.10^-9 and does not result from a single failure. - "Complete loss of thrust due to Propulsion system" has a failure rate lowere than 1.10^-7. - "Incapacity to depower actuators due to propulsion system" has failure rate lower than 1.10^-4.'
[PropSys_0004]	'The Desing Assurance Level associated to the functions of the Propulsion system shall be as follows : - Control Propeller 1 : FDAL A - Control Propeller 2 : FDAL A - Control Propeller 3 : FDAL A - Control Propeller 4 : FDAL A

2

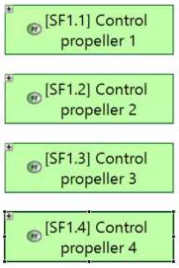
External System Functional Analysis / System specification :

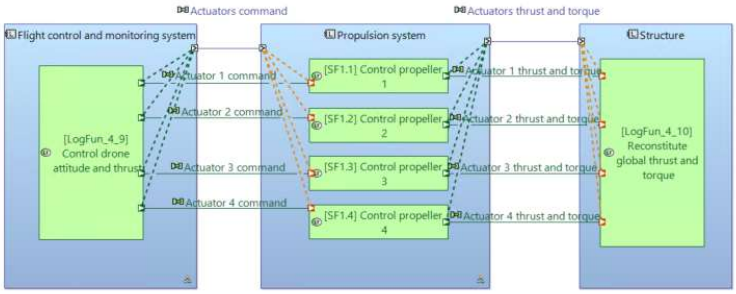
The SE activity at system layer starts with system specification, including, as for **Aircraft functional Analysis / Aircraft specification,** the description of functions, the interactions of these functions between them based on usual system functional analysis and diagrams (functional data flow, system states and modes, scenarios ans sequence diagrams).

These analysis are external to the system or black box analysis, as they consist in describing the functions visible by the other external systems and in interaction with them.

System functional requirements are produced that are declined then in sub-system and item requirements.

Example of system function list and corresponding functional Architecture :





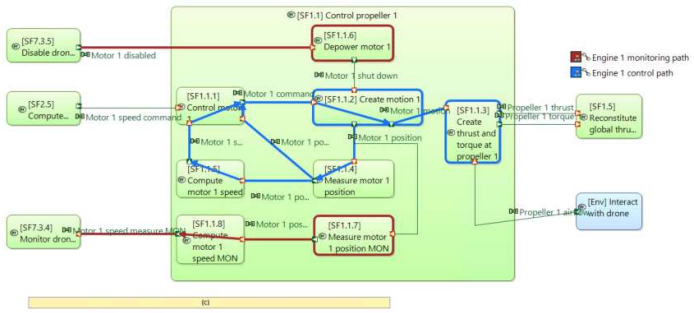
Example of functional System requirements :

Requirement Id	Requirement text
[PropSys_0001]	The Propulsion system shall be composed of 4 identical propulsion units.
[PropSys_0002]	'The Propulsion system shall ensure the following functions : - Control propeller 1 - Control propeller 2 - Control propeller 3 - Control propeller 4'
[PropSys_0003]	The Propulsion system shall be designed so that the following Failure Conditions : - "Erroneous thrust due to Propulsion system" has failure rate lower than 1.10^-9 and does not result from a single failure. - "Complete loss of thrust due to Propulsion system" has a failure rate lowere than 1.10^-7.
[PropSys_0004]	'The Desing Assurance Level associated to the functions of the Propulsion system shall be as follows : - Control Propeller 1 : FDAL A - Control Propeller 2 : FDAL A - Control Propeller 3 : FDAL A

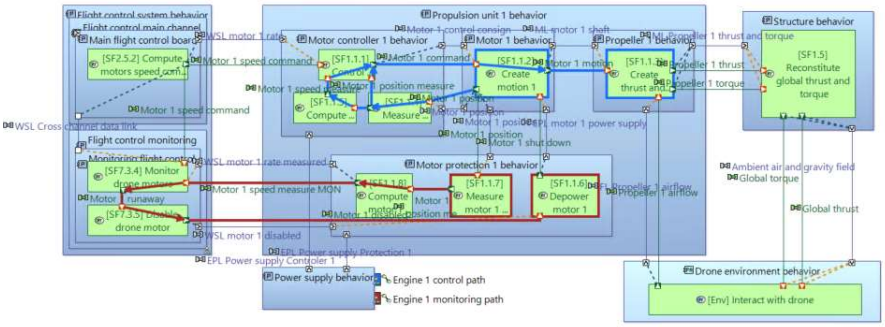
3

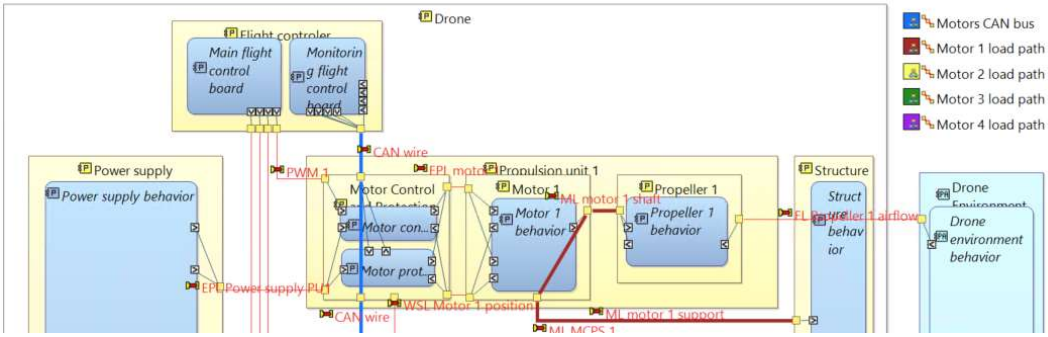
System Architecture / System Specification allocated to items :

In that phase, system engineer allocates previous external system requirements to sub-systems or items and refines these requirements. He uses functional, logical and physical views to describe internal functions of the system and interactions between them.

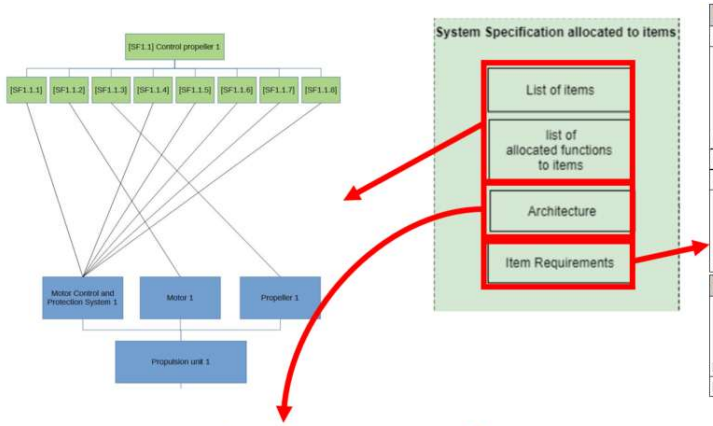


Example of Functional, logical and physical architecture design :





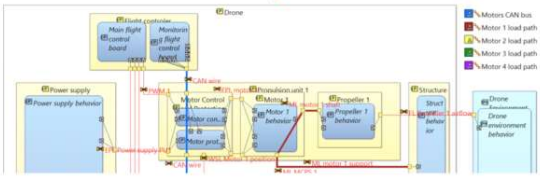
System engineer can then produce specification for items :



Requirement Id	Requirement text
Motor_0001	The motor shall be a brushless electrical motor.
Motor_0002	The motor shall receive a tri-phased electrical power supply from the MCPS. Power supply characteristic : - max input voltage : XX V - max peak current : XX A - Max continuous current : XX A'
Motor_0003	The motor shall have the following performances : to be defined
Motor_0004	The motor weight shall be lower than XXX g.
Motor_0005	The motor shall be fixed on the arm of the drone structure. Fixation characteristics : - max loads : TBC - removable

Requirement Id	Requirement text
Propeller_0001	The propeller shall have the following geometrical characteristics : - Diameter : XX mm - Number of blades : XX - Pitch : XX mm'
Propeller_0002	The propeller weight shall be lower than XXX g.

Items requirements



Requirement Id	Requirement text
Motor_propeller_0001	The motor axis shall allow the propeller fixing as defined below : - Axis diameter : XX mm - Fixing technology : to be defined - Max loads (axial thrust and torque) : to be defined

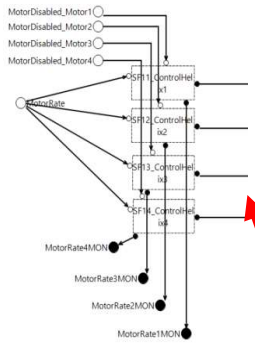
Interface requirements

4 PSSA Results

"architecture" activity produces as output "system specification allocated to items" which are taken as input data of the "PSSA". The "PSSA" then produces the "cutset", "safety requirements for item level", the "safety requirements for system architecture" and the "safety requirements for interfaces".

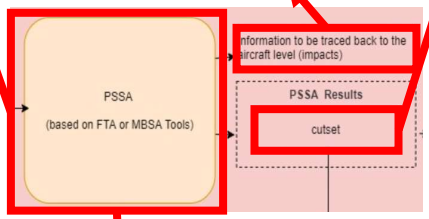
PSSA can be realized using FTA or MBSA tools and can reveal additional FC to be taken into account at aircraft level (considered as "information to be traced back to the aircraft level).

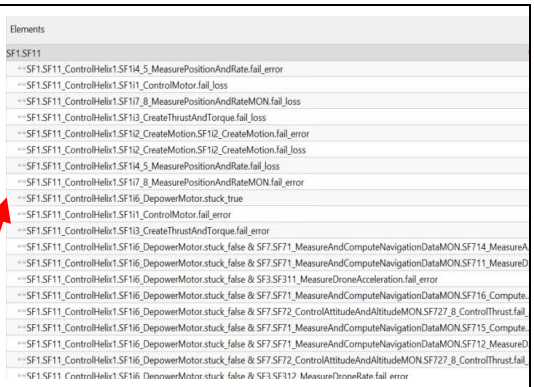
Example of cutset on Aida study case :



MBSA representation of the propulsion system for AIDA

The consequences of the failure mode « Propeller release » must be analyzed at aircraft level →Additional FC to be taken into account: « High energy part release, leading to personal injury » (HAZ)





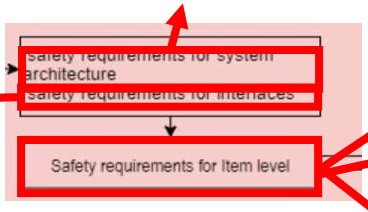
Minimal cutsets of order 1 and 2 for FC01 CA

Feared situation	Calculated probability
FC1_CAT_Uncontrolled_drone_crash_in_unauthorized_arez	4.8143E-5 /h
FC3_MAJ_Loss_of_drone_capability_mission_abortion	7.059E-3 /h
FC2_HAZ_Uncontrolled_drone_crash_in_authorized_arez	8.8252E-5 /h

FC evaluation results

Example of safety requirements for system architecture, interfaces or item level :

Requirement Id	Requirement text
FCS_0001	The Flight control system shall consist in two independant channels : - the flight control main channel - the flight control monitoring channel'



Requirement Id	Requirement text
Motor_propeller_0002	The interface between the motor and the propeller shall respect the following failure rates : - Propeller release :<1.10-7 - Complete loss of torque transmission : <1.10^-6

Requirement Id	Requirement text
Motor_0006	The motor shall respect the following failure rates : - Complete loss of rotation capability : <1.10^-6 - Erroneous rotation speed : <1.10^-6

Requirement Id	Requirement text
Propeller_0003	The propeller shall respect the following failure rates : - Complete loss of thrust due to propeller : <1.10^-6 - Partial loss of thrust due to propeller : <1.10^-6

Requirement Id	Requirement text
MCPS_0015	The MCPS shall respect the following failure rates : - loss of controlled electrical power supply to the motor : <1.1 - erroneous electrical power supply to the motor : <1.10^-6 - loss of motor depowering capability : <1.10^-5 - uncontrolled motor depowering :<1.10^-6 - loss of motor rotation speed measure : <1.10^-5 - erroneous motor rotation speed measure : <1.10^-6
MCPS_0016	The MCPS shall ensure that no single failure can lead to the simultaneous occurence of the following events : - erroneous electrical power supply to the motor - erroneous rotation speed measure
MCPS_0017	The Design Assurance Level associated to the MCPS is : IDAL A

4.3 *Verification / Validation activities*

To be completed in a further release

§ 4.1 and § 4.2 were design activities aiming at producing requirements to properly design aircraft, systems and items. Following SA activities are verification / validation activities and allow to check the compliance to FCs and DAL requirements at system and aircraft level.

FMEA/FMES

To be detailed

SSA Results :

SSA analysis is the latest safety analysis of the system level. This analysis is also the starting point of validation / verification activities. It takes as input the outputs of the "PSSA" and the "FCs", and produces the "safety requirement compliance" documents.

The SSA activity has not actually been performed on AIDA. So, following examples are dummy examples only to an illustration need :

Safety objectives				Compliance		
List of Failure Conditions	FC title	Criticity	Failure rate objective	Achieved failure rate	"No single failure" criteria	Compliance
FC_prop_01	Erroneous thrust due to Propulsion system	CAT	1.10^-9	4,35.10^-6	Not respected	NO
FC_prop_02	Incapacity to depower actuators due to Propulsion system	HAZ	1.10^-4	2,6.10^-5	N/A	YES
FC_prop_03	Complete loss of thrust due to Propulsion system	HAZ	1.10^-7	2,3.10^-7	N/A	NO

DAL requirements		Compliance	
Function	Allocated FDAL	Achieved FDAL	Compliance
Control propeller 1	A	A	YES
Control propeller 2	A	A	YES
Control propeller 3	A	A	YES
Control propeller 4	A	A	YES

ASA

To be detailed

4.4 *Aircraft Manufacturer / System Supplier interaction*

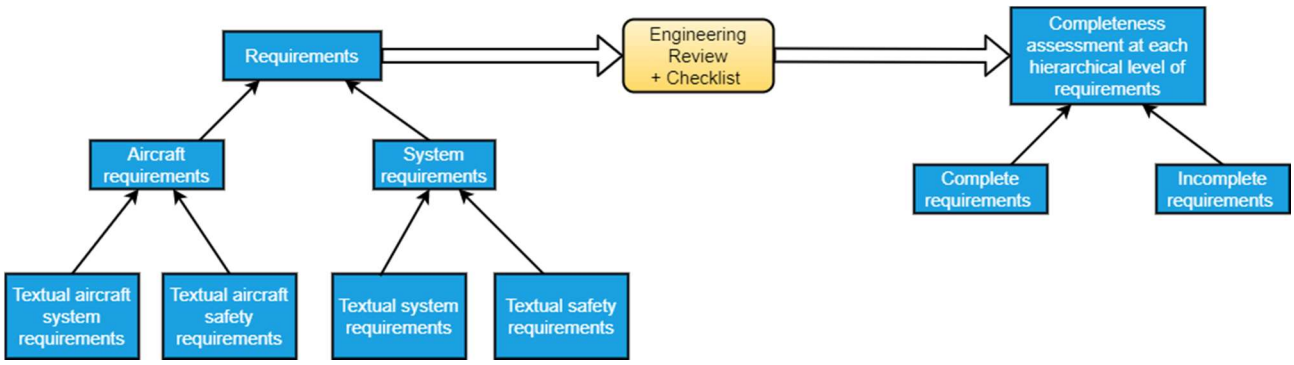
To come in a further release

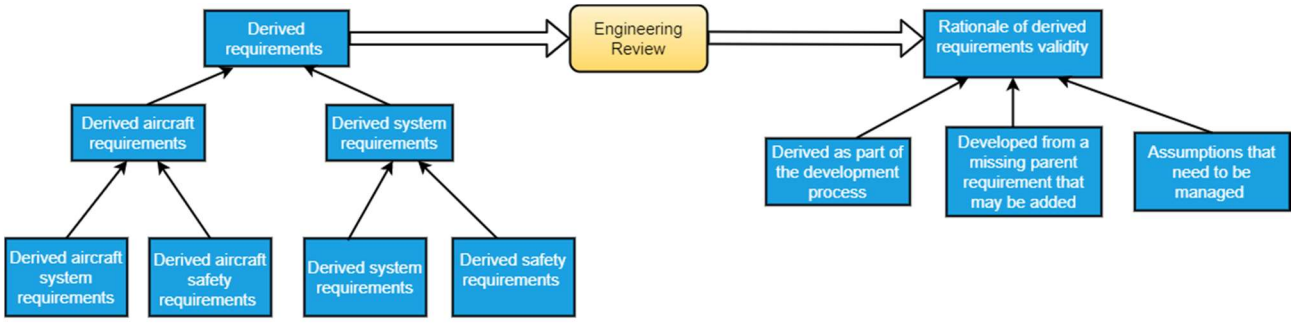
4.5 *Traceability View*

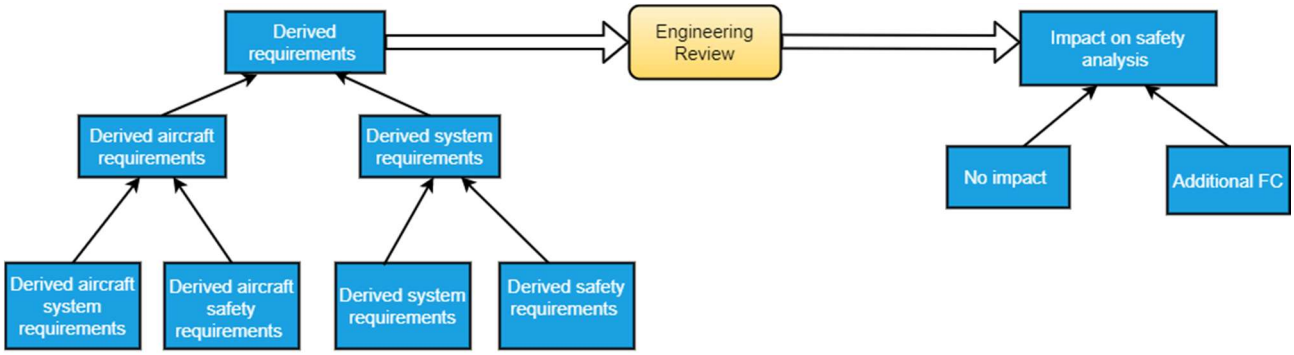
To come in a further release

4.6 Review view

Regardless of the requirements type (system requirements/ safety requirements) and their hierarchical level (aircraft level/system level), the ARP4754A urges the use of engineering reviews for three purposes (cf. section 3.3). Indeed, according to the ARP4754A an engineering review can be used to (1) assess the completeness of requirements, (2) determine the rationale of derived requirements validity, and (3) find out the impact of derived requirements on safety analysis. These three cases in which an engineering review is used are illustrated in the following figures:







In a next step, we intend to specify the different reviews that need to be performed at aircraft and system levels, while considering the three previous categories of reviews.

5 Conclusion

In the next steps of our study, we propose to:

- Present the main results of SystemX internship and consolidate these results for ensuring dynamic consistency between system and safety teams;

- Align SA results format and associated glossary: we noticed in § 4.1 that the same concepts could be displayed differently (Failure condition/Failure mode/function failure), depending on internal partner templates. Indeed, there is no unique data representation format that is shared between the different partners;
- Capture the review view and develop a checklist –based approach to assist the conduct of an SE/ SA review;
- Develop a general conceptual model of traceability (traceability view), with associated instantiation rules (guidelines: what artifacts to trace, why, and when);
- Investigate how scenario approach could help ensuring consistency: this approach is used at aircraft level to guide the AFHA analysis. We plan to check whether such an approach is relevant for other safety analyses.