Groupe de travail Ingénierie des Systèmes **Rapport 2017**

Commission R&D

GIFAS

Ref : GIFAS/5011/09-2017

LISTE DES AUTEURS

Nom	Prénom	Fonction	Société
ABIDA	Wassim	Primary Flight Control Systems Manager	UTAS (United Tech. Actuation syst.)
ALIX	Christophe	Direction Technique, Systems KTD – Strategy & Innovation Manager	THALES
BARICHARD	Xavier	Manager Recherche & Technologie, Innovation EuMEA Engineering	ROCKWELL-COLLINS FRANCE
BASORA	Luis	Systems Engineering Research Engineer	ONERA
BOUSSU	Stéphane	Head of Airworthiness Operations	AIRBUS
de CHAZELLES	Pierre	Systems Engineering Senior Advisor	AIRBUS
DEMATHIEU	François	Responsable Systèmes UxAV	DASSAULT AVIATION
FILLON	Aymeric	Responsable Ingénierie Système	SAFRAN
JANJAUD	Patrick	Processes & Methods, Development Quality, Airworthiness Manager	LIEBHERR AEROSPACE
HENRIQUEL	Xavier	Electro-Mechanical Group	UTAS
MILLOT	Philippe	Directeur Méthodes Ingénierie Système	Thales Avionics
MEUNIER	René	Systems Engineering Senior Expert	ex AKKA Technology / SAFRAN
MOYSAN	Arnaud	Responsable développement produits, et responsable processus "Concevoir"	SAFRAN VENTILATION SYSTEMS
PACI	Frédéric	Systems R&T Manager - Systems Engineering Senior Expert	ZODIAC AEROTECHNICS
PIGNIÉ	Gérald	Executive Expert Guidance, Navigation and Control & Systems Engineering	AIRBUS SAFRAN LAUNCHERS
TRIAY	Gilles	Directeur Latécoère Services	LATECOERE SERVICES

Coordinateur du Groupe de Travail : Gérald Pignié

RESUME DE SYNTHESE / EXECUTIVE SUMMARY

DATE : 31 Mai 2017

AUTEUR(S) : Membres du Groupe de Travail Ingénierie des Systèmes de la Commission R&D du GIFAS

TITRE : Rapport GIFAS sur l'Ingénierie des Systèmes. Première Edition

Contexte et enjeux

Pour **faire face aux nouveaux défis opérationnels** (par exemple : augmentation du trafic aérien, optimisation de la consommation énergétique, amélioration des aspects « privacy », arrivée massive des drones civiles et militaires, etc.), les secteurs aéronautique, défense, et spatial sont amenés à développer des systèmes de plus en plus complexes :

- les systèmes doivent intégrer des différenciations stratégiques par la mise en œuvre des meilleures technologies, moyens de production et services,
- Les schémas de collaboration tant internes qu'externes se complexifient (intégration multidisciplinaire, nouvelle organisation du travail collaboratif en interne, nouveaux partenaires, nouvelles typologies de contrat sur le cycle de vie du produit, …),
- L'environnement d'utilisation et l'environnement réglementaire de nos systèmes sont de plus en plus contraints (ED79A/ARP4754A[1], ACARE[2] …),
- La compétition accrue appelle une grande réactivité et une capacité à délivrer de façon fiable des solutions performantes, optimisées en coûts, avec des cycles de développement toujours plus courts.

Dans ce cadre, la mise en œuvre des pratiques **d'ingénierie des systèmes** est un **levier incontournable** :

- Formalisation des processus de conception et traçabilité des données, depuis la capture du besoin client, la définition des missions, jusqu'à la validation/qualification, et pour certains systèmes, la certification de la solution.

---

1 Nota : *L'ED79A/ARP4754A (Aerospace Recommended Practice) décrit les processus de développement à dérouler selon un niveau de rigueur demandé/négocié pour minimiser les erreurs de conception. Les Autorités l'imposent aux avionneurs comme standard de certification, standard qu'ils déclinent à leurs partenaires et fournisseurs.*

2 Nota : *ACARE : Advisory Council for Aviation Research and Innovation in Europe, organisme qui fournit des orientations stratégiques, techniques et institutionnelles potentielles, à la Commission Européenne.*

- Levée de risque et optimisation au plus tôt des systèmes[3] proposés – concept opérationnel, architecture, conception, développement, intégration, vérification, validation, industrialisation, production, opérations, retrait du service.
- Formalisation des collaborations entre les métiers au sein de l'entreprise et de l'entreprise étendue.
- Support à l'innovation, au travers d'une analyse approfondie des missions, des fonctions, et de leur valeur.

Constat

L'analyse des échecs techniques (abandons de programmes) ou économiques (dépassements de coûts et délais quasi-systématiques dans certains domaines), constatés sur de nombreux grands programmes, dans le périmètre de l'aéronautique, du spatial et de la défense, met fréquemment en évidence des défauts dont l'origine concerne des manques dans la maîtrise de l'ingénierie des système, bien souvent liés à la sous-estimation initiale de la complexité des programmes (exemples : oubli ou sous-estimation de parties prenantes, besoins insuffisamment exprimés, mauvaise maîtrise des interfaces, responsabilités et rôles des acteurs mal définis, …).

Dix recommandations du Groupe de Travail Ingénierie des Systèmes

A l'issue de la réflexion commune conduite, de nombreux constats ont été portés, et près de 100 recommandations ont été rédigées. Les dix plus importantes sont les suivantes :

- **R1** : L'ingénierie des systèmes introduit une vision transverse des processus et de l'entreprise, qui **fédère les disciplines et les spécialités de l'organisation traditionnelle** (spécialités techniques, programmes, assurance qualité, industrialisation, production, achats, services, ...). Afin d'être en mesure d'appréhender la complexité des systèmes futurs et d'être innovantes, nos sociétés se doivent de mettre en place de nouvelles organisations, permettant de déployer au mieux cette dimension transverse.

- **R2** : Promouvoir l'utilisation du Model-Based System Engineering (MBSE), car c'est un des moyens les plus adaptés pour **partager et gérer de façon cohérente** : scenarii opérationnels, capacités, chaines fonctionnelles, propriétés non fonctionnelles, interfaces, etc. de manière efficace et non ambigüe (en particulier : éviter les ambigüités liées à une description uniquement textuelle).

- **R3** : **Mettre à profit les phases amont**, dont la phase d'architecture, **afin de mettre en place les processus d'ingénierie collaborative**, ainsi que les méthodes et outils associés. Bien le refléter dans les contrats. Afin d'y parvenir, il peut être utile de faire une mise en correspondance (« mapping ») complète des méthodes et outils de chaque partie prenante, avant de statuer sur ce qu'on échange, et en vue de quelle finalité.

- **R4** : **Utiliser au mieux la validation amont** (par exemple avec des outils de simulation technico-opérationnelle) pour, en particulier (liste non limitative),

---

[3] Nota : *Un système est un ensemble d'éléments (matériels, logiciels, compétences humaines, processus, informations, services, et autres éléments supports) intégrés de telle sorte qu'ils fournissent, du fait de leurs interactions, les services correspondant à sa mission (objectifs à réaliser).*

clarifier les besoins du client, définir au plus tôt les périmètres opérationnel, d'emploi et d'usage, réduire la complexité liée à la multiplicité des contraintes (en utilisant une approche par scénarii par exemple), et simplifier ainsi la vérification aval.

- **R5** : Identifier, formaliser, et **maintenir le métier de l'ingénierie des systèmes dans nos entreprises**, prévoir une gestion prévisionnelle des compétences associées (référentiel de connaissances, reconnaissance, management des compétences, recours aux normes, et système qualité, ...) et promouvoir les formations :
    - Dans l'ensemble des écoles d'ingénieurs et des universités,
    - Au sein de nos entreprises,
    - Parmi tous les acteurs de l'entreprise étendue (acteurs de la supply chain : fournisseurs et prestataires).
- **R6** : **Identifier** clairement l'ensemble des **parties prenantes, et leur rôle** en fonction de la phase du cycle de vie. Prendre en compte l'ensemble de leurs contraintes, qu'elles soient organisationnelles, techniques, ou autres (politiques, économiques, environnementales, sociétales, …), pour alimenter les études de compromis et les prises de décision.

- **R7** : **Définir**, partager, et négocier **la stratégie d'intégration, de vérification, et de validation**, dès les phases amont du cycle de développement, entre client et fournisseur. Ceci permet, entre autres, de mieux maitriser les risques et de réduire les coûts.

- **R8** : Mettre en place une **démarche collaborative**, au niveau de **l'entreprise étendue** ; en particulier (proposition non limitative) :

    - Partager et négocier, dès le début de l'avant-projet, conformément aux périmètres de responsabilité et processus de décision définis, les attendus en matière de processus d'ingénierie des systèmes collaborative (dont l'ingénierie des exigences), et de certification système. Les tracer dans le contrat. Prévoir explicitement de négocier au cours du projet les attendus, non encore mis en œuvre dans le contrat, qui peuvent apparaître.
    - Travailler ensemble au niveau des processus, afin d'acquérir une compréhension commune (harmonisation du vocabulaire, …). Une telle approche permettra de rendre compatibles les différentes méthodes et processus IS outillés des parties prenantes. L'ISO 15288 pourrait servir de standard de convergence.
    - Favoriser le travail collaboratif entre les parties prenantes, expliciter et capturer les données techniques et programmatiques (cadres d'architectures et modélisation).
    - Agréer, avant contractualisation, entre donneur d'ordre et fournisseur(s) les jalons de développement (revues et/ou « Maturity Gates »), les contenus fonctionnels des livrables, et leur jalonnement, en cohérence avec leur utilisation (système, équipement, logiciel). Telle fonction devant être disponible pour telle application (banc sol, banc volant, banc d'intégration, 1er vol…). Le traduire dans la négociation du contrat, en commun avionneur / plateformiste / donneur d'ordre - fournisseur (« avionneur – systémier »).

- **R9** : Mettre en place, conjointement avec les autorités de certification, une **réflexion visant à diminuer la documentation livrable** (suppression de la documentation livrable difficilement exploitable), et de remonter de manière plus simple les preuves nécessaires à la certification. Cette réflexion pourrait être portée dans un premier temps par un Groupe de Travail GIFAS, en lien avec l'EASA-FAA, et au besoin les autres autorités de certification (ministères de la défense européens, ou autres).

- **R10** : Afin de rester dans une approche « gagnant-gagnant », lorsqu'on effectue une analyse de la valeur des exigences de haut niveau, il peut être fructueux de comparer et de partager, entre client et fournisseur(s), une solution conçue ad hoc pour répondre au besoin exprimé, et une solution issue d'une **ligne de produits existants** (solution de type **réutilisation**) plus attractive économiquement, même si elle répond de manière moins parfaite à ce besoin.

Sommaire

1. QU'EST-CE QUE L'INGENIERIE DES SYSTEMES? ORIGINES ET MOTIVATION

Pour connaître les motivations du Groupe de Travail GIFAS, le lecteur pourra se reporter au paragraphe §1.8 .

1.1 QU'EST-CE QU'UN SYSTEME ?

Beaucoup d'organisations constatent, depuis une trentaine d'années, que leurs produits et leurs services sont devenus de plus en plus complexes. Cela a engendré une difficulté accrue dans le développement de ces produits jusqu'à même atteindre un point tel que les efforts nécessaires pour maîtriser la complexité peuvent dépasser leurs capacités ou leurs compétences.

A ce point, les notions de produits ou de services se complètent et s'associent sous la notion de « Système »[4], qui peut se définir comme « une combinaison d'éléments en interaction, organisés de façon à réaliser un ou plusieurs objectifs dans son environnement. »

Un système relevant de l'Ingénierie des Systèmes est donc formé d'éléments (matériels, logiciels, compétences humaines, processus, informations, services, et autres éléments supports) intégrés de telle sorte qu'ils fournissent, du fait de leurs interactions, les services correspondant à sa mission (objectifs à réaliser).

On notera en premier lieu que cette mission doit être définie. Après avoir examiné et caractérisé le cadre du problème à traiter, de la mission, ce sont les activités de l'analyse opérationnelle, qui permettront de capturer et de formuler de manière claire et non ambigüe les exigences de haut niveau s'appliquant au système.

Ce travail sera complété en aval par les différents points de vue architecturaux, l'analyse fonctionnelle, l'ingénierie des exigences, associée de plus en plus systématiquement à une modélisation fonctionnelle, qui permettront de définir les exigences détaillées du système, de ses interfaces, et de ses constituants.

Ce sera l'objet abordé au chapitre 5 du présent rapport.

On notera également que le système global, que l'on pourra par la suite appeler Solution, est bien l'ensemble constitué d'une part par le « Système Principal » ou le « Système Réalisé » (« System of Interest », ou « End-Product », en anglais), souvent considéré comme la « partie noble » (par exemple : avion, radar, satellite, missile, …), et d'autre part les « Systèmes de Soutien » ou « Systèmes Contributeurs » (vocabulaire AFIS pour traduire l'anglais « Enabling Systems »), que l'on pourra aussi dénommer systèmes de support, tels que décrits par le schéma 1.1, en début de la page suivante.

---

4 Nota : *En fait c'est la démarche qui est de nature systémique. Cette démarche peut s'appliquer génériquement à tout type de système, de produit ou de service. A titre d'exemple, on peut citer : un système d'armes, un aéronef, une flotte d'aéronefs, un satellite, un service de communications satellitaires, un service de lancement, un lanceur spatial ou un missile, un système avionique sur avion, un système de conditionnement d'air, un propulseur, un train d'atterrissage, …*

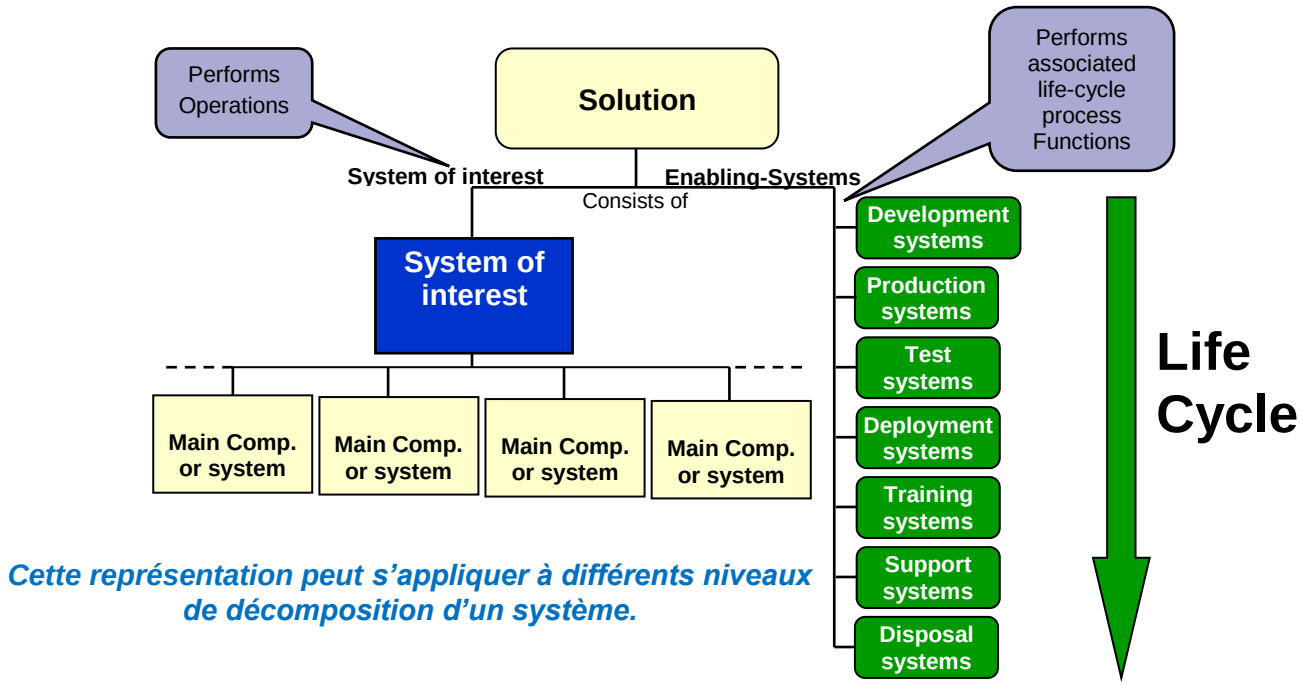


Schéma 1.1 Système Global ou Solution et Système Principal (Source : d'après EIA 632 ; courtoisie de Pierre de Chazelles, Airbus).

Comme exemple de Systèmes de Soutien, on trouvera les moyens de tests, les moyens de déploiement, de support, de formation, de retrait du service … C'est bien ce système global qui fournit le service attendu.

On pourra noter que cette vision du schéma 1.1 est récursive : chaque composante principale (ou sous-système) du système évoqué peut elle-même être vue comme un système à part entière, et décomposée sur ce même principe. Ainsi la notion de système doit être vue comme relative.

Un système passe par différentes phases de vie allant de l'émergence de son besoin jusqu'à son retrait de service. L'Ingénierie des Systèmes doit non seulement définir le système, mais aussi tous les processus et produits nécessaires ou associés à son cycle de vie, tels que définis dans le schéma 1.2 ci-dessous.

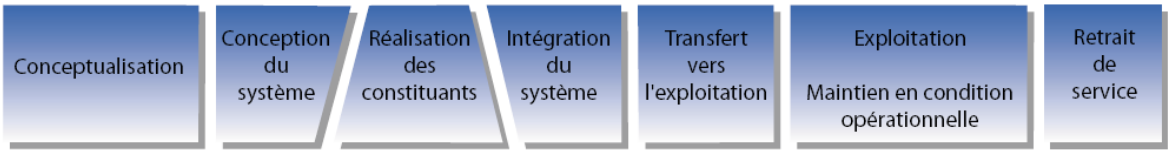


Schéma 1.2 Cycle de vie d'un système (source AFIS)

On notera qu'un nouveau système peut dans certains cas bénéficier de systèmes existants (« Legacy Systems » en anglais), et qu'ainsi on ne part pas d'une situation vierge. On notera également qu'un nouveau système peut avoir à s'insérer dans un ensemble de systèmes existants, sans les perturber ni dans leurs interfaces ni dans leurs services rendus.

Ainsi différents systèmes apportant chacun sa valeur ajoutée peuvent coexister, avec des fonctionnements liés ou non suivant les cas, et des cycles de vie indépendants.

La notion permettant d'aborder cet aspect d'immersion d'un système dans un ou plusieurs ensembles plus vastes est connue sous le nom d'approche « Systèmes de systèmes » (en paraphrasant l'anglais « Systems of Systems »).

Enfin, on peut avoir à considérer, au lieu d'un seul système (ou produit), un ensemble de systèmes, partageant des éléments communs et adaptés à différents clients ou marchés, et susceptibles d'évoluer et de conduire à des variantes. Par la suite, cet aspect sera traité au travers de la notion de ligne de produits.

1.2 ORIGINES/HISTORIQUE DE L'INGENIERIE DES SYSTEMES

Selon le Handbook de l'INCOSE (International Council on Systems Engineering), l'origine de l'ingénierie des systèmes remonte aux années 1930.

On notera comme grandes étapes :

1937	Une équipe pluridisciplinaire britannique analyse dans sa globalité le système de défense aérienne.
1939-1945	Les laboratoires Bell Labs conduisent le développement du système NIKE, premier projet de missiles anti-aériens. Les Bell Telephone Laboratories sont les premiers à utiliser le terme « Systems Engineering »
1951-1980	Le MIT conduit le design et le management du système SAGE de défense aérienne
1956	Invention de la méthodologie d'analyse des systèmes par la RAND Corporation
1962	Publication de *A Methodology for Systems Engineering* (Arthur D. Hall)
1968-1969	Jay Forrester : Principles of Systems, Urban Dynamics (*Modelling Urban Systems*), Pegasus Communications
1990	La société savante NCOSE (National Council on Systems Engineering, société américaine) est créée
1995	NCOSE se transforme en INCOSE (International Council on Systems Engineering), pour incorporer la vision internationale
1995	La NASA publie son premier "NASA System Engineering Handbook"
2000	Création de l'AFIS, comme chapitre français de l'INCOSE, de statut association loi de 1901.

Table 1.1 Grandes étapes de création de l'IS (source : Handbook de l'INCOSE)

1.3 NORMES ET STANDARDS RELIES A L'INGENIERIE DES SYSTEMES

En parallèle différents standards et normes ont été créés, dont certains proviennent du monde de l'ingénierie logicielle et avionique. Du fait que les sources viennent du monde de la qualité, du management, et de l'ingénierie des systèmes électriques, avioniques et logiciels, et qu'elles adressent différents domaines tels que la défense, l'aéronautique civile et le spatial, on trouve naturellement beaucoup de normes, qui sont en fait très largement complémentaires.

Parmi les plus importantes on citera ici la norme ISO/IEC 15288 « Systems Engineering – System Life-Cycle Processes » (première version en 2002, deuxième version en 2008, dernière mise à jour en mai 2015), le triplet DO-178 (version B ou C), DO-254 et ED79/ARP4754 (version d'origine et version A), pour l'aéronautique civile, et les normes ECSS qui adressent largement l'ingénierie des systèmes (plusieurs documents dédiés), pour le spatial.

C'est dans le monde de la défense, aux Etats-Unis, qu'est apparue la première norme d'ingénierie des systèmes, la MIL-STD-499 "Military Standard: System Engineering Management" (17 Jul 1969). Cependant, en 1994, un Mémorandum du secrétaire à la défense américain, William Perry, supprime le recours à des normes spécifiques sur les programmes d'acquisition du département de la défense (DoD), et pousse les fournisseurs d'équipements militaires à adopter des pratiques commerciales en accords avec le standard EIA 632 IS (Standard Intérimaire), puis avec le standard IEEE 1220 (Version d'essai) en lieu et place de la MIL-STD-499A. De ce fait la MIL-STD-499B n'a jamais été approuvée, et la MIL-STD-499A a été annulée sans remplacement en 1995.

Un gros travail de formalisation a donc été entrepris, par les industriels comme par les agences et les personnels étatiques, via des standards ISO et IEEE tels que l'ISO/IEC 15288, l'ISO/IEC 26702, l'EIA/ANSI 632, et l'IEEE 1220, auxquels il convient de rajouter pour l'aéronautique l'ED79/ARP4754A et l'ED135/ARP4761, et pour l'espace les ECSS (pour « European Cooperation for Space Standardisation » ; pour l'ingénierie des systèmes, on y trouve en particulier : ECSS-E-ST-10C, ECSS-E-ST-10-xx, ECSS-M-ST-10C Rev.. 1, et ECSS-M-ST-10-01C, …).

L'instanciation et la déclinaison pratique de ces standards sur nos secteurs d'activité est déjà très largement en cours. Cependant, cette déclinaison est conduite de manière plus ou moins spécifique, dans chacune de nos entreprises. Une mise en commun du retour d'expérience reste, en partie au moins, à faire.

On trouvera plus de détails sur ce thème au chapitre 4 du présent rapport.

1.4 LES DIFFICULTES RENCONTREES SUR LES GRANDS PROGRAMMES AYANT CONDUIT A LA STRUCTURATION DE L'IS (SOURCE AFIS)

L'analyse des échecs techniques (abandons de programmes) ou économiques (dépassements de coûts et délais quasi-systématiques dans certains domaines), constatés par le passé sur de nombreux grands programmes, dans le périmètre de l'aéronautique, du spatial et de la défense, met fréquemment en évidence des défauts dont l'origine concerne des manques dans la maîtrise de l'ingénierie des systèmes, bien souvent liés à la sous-estimation initiale de la complexité systémique des programmes.

A titre d'exemples, on peut citer : Les dépassements économiques majeurs et deux accidents en vol, sur le programme de Navette spatiale américaine, l'échec du programme européen d'avion spatial Hermès, la sous-estimation flagrante du coût du véhicule spatial automatique européen ATV – même si celui-ci a par la suite réussi ses cinq missions quasi parfaites de rendez-vous et docking, les difficultés d'industrialisation de l'Airbus A380 – bien que le prototype ait brillamment réussi ses essais en vol, et probablement également le manque de maîtrise dans l'intégration de technologies en rupture, pour le Boeing 787. Dans d'autres domaines industriels, on peut citer: l'incendie du porte-avion américain USS Forrestal, la conception et la mise en service du tunnel sous la Manche, la conception du porte-avion Charles de Gaulle, celle des centrales nucléaires EPR en Finlande et à Flamanville, etc…), ainsi que les difficultés de mise en service de systèmes tel le système de réservation de la SNCF, … Parmi ces origines nous pouvons citer :

- Oubli ou sous-estimation de parties prenantes,
- Méconnaissance du domaine opérationnel,
- Attentes de certaines parties prenantes mal perçues, et/ou mal ou non formalisées,
- Spécifications imprécises et incomplètes (Besoins insuffisamment exprimés),
- Processus de gestion des exigences déficient,
- Communication entre acteurs non maîtrisée ;
- Mauvaise maîtrise des interfaces,
- Solutions non justifiées, ,
- Solutions non validées (par exemple: manque de maturité d'une technologie au début d'un développement),
- Mauvaise maîtrise de la configuration,
- Responsabilités et rôles des acteurs mal définis,
- Ressources et compétences mal planifiées et non disponibles lors de leur sollicitation,
- Formation des utilisateurs insuffisante,
- Problèmes de logistique, d'exploitation, et de maintenance non anticipés,
- Evaluation des coûts et planning insuffisamment étayée,
- Ignorance, ou déni de la complexité, …

Selon des statistiques effectuées par l'INCOSE en 1995 et en 2004, et relayées en France par l'AFIS (Association Française d'Ingénierie Système, chapitre français de l'INCOSE), on constatait encore dans un passé relativement récent (10-15 ans), des taux encore élevés de défaillance partielle ou totale, dans des grands projets systèmes. Plus précisément :

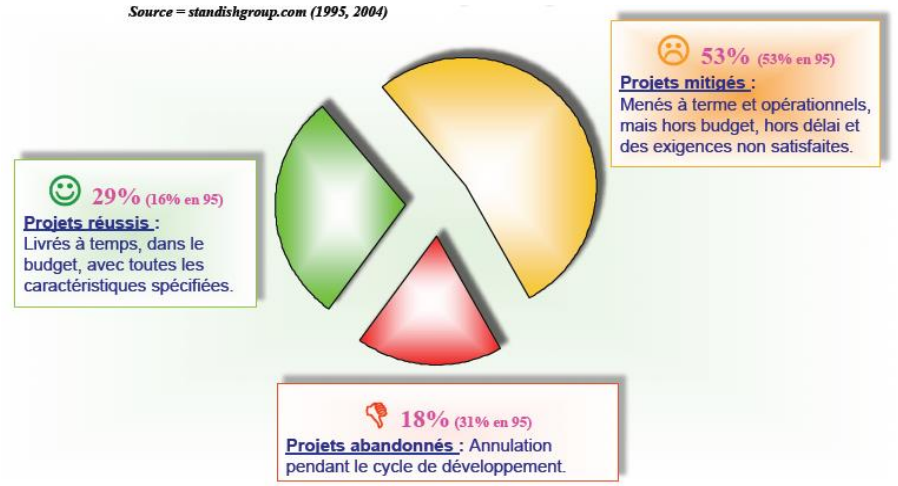
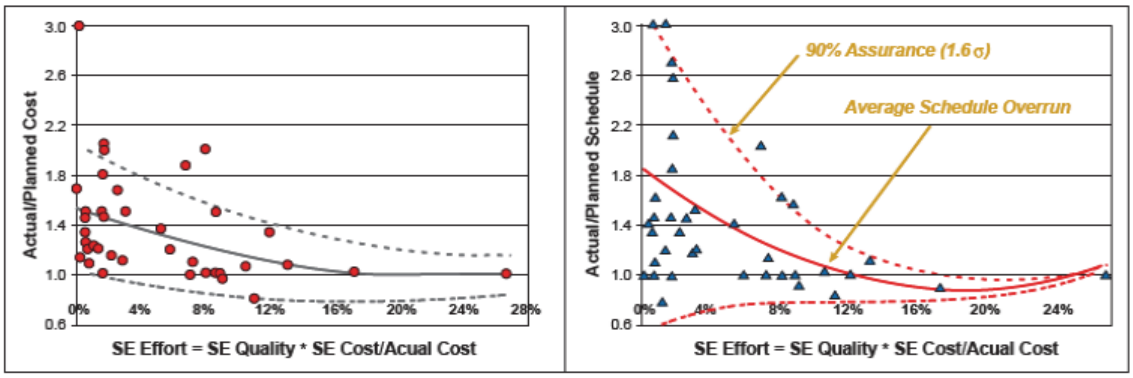


Schéma 1.3 Statistiques sur le succès des grands projets « système » américains (AFIS)

On a constaté, au cours des décennies passées, que l'aboutissement à un système satisfaisant requiert des organisations spécifiques et une étroite coordination des moyens. La structuration de l'Ingénierie des Systèmes en tant que discipline est l'un des résultats de ces expériences. Une analyse conduite par l'INCOSE déjà cité plus haut a permis de dégager une nette corrélation entre l'effort d'ingénierie des systèmes consenti sur un programme et sa capacité à tenir ses performances, ses délais et ses coûts :



Dépassements de coûts et de délais corrélés avec l'effort d'ingénierie système

Eric Honour, Understanding the Value of Systems Engineering, *INCOSE, 1996.*

Schéma 1.4 Corrélation entre les performances des grands projets « système » américains,en matière de tenue des coûts et délais, et leur effort d'ingénierie des systèmes.

Cependant, si des progrès très significatifs ont été accomplis, avec des taux d'échecs en forte baisse, de nombreux chantiers d'améliorations restent à conduire.

1.5 LES SOCIETES SAVANTES TRAITANT DE L'IS (INCOSE ET AFIS)

Le rôle majeur de l'AFIS, Association Française d'Ingénierie Système, et au niveau international de l'INCOSE (International Council for System Engineering, dont l'AFIS constitue le « chapitre » français) est de confronter les expériences, et d'imaginer des solutions, pour améliorer les pratiques, de promouvoir le développement de l'Ingénierie des Systèmes, et de la recherche associée. On pourra se reporter à la vision 2020 de l'AFIS, et à « l'horizon 2025 » de l'INCOSE (en anglais), cités en référence.

A noter que le nombre de sociétés spécialisées, de colloques, congrès, séminaires sur l'IS est en augmentation constante.

1.6 APPORTS ATTENDUS DE L'IS (SOURCE AFIS)

L'approche ingénierie des systèmes est déjà largement répandue dans nos domaines d'activité, mais compte tenu de la complexité croissante de nos systèmes, son extension et sa systématisation, avec une approche processus rigoureuse et outillée, est impérative.

Globalement, on attend de la bonne mise en œuvre de l'Ingénierie des Systèmes, du fait de son approche coopérative et interdisciplinaire d'ingénierie globale, une amélioration sur :

- L'adéquation aux besoins et la qualité des produits et systèmes,
- L'anticipation des problèmes et de la maîtrise des risques concernant tant le projet que le système et son environnement tout au long du cycle de vie,
- La maîtrise de la complexité des grands systèmes et produits complexes,
- La tenue des délais, et des temps de développement,
- La maîtrise des coûts, avec notamment une anticipation très en amont du coût global du cycle de vie (production, tests, déploiement, support, formation, retrait du service),
- L'efficacité dans la maîtrise de la coopération de la transdisciplinarité et de multiples acteurs,
- La satisfaction de toutes les parties prenantes, et, en guise de synthèse, une meilleure optimisation du compromis global enjeux sur contraintes, tant sur les produits et systèmes, que les lignes de produits.

Ainsi, le déploiement et la mise en œuvre d'une bonne Ingénierie des Systèmes, appuyée sur des processus rigoureux et outillés, permettent-ils aux entreprises de maintenir et d'améliorer leur compétitivité. L'intérêt de la bonne mise en œuvre de l'ingénierie des systèmes apparaît tout particulièrement dans les phases amont de spécification et de conception du système. En effet, comme l'illustre la figure ci-dessous, la majeure partie du coût global de possession (réalisation et utilisation) d'un système résulte des décisions prises lors de ces phases.

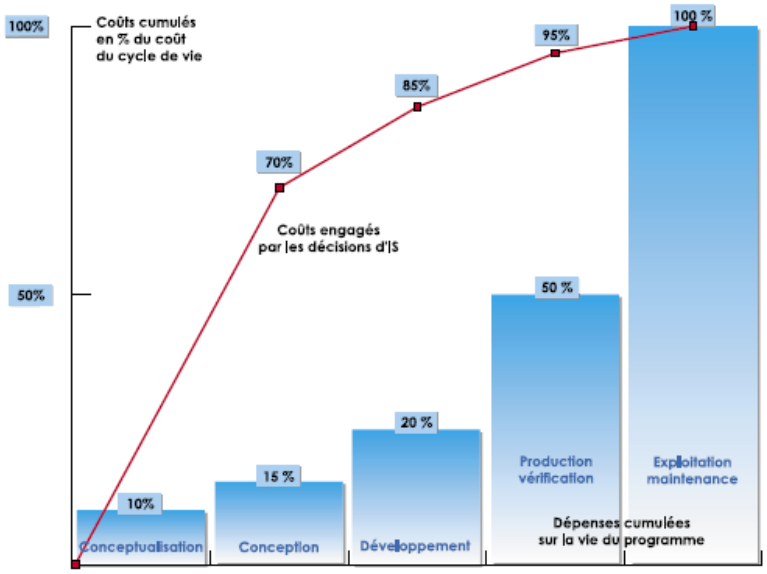


Schéma 1.5 Evolution des coûts cumulés des grands projets « système »
(*) Source : Defense System Management College 9-1993, citée par l'AFIS

A ce titre, il convient de ne pas oublier que l'analyse du soutien logistique doit être conduite dès le début du projet, pour optimiser les coûts de mise en service et d'utilisation du système.

L'importance de l'ingénierie des systèmes est illustrée sur le schéma suivant 1.6a :

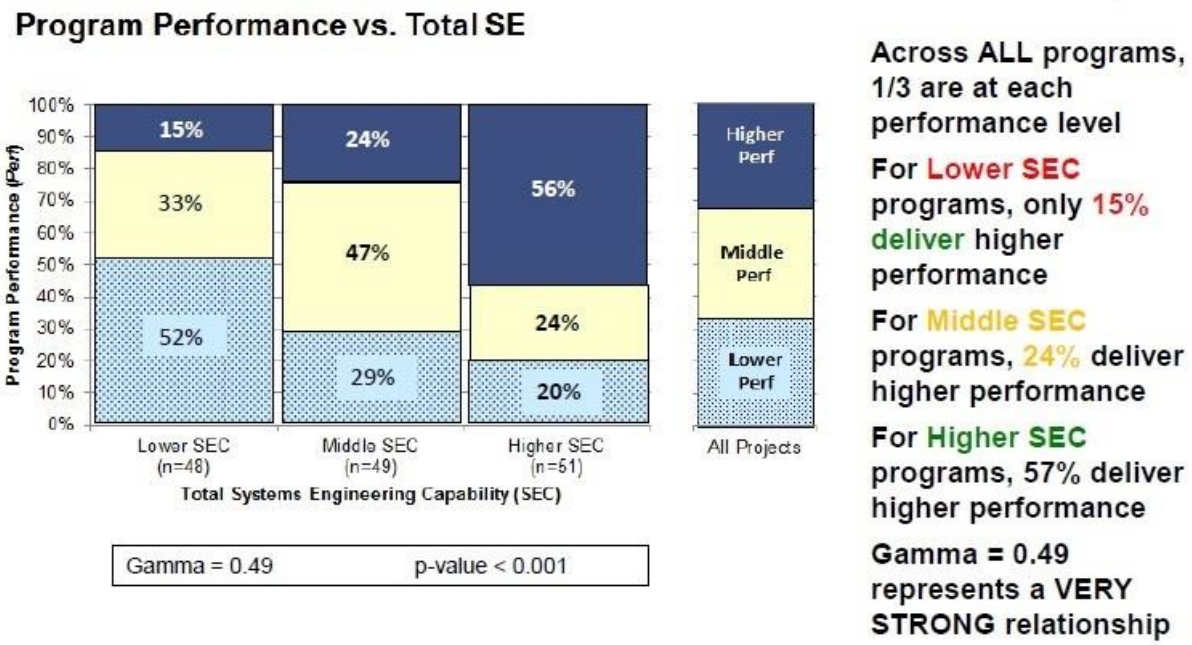


Schéma 1.6a Impact de la maturité des processus d'IS sur les performances des grands projets. Source: The 2012 SE Effectiveness Study, Joseph P. Elm & Dr. Dennis Goldenson, Software Engineering Institute, copyright Carnegie Mellon University and IEEE, in INCOSE Workshop June 24-26 2013, Philadelphia PA (work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003)

L'importance de l'ingénierie des systèmes est encore plus évidente si l'on regarde les programmes présentant des challenges forts (techniques, programmatiques, …), comme le montre le schéma 1.6b :

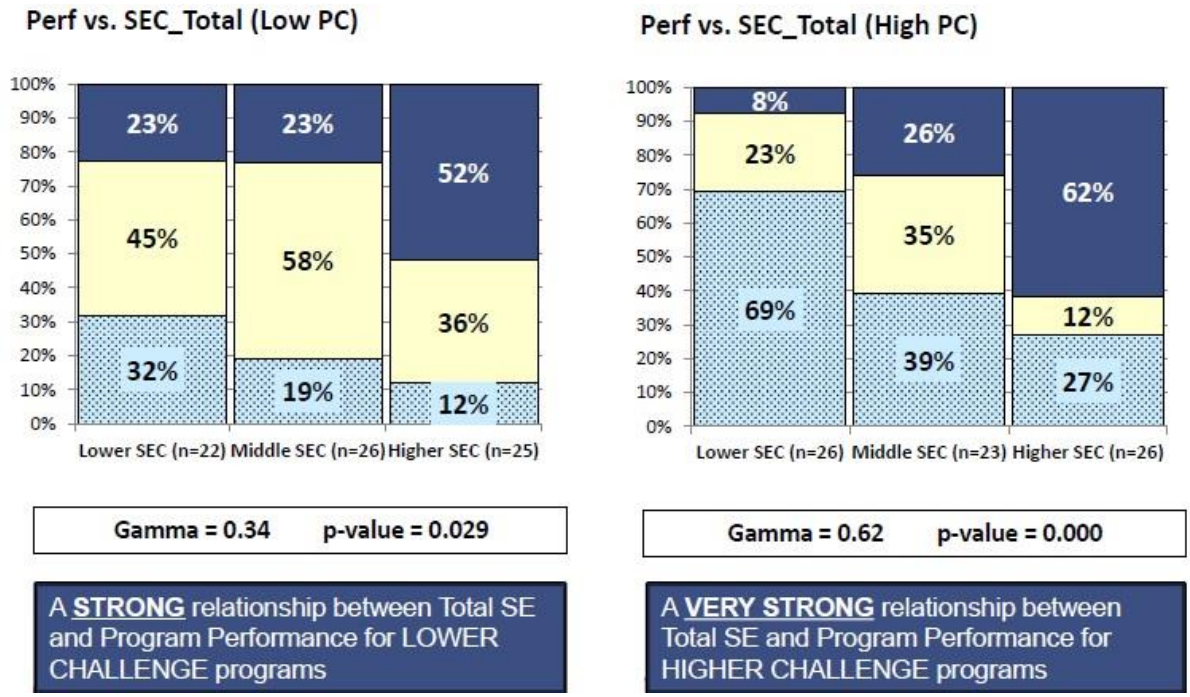


Schéma 1.6b Impact de la maturité des processus d'IS sur les performances des grands projets, selon que les projets sont à forts ou faibles challenges. Source : The 2012 SE Effectiveness Study, Joseph P. Elm & Dr. Dennis Goldenson, Software Engineering Institute, copyright Carnegie Mellon University and IEEE, in INCOSE Workshop June 24-26 2013, Philadelphia PA (work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003)

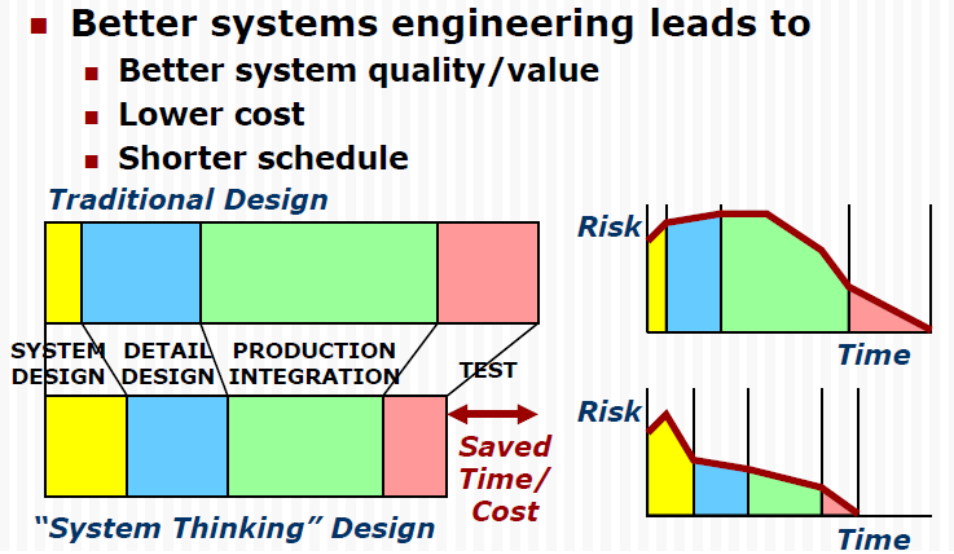


Schéma 1.7 Impact de la maturité des processus d'IS sur les performances des grands projets, selon la thèse d'Eric Honour, (« Systems Engineering Return on Investment, PhD thesis », Univ South Australia 2013)

L'Ingénierie des Systèmes (IS) n'est pas une révolution mais une démarche systématique, qui intègre de manière structurante les retours d'expérience, tant pour les méthodes que pour les bonnes pratiques. Cependant, sans être une révolution, l'approche systémique, par opposition à l'approche des spécialistes d'une discipline, constitue un choc culturel.

Pour chaque projet, la mise en œuvre de l'IS doit être adaptée à la nature (volume, complexité) du système, au rôle de l'organisme concerné (maîtrise d'ouvrage, maîtrise d'œuvre, ...) et à son organisation, ainsi qu'aux phases du cycle de vie du système (réponse à appel d'offres, recueil des exigences, études de faisabilité, conception, production...). Comme déjà évoqué, les efforts d'ingénierie des systèmes apportent un avantage concurrentiel majeur, tant sur la maîtrise des coûts que sur la maîtrise de la complexité.

Paradoxalement, la complexité doit être vue comme un avantage, lorsqu'elle contribue à l'amélioration du service rendu. En effet, on se pose de plus en plus le problème de l'optimisation globale des systèmes, en considérant l'ensemble de leur cycle de vie. En effet, nos entreprises et nos donneurs d'ordres visent à abaisser le coût de possession global des produits de façon significative[5] et/ou à maîtriser l'introduction des sauts technologiques, de façon, in fine à donner un avantage concurrentiel discriminant (Exemples : pilotage à 2, commandes de vol électrique, optimisation du couple lanceur - satellite à propulsion électrique, …). La complexité constitue aussi de facto une protection contre les nouveaux entrants, en particulier issus des pays émergents.

Dans les cas où l'on vise à la réutilisation d'éléments ou de sous-systèmes, l'IS doit aussi servir à maîtriser le risque d'un changement d'environnement à moindre coût.

On notera que l'Ingénierie des Systèmes ne se substitue pas à la Gestion de Projet mais qu'elle en est complémentaire. A ce titre le schéma suivant propose un positionnement de la gestion de programme, de l'ingénierie des systèmes et de l'implémentation/la production, faisant apparaître des spécificités et des recouvrements :

5 Nota : *A l'exception notable des Avions d'Affaire, où le coût de possession est peut-être un critère d'optimisation moindre que la disponibilité opérationnelle de l'avion.*

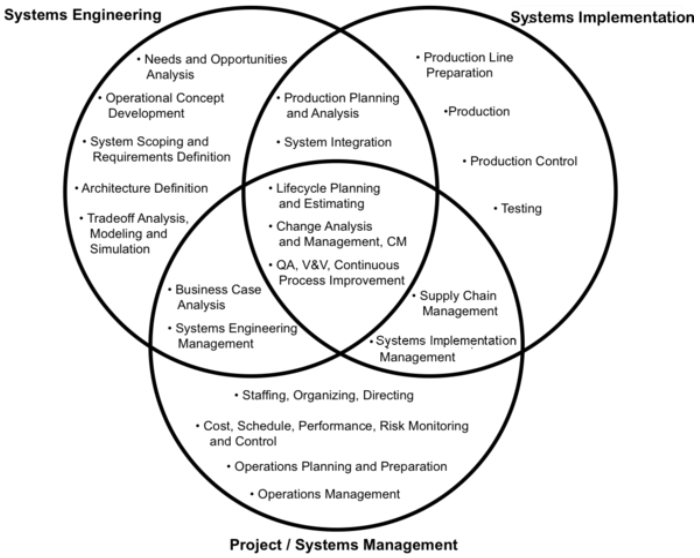


Schéma 1.8 Rapport entre Ingénierie Système, le Management de Projet, et l'implémentation/la production ; Source : SEBoK[6] Original

Pour la mise en œuvre de l'IS, les différentes spécialités doivent être impliquées dans une approche collaborative. Cette collaboration repose sur la mise en place d'une équipe intégrée d'IS constituée de spécialistes des démarches, méthodes et outils de l'IS, ainsi que de spécialistes des métiers, produits et technologies.

L'objectif global de l'IS est l'optimisation d'ensemble de nombreux critères (qualité du produit, coûts et délais associés, rentabilité...). Cette optimisation est généralement le résultat de compromis entre différentes solutions envisageables. Les décisions prises au cours du projet doivent être justifiées et tracées.

La démarche d'IS permet, progressivement, de construire la définition du système et de la justifier. Tout au long de son déroulement, les activités de spécification et de conception - qui sont au cœur de la démarche - reposent sur des activités de soutien dont les principales sont:

- ❑ L'ingénierie des exigences, et la maîtrise de la configuration,
- ❑ Les évaluations, les vérifications, et les validations,
- ❑ La maîtrise des risques, et les revues.

---

[6] Nota : *SEBoK : System Engineering Body of Knowledge : "Guide to the Systems Engineering Body of Knowledge" (SEBoK) v1.3.2, BKCASE, April 14, 2015*

1.7 BREF APERÇU DE L'IS DANS L'INDUSTRIE ET LES SERVICES HORS AERONAUTIQUE (PARTIELLEMENT SOURCE AFIS)

Au travers de l'AFIS, un travail important de partage des meilleures pratiques en Ingénierie des Systèmes, entre grands industriels français, a eu lieu ces dix dernières années. Il a permis en particulier de faire reconnaître l'importance du rôle de la coordination pluridisciplinaire pour mener à bien tout projet de grande ampleur, et la nécessité d'en formaliser les pratiques performantes.

Dans le domaine de l'automobile, on constate, ces dix dernières années une évolution forte, avec une complète révolution des processus d'ingénierie des systèmes, motivée en particulier par l'introduction massive de l'électronique, la réduction des cycles, et la recherche d'optimisation économique, au travers de la notion de lignes de produits. Dans le domaine naval, les grands projets de navire font également de plus en plus appel à des démarches d'ingénierie des systèmes très intégrées, vue la très grande complexité des produits.

Un secteur d'application important de l'IS est aussi le domaine des transports, de la sécurité au sens large, des systèmes urbains interconnectés (la ville vue comme un système de systèmes, concept de « Smart City » en anglais), ainsi que le domaine de l'énergie, et bien d'autres encore.

Parallèlement, pour appuyer les processus déployés, et les méthodes employées, et malgré l'apparition de nombreux outils ou suites d'outils commerciaux, la communauté d'IS manque encore cruellement d'outils puissants, intégrés, et collaboratifs, par comparaison aux outils de la CAO ou du PLM (Product Lifecycle Management).

1.8 MOTIVATION D'UN GROUPE DE TRAVAIL GIFAS

Comment être collectivement plus efficaces ? Pourquoi faut-il évoluer ? Quel intérêt de structurer la réflexion et les bonnes pratiques au niveau de nos professions ?

Au-delà des travaux conduits par l'INCOSE et l'AFIS, de portée générale pour l'ensemble de l'industrie et des services, il y a, dans notre domaine de l'Aéronautique, de la Défense et de l'Espace, des spécificités qui rendent utile la structuration d'un groupe de travail sectoriel, au sein de la commission R&D du GIFAS.

Les architectes-ensembliers et ingénieurs système représentent aujourd'hui une force de travail respectable, estimée suivant les entreprises de nos secteurs et les produits considérés, dans une fourchette de 15% à 25% de la main d'œuvre d'ingénierie[7]. Ce métier, en soi, n'est pas nouveau, cependant il reste sous-estimé ou méconnu, alors que son importance va en croissant, avec la complexité de nos systèmes[8]. Plus généralement, l'importance de l'approche système est souvent sous-estimée dans nos entreprises. Il y a un besoin croissant d'ingénieurs formés à la discipline de l'IS.

Parmi les thèmes majeurs ayant un poids fort dans le monde de l'Aéronautique, de la Défense et de l'Espace, on peut citer :

- Le besoin de mieux maîtriser la performance globale des systèmes, et la maturité des systèmes, tenant compte de leur environnement,
- L'impératif de développer des systèmes sûrs (aspect sûreté, « Safety », en anglais),
- Le besoin de développer des systèmes robustes aux malveillances matérielles et cybernétiques[9] (aspect sécurité, « Security » en anglais),
- Le besoin vis-à-vis de la déclinaison de l'ARP 4754A[10], dans l'aéronautique civile,
- Les évolutions lourdes des systèmes de gestion du trafic aérien,
- Le renforcement des exigences de la DGA, relativement aux standards et méthodologies d'ingénierie des systèmes, vis à vis de ses fournisseurs,
- Pour la gestion du trafic aérien, et les programmes de défense, la généralisation de l'usage des cadres d'architecture (« Architecture Frameworks » en anglais : NAF, DODAF),
- Le renforcement des exigences de l'agence spatiale européenne, relativement aux standards et méthodologies d'ingénierie des systèmes (ECSS), vis-à-vis de ses fournisseurs,

---

7 Note : *Le pourcentage, en tendance, sera plus élevé pour les entreprises traitant principalement de fonctionnel (logiciels, avionique, …), et sans doute moindre pour des entreprises plus orientées sur des activités mécaniques, où la part du fonctionnel est moindre.*

8 Note : *La prise de conscience est très variable, selon nos entreprises : certaines sont conscientes du ROI, alors que d'autres voient encore dans l'Ingénierie des Systèmes une source de surcoût, dont la valeur ajoutée n'est pas démontrée.*

9 Nota : *Cette problématique prend une importance croissance. En l'état la discipline Sécurité (Security en anglais) n'est pas encore aussi structurée que la discipline Sûreté (Safety en anglais).*

10 Note : *Et aussi de l'ARP4761.*

- La formalisation et la contractualisation plus stricte des exigences entre grands intégrateurs et leurs sous-systémiers,
- Plus généralement la cascade et la déclinaison des exigences de plus en plus formalisée, tout au long de la chaîne de valeur, ce qui entraîne la nécessité de maîtriser en commun et de donner un sens clair et communément admis aux principaux concepts et aux principales méthodologies de l'IS,
- La prise de conscience parmi les industriels de la nécessité de mieux maîtriser l'ensemble du cycle de vie des produits et services, depuis la conception amont, le développement, la transition vers l'industrialisation et l'entrée en service, la production, le maintien en condition opérationnelle, et les opérations associés, jusqu'au retrait du service et au démantèlement,
- La prise en compte du besoin des opérateurs (compagnies aériennes, équipages, VIPs, …), et des passagers, de disposer à bord de moyens de connexion (accès internet, pour les passagers, envoi de données de maintenance, vers un système sol ad hoc, pour la maintenance prédictive, et la correction de pannes, EFB[11] pour les équipages…). A noter que de telles exigences impactent lourdement la sûreté et la sécurité.
- La nécessité, pour l'ingénierie des systèmes d'être, au-delà des bénéfices déjà annoncés, efficiente, et maîtrisable à des coûts raisonnables, contribuant ainsi à l'amélioration de la compétitivité globale de nos entreprises,
- La nécessité d'offrir des avantages compétitifs à nos entreprises, vis-à-vis des nouveaux entrants.

Il est de ce fait apparu nécessaire, à la Commission R&D du GIFAS, de:

- Structurer un langage clair et commun et des méthodologies communes, pour les équipes d'ingénierie de nos entreprises, amenées à travailler ensemble au sein de ce qu'on appelle communément une « entreprise étendue », pour la conception et la production de nos systèmes et produits,
- Partager un retour d'expérience,
- Fournir une vision commune de l'Ingénierie des Systèmes à nos dirigeants,
- Bâtir un ensemble de recommandations partagées, pour nos professions,
- Délivrer un message fort sur les soutiens attendus, vis-à-vis des pouvoirs publics français et européens.

Précisons que ce Groupe de Travail n'a pas vocation à se substituer à la société savante AFIS (Association Française d'Ingénierie Système, chapitre français de l'association INCOSE - International Council on System Engineering), qui réfléchit de manière beaucoup plus large sur les processus, méthodes, et outils de l'Ingénierie des Systèmes en général, et sur les nouvelles méthodes et technologies, pour les besoins de l'ensemble de l'industrie.

---

[11] Nota : *EFB : Electronic Flight Bag*

2. DESCRIPTION DES ACTIVITES DE L'IS

Dans ce chapitre, on s'appuie très largement sur des définitions et des concepts issus de l'AFIS ou de l'INCOSE. On décrit successivement les activités de l'ingénierie des systèmes. Cependant il nous semble utile de préciser que cette liste ne décrit pas nécessairement l'ordre chronologique des activités.

2.1 CHAMP D'APPLICATION DE L'INGENIERIE DES SYSTEMES, ACTIVITES ET PROCESSUS

L'Ingénierie des Systèmes est une démarche méthodologique coopérative et interdisciplinaire, qui englobe l'ensemble des activités adéquates pour concevoir, développer, faire évoluer et vérifier un système apportant une solution optimisée sur tout le cycle de vie aux besoins d'un client tout en étant acceptable par tous (IEEE1220, AFIS). On peut voir l'ingénierie des systèmes comme le chef d'orchestre permettant aux spécialistes (instrumentistes) de travailler harmonieusement ensemble.

En ce sens, l'IS ne se substitue à aucune spécialité métier traditionnelle, mais vient en plus, afin d'offrir un support, et de garantir la cohérence des travaux conduits par les spécialistes (intégration).

Recommandation (voir Recommandations R2.15.1 et R2.15.2) : Cette nouvelle spécialité est à développer, et même si des éléments existent dans nos entreprises, on se doit de renforcer tant la formation que le cursus métier associé, et le champ d'expertise[12]. Ce type de formation pourrait d'ailleurs être partagé entre les donneurs d'ordres (plateformistes) et les systémiers ou sous-systémiers.

On notera, comme déjà évoqué au chapitre 1, que l'Ingénierie des Systèmes ne se substitue pas à la Gestion de Projet mais qu'elle en est complémentaire.

On a constaté que les types d'activité à réaliser au titre de l'Ingénierie des Systèmes, constituaient des invariants par rapport aux différents projets et secteurs d'application. C'est donc sur les processus qui enchaînent ces activités que s'est peu à peu fondée une certaine formalisation générique du métier d'IS.

On en a déduit des modèles de maturité permettant d'évaluer la capacité d'un organisme d'IS à maîtriser son métier, à l'aulne de sa maîtrise des processus, ainsi que de définir des chemins de progression.

Il en résulte des normes définissant les processus d'IS et leurs activités.

---

12 Nota : *Dans les groupes Thalès et Dassault, cette spécialité est déjà bien structurée. Chez Airbus, et chez ASL (Airbus Safran Launchers), elle est de plus en plus reconnue, et est en cours de structuration, avec des niveaux de maturité différents selon les entités (On note une bonne reconnaissance globalement au sein de la division Defence & Space d'Airbus). Dans les trois groupes (Thalès et Dassault, Airbus), mais également chez Safran, elle fait l'objet de formations spécialisées. Les cursus de carrière associés, suivant les cas, sont plus ou moins structurés et organisés.*

2.2 METHODES ET OUTILS

Les méthodes d'Ingénierie des Systèmes fournissent des démarches techniques pour réaliser les activités. Elles reposent notamment sur des approches de modélisation et de simulation pour valider des exigences, vérifier, évaluer ou comparer des solutions. Elles dépendent des secteurs d'application et résultent de choix industriels. La mise en œuvre des méthodes est assistée par des outils très généralement informatisés, que l'on cherche à intégrer dans l'atelier d'Ingénierie des Systèmes, dont ils partagent les informations de la base de données intégrée.

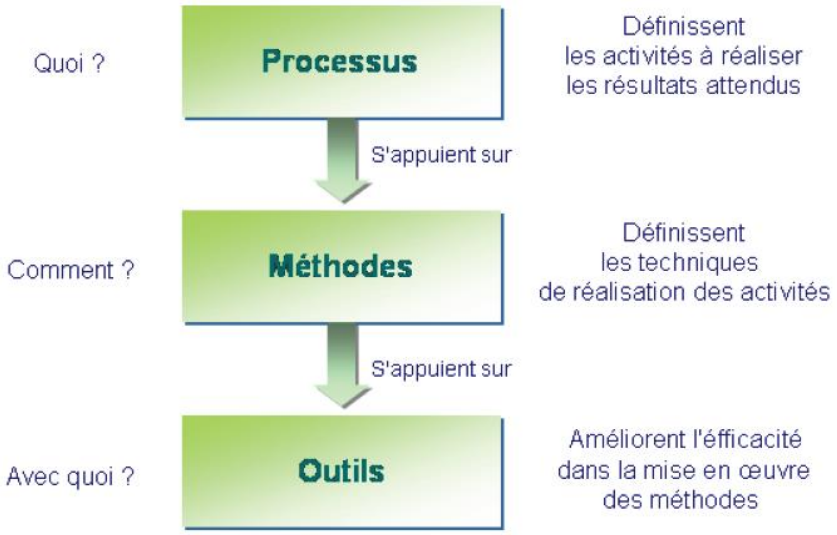


Schéma 2.1 Relations entre Processus, Méthodes, et Outils.
(On parlera, pour l'ensemble de Processus Outillé.)

Le pilotage des processus, la maîtrise des méthodes et outils s'appuient sur des organisations dédiées, gérant des compétences en IS.

Les processus d'Ingénierie des Systèmes, eux-mêmes sont conçus, en conformité avec les normes générales (telles que l'ISO 9001-v2000 ou l'EN9100), ou sectorielles (l'ARP 4754 A, pour l'aéronautique, les ECSS pour le spatial) et avec les exigences issues des systèmes de management globaux et du système qualité de nos entreprises (Business Management System ou Company Management System).

2.3 PRESENTATION DES PROCESSUS DU CYCLE DE VIE SYSTEME SELON L'ISO/IEC 15288:2015

La norme ISO/IEC 15288:2015 identifie quatre groupes de processus qui structurent une organisation d'ingénierie sur le cycle de vie du système d'intérêt. Une vue graphique de ces quatre groupes est donnée par le schéma 2.2, en page suivante.

- Le groupe des Processus d'Ingénierie et autres Processus Techniques inclut (sans hiérarchisation, ni notion d'ordre chronologique ou autre):

  - ❑ L'analyse du problème global, de la mission, des opportunités
  - ❑ La définition des exigences des parties prenantes au projet[13],
  - ❑ L'analyse des exigences,
  - ❑ La définition de l'architecture,
  - ❑ La conception du système,
  - ❑ L'analyse du système,
  - ❑ L'implémentation,
  - ❑ L'intégration,
  - ❑ La vérification,
  - ❑ La transition,
  - ❑ La validation,
  - ❑ Les opérations,
  - ❑ La maintenance,
  - ❑ Le retrait du service et le démantèlement[14].

- Le groupe des Processus Projet inclut (sans hiérarchisation, ni notion d'ordre chronologique ou autre) :

  - ❑ La planification du projet (« project planning »),
  - ❑ L'évaluation et le contrôle du projet,
  - ❑ La gestion des décisions,
  - ❑ la gestion des risques,
  - ❑ La gestion de configuration,
  - ❑ La gestion de l'information,
  - ❑ La collecte et l'exploitation des mesures,
  - ❑ L'assurance qualité.

- Le groupe des Processus de Gestion[15] inclut la négociation des appels d'offre, l'écriture des « statements of work », l'acquisition des exigences associées aux différents contrats, la gestion des relations clients-fournisseurs (pilotage technique des contrats), et le pilotage de la chaîne d'achat/fourniture interne et externe (« Supply Chain »).

---

13 Note : *Parties prenantes = Stakeholders, en anglais.*

14 Note : *Retrait du service et Démantèlement = Disposal, en anglais.*

15 Note : *Processus de Gestion = Agreement Processes, en anglais.*

- Le groupe des Processus Organisationnels et Support inclut :
  - ❑ Le management du modèle du cycle de développement (« life-cycle model management »)
  - ❑ Le management des infrastructures,
  - ❑ Le management du « project portfolio »,
  - ❑ La gestion des ressources humaines,
  - ❑ La gestion de la qualité,
  - ❑ La gestion des connaissances.

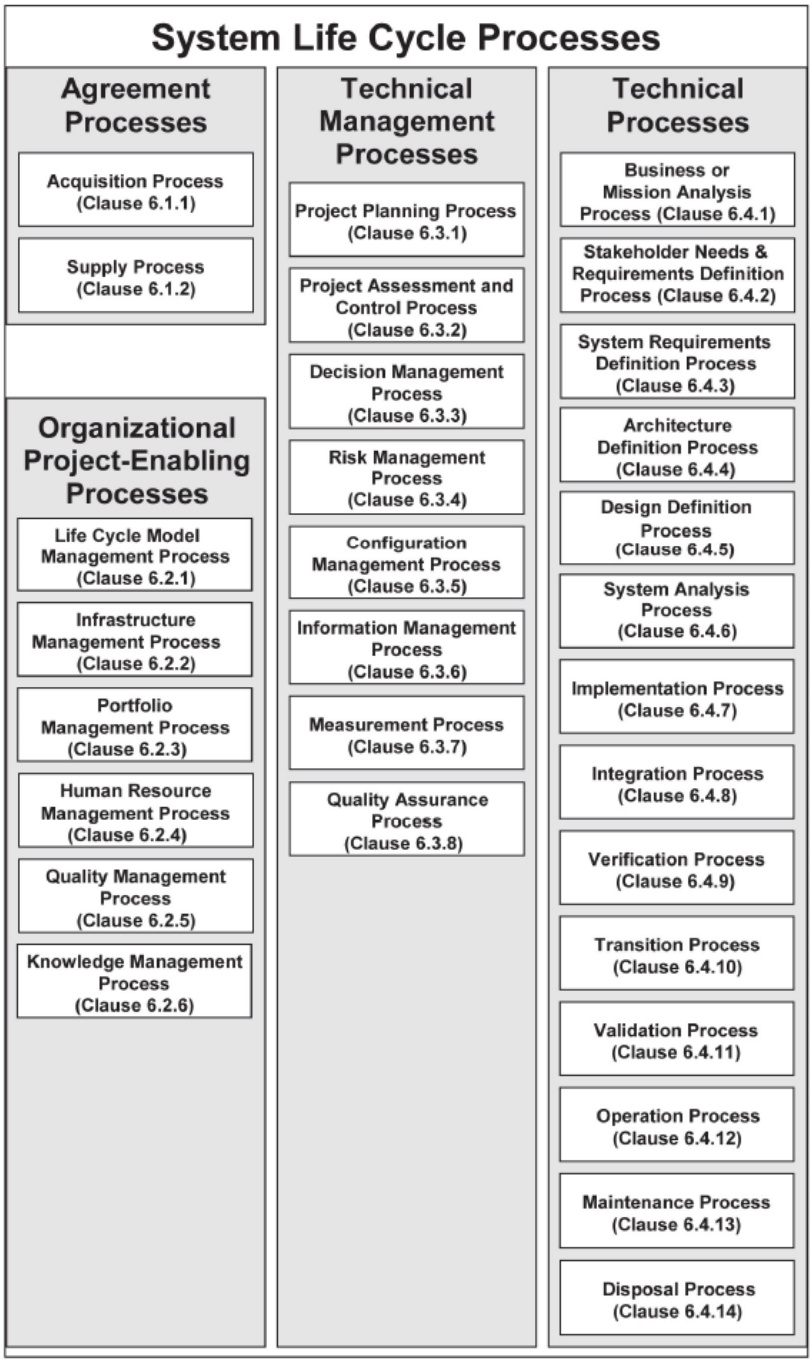


Schéma 2.2 Vue générale des processus du cycle de vie système selon l'ISO/IEC 15288:2015

On notera que cette vision de l'ISO 15288:2015 est une vision statique, ne mettant pas en relief les relations entre les différentes activités / différents processus, ni leur enchaînement chronologique.

Une représentation en forme de V du cycle de vie (« V-Cycle ») est présentée, en anglais, sur le schéma 2.3 suivant :

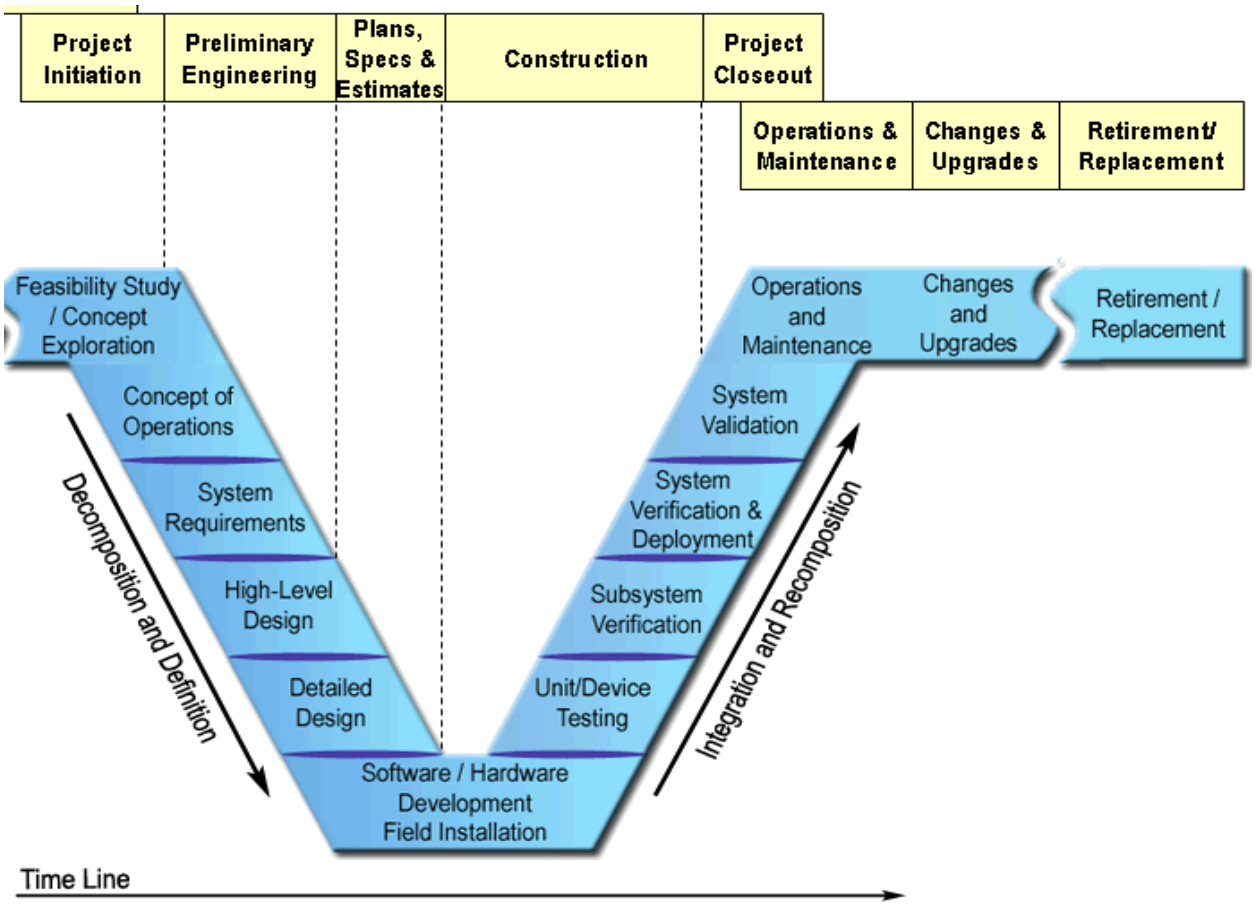


Schéma 2.3 Vue générale du cycle de vie du Système, jusqu'au retrait du service. On notera que cette représentation implicitement fait un zoom sur la partie développement du cycle.

Le paragraphe suivant aborde plus précisément la partie centrale de ce cycle de vie du système, nommée cycle de développement.

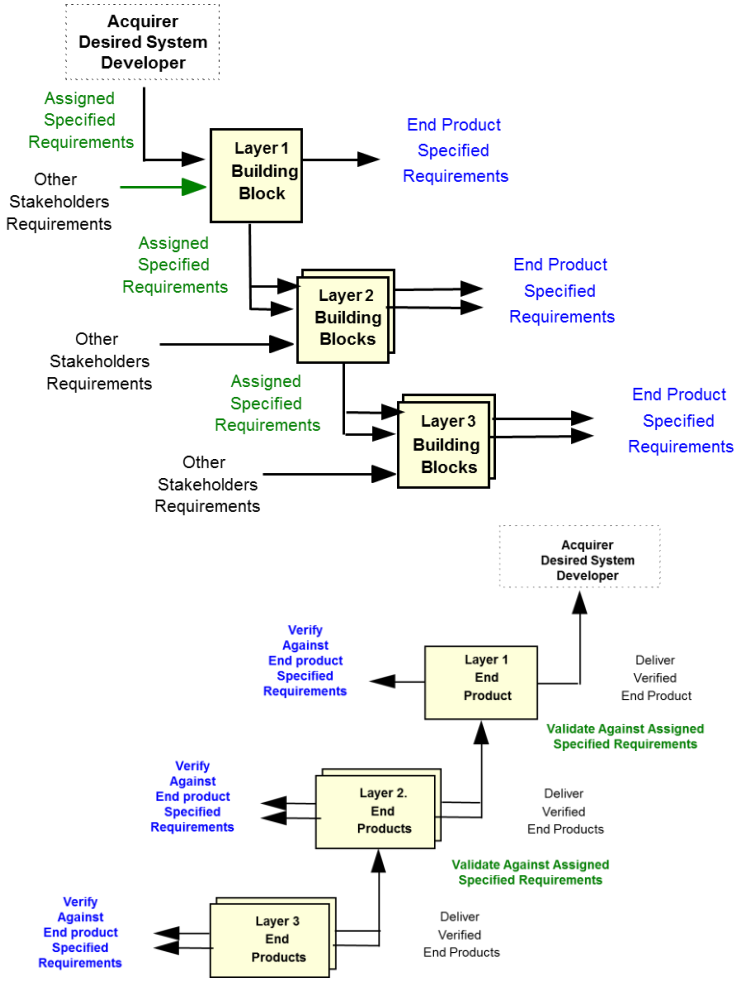
On notera que ce schéma ne fait pas apparaître que nous ne sommes en général pas dans un processus linéaire. En effet, chaque étape est généralement conduite de manière itérative, et il peut donc y avoir des allers- retours entre activités (on parle parfois de cycles en W, ou comportant plusieurs « petits W »).

2.4 PRESENTATION DU CYCLE DE DEVELOPPEMENT EN V

Le processus de développement peut être de manière très générale présenté par un diagramme en V, comme déjà esquissé dans le schéma 2.3, et représenté dans les schémas 2.4 et 2.5 (A noter que cette dernière représentation ne couvre que la partie développement du cycle de vie d'un système). Ce diagramme en V fait apparaître, dans sa branche gauche, « descendante », l'approche du haut vers le bas (« top-down »), consistant à analyser les exigences système, faire une analyse fonctionnelle et une analyse de la valeur, définir l'architecture générale du système (définition des fonctions, décomposition en sous-systèmes, définition des interfaces, …), et définir les allocations associées à chacun des sous-systèmes.

Au niveau de chaque sous-système, ce même processus est reproduit, et il est également reproduit au niveau de chacun des composants (mécaniques, électriques, hardware, software, ou « mixtes », selon les cas).

Après développement des composants, la remontée du V représente les tâches d'ingénierie consistant à tester les éléments, à vérifier qu'ils satisfont à leurs exigences, à vérifier les interfaces, à intégrer les composants, puis les sous-systèmes, à vérifier qu'ils sont conformes à l'usage attendu, jusqu'à intégrer et vérifier le système complet, et à démontrer qu'il répond à l'ensemble de ses exigences, et assure bien l'usage attendu par les clients.



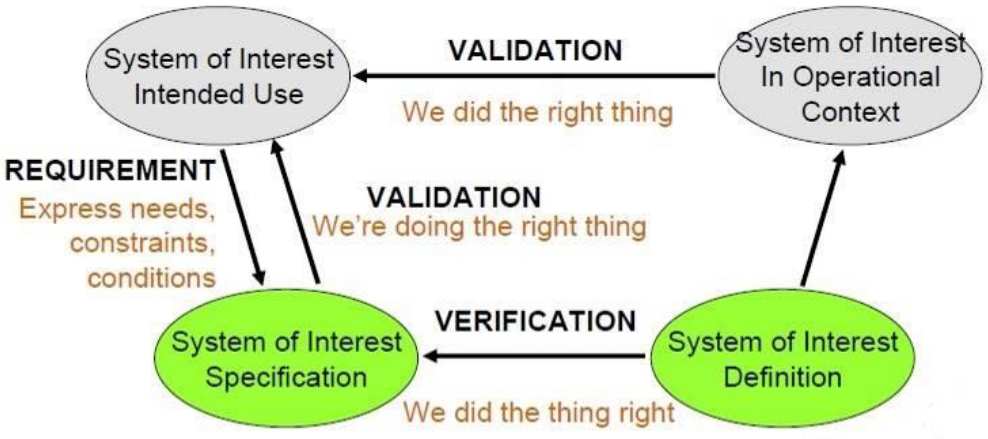
Schémas 2.4 et 2.5 : Top down development and bottom up realization (selon EIA 632)

A noter que ce cycle traverse généralement des organisations différentes, et dans certains cas des entreprises différentes, ce qu'on a tenté de traduire au travers du code des couleurs différents pour les différents niveaux. On notera que généralement le passage d'un niveau au niveau inférieur, dans la descente du V, est (ou devrait être) le résultat de négociations.

On notera que les termes Vérification and Validation peuvent être sources de confusion. Afin d'éviter toute ambigüité, nous proposons l'approche/définition suivante :

On vérifie qu'un produit, ou un sous-produit est conforme à ses spécifications (vérification de l'implémentation), à l'aide de calculs, simulations, essais, analyses ou revues … On dira en anglais: « The system does the thing right ».

On valide la définition du produit, à l'aide de calculs, simulations, essais, analyses ou revues …, afin de s'assurer que le système qui a été défini répond effectivement au besoin du client (« intended use »). On dira en anglais: « The system does the right thing ». Cette dernière activité requiert donc la participation active du client. On pourra se reporter au schéma 2.6 suivant :



Validation

- Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled [ISO 9000: 2005]

Verification

- Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled [ISO 9000: 2005]

Schéma 2.6 Verification and Validation[16] selon l'ISO 9000: 2005

On notera en particulier que les deux flèches validations dans le Schéma 2.6 sont de même nature (validation de l'usage attendu du système), même si les activités

16 Nota : *Si les termes Verification & Validation posent peu de problème d'ambiguïté en anglais, il n'en va pas de même en français, où certains auteurs ou organisations traduisent l'anglais « verification » par le français « validation » et l'anglais « validation » par le français « qualification ». Parfois aussi le mot « qualification » est utilisé en français uniquement pour décrire la validation finale du système global. On s'en tiendra ici à la traduction littérale de vérification et de validation.*

correspondantes ne sont pas du tout situées dans le temps à la même date, et ne mettent pas en jeu les mêmes moyens (exemple typique : simulateur amont, pour la flèche validation sur la gauche, vs. essai en vol, pour l'autre).

L'objectif de la validation amont (« early validation » en anglais, correspondant à la flèche validation sur la gauche du schéma 2.6) est de s'assurer que l'« intended use » est bien capturé dans les exigences. L'« early validation » est donc par essence vertueuse, mais elle peut parfois poser des problèmes contractuels entre le client et son fournisseur (risque de transfert de savoir-faire, …), ou des problèmes de démonstration au niveau de la certification (exemple on ne peut pas transférer des modèles, si le moyen qui les a générés n'est pas lui-même certifié.) La validation finale (celle de la flèche du haut) correspond, elle, à la validation soit du produit, soit de modèles hautement représentatifs du produit, permettant de démontrer la conformité à l'usage attendu.

2.5 CONTEXTE OPERATIONNEL ET ANALYSE OPERATIONNELLE

En amont de la capture des exigences, il est recommandé de commencer la réflexion sur le système envisagé par une analyse du concept opérationnel, ou concept des opérations (en anglais « CONOPS »), afin d'identifier les limites (services rendus, interfaces…) du système, caractériser son environnement opérationnel, et définir des paramètres clés pour son analyse.

Cette première analyse doit être complétée par une analyse opérationnelle, permettant, en passant en revue le cycle de vie complet du système (y compris le développement, la production, la mise en service, les opérations, le maintien en condition opérationnelle, et le retrait du service), d'identifier et caractériser les Cas d'Utilisation (« Use Cases », en anglais) importants. Il s'agit d'identifier les principaux services attendus et leurs interactions avec l'environnement opérationnel. Au cours de cette analyse opérationnelle, on définit des Scénarios opérationnels qui affinent les Cas d'Utilisation en précisant la séquence des interactions entre le système et les différents constituants de son environnement. Ce travail peut être long et complexe. En effet, il est souvent assez complexe, pour nos maîtres d'ouvrage, d'avoir une vision claire de leur(s) besoin(s), pour le développement de systèmes modernes, aux fonctionnalités très étendues.

Cette démarche prend encore plus d'importance, lorsqu'on aborde l'analyse sous l'angle Système de Systèmes (voir chapitre 10).

2.6 SPECIFICATION, CAPTURE, ANALYSE ET GESTION DES EXIGENCES

La suite de la première partie du cycle de développement en V est donc dédiée à la capture des exigences proprement dite, à leur analyse, en particulier pour vérifier qu'elles sont correctement exprimées (pas d'exigence ambigüe, mal rédigée, invérifiable, …) et qu'elles ne sont pas contradictoires entre elles (ce qui peut se produire lorsqu'il y a un grand nombre d'exigences).

On notera que le point de départ de ce travail est généralement un cahier des charges fourni par le client, plus ou moins détaillé selon les cas, et résultat d'une analyse opérationnelle plus ou moins poussée. Ce cahier des charges ne constitue pas un ensemble complet d'exigences et est presque toujours réécrit/reformulé et complété par des exigences émises par le concepteur. Le tout étant défini au travers d'une analyse fonctionnelle (décrite au §2.7). Ainsi analyse fonctionnelle et capture des exigences sont des activités imbriquées.

Ce travail de capture est (ou devrait être) complété par une analyse de la valeur, permettant de challenger les exigences, au regard des services rendus et des coûts qu'elles sont susceptibles d'engendrer, autant en développement (coûts non récurrents) qu'en opération/production/exploitation (coûts récurrents). Concernant le processus de sélection/amélioration/consolidation des exigences, on parlera d'élicitation. In fine une exigence est donc le résultat d'une négociation client-fournisseur, négociation explicite ou non, suivant les cas.

Idéalement, cette négociation technique devrait être reflétée dans la négociation contractuelle, mais ce n'est pas toujours le cas.

Lorsqu'une exigence est implémentée, on est donc en mesure de justifier la raison pour laquelle elle a été implémentée, et on doit aussi s'interroger sur le processus qui permettra in fine sa vérification (cela permet d'éviter de conserver des exigences invérifiables …). Ceci est illustré par le schéma 2.7 suivant :

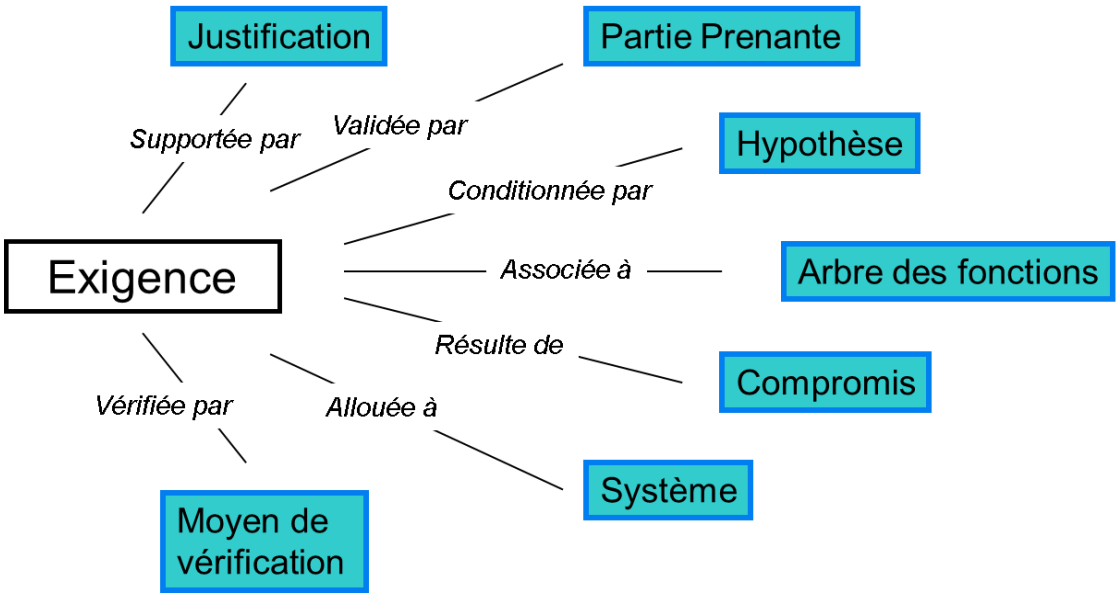


Schéma 0.7 : Exemples d'informations/relations/propriétés/attributs associés à une exigence

Les activités décrites ci-dessus de capture et analyse des exigences se retrouvent cascadées tout au long de la descente du V du développement, pour le passage entre les différents niveaux.

Elles sont également imbriquées avec les activités d'analyse fonctionnelle décrites au paragraphe 2.7.

On doit aussi suivre, tout au long du développement, l'évolution des exigences, car il est, selon notre expérience, bien rare qu'aucune d'entre elles n'évolue au cours d'un développement. A ce titre il conviendra de se munir de méthodologies et d'outils permettant de faire des analyses de l'impact de l'évolution d'une ou plusieurs exigences.

On doit enfin être capable de relier les exigences s'appliquant au niveau d'un composant ou d'un sous-système, avec les exigences de plus haut niveau auxquelles elles se rattachent. On parle parfois d'arborescence des exigences. Globalement, l'ensemble des processus mis en œuvre pour ce faire constitue la gestion des exigences. A noter que pour soutenir ces activités, on utilise très souvent des progiciels du commerce, tel DOORS (IBM, le plus répandu), ou bien Integrity, Polarion, ….[17]

Au total, pour l'ensemble des activités reliées à la capture, l'analyse, l'élicitation et la gestion des exigences, on parlera d' « Ingénierie des Exigences ». Cette Ingénierie des Exigences est décrite au chapitre 5 du présent rapport.

A noter que certains auteurs ont tendance à réduire l'Ingénierie des Systèmes à la seule Ingénierie des Exigences. Ce serait une vision très réductrice et même une faute de le faire, car l'Ingénierie des Systèmes adresse de manière tout aussi pertinente les autres activités d'ingénierie qui contribuent à la descente du cycle en V, et à la remontée de la branche droite du V (tests, intégration, vérification, validation, …)

Enfin, une tendance de plus en plus forte consiste à modéliser très tôt dans le cycle, le système à développer, pour mieux anticiper les conséquences des différentes décisions. Ceci peut et doit se faire dès la capture/validation des exigences pour tout ou partie d'entre elles, et peut se poursuivre tout au long de la décomposition fonctionnelle et matérielle, et de la cascade des exigences, qui caractérisent la branche gauche du cycle en V. On parlera d'Ingénierie des Systèmes fondée sur des Modèles (traduction de l'anglais « Model Based System Engineering », ou MBSE). On notera que la démarche MBSE ne s'oppose pas aux processus de l'Ingénierie des Systèmes, mais en est un support puissant.

Nous l'introduisons en dernier, car cette approche est plus récente que celle concernant l'ingénierie des exigences. La démarche MBSE est décrite au chapitre 9.

---

17 Nota *Pour des projets de petite taille (quelques centaines d'exigences max), certains industriels utilisent des tableurs de type Excel pour supporter leur gestion d'exigences.*

2.7 ANALYSE FONCTIONNELLE, MODELISATION FONCTIONNELLE

L'analyse fonctionnelle (AF), activité intimement imbriquée avec la capture des exigences est une activité consistant, en écho aux opérations et scénarios, à identifier les Fonctions du Système et à les raffiner (i.e. les décomposer).

Lorsqu'un jeu d'exigences de haut niveau (« top programme requirements »), définissant les services attendus du système, a été émis par le client, et les autres parties prenantes, il convient de les capturer, les compléter et de les justifier. Cela se fait avec l'aide d'analyses et de modélisations fonctionnelles, qui vont consister à décomposer le système à concevoir en fonctions.

L'analyse fonctionnelle décrit les Flots (Flows) entre les (sous-)Fonctions. Ces flots couvrent les données échangées bien évidemment mais pas seulement (exemples : alimentation électrique, phénomène physique…)

L'AF a également en charge la description comportementale de l'enchainement et/ou de la parallélisation des (sous-)Fonctions, l'itération de la décomposition fonctionnelle, jusqu'à pouvoir la mettre en regard d'une Architecture système, et l'allocation des (sous-)Fonctions aux composants (physiques) du système.

Cette activité, dans le processus d'ingénierie des exigences, permet donc de structurer les exigences en les rattachant aux fonctions ou aux interfaces entre fonctions. Comme déjà dit l'analyse fonctionnelle est donc très imbriquée avec la capture et la déclinaison des exigences. Et ce type d'activité se poursuit, à différents niveaux tout au long de la branche descendante du cycle en V.

Une fonction est une tâche, ou une activité exécutée pour atteindre un résultat attendu. On définit ainsi deux catégories de fonctions :

- Les fonctions de service, destinées à répondre à un besoin du système
- Les fonctions techniques, ou fonctions contraintes, ou fonctions d'adaptation, introduites par les interactions entre les différents constituants, ou les interactions à maitriser avec l'environnement extérieur (par exemple : assurer la capacité d'un système à tenir une plage de fonctionnement en température).

Ainsi, les services rendus par le système seront les résultats générés par les fonctions de service, à l'interface entre le système et l'environnement d'utilisation, et par les fonctions de service internes au système.

Dans le processus global d'ingénierie des systèmes, on peut placer l'Analyse fonctionnelle comme le montre le schéma 2.8, tiré d'un document DoD US. Cependant ce schéma ne fait que faiblement apparaître la forte imbrication de l'analyse fonctionnelle avec la capture et la déclinaison des exigences.

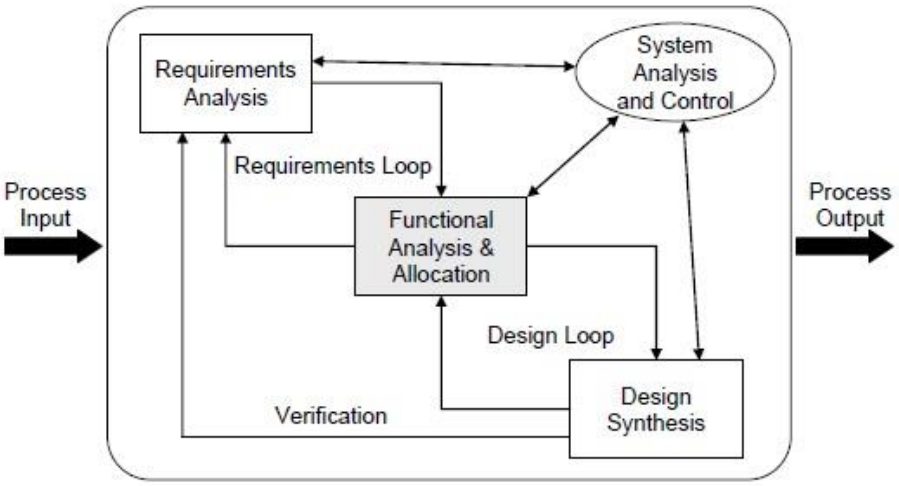


Schéma 2.8 L'analyse Fonctionnelle dans le processus global d'ingénierie des systèmes (source : The FAR Approach – Functional Analysis/Allocation and Requirements Flowdown Using Use Case Realizations, Magnus Eriksson, Kjell Borg, Jürgen Börstler ; 16th Intern. Symposium of the International Council on Systems Engineering (INCOSE'06), Orlando, FL, USA, Jul 2006)

Comme on peut s'en douter, l'analyse fonctionnelle peut s'appliquer à différents niveaux : le système de systèmes, le système ou le sous-système, ces notions n'étant de plus que relatives (suivant qu'on est la DGA, le maître d'ouvrage d'un grand système d'armes, un constructeur d'avion, ou un grand sous-systémier - appelé systémier dans l'aéronautique civile – par exemple un concepteur de trains d'atterrissage, de systèmes de conditionnement d'air, ou un concepteur de portes d'avion, ou un concepteur de propulseurs, ou enfin un concepteur/fournisseur d'équipements).

On rattache généralement à l'analyse fonctionnelle le travail consistant à passer de l'arbre des fonctions ou arbre fonctionnel (en anglais : functional tree), à l'arbre des produits (en anglais : product tree). Le passage se fait au travers des matrices de projection fonctions / sous-systèmes ou composants et des matrices de connexion, permettant de matérialiser les liens entre ces sous-systèmes et composants. Ceci est illustré par le schéma 2.9 suivant :

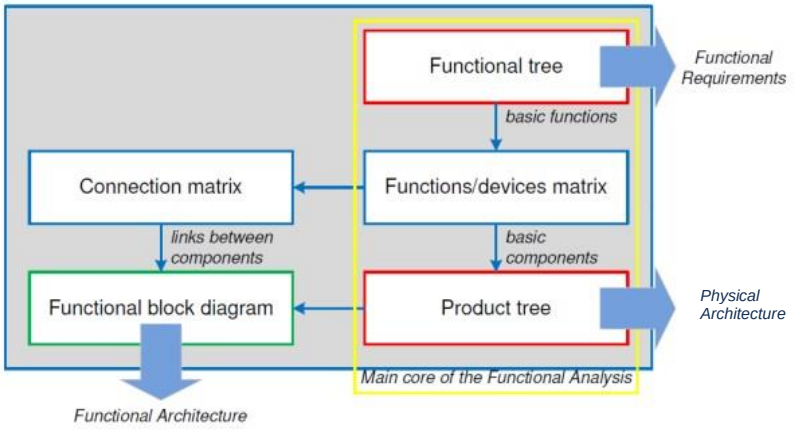


Schéma 2.9 : Analyse Fonctionnelle, Functional Tree et Product Tree (source : Functional Analysis in Systems Engineering: Methodology and Applications, Nicole Viola, Sabrina Corpino, Marco Fioriti and Fabrizio Stesina, Politecnico di Torino, Italie)

Les deux schémas suivants 2.10 et 2.11 donne respectivement un exemple du lien entre Analyse Opérationnelle, Analyse Fonctionnelle, et Architecture système, et un exemple d'arbre fonctionnel:

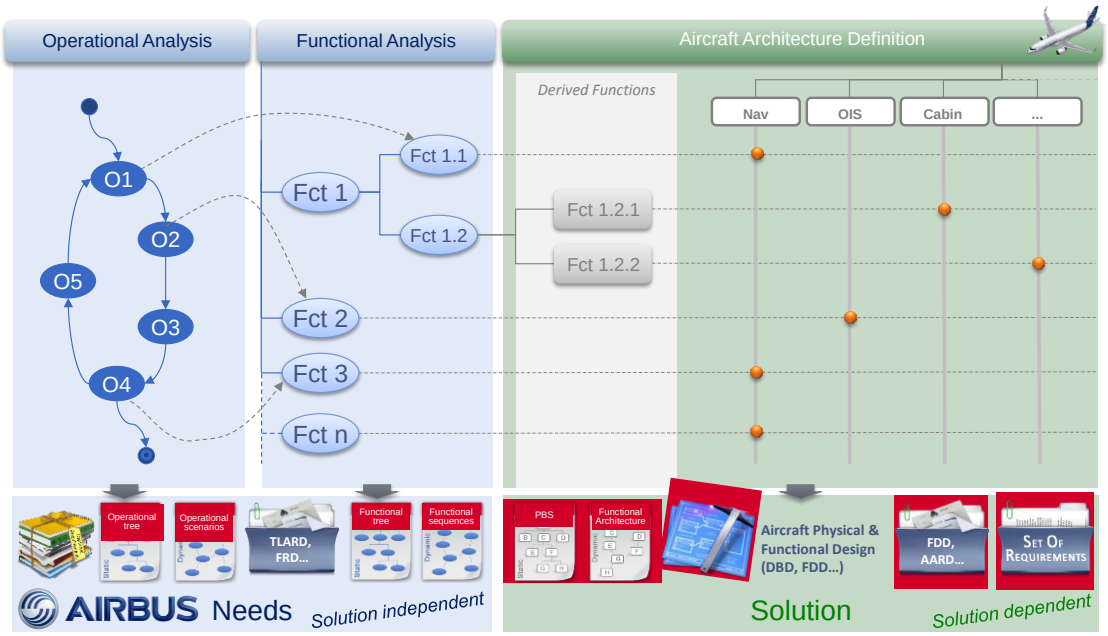


Schéma 2.10 : Approche Fonctionnelle (Pierre de Chazelles, Airbus)

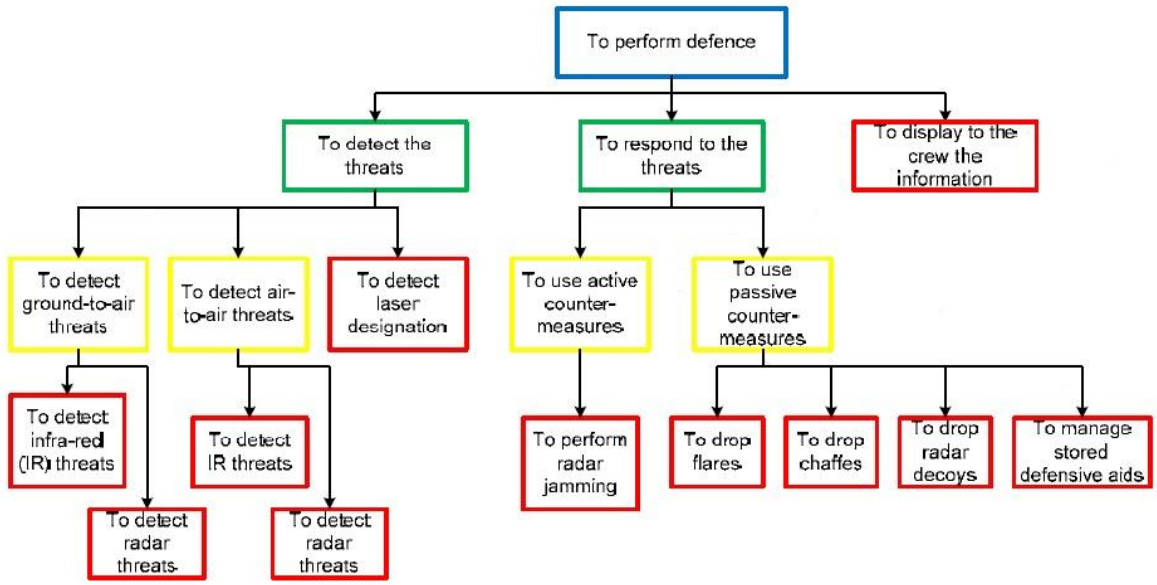


Schéma 2.11 : Exemple d'arbre fonctionnel pour un système de défense (source : Functional Analysis in Systems Engineering: Methodology and Applications, Nicole Viola, Sabrina Corpino, Marco Fioriti and Fabrizio Stesina, Politecnico di Torino, Italie)

On trouvera des recommandations relatives à l'analyse fonctionnelle, dans le chapitre dédié à l'ingénierie des exigences.

2.8 ARCHITECTURE ET CONCEPTION

La norme ISO/IEC/IEEE 15288:2015 différencie maintenant deux processus[18] : en anglais « Architecture Definition Process (clause 6.4.4) » et « Design Definition Process (clause 6.4.5) ».

Cela permet de différencier les caractéristiques fondamentales et stables de l'architecture, applicables par exemple à toute une ligne de produits, de la conception (design) détaillée, qui dépend, elle, beaucoup de la date de réalisation et de la maturité des technologies.

Ainsi de multiples conceptions distinctes dans une ligne de produits, peuvent-elles être toutes consistantes avec une seule architecture générale.

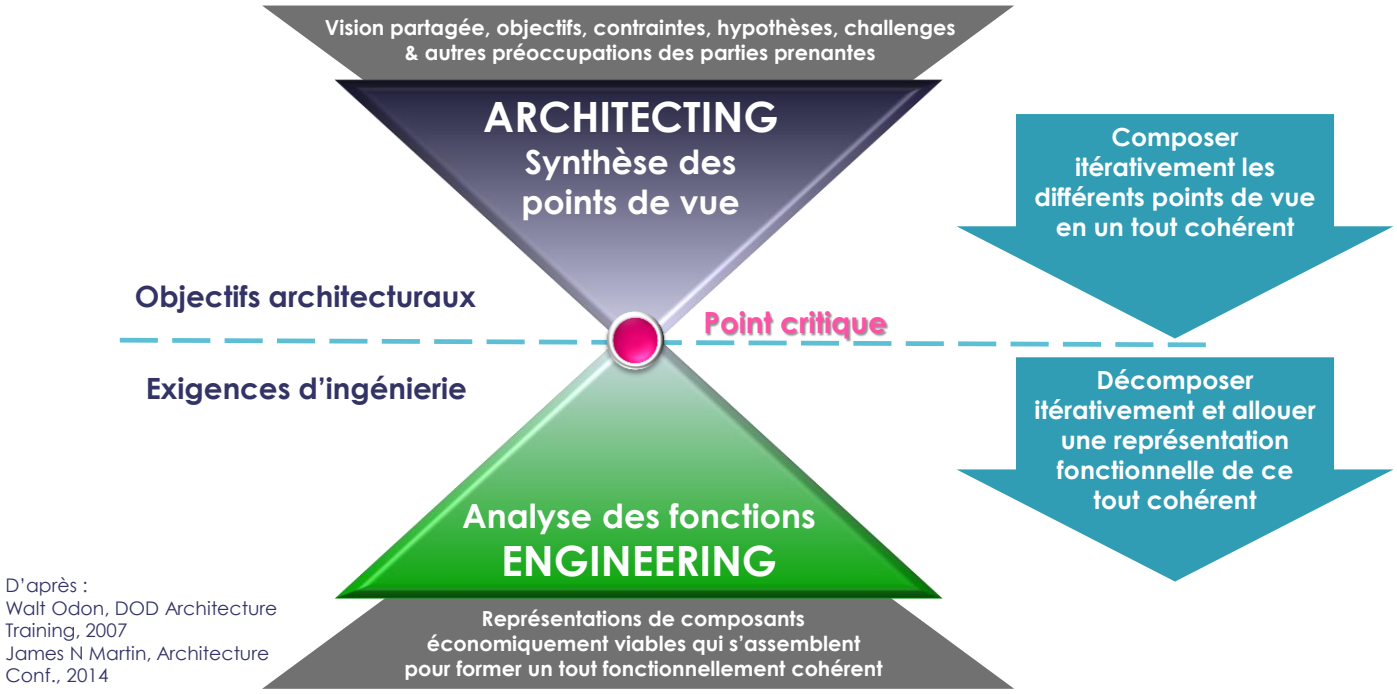


Schéma 2.12 : Architecture et Conception : Les deux faces d'un même problème (Architecting and Engineering : Two sides of the same problem - credit : Walt Odon, DOD Architecture Training, 2007 & James N Martin, Architecture Conf., 2014)

18 Nota : *Ce n'était pas le cas dans la version antérieure ISO 15288:2008.*

2.8.1 Architecture[19]

L'architecture représente l'organisation fondamentale d'un système, représenté d'une part par ses constituants (fonctions, « sous-systèmes », ou constituants physiques), leurs interactions, et leurs relations avec l'environnement, et d'autre part par les principes guidant sa conception et son évolution.

Les objectifs recherchés par les travaux d'architectures couvrent l'élaboration d'architectures système candidates qui répondent aux besoins des parties prenantes et satisfont les exigences, la sélection des solutions préférées et leur documentation selon les différents points de vue des partie prenantes.

Il est important d'assurer le partage et la bonne compréhension de ces éléments architecturaux au sein de la communauté des parties prenantes, car ils représentent la compréhension commune et négociée du problème à traiter.

Cette activité est structurante, en interface avec les autres activités amont et garante de la stabilité du référentiel de conception ; elle peut avantageusement être menée de façon itérative.

Ce processus est généralement déroulé de manière collaborative, et adresse l'architecture générale du système global, les exigences de haut niveau et les relations entre MOA et MOE[20]. C'est typiquement au niveau de ce processus que des décisions de type Go/NoGo seront prises, par exemple à l'issue d'une revue de spécification (System Requirements Review).

Par exemple, dans le domaine de la Défense, ce processus peut être soutenu par un contrat de faisabilité et définition préliminaire. On parlera aussi de contrat de phase A, dans le domaine spatial (ESA).

Une sortie typique d'un tel processus dans des phases préliminaires (cf. la notion de « critical point dans le schéma 2.11) peut être la signature d'un contrat de réalisation.

On notera toutefois qu'il s'agit d'un processus qui n'est pas cantonné aux phases amont, et qu'il permet de maitriser les évolutions pouvant arriver au cours d'un programme. Ainsi, lorsqu'une remise en question d'exigences de haut niveau a lieu, ou bien lorsqu'on décide de rajouter des fonctions nouvelles, ce même processus peut /doit être déroulé à nouveau, afin d'en tirer les conséquences et de reprendre convenablement la conception.

---

19 Nota : *En anglais le terme architecting représente une activité, dont le produit est l'architecture générale (ou « espace du problème » - traduisant la compréhension du problème). Ce terme n'englobe donc pas la totalité des activités communément regroupées en français, sous le terme d'architecture. L'architecting se centre sur la capture et la stabilisation des besoins et contraintes de haut niveau, au travers d'un processus collaboratif.*

20 Nota : *MOA : Maîtrise d'OuvrAge, et MOE : Maîtrise d'OEuvre.*

2.8.2 Conception[21]

Le processus de conception a pour objectif de concevoir une solution permettant de satisfaire les exigences du système. Pour ce faire, le processus doit d'abord compléter la structure fonctionnelle (qui n'est pas entièrement déterminée par l'activité d'architecting), puis définir les différentes solutions possibles, afin de réaliser les fonctions (projection sur l'architecture physique), leurs principes d'implémentation et de réalisation, ainsi que les risques techniques et économiques qui y sont associés. Il doit effectuer les choix nécessaires parmi ces différentes solutions, en considérant leurs avantages compétitifs respectifs (par exemple : potentiel de croissance, robustesse à des changements d'environnement non nécessairement spécifiés, …), les opportunités et les risques associés à chaque solution potentielle, les coûts récurrents et non récurrents associés, …

Les grandes phases associées aux tâches d'architecture et de conception sont en général (c'est le cas dans le monde spatial européen et dans les grands programmes de défense stratégique de la DGA) sanctionnées par des grandes revues système telles la Revue de Définition Préliminaire Système (System Preliminary Design Review) et la Revue Critique de Définition Système (System Critical Design Review), permettant de s'assurer de la bonne implémentation de l'architecture fonctionnelle et physique, et permettant d'autoriser, en cas de succès la poursuite des travaux de développement.

Cependant, ces activités seront complétées tout au long du cycle du développement autant que de besoin.

Pour le développement des aéronefs, l'ED79/ARP4754 propose un processus générique de développement des systèmes.

Son idée maîtresse repose sur l'identification et la description par le développeur dans un plan de développement, des processus de développement à suivre, et la mise en place d'un plan d'assurance qualité décrivant le moyen de s'assurer de l'application de ces processus (preuve), sans imposer de revue particulière. Chaque avionneur a défini et mis en œuvre son propre système de revues à l'issue de chacune des phases du développement.

---

21 Nota : *Traduction de Design, ou Concept Design, en anglais. Dans ce processus, qui est de nature plus interne (chaque contributeur étant centré sur son activité propre), ou tournée vers les fournisseurs de ce contributeur, on retrouvera des activités d'architecture détaillée.*

2.9 ACTIVITES DE MODELISATION, ET DE DESIGN VIRTUEL (VIRTUAL DIGITAL MOCK UP)

Pour assurer les tâches d'architecture et de conception, on s'appuie de plus en plus sur des environnements informatiques de support, tels que l'environnement de design virtuel aussi appelé maquette numérique (Digital Mock Up, ou encore DMU environnent, en anglais). La maquette numérique est une représentation géométrique 3D du produit. Ses composants élémentaires portent la description géométrique. Ses composants sont agrégés et organisés en arbre (PBS). A un composant est associée une liste d'attributs.

Le niveau de détail géométrique et la quantité de composants augmentent de façon classiquement exponentielle pendant le développement. Les données de la DMU doivent donc être contrôlées par un système de gestion de configuration.

La DMU contient les données de structure (murs et couverture pour un bâtiment, structures mécaniques pour un aéronef, un missile ou un véhicule spatial), les équipements et les systèmes de circulation de fluides (liquide, électrique, pyrotechnique, ventilation…).

La disponibilité permanente du meilleur état de la définition permet de concevoir dans le contexte du produit et de limiter drastiquement les erreurs de type « collision au montage ». Le contrôle de non collision peut d'ailleurs être renforcé par ce qu'on appelle des calculs de clash.

Cette référence permet aussi de mieux concevoir les outillages de production et de maintenance, les procédures d'intégration, etc….

Beaucoup de sociétés de service en informatique (« Tools Vendors ») commercialisent des logiciels qui assurent tout ou partie de ce rôle. A ce titre on pourra citer CATIA V6 de Dassault Systems, mais beaucoup d'autres acteurs sont présents sur ce marché, et beaucoup de grands systémiers (dans le monde de l'aéronautique, de l'espace et de la défense) procèdent au développement d'outils propriétaires, ou à la customisation d'outils commerciaux.

Les sociétés s'organisent aussi afin de faciliter les flux d'échanges de données techniques entre les différentes disciplines, pour gagner en efficacité et permettre la prise en compte d'enjeux de conception dits « multi-physiques », ou transdisciplinaires (par exemple : optimisation pluridisciplinaires, mettant en œuvre différents critères à optimiser, etc…).

A ce titre on peut évoquer la notion encore récente de maquette numérique fonctionnelle (« Functional DMU » en anglais), qui désigne les moyens, méthodes et outils permettant de gérer un référentiel technique commun, le plus unifié possible, mais permettant à chaque discipline d'effectuer ses travaux et d'échanger avec les disciplines en interfaces.

Une haute qualité des données est le préalable aux utilisations les plus avancées: simulation de la cinématique, des processus, du manufacturing, couplage aux outils de calcul, association aux bases de données fonctionnelles (électrique, fluidique…). Par exemple, au sein de certaines entités du groupe Airbus, des activités aussi variées que l'analyse de compatibilité Electromagnétique (CEM ou bien EMC en anglais) et l'analyse thermique s'appuient sur les mêmes modèles de référence Catia, dans lesquels figurent les attributs fonctionnels nécessaires. Chaque activité métier utilise alors des outils permettant de ne conserver que les

attributs pertinents pour l'activité, avant d'attaquer une modélisation métier spécifique (maillage par exemple.)

Recommandation R2.9.1 : Malgré l'intérêt perçu sur la connexion entre la modélisation fonctionnelle et la modélisation physique, nous recommandons de bien réfléchir, au cas par cas, à la valeur ajoutée d'une telle connexion, la rentabilité de l'investissement, et la capacité de maintenir dans le temps une telle base de données intégrée.

2.10 L'IS DANS L'ENTREPRISE ETENDUE

Les enjeux associés aux tâches de conception et design, à l'environnement de design virtuel, aux flux d'échanges de données techniques ne se limitent pas aux frontières de l'entreprise, fut-elle un grand plateformiste ou un grand systémier. On doit en effet replacer ces tâches dans une perspective plus large, incluant les différents sous-traitants en charge du design de sous-systèmes, équipements, et composants, matériels comme logiciels (ou bien souvent « mixtes »). Ce point sera développé au chapitre 8.

2.11 ACTIVITES D'INTEGRATION, DE VALIDATION, ET DE VERIFICATION

Jusqu'à présent nous avons principalement abordé et analysé la branche descendante du cycle de développement en V (branche gauche), qui se focalise sur la décomposition fonctionnelle et physique et sur la cascade des exigences, aux différents niveaux.

Lorsque tous les systèmes, sous-systèmes et équipements contribuant au Système Global (aussi appelé Solution) ont fait l'objet d'une spécification, et que les équipements élémentaires ont été développés[22] (ou pris sur étagère), reste à conduire l'ensemble des activités consistant à intégrer ces équipements pour constituer les sous-systèmes, et systèmes, jusqu'au Système Global, et à vérifier l'adéquation avec leurs exigences respectives, et à valider qu'ils procurent bien le service attendu (on pourra se référer au schéma 2.6 Verification & Validation du paragraphe §2.4.)

L'ensemble de ces activités est désignée par l'acronyme IV&V, pour « Integration, Validation, and Verification » (en anglais).

L'objectif du processus d'intégration est de procéder à l'assemblage des différents composants, éléments, équipements, sous-systèmes et systèmes, jusqu'à la réalisation finale du système global (plateforme, système de défense, etc .)

L'objet du processus de Vérification (« Verify », « verification » en anglais) est de confirmer que les exigences spécifiées pour le produit sont bien satisfaites par le

---

22 Nota : *Cet évènement ou cet ensemble d'évènements ne correspond pas nécessairement à une même date pour chaque sous-système/système considéré. Ce qui importe est que les activités de remontée de la branche aval du V (branche droite) soient conduites de façon à assurer de manière satisfaisante les points de rendez-vous nécessaires, et in fine qu'elles permettent l'intégration finale, la vérification et la validation du Système Global, dans des conditions satisfaisantes (coût/planning).*

produit défini, au travers de démonstrations (reposant sur des méthodes variées : tests, analyses, revues, …) conduites tout au long de l'intégration.

L'objet du processus de Validation (« Validate », « validation » en anglais) est d'apporter la preuve que les services fournis par un système en utilisation sont conformes aux besoins des parties prenantes, et que le système réalise ce qu'on attend de lui dans son environnement opérationnel.

Concernant les confusions possibles de vocabulaire entre français et anglais, on renvoie le lecteur au paragraphe 2.4, au schéma 2.6, et à la note de bas de page associée.

Ces deux processus font partie du développement du Système Global, et doivent démarrer tôt dans le cycle de vie, afin d'optimiser la stratégie d'IV&V (optimum dans la réalisation des opérations d'intégration, de vérification et de validation, en considérant les coûts, les délais, la répartition industrielle, la constitution des plateformes, et la disponibilité des moyens de tests.)

En particulier, dans de nombreux programmes militaires, une première version du Plan Général d'Essai (PGE) est soumise à revue, dès la revue de Définition Préliminaire (RDP). Naturellement ce PGE sera complété et développé tout au long du développement.

En raison de la proximité entre les activités, et parfois les moyens à utiliser, pour "Verify" et pour "Validate", et dans le but de rationnaliser l'ensemble, les logiques correspondantes sont souvent élaborées en étroite synergie.

On va dans la suite (chapitre 6) décrire de manière plus détaillée comment dérouler le processus de vérification, et le processus de validation.

2.12 CONDUITE DES ACTIVITES D'OPERATIONS, DE SERVICES, DE MCO ET DE SUPPORT LOGISTIQUE INTEGRE

L'IS doit anticiper et optimiser les activités de déploiement du système, les activités d'opérations, de services, de maintien en condition opérationnelle (MCO) et de support logistique intégré - autrement dénommé soutien logistique intégré (SLI), associées à un système. Elle doit couvrir l'intégralité du cycle de vie jusqu'au retrait de service complet du système.

Nous nous permettons d'insister sur ce point, car par le passé de nombreux échecs ont été constatés, relatifs à la sous-estimation des activités aval et de leur complexité, conduisant dans certains cas à un besoin de refonte en profondeur (et donc coûteux) du système.

Ces activités essentielles dans le cycle de vie d'un système doivent d'abord être définies et négociées, avec le maître d'ouvrage (et l'opérateur lorsqu'il est différent), très en amont lors de de la capture et de l'élicitation des exigences, et ceci au même titre que les autres exigences applicables au système.

Ensuite, au même titre que le reste du système, elles doivent faire l'objet d'une analyse fonctionnelle, de trade-off, de prototypage et de structuration (« architecture »). Le prototypage (la simulation) permettra de se convaincre que l'architecture choisie pour le système permet bien de délivrer les services attendus en opération, en tenant compte de l'ensemble des contraintes opérationnelles (à titre d'exemple : répartition des charges de travail des opérateurs, sûreté et sécurité des opérations, conformité aux lois en vigueur sur le territoire où le système est déployé, prise en compte des contraintes d'approvisionnement, des contraintes de co-activités, des obsolescences, des différentes sources de risques sur le système, des exigences de sécurité des systèmes d'information, …).

2.13 GESTION DES EVOLUTIONS

Le processus de gestion des évolutions est un processus itératif, couvrant la maîtrise technique et administrative de la configuration des éléments suivants :

1. les exigences du système,
2. les éléments qui constituent le système,
3. les données de certification applicables,
4. les installations et les outils, lorsque la configuration est indispensable, pour établir la conformité à la certification d'assurance du développement.

En outre, la norme ARP4754A, de manière similaire aux DO178 et DO254, porte un accent particulier sur la gestion de configuration et la nécessaire formalisation du processus de modification des exigences de spécifications.

Parler d'évolutions oblige à clarifier les notions primordiales suivantes :

- Le **jalon** à partir duquel les acteurs de l'entreprise étendue appliquent un processus officiel et tracé de gestion des modifications
- Les **analyses d'impact** et **interactions** entre les différentes bases de données et disciplines : spécifications (incluant impacts fonctionnels et sécurité), nomenclatures et documentations de définition, nomenclatures et outillages de fabrication, nomenclatures et documentations de maintenance
- La **classification** de ces modifications (tout particulièrement dans le monde de l'aéronautique civile) et le processus de délégation / notification / approbation à mettre en place entre les clients et fournisseurs
- Le caractère **itératif** des activités de IV&V à assurer.

Ces défis obligent non seulement à formaliser les **processus**, à former les utilisateurs aux principes de gestion de **configuration**, mais aussi à établir des liens forts entre les différents outils et environnements (exigences, PLM, fabrication, maintenance) afin d'assurer un bon niveau de **traçabilité**.

2.14 GESTION DES FAMILLES DE PRODUITS

La gestion de lignes de produits, ou de familles de produits, conduit à introduire des activités spécifiques en Ingénierie des Systèmes.

Ceci a conduit l'AFIS à publier un document intitulé « L'Ingénierie Système d'une Ligne de Produits » (éditions CEPADUES, sous la direction d'Alain Le Put).

Les aspects standardisation et réutilisation (re-use) seront détaillés au paragraphe 6

2.15 RECOMMANDATIONS

On rappelle ici les recommandations formulées dans le chapitre 2 :

Recommandations :

- R2.15.1 : L'ingénierie système en tant que spécialité est à développer. Même si des éléments existent dans nos entreprises, on se doit de renforcer la formation afin d'harmoniser le métier, et de fournir une compréhension commune du champ d'expertise, au sein d'une même entreprise.
- R2.15.2 : Une formation type à l'ingénierie système pourrait être partagée entre les donneurs d'ordres (plateformistes), et les systémiers ou sous-systémiers, par exemple dans la perspective d'un projet en commun.
- R2.9.1 : Malgré l'intérêt perçu sur la connexion entre la modélisation fonctionnelle et la modélisation physique, nous recommandons de bien réfléchir, au cas par cas, à la valeur ajoutée d'une telle connexion, la rentabilité de l'investissement, et la capacité de maintenir dans le temps une telle base de données intégrée.

3. EN QUOI L'INGENIERIE DES SYSTEMES PEUT-ELLE RENDRE NOS PRODUITS ET SERVICES FUTURS PLUS PERFORMANTS ET ATTRACTIFS ?

3.1 ENJEUX

Les trois familles d'enjeux clés auxquels l'Ingénierie des Systèmes doit répondre pour le secteur aéronautique, défense, et spatial sont :

1) Répondre aux évolutions des marchés.

2) Concevoir des architectures innovantes, permettant d'améliorer la rentabilité et le positionnement de nos produits.

3) Maitriser la conception de nos systèmes, de plus en plus contraints, dans un environnement complexe (normes, …).

3.2 REPONDRE AUX EVOLUTIONS DES MARCHES.

Les marchés aéronautique, défense, et spatial sont en mutation, lente, mais certaine :

- Apparition de nouveaux acteurs (nouveaux avionneurs, nouveaux concepteurs de systèmes spatiaux tel des lanceurs, nouveaux sous-systémiers et équipementiers),
- Les besoins et les types d'utilisateurs finaux (« end users » en anglais : compagnies « low cost » ou non, passager, aéroport, agence, opérateurs de satellites, …) sont en évolutions croissantes,
- Le « Time to Market » d'un aéronef, d'un véhicule spatial, ou d'un système d'arme s'est nettement réduit (c'est particulièrement le cas pour l'aéronautique civile),
- Apparition de l'approche « développement incrémental » sur des familles d'avion.

Les normes liées aux processus de développement telles l'ARP 4754A et l'ARP 4761, imposent de nouvelles contraintes de certification, auxquelles on ne peut répondre que par l'utilisation de processus d'Ingénierie des Systèmes, avec des méthodes outillées.

D'autres normes répondent à des attentes Sociétales, par exemple en termes de pollution. Ces attentes sont de plus en plus fortes comme le montrent l'évolution des normes environnementales – ex : visions ACARE 2020 sur les réductions d'émission de CO2 de 50%, de Nox de 80%, et de bruit de 50% - contraint les industriels à contraindre et optimiser les systèmes conçus. Là encore, l'ingénierie des systèmes est une solution non suffisante mais nécessaire pour répondre à ces enjeux.

3.3 CONCEVOIR DES ARCHITECTURES INNOVANTES

Afin de rester compétitif et attractif l'ensemble de la chaine de la valeur comprise au sens de l'entreprise étendue (« supply chain »), dans nos plateformes et systèmes aéronautiques défense et spatiaux, doit proposer des solutions innovantes fiables et rentables. Pour ce faire il faut :

- Identifier et décliner les besoins et les exigences 'Vraies' (celles qui portent de la valeur). Penser en termes de Business Models,
- Optimiser et intégrer au plus tôt l'ensemble du système,
- Concevoir en s'appuyant sur des notions de maturité, telles TRL (Technology Readiness Level), IRL (Integration Readiness Level), SRL (System Readiness level), MRL (Manufacturing Readiness Level), afin de maîtriser les risques liés à l'introduction d'innovations,
- Maitriser la réutilisation, lorsque ce concept est pertinent.

3.4 MAITRISER LA CONCEPTION DE NOS SYSTEMES DE PLUS EN PLUS CONTRAINTS DANS UN ENVIRONNEMENT COMPLEXE

La complexité peut s'exprimer sous plusieurs formes :

- L'augmentation du nombre de technologies disponibles et la réduction du cycle de montée en maturité de ces technologies[23],
- L'intégration d'un grand nombre de technologies,
- L'intégration d'un grand nombre de fonctionnalités internes à un système donné,
- L'augmentation du nombre d'interfaces entre le système considéré (moteur, centrale inertielle, cockpit, avion, hélicoptère, flotte, …) et le monde extérieur[24],
- Le nombre d'acteurs croissant et d'interactions entre ces acteurs, dans la conception d'un système,
- Les concepts d'optimisation entre les grandes fonctions du système (pour un avion civil, on parlera d'optimisation « trans-ATA » ou « multi-ATA »).

Par ailleurs, cette complexité doit être maîtrisée dans un contexte contractuel parfois difficile (inflation des exigences de la part du donneur d'ordre, contraintes de conception imposées par le client, et par les normes, nécessité de vendre le juste service au juste prix, au travers d'une bonne maîtrise de l'analyse de la valeur).

---

23 Nota : *Il s'agit ici de la réduction du temps alloué à cette montée en maturité, et pas des activités à réaliser.*

24 Nota: *Le monde extérieur incluant les autres systèmes, avec lesquels le système considéré est en interface.*

Quand la complexité d'intégration d'un système augmente, la capacité à gérer efficacement les interfaces produit et les interactions projet devient cruciale : ces nouveaux défis nécessitent donc d'utiliser de nouveaux processus avec des méthodes outillées, comme le suggère le modèle COSYSMO illustré dans le schéma 3.1 suivant :

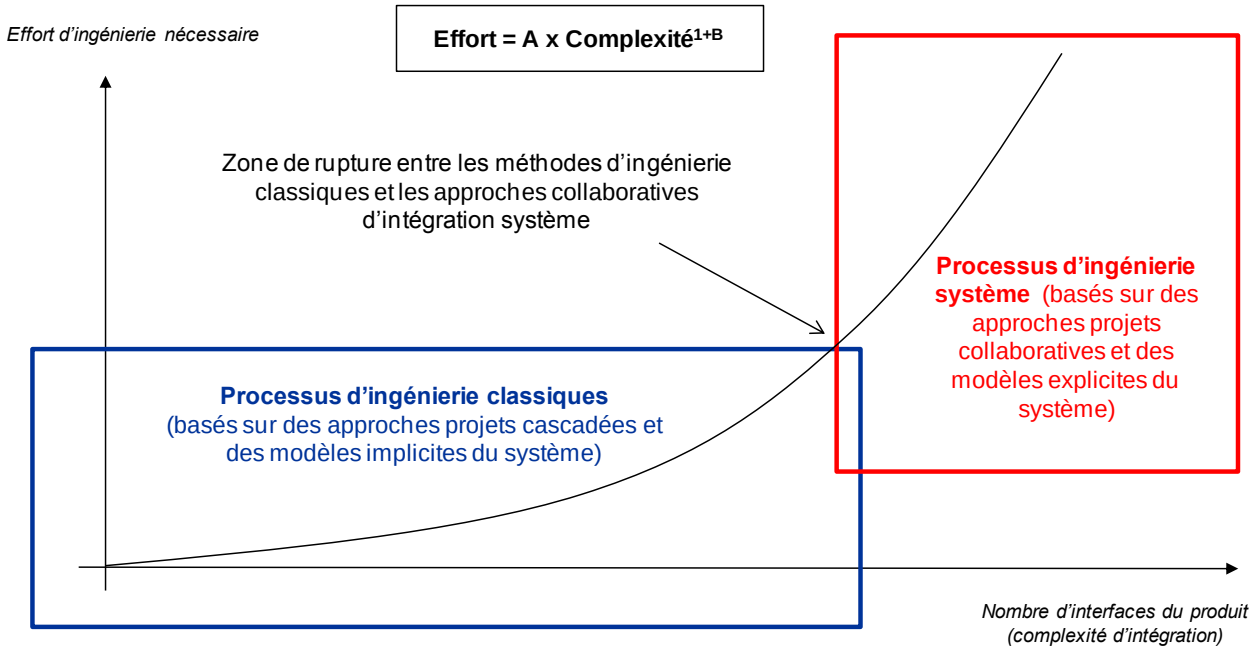


Schéma 3.1 : Modèle COSYSMO

4. NORMES, GUIDELINES, ET PROCESSUS (INTRODUCTION SUCCINCTE)

4.1 NORMES ET STANDARDS RELIES A L'INGENIERIE DES SYSTEMES

Normes = traduction française de standards

La normalisation a pour objet de fournir des documents de référence comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux [décret n°84-74 du 26/01/1984].

Une norme permet de :

- ❑ échanger (harmoniser règles et pratiques ; complément à la réglementation),
- ❑ développer (faciliter le transfert de technologies nouvelles),
- ❑ orienter (contribuer à l'information de l'utilisateur : facteur de confiance),
- ❑ innover (anticiper, faire évoluer ses produits).

L'historique de la création des normes et standards relatifs à l'ingénierie des systèmes est donné dans le tableau 3.1 en page suivante. Ces normes et standards se sont largement structurés à partir de sources venant du monde de la qualité, du management, et de l'ingénierie des systèmes électriques, avioniques et logiciels,

Du fait que certaines sont généralistes et que d'autres adressent les domaines de la défense, de l'aéronautique civile et du spatial, on trouve naturellement beaucoup de normes, qui sont en fait très largement complémentaires.

Remarque : A noter que le "INCOSE System Engineering Handbook" n'est pas une norme, mais un « Handbook » construit sur la norme ISO/IEC 15288.

1969	Mil-Standard 499 Military Standard: System Engineering Management (17 Juillet 1969)
1974	Mil-Standard 499A Military Standard: System Engineering Management (24 Août 1974)
1979	US Army Field Manual 770-78 System Engineering
1982	Parution de la DO-178 Software Considerations in Airborne Systems & Equipment Certification.
1988	DOD-STD-2167A Defence Systems Software Development
1992	DO-178B Software Considerations in Airborne Systems & Equipment Certification (version Européenne: ED12B)
1993	MIL-STD-499B Military Standard: System Engineering Management (draft jamais publié.)
1994 1995	Un Mémorandum du secrétaire à la défense américain, William Perry supprime le recours à des normes spécifiques sur les programmes d'acquisition du département de la défense (DoD), et pousse les fournisseurs d'équipements militaires à adopter des pratiques commerciales en accord avec le standard EIA 632 IS (Standard Intérimaire), puis avec le standard IEEE 1220 (Version d'essai) en lieu et place de la MIL-STD-499A. De ce fait la MIL-STD-499B n'a jamais été approuvée, et la MIL-STD-499A a été annulée sans remplacement en 1995.
1996	Parution de la recommandation ARP 4754, dans le domaine aéronautique Parution de la recommandation ARP 4761, aussi dans le domaine aéronautique.
1999	Parution de l'EIA 632 Processes for engineering a system (Janvier 1999)
1999	Parution de l'IEEE 1220 Standard for application and Management of the Systems Engineering Process (Janvier 1999)
2000	Parution de l'ISO 9001 v 2000 (approche par processus)
2002	Parution de la norme ISO/IEC 15288:2002 Systems Engineering – System Life-Cycle Processes, AFNOR Z 67-288 (Ingénierie Systèmes – Processus de cycle de vie des systèmes) (1er Novembre 2002)
A partir de 2002. *(Les différentes normes citées, dans leur dernière version, sont parues principalement entre 2008 et 2012.* *Le dernier corpus de normes a été agréé au 22 mai 2014)*	Parution des normes ECSS (European Cooperation for Space Standardisation) de l'ESA ; avec en particulier, pour l'ingénierie des systèmes : ECSS-E-ST-10C « Space engineering-System engineering general requirements », ECSS-M-ST-10C Rev. 1 « Space project management-Project planning and implementation », ECSS-M-ST-10-01C « Space management-Organization and conduct of reviews », ECSS-E-ST-10-02C « Space engineering-Verification », ECSS-E-ST-10-03C « Space engineering-Testing », ECSS-E-ST-10-06C « Space engineering-Technical requirements specification », ECSS-E-ST-10-11C « Space engineering-Human factors engineering » (D'autres normes d'Ingénierie des Systèmes existent dans les ECSS, mais sont vraiment spécifiques au spatial, par exemple : ECSS-E-ST-10-04C « Space engineering-Space environment » ; enfin des normes ECSS relatives à l'assurance produit ont des liens forts avec l'Ingénierie des Systèmes).

2003	Parution de l'EN 9100, reprenant en la complétant l'ISO 9001 v2000.
2003	Deuxième édition de l'EIA 632
2005	Parution de la RTCA DO-254 / Eurocae ED-80 "Design Assurance Guidance for Airborne Electronic Hardware" ; La réunion du matériel DO-254 et du logiciel DO-178B forment un système embarqué qui est régi par un standard dédié ARP4754. L'ensemble forme une approche cohérente des méthodes de développement des systèmes embarqués pour les applications aéronautiques.
2005	Traduction Française de la RG.Aéro 00077 « Guide pour le Management de l'Ingénierie Système »
2008	Parution de la norme ISO/IEC 15288:2008 Systems Engineering – System Life-Cycle Processes
2009	Parution de l'EN 9100 version 2009
2010	Parution de la recommandation ED79A/ARP 4754A, dans le domaine aéronautique Parution de la DO-178C
2014	Parution de la RG AERO 00044 " Guide d'application de l'ARP 4754A"
2014	La RG.Aéro 00077 est devenue une norme EN (EN 9277)
2014	Parution d'une mise à jour de l'ensemble des normes ECSS au 22 mai 2014
2015	Version révisée de l'ISO/IEC 15288 (ISO/IEC 15288: 2015).
2015	Parution de la norme ECSS-E-ST-10-24C « Space engineering - Interface management » au 1er juin 2015)
2015	Parution de la norme ISO 29110 " System and Software Engineering for Very Small Entities" (partie de la norme ISO 29110 qui adresse les aspects système.)
2016 (AC)	Révision de l'ARP 4761 (en cours)

Table 4.1 Grandes étapes de création des normes et standards de l'Ingénierie des Systèmes, en général, et standards spécifiques de l'aéronautique, de la défense et du spatial.

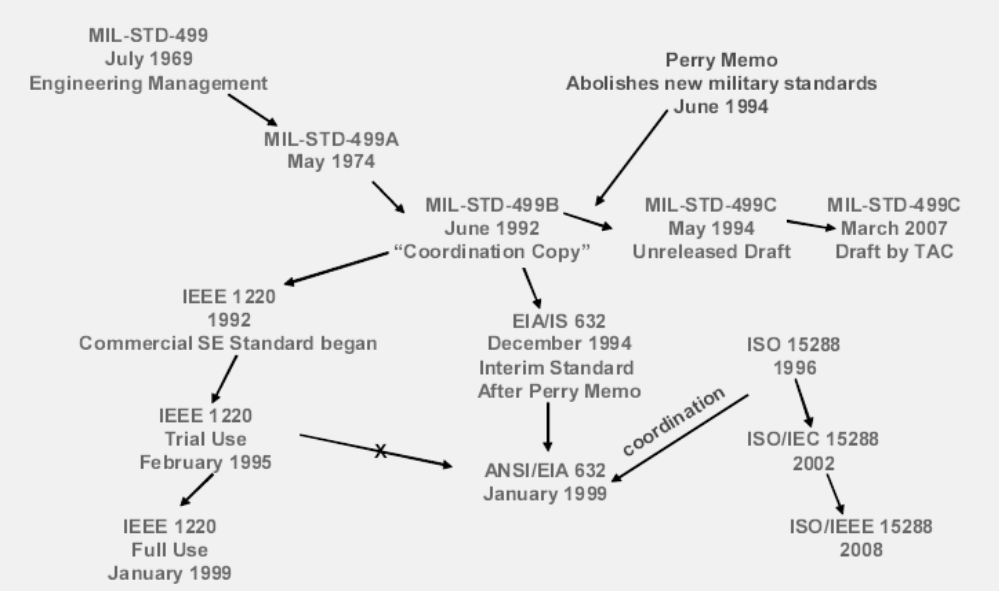


Schéma 4.1 Historique des normes et standards de l'IS, jusqu'en 2008 environ : héritages entre normes et standards

Un gros travail de formalisation a donc été entrepris, par les industriels comme par les agences et les personnels étatiques, via des standards ISO et IEEE, tels que l'ISO 15288, l'ISO-IEC 26702 et l'IEEE 1220 cités plus haut (§0.2), auxquels il convient de rajouter pour l'aéronautique l'ED79/ARP4754A, et pour l'espace les ECSS (ECSS-E-ST-10C, ECSS-E-ST-10-xx, ECSS-M-ST-10C Rev.. 1, et ECSS-M-ST-10-01C).

Ci-dessous une sélection des normes structurantes actuelles pour l'ingénierie des systèmes aujourd'hui, tous domaines confondus (on notera que certaines d'entre elles sont très récentes, on notera également que les normes spécialisées par domaine tels l'aéronautique civile ou l'espace ne figurent pas dans cette table):

Référence	Titre	Commentaire
ISO/IEC/IEEE 24765	Systems and software engineering — Vocabulary	Ce glossaire fournit les définitions pour la plupart des normes ISO relatives à l'architecture et l'ingénierie des systèmes.
ISO/IEC/IEEE-15288	Systems and software engineering — System life cycle processes	Cette norme est très largement utilisée, parfois imposée par les clients. Le contenu de l'INCOSE Handbook est construit sur cette norme ISO.
IEEE-15288.1:2015	IEEE Standard for Application of Systems Engineering on Defense Programs	Contexte Défense
IEEE-15288.2:2015	IEEE Standard for Technical Reviews and Audits on Defense Programs	Contexte Défense
ISO/IEC/IEEE 15289	Systems and software engineering — Content of life-cycle information products (documentation)	La traçabilité à cette norme est parfois demandée par les clients.
NATO AAP-48	NATO System Life Cycle Processes	Cette norme est une déclinaison détaillée pour les besoins de l'OTAN de la norme ISO-15288. Elle est parfois imposée par l'OTAN ou les prescripteurs militaires institutionnels.
ANSI/EIA-632	Processes for Engineering a System	Cette norme, assez ancienne, est à l'origine de la description des concepts de solution, enabling systems, building blocks, arborescence système (Product Breakdown Structure, PBS).
ISO/IEC TR 24748-1	Systems and software engineering — Life cycle management — Part 1: Guide for life cycle management	La traçabilité à cette norme est parfois demandée par les clients.
ISO/IEC/IEEE 42010	Systems and software engineering — Architecture description	Cette norme définit la plupart des termes et des concepts nécessaires à l'architecture système, et utilisés directement par les méthodes et outils tels que NAF, ARCADIA/Capella
TOGAF 9.1	The Open Group Architecture Framework	TOGAF est considérée comme la principale méthode d'architecture système
NAF V3	NATO Architecture Framework V3	Pour les systèmes complexes et les systèmes de systèmes, ce formalisme est maintenant exigé par l'OTAN, l'EDA (Agence de Défense Européenne) et l'ESA

RG Aéro 000 14C / 15A	Définition d'un produit - Guide pour l'élaboration du Dossier de Définition Justification de la définition - Guide pour l'élaboration du Dossier de Justification de la Définition	
ANSI/AIAA G-043A-2012	Guide to the Preparation of Operational Concept Documents	

Table 4.2 Grandes normes de l'ingénierie des systèmes (hors domaines spécifiques)

L'instanciation et la déclinaison pratique de ces standards sur nos secteurs d'activité est déjà très largement en cours. Cependant, cette déclinaison est conduite de manière plus ou moins spécifique, dans chacune de nos entreprises. Une mise en commun du retour d'expérience reste à faire.

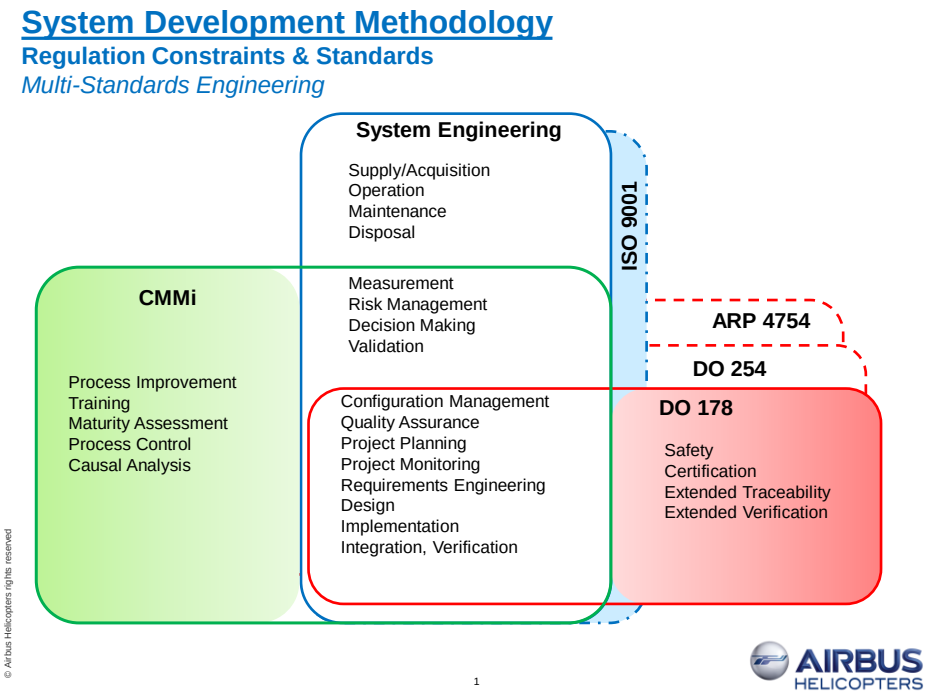


Schéma 4.2 Domaines d'application des différentes normes et standards de l'IS (Courtoisie Jean-Marc Quiot, Airbus Helicopters)

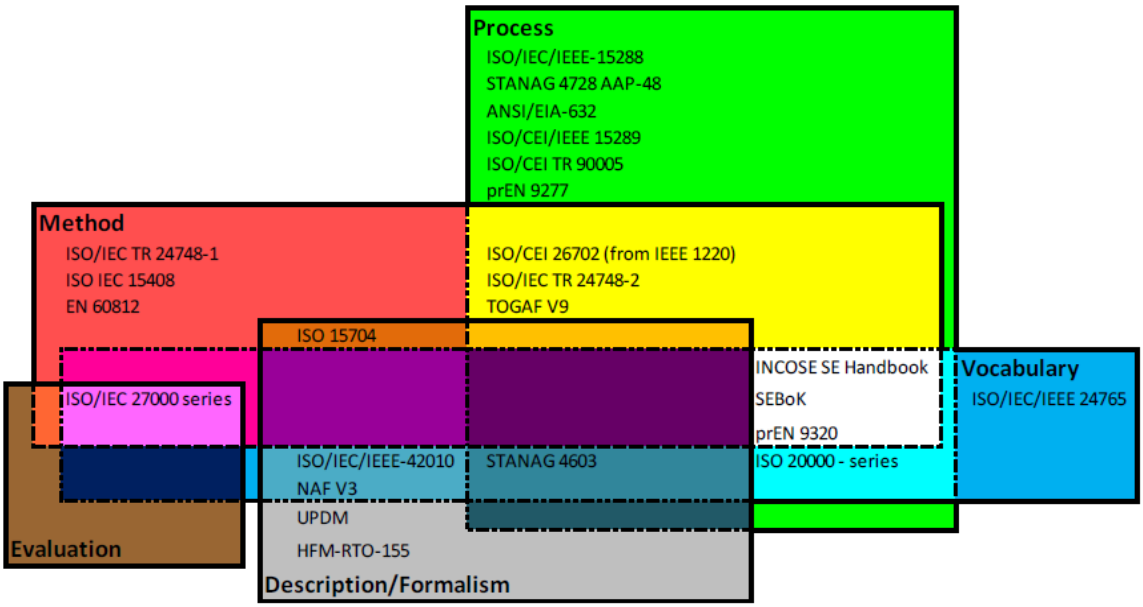


Schéma 4.3 Extrait du rapport EDSTAR - Expert Group 20 System Architecture : EG 20 Characterisation MAP for identified standards - Summary Table.

4.2 ISO 15288

C'est le principal standard international de référence. La dernière édition est l'édition 2015. On renvoie le lecteur au chapitre 2.3, qui décrit les processus de référence de l'ISO 15288, version 2015.

4.3 SE HANDBOOK INCOSE, SEBOK & PM/SE

4.3.1 INCOSE SE Handbook

C'est la référence qu'utilise l'INCOSE pour la certification des ingénieurs. Il s'appuie directement sur la norme ISO 15288, mais est naturellement plus détaillé (c'est un handbook de 305 pages !). La dernière édition en date de cet INCOSE SE Handbook est la version 4, datée de 2015

L'ISO décrit les processus de base, alors que le Handbook détaille les bonnes pratiques liées à la mise en œuvre de ces processus.

On notera que l'INCOSE procède à des certifications, sur la base de la connaissance du Handbook.

4.3.2 SE BoK

Le System Engineering Body of Knowledge (BoK) est un guide interactif qui recueille le retour d'expérience et les bonnes pratiques de nombreux ingénieurs, dans des domaines variés… C'est un panorama large, et une source d'enrichissement pour les normes futures (ISO) et les futures versions du SE Handbook.

4.4 EIA 632 – PROCESSES FOR ENGINEERING A SYSTEM

Ce standard américain publié par la SAE[25] est le résultat d'un travail conjoint entre l'EIA (Electronic Industries Alliance) et l'INCOSE. Il a été développé entre 1994 et 1998. Le document a été officialisé en janvier 1999 et confirmé en septembre 2003.

Ce document a pour but de servir de référence pour la construction des référentiels d'entreprise.

Il identifie 33 exigences, qui contraignent 13 processus génériques, qui couvrent l'ingénierie d'un système, quelle que soit sa place dans la hiérarchie de la structure du système, et la phase du cycle de vie dans laquelle le système est développé de façon incrémentale. Les processus sont applicables à l'ingénierie ou la réingénierie du système d'Intérêt (appelé dans le standard « End-Product ») et des « Systèmes de Soutien » ou « Systèmes Contributeurs », parfois nommés aussi « Systèmes Capacitants » (appelés dans le standard « Enabling products »). Le standard n'identifie pas de méthode, ni d'outil en support des processus. Ceux-ci devant constituer la réponse propre à chaque projet ou à chaque entreprise.

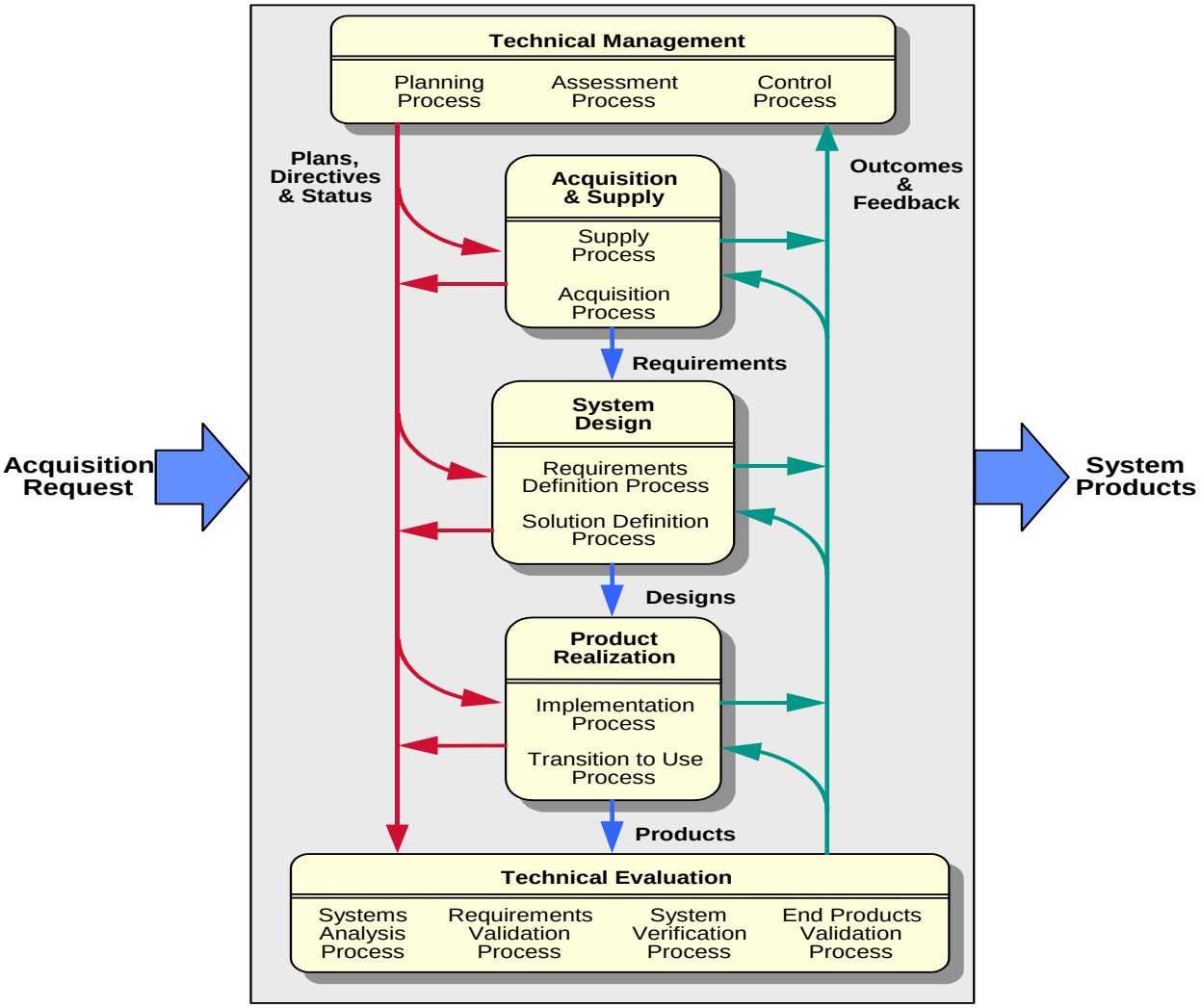


Figure 4.4 —Modèle des processus EIA 632

25 SAE: *Society for Automobile Engineers*

On notera que ce standard propose un modèle de processus concourants :

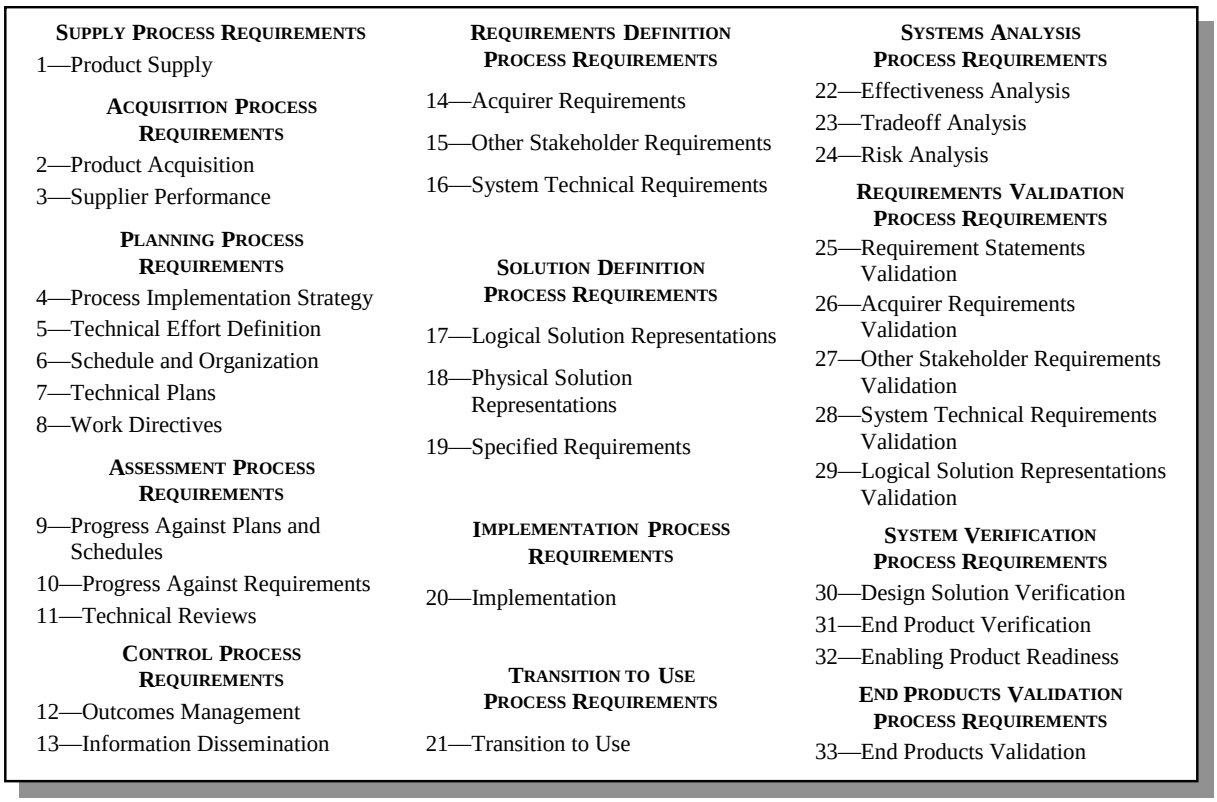


Schéma 4.5 —Relation entre les exigences et les processus

La liste des exigences proposées par l'EIA 632 est la suivante :

Requirement 1—Product Supply

For a system, or portion thereof, supplied to an acquirer, the developer (when acting as the supplier) **shall** establish and satisfy an agreement with the acquirer.

Requirement 2—Product Acquisition

For a system, or portion thereof, acquired from a supplier, the developer (when acting as the acquirer) **shall** establish an agreement with that supplier.

Requirement 3—Supplier Performance

The developer (when acting as the acquirer) **shall** manage supplier performance to ensure that the technical effort to be accomplished by the supplier provides end products that satisfy the assigned requirements.

Requirement 4—Process Implementation Strategy

The developer **shall** define a strategy for implementing the adopted processes of this Standard as a basis for project technical planning and that is in accordance with the agreement.

Requirement 5—Technical Effort Definition

The developer **shall** define a technical effort that is in accordance with the process implementation strategy

Requirement 6—Schedule and Organization

The developer **shall** schedule and organize the defined technical effort.

Requirement 7—Technical Plans

The developer **shall** create technical plans to ensure an integrated and cost effective technical effort in accordance with the defined schedule and organization.

Requirement 8—Work Directives

The developer **shall** create work directives that implement the planned technical effort.

Requirement 9—Progress Against Plans and Schedules

The developer **shall** assess the progress of the technical effort against applicable technical plans and schedules.

Requirement 10—Progress Against Requirements

The developer **shall** assess the progress of system development by comparing currently defined system characteristics against requirements.

Requirement 11—Technical Reviews

The developer **shall** conduct technical reviews of progress and accomplishments in accordance with appropriate technical plans.

Requirement 12—Outcomes Management

The developer **shall** manage the outcomes of the technical effort.

Requirement 13—Information Dissemination

The developer **shall** ensure that required and requested information is disseminated in accordance with the agreement, project plans, enterprise policies, and enterprise procedures.

Requirement 14—Acquirer Requirements

The developer **shall** define a validated set of acquirer requirements for the system, or portion thereof.

Requirement 15—Other Stakeholder Requirements

The developer **shall** define a validated set of other stakeholder requirements for the system, or portion thereof.

Requirement 16—System Technical Requirements

The developer **shall** define a validated set of system technical requirements.

Requirement 17—Logical Solution Representations

The developer **shall** define one or more validated sets of logical solution representations that conform with the technical requirements of the system.

Requirement 18—Physical Solution Representations

The developer **shall** define a preferred set of physical solution representations that agrees with the assigned logical solution representations, derived technical requirements, and system technical requirements.

Requirement 19—Specified Requirements

The developer **shall** specify requirements for the design solution.

Requirement 20—Implementation

The developer **shall** implement the design solution in accordance with the specified requirements to obtain a verified end product.

Requirement 21—Transition to Use

The developer **shall** transition verified products to the acquirer of the products in accordance with the agreement.

Requirement 22—Effectiveness Analysis

The developer **shall** perform effectiveness analyses to provide a quantitative basis for decision making.

Requirement 23—Tradeoff Analysis

The developer **shall** perform tradeoff analyses to provide decision makers with recommendations, predictions of the results of alternative decisions, and other appropriate information to allow selection of the best course of action.

Requirement 24—Risk Analysis

The developer **shall** perform risk analyses to develop risk management strategies, support management of risks, and support decision making.

Requirement 25—Requirement Statements Validation

The developer **shall** ensure that technical requirement statements and specified requirement statements, individually and as sets, are well formulated.

Requirement 26—Acquirer Requirements Validation

The developer **shall** ensure that the set of defined acquirer requirements agrees with acquirer needs and expectations.

Requirement 27—Other Stakeholder Requirements Validation

The developer **shall** ensure that the set of defined other stakeholder requirements agrees with other stakeholder needs and expectations with respect to the system.

Requirement 28—System Technical Requirements Validation

The developer **shall** ensure that the set of defined system technical requirements agrees with the validated acquirer and other stakeholder requirements.

Requirement 29—Logical Solution Representations Validation

The developer **shall** ensure that each set of logical solution representations agrees with the appropriately assigned subset of system technical requirements.

Requirement 30—Design Solution Verification

The developer **shall** verify that each end product defined by the system design solution conforms to the requirements of the selected physical solution representation.

Requirement 31—End Product Verification

The developer **shall** verify that an end product to be delivered to an acquirer conforms to its specified requirements.

Requirement 32—Enabling Product Readiness

The developer **shall** determine readiness of enabling products for development, production, test, deployment/installation, training, support/maintenance, and retirement or disposal.

Requirement 33—End Products Validation

The developer **shall** ensure that an end product, or an aggregation of end products, conforms to its validated acquirer requirements.

4.5 GUIDELINE D'INGENIERIE DES SYSTEME POUR LES PME

Pour les PME, on peut simplifier l'approche et utiliser, pour le déploiement de l'IS, le standard ISO/IEC 29110 "Systems and Software Engineering - Lifecycle Profiles and Guidelines for Very Small Entities (VSEs)" (norme composée de cinq parties ISO/IEC TR 29110-1 à ISO/IEC TR 29110-5), qui est promu par l'AFIS.

Il présente deux originalités:

- Ce standard définit quatre types de profils utilisateurs (entrée, basique, intermédiaire, avancé), et adapte les préconisations de déploiement à ces profils,
- Il comporte des trousses de déploiement par thème, pour faciliter la mise en place du processus IS.

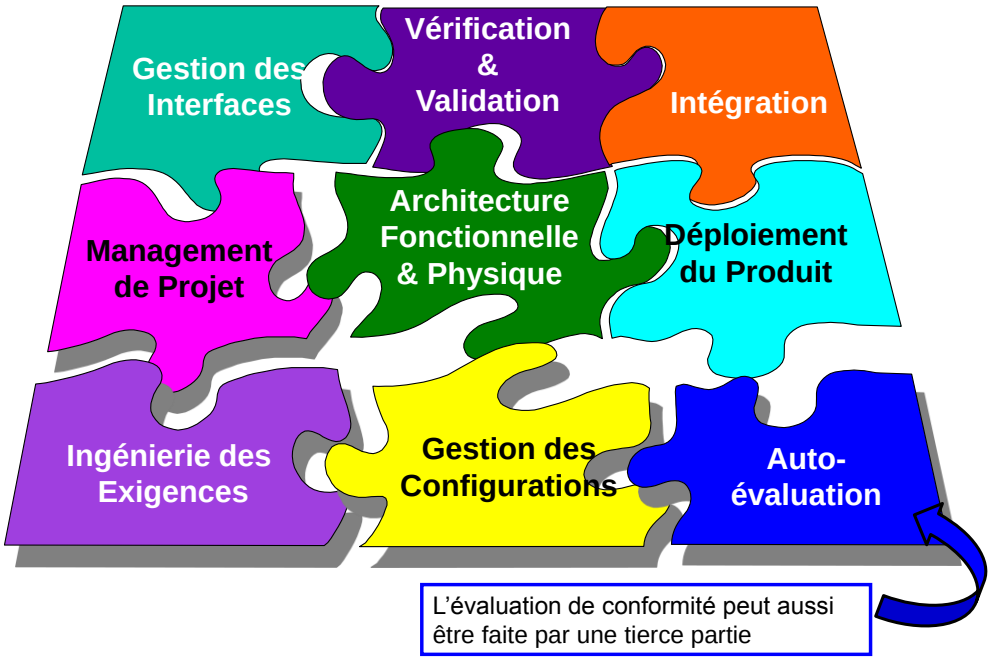


Schéma 4.6 Les thèmes du guide ISO 29110

4.6 NORMES POUR L'AERONAUTIQUE (CIVILE ET MILITAIRE)

Dans l'aéronautique civile, la règlementation, pour faire face à la complexité des systèmes et assurer la qualité de leurs développements, définit un cadre de recommandations méthodologiques dont le schéma suivant donne une vue d'ensemble :

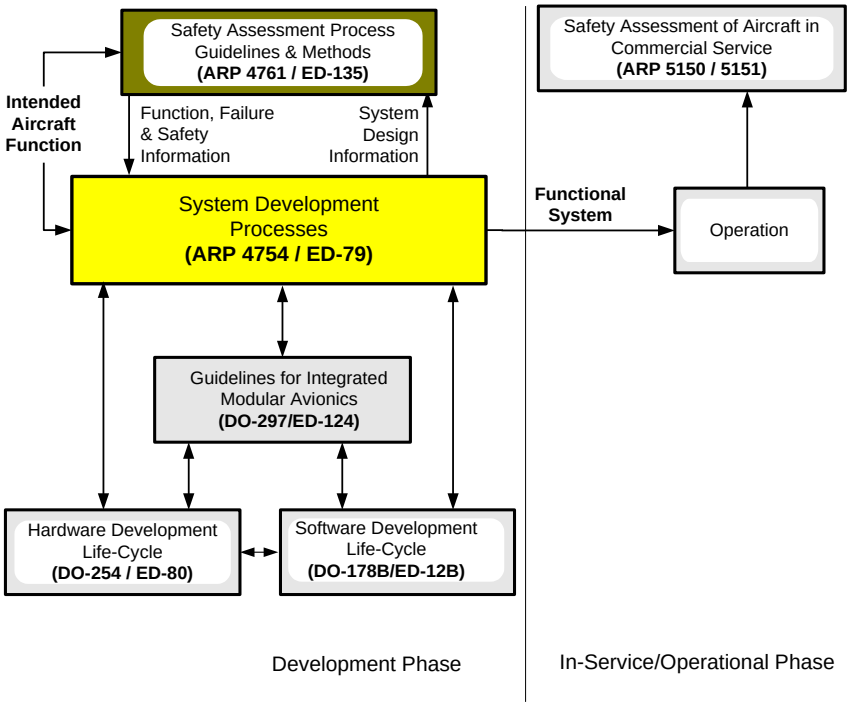


Schéma 4.7 Cadre méthodologique réglementaire (Aéronautique civile)

Ce cadre est constitué d'un ensemble de recommandations duales (des ED élaborées par l'Eurocae côté européen ; et des ARP du SAE ou des DO du RTCA côté USA). Parmi celles-ci deux concernent directement l'Ingénierie des Systèmes :

- L'ED79/ARP4754 (1996) « Certification Considerations for Highly-Integrated or Complex Aircraft Systems » et sa mise à niveau ED79A/ARP4754A (2010) « Guidelines for development of civil aircraft and systems ».
- Ce document est le document chapeau autour duquel s'organisent les autres.
- L'ED135/ARP4761 « Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment »

Concernant les avions militaires et les drones, une tendance (en France avec DGA, et en Europe) est de pousser à l'application de ces deux mêmes ED/ARP.

4.6.1 L'ED79A/ARP4754A et son interprétation

L'ED79/ARP4754 introduit une approche de certification fondée sur la maîtrise du processus de développement pour démontrer la maîtrise de la qualité du produit, en lieu et place de l'approche antérieure fondée directement sur la démonstration de qualité du produit.

L'ED79/ARP4754, dans ses versions 96 et A, a structuré et formalisé les activités afin d'assurer une meilleure maîtrise du développement d'un aéronef. Ces activités doivent être décrites, planifiées et contrôlées de façon plus ou moins poussée en fonction de la criticité de la fonction, du système, du sous-système ou de l'item à développer.

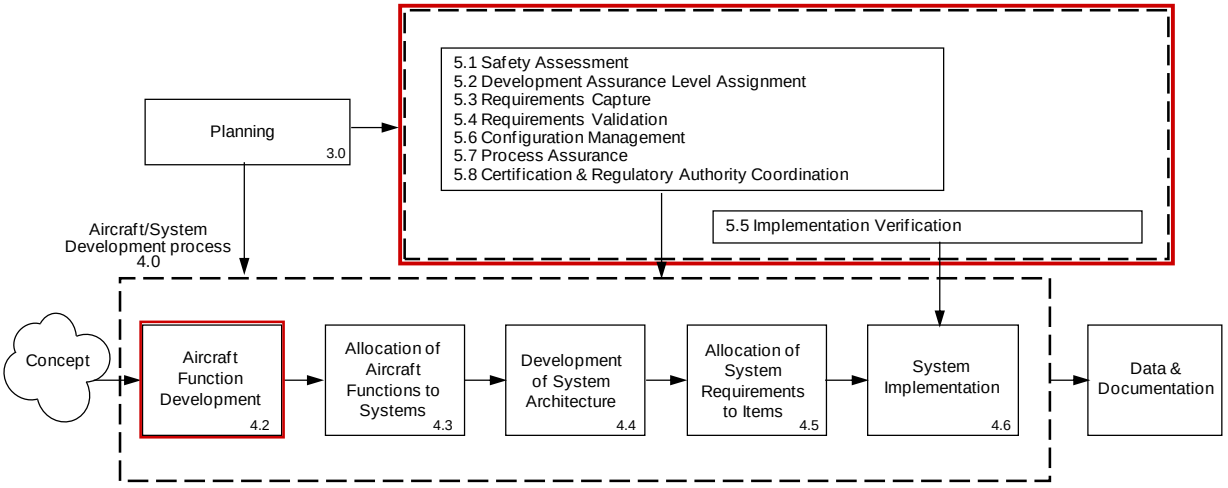


Schéma 4.8 Le modèle de développement de l'ED79/ARP4754

Comme le montre le schéma ci-dessus, l'ED79/ARP4754 considère trois séries de processus :

- Le processus de développement proprement dit (4.) : le domaine couvert va des fonctions avion aux « items » en passant par les systèmes. Les équipements sont des systèmes, les « items » relèvent de composants SW ou HW. Cette structuration autour de ces 3 niveaux se retrouve aussi dans l'ED135/ARP4761.

- Les processus support de l'IS (appelés « Integral process » en anglais) : c'est sur ces activités que portent le gros des recommandations :

  - Activités nécessaires pour garantir la sûreté de fonctionnement : Introduites ici, elles sont détaillées dans ED135/ARP4761.

  - Assignation du niveau d'assurance (DAL[26]) en fonction de la criticité.

  - Assurance des Processus : il s'agit de la mise en place d'activité de type qualité chargé de veiller à bonne l'application des méthodes d'IS.

  - Gestion des exigences.

---

26 Nota : *DAL: Development Assurance Level (auparavant : Design Assurance Level)*

    - Validation des exigences et des hypothèses, ce qui revient à se poser la question : a-t-on écrit la bonne spécification ?

    - Vérification de l'implémentation afin de démontrer la conformité aux exigences, ce qui revient à se poser la question : a-t-on réalisé le bon produit (à savoir celui en accord avec la spécification) ?

    - Gestion de configuration en développement. Ceci inclut la gestion des évolutions.

    - Négociation et justification en vue de l'obtention de la certification de type.

  - La planification de l'ensemble de ces activités en début de développement puis sa mise à jour (3.).

- Constat : L'ARP 4754A est un mélange d'exigences implicites et de solutions préconisées. Elle donne donc lieu à interprétation par ceux qui ont à l'utiliser. Par exemple la notion d'indépendance, notamment lors du processus de revues de validation & vérification, en fonction de criticités, est sujette à interprétation, et peut conduire à des surcoûts.

- Constat : En corollaire du constat précédent, on voit apparaitre des documents d'aide à l'interprétation dont la cohérence n'est pas garantie. On citera : SAE aerospace information Report (AIR6110) ou RGAero 000 44. Les industriels ont donc un effort substantiel pour faire l'interprétation la plus juste par rapport à leur besoin.

- Constat : D'autres standards sont applicables selon les donneurs d'ordres qui requièrent des activités similaires souvent identifiées ou décrites de façon différentes (cf. Validation et Vérification)

- Constat : Des frontières entre les mondes ARP4754 et DO178/254, et des activités à mener qui ne sont pas toujours limpides L'ARP 4754-A restant interprétable.

- Constat : Le risque lié à ces approches dissociées est potentiellement de conduire à de grandes divergences d'interprétation, ainsi qu'à une acceptation difficile et tardive par l'autorité de certification. Ceci peut entrainer au final des demandes de démonstrations de plus en plus importantes par les autorités. Il peut donc être considéré comme moins risqué de démontrer l'adhésion aux principes de l'ED79/ARP4754A, plutôt que de développer une méthode alternative. Cependant, ceci ne signifie pas pour autant que l'on doit appliquer / démontrer la conformité à l'ED79/ARP4754A « à la virgule près ».

- Constat : L'application de l'ED79/ARP4754A a obligé les avionneurs, les systémiers et sous-systémiers, mais aussi les équipementiers à revoir en profondeur leur processus de gestion des exigences et de V&V, en déployant systématiquement aux niveaux systèmes et équipements des méthodologies jusqu'alors principalement réservés aux projets critiques et aux développements Hardware électronique / Logiciel.

4.6.2 L'ARP4761/ED-135 – Comment décliner les exigences de sûreté («safety») ?

4.6.2.1 **Généralités**

L'ED135/ARP4761 définit un ensemble d'activités couvrant l'évaluation de la Sûreté («safety»), avec principalement la description de méthodes d'analyse courantes pour cette évaluation de la sûreté, dont :

- FHA : Functional Hazard Assessment,
  Il s'agit d'analyses fonctionnelles qui s'intéressent aux modes de défaillances des fonctions et à leur impact en terme de "dangerosité". Elles sont quantitatives et classent les événements selon les niveaux de la réglementation (Catastrophic, Hazardous, Major, Minor, No effect). Typiquement, elles sont menées au niveau avion(AFHA) et systèmes (PFHA).
- X Safety Assessment:
  Il s'agit d'analyses quantitatives qui prennent les événements précédents en leur assignant des objectifs quantitatifs qui sont dérives sur l'architecture retenue et ses constituants. Une méthode typiquement utilisée est celle des arbres de pannes.
  Il faut distinguer l'état préliminaires (PSSA : Preliminary System Safety Analysis) faite avant l'implémentation de l'état consolidé (SSA : System Safety Analysis). La PSSA descend des objectifs pour le design alors que la SSA conforte la tenue des objectifs avec des données de fiabilité réels (AMDEC).
  En anglais, on fait référence à des :
    - FMEA : Failure Mode and Effects Analysis,
    - FMES : Failure Modes and Effects Summary,

  Ces évaluations sont réalisées au niveau systèmes et auparavant avion (sur la base d'une architecture constituée de systèmes « boîtes noires »)

- CCA : Common Cause Analysis, incluant :
    - ZSA : Zonal Safety Analysis,
    - PRA : Particular Risks Analysis,
    - CMA : Common Mode Analysis.

Le processus global peut être synthétisé par le schéma ci-dessous :

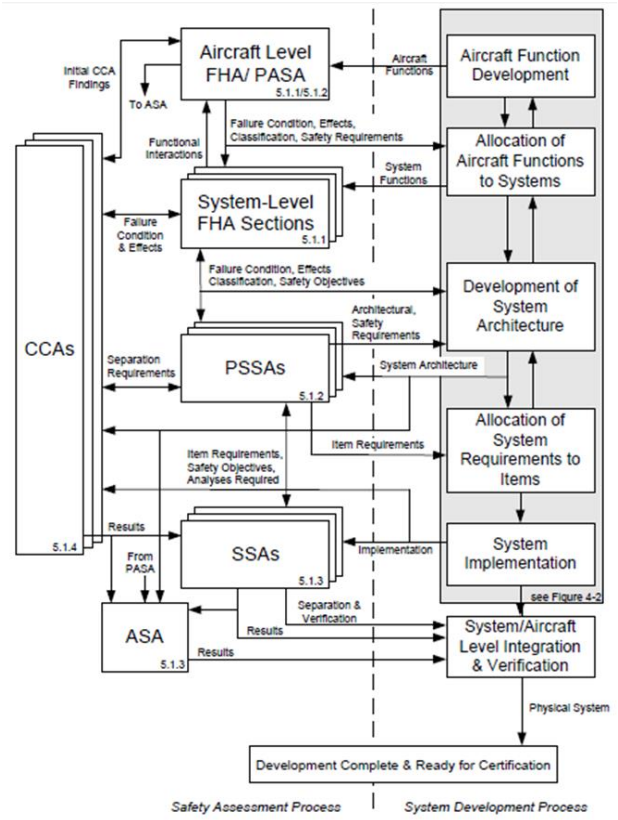


Schéma 4.9 : Relation analyses sûreté («safety») vs développement d'un système (d'après ED79A/ARP4754A)

Les processus de conception et d'évaluation de ces systèmes deviennent de plus en plus complexes en particulier les analyses de sûreté («safety»)[27]. La sûreté doit être prise en compte de manière globale, et pas uniquement localement. En effet les propriétés de sûreté sont des propriétés émergentes, qui résultent d'interdépendances existant dans le système, et dans l'interaction avec son environnement. De ce fait, il est absolument nécessaire que ces propriétés soient étudiées globalement, au niveau du système complet, si l'on souhaite qu'elles soient respectées. Il est alors nécessaire d'éliciter d'une manière globale les exigences de sûreté. Ces dernières seront ensuite déclinées, au fur et à mesure, au niveau local et devront être satisfaites, par les différents composants du système.

De surcroit, les propriétés de sûreté du système doivent être considérées dès le début de la conception. En effet, elles ne peuvent que difficilement être introduites ou même mesurées a posteriori[28], et doivent être traitées le plus tôt possible pour limiter leurs impacts sur les délais et les coûts de conception.

---

27 Nota : *On emploie à dessein le mot anglais « safety », pour éviter l'ambigüité existant en français entre sûreté et sécurité.*

28 Nota : *Une introduction tardive est en effet génératrice de risques !*

4.6.3 Déclinaison des exigences de Safety

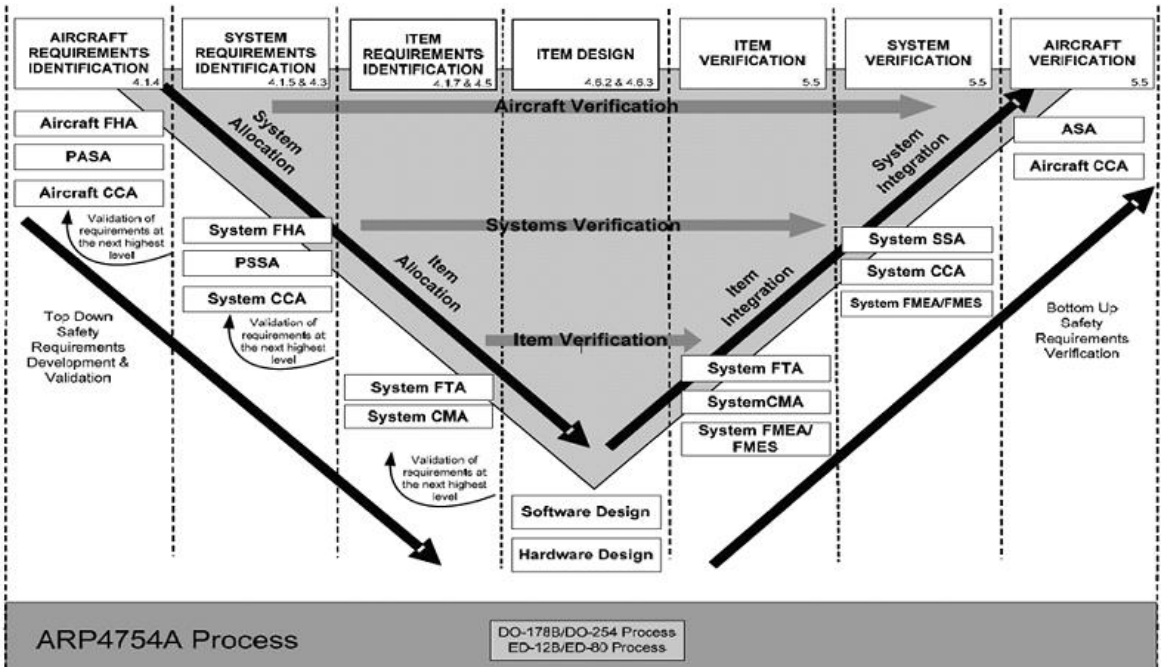


Schéma 4.10 : Processus ARP 4754A

L'objectif de la méthodologie est de pouvoir lier les exigences de safety, définies au niveau système, avec celles définies au niveau des sous-systèmes. Ces liens correspondent alors à la déclinaison des exigences.

Le processus de déclinaison est une analyse itérative qui fait partie intégrante du développement du système.

Ce processus commence par l'analyse des défaillances du système d'intérêt (en l'occurrence l'avion) qui peuvent conduire à une situation catastrophique ou, tout du moins, à un événement non-souhaité. Cette analyse est documentée par l'« aircraft FHA », dès les premiers stades du développement, lors de l'allocation des fonctions et exigences avions aux systèmes de l'avion.

L'analyse se poursuit par l'étude des causes de ces défaillances en s'appuyant sur l'architecture du système. Il s'agit de trouver les origines des défaillances systèmes au niveau des sous-systèmes. Cette étape peut s'appuyer sur des outils tels que les arbres de défaillances (FTA), ou encore les chaines de Markov.

L'analyses de causes communes (CCA) est également menée pour atténuer (« mitigate », en anglais) les modes communs de panne (erreur de développement, pannes génériques, propagation de pannes, etc.)

Les exigences safety issues de la réglementation sont alors raffinées du système, aux sous-systèmes puis déclinées aux composants principalement sous la forme:

- d'exigences quantitatives : définissant des taux de pannes /de disponibilité des fonctions et sous fonctions.
- d'exigences de dissimilarité dans le choix des composants, et d'indépendance entre les équipes de développement des fonctions redondantes
- d'exigences de niveau de DAL[29] applicables au développement de composants complexes : Le niveau de DAL demandé va du DAL A (processus de développement les plus rigoureux) pour les fonctions les plus critiques au DAL E.

La justification de cette déclinaison est détaillée dans la PSSA et se fonde sur les analyses mentionnées ci-dessus.

4.6.4 Assignation du niveau de Design Assurance

Dans l'ARP 4754 version 1996, une attention particulière est portée à l'allocation du Design Assurance Level qui contraint fortement le développement des composants complexes. L'architecture du système et notamment les différentes redondances assurant une même fonction peuvent être prises en compte pour minimiser le niveau de Design Assurance.

La version A de l'ARP 4754 a étendu le concept du niveau d'assurance de développement au niveau Fonctionnel (FDAL), l'ancienne notion au niveau des items étant rebaptisée IDAL (Item Development Assurance).

La notion de « Development Assurance » est considérée comme plus large que celle de « Design Assurance », c'est-à-dire nécessitant de prendre aussi en compte des activités d'assurance à réaliser au niveau aéronef et systèmes, en plus de celles classiquement recommandées pour le matériel électronique et le logiciel par les DO-254 / ED-80 et DO-178 / ED-12.

---

29 Nota : *DAL : « Development Assurance Level », dans l'ARP4754A (auparavant l'ARP 4754 parlait de « Design Assurance Level »).*

4.7 NORMES ECSS POUR L'ESPACE

Les standards ECSS (pour « European Cooperation for Space Standardization ») ont été développés avec une forte implication de l'Agence Spatiale Européenne (ASE, plus connue sous le sigle anglo-saxon d'ESA), et avec le soutien des agences nationales (CNES, DLR, …) et des industriels européens du secteur de l'Espace (rassemblés dans l'association EUROSPACE). Les différentes normes ont été établies à partir de 1994, mais leurs dernières versions (édition C) sont parues principalement entre 2008 et 2014. Ce dernier corpus de normes édition C a été agréé au 22 mai 2014. A noter que les normes ECSS vont devenir très prochainement des normes EN.

Les normes/standards ECSS étaient organisés en trois branches : Management, Ingénierie (« Engineering » en anglais) et Assurance Produit (« Product Assurance » en anglais). Une quatrième branche « Space Sustainability » (Espace Durable en français) s'est ajoutée ultérieurement. On notera qu'un travail permanent est effectué par l'ECSS afin d'actualiser les documents normatifs existant, et d'en créer de nouveaux, en complément. Les documents se déclinent en différents types :

- ST – Standard
- AS – Adopted Standard
- HB – Handbook
- AH – Adopted Handbook
- TM – Technical Memorandum

L'organisation générale des normes/standards de l'ECSS est décrite dans le schéma suivant :

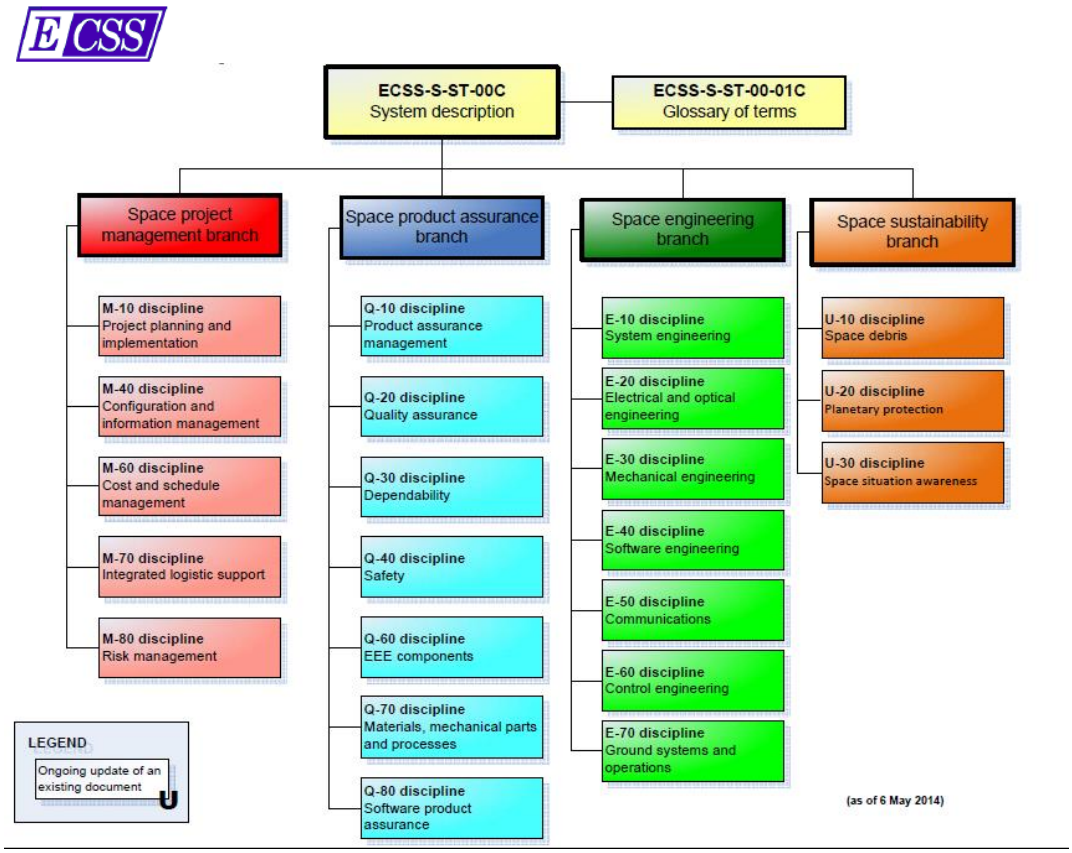


Schéma 4.11 Organisation générale des normes/standards de l'ECSS (Mai 2014)

Concernant l'Ingénierie des Systèmes, les principaux documents constituant des standards d'ingénierie sont les suivants, comme décrits dans le schéma suivant :

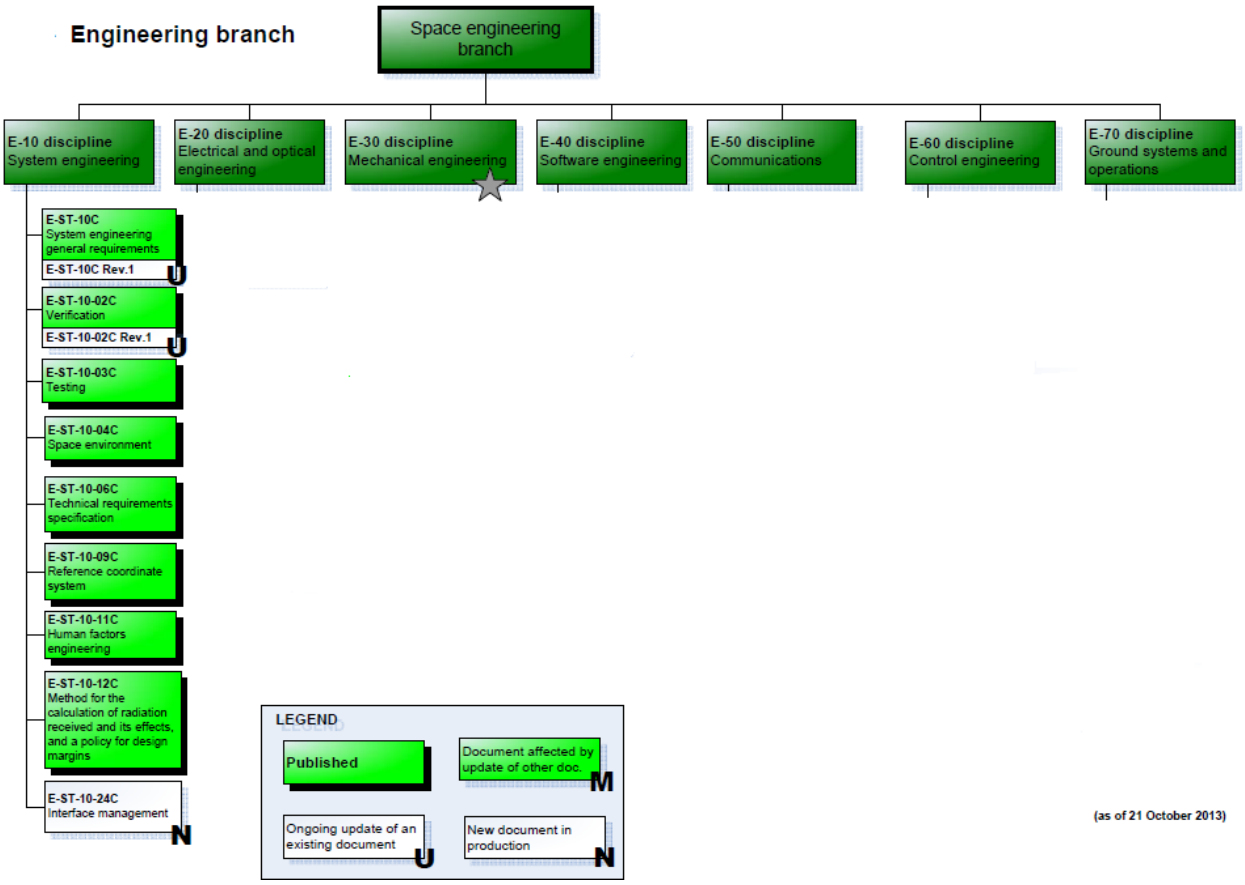


Schéma 4.12a Principaux standards « engineering » de l'Ingénierie des Système dans les ECSS (N : nouveau document, U : Update de document M : modification induite par un update de document) (Mai 2013)

- ECSS-S-ST-00-01C ECSS system - Glossary of terms
- ECSS-E-ST-10C System engineering general requirements (*recommandations générales sur l'implémentation et le processus de l'ingénierie des systèmes sur les systèmes spatiaux, afin d'assurer un référentiel technique solide, de maîtriser les risques et les coûts, de définir les tâches d'ingénierie des systèmes à conduire, et de préparer l'intégration, le contrôle, et la vérification.*)
- ECSS-E-ST-10-02C Space engineering – Verification (*description des exigences relatives à la vérification*)
- ECSS-E-ST-10-03C Space engineering – Testing (*description des exigences relatives aux essais et tests*)
- ECSS-E-ST-10-04C Space engineering – Space Environment (*description des exigences relatives à l'environnement spatial*)
- ECSS-E-ST-10-05A Space engineering – Functional Analysis (*non repris en tant que tel dans la version C, car intégré à d'autres standards*)
- ECSS-E-ST-10-06C Space engineering – Technical requirements specification (*définition des exigences à capturer, et de la documentation associée*)
- ECSS-E-ST-10-09C Space engineering – Reference coordinate system (*description des exigences relatives aux systèmes de coordonnées, et référentiels*)
- ECSS-E-ST-10-11C Space engineering – Human Factors Engineering (*description des exigences relatives au facteur humain*)
- ECSS-E-ST-10-12C Space engineering – Method for the calculation of radiation received and its effects, and a policy for design margins[30] (*méthodes relatives au calcul des radiations spatiales reçues par les véhicules spatiaux, et à leurs effets*)
- ECSS-E-ST-10-24 Space engineering – Interface control (Nouveau document, première parution 01/06/2015; *description des exigences relatives au contrôle des interfaces*)
- ECSS-M-ST-10C Space project management – Project planning and implementation
- ECSS-M-ST-40C Space project management – Configuration and information management
- ECSS-Q-ST-20-10C Off-the-shelf items utilization in space systems

Schéma 4.12b Principaux standards de l'Ingénierie des Système dans les ECSS

30 Nota : *Dans cette liste, on peut considérer que certains standards étiquetés E-10 comme le E-ST-10-04C « Space Environment », l'ECSS-E-ST-10-09C « Reference coordinate system », et l'ECSS-E-ST-10-12C « Method for the calculation of radiation received and its effects, and a policy for design margins » sont très spécifiques du domaine spatial, même s'ils ont indéniablement un caractère système.*

La vision de l'Ingénierie des Systèmes des ECSS peut être succinctement décrite au travers des deux schémas suivants, empruntés à l'ECSS-E-ST-10C « System engineering general requirements », montrant respectivement les frontières et les interfaces de l'IS et ses principales fonctions, et leurs relations :

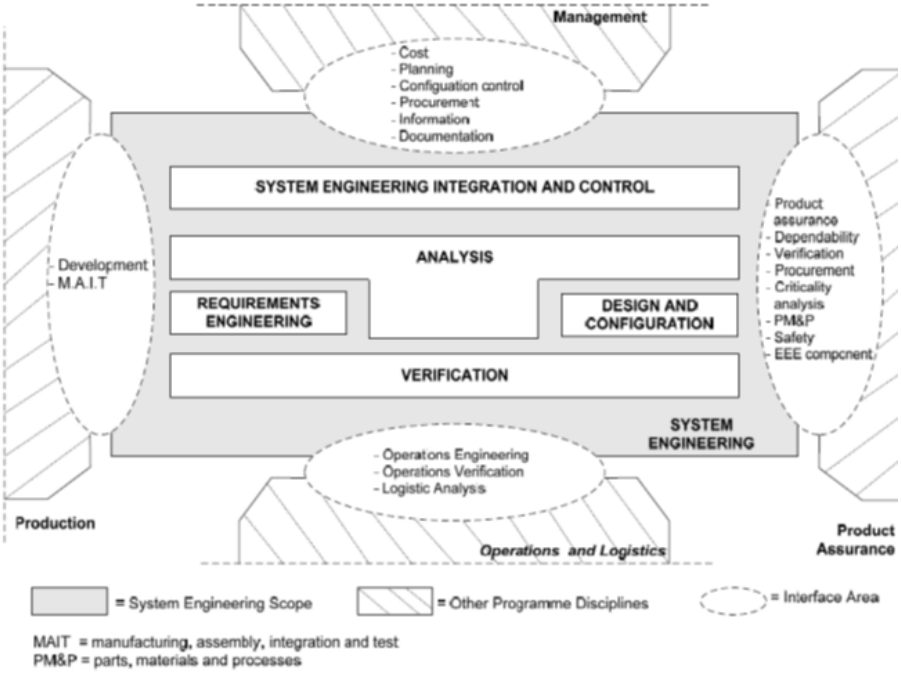


Schéma 4.13 : "System engineering functions and boundaries", vision des ECSS

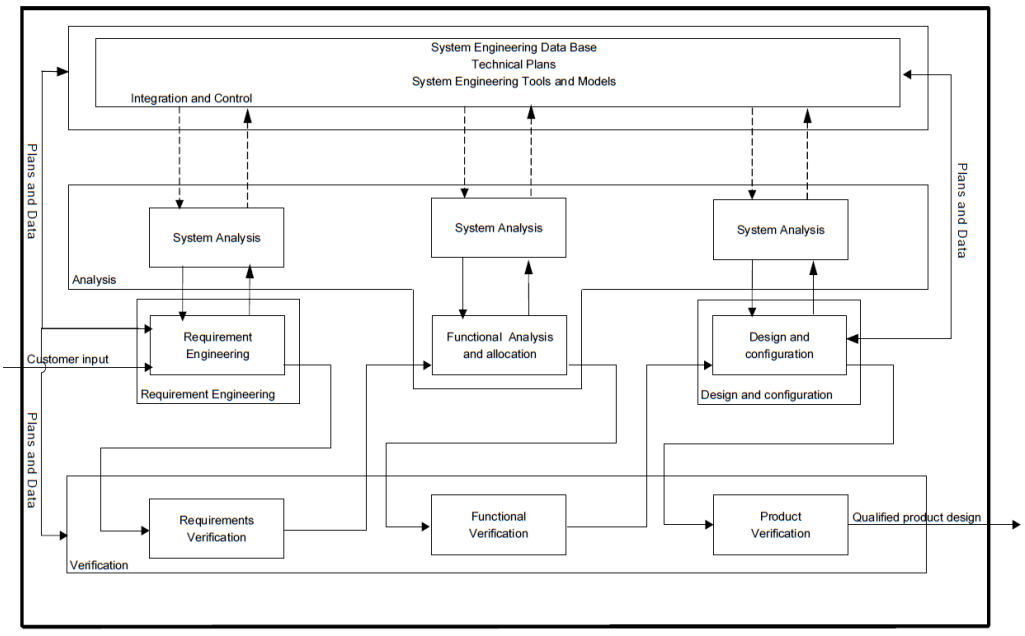


Schéma 4.14 : "System engineering functions and relationships", vision des ECSS

4.8 NORMES POUR LA DEFENSE

Les normes du domaine de l'ingénierie des systèmes aujourd'hui sont pour la plupart issues de normes promues par les grandes institutions de la défense, américaines puis européennes. Dans un second temps, les normes essentielles de l'architecture et de l'ingénierie des systèmes ont été reprises, adaptées et publiées, dans un cadre élargi à l'ensemble des domaines d'activités (cf. schéma 4.1).

Le monde de la défense reste aujourd'hui un grand pourvoyeur de documents normatifs, dans le but de garantir l'interopérabilité technique des moyens en opération, mais aussi d'organiser et maîtriser certaines caractéristiques telles que le niveau de performances, la réutilisation, la disponibilité, le coût total de possession, la compatibilité des moyens de soutien, etc. sur le cycle de vie global.

Les appels d'offres et contrats de solutions de défense font largement référence à ces normes, selon une sélection propre à chaque cas particulier.

Côté US, les 'Standards' militaires recouvrent les Handbook (MIL-HDBK), Defense Specification (MIL-SPEC), Defense Standard (MIL-STD), Performance Specification (MIL-PRF) et Detail Specification (MIL-DTL).

Côté UK, l'agence 'Defence Standardisation' gère essentiellement les Defence Standards (DEF-STAN).

Pour ce quoi concerne l'OTAN, il s'agit de Standardization Agreements (STANAG), ratifiés par les Nations pour application dans leurs Forces. Enfin, notons pour l'Europe de la Défense, la création en 2011 de EDSTAR European Defence Standards Reference System, sous le contrôle de l'Agence de Défense Européenne (EDA), avec pour ambition une utilisation optimisée des normes civiles et militaires dans les contrats des agences de défense de chaque nation.

De façon concrète, l'Agence de Défense Européenne (EDA), par le biais du Groupe d'Experts N°20, propose une sélection de bonnes pratiques, normes et standards pour l'Architecture et l'Ingénierie des Systèmes, dans un rapport de novembre 2014[31], Un outil en ligne, regroupant les bonnes pratiques et recommandations des experts, quant à une sélection de normes applicables à un domaine technique, est également disponible: https://edstar.eda.europa.eu/standards .

31 Nota : *disponible en ligne:* https://edstar.eda.europa.eu/docs/librariesprovider7/standards-docs/edstar---eg-20---system-architecture---final-report_after-jmc-edstar-presentation.pdf?sfvrsn=2.

Si on laisse de côté les normes directement liées à des domaines d'opérations militaires ou des technologies particulières, les actions principales engagées concernant les normes de l'ingénierie des systèmes sont:

- Au niveau français et européen par le BNAe :
  - RG 000 77 : Guide pour le management de l'Ingénierie Système
    - Développement en recommandation générale
    - Promotion en norme européenne: ASD-STAN PREN 9277 P1 « Program Management – Guide for the management of Systems Engineering (janvier 2013).
  - RG 000 120 : Recommandation générale pour l'acquisition et la fourniture de systèmes ouverts
    - Développement en recommandation générale
    - Promotion en ASD-STAN
  - RG 000 08 : Guide pour l'élaboration de la spécification technique de besoin
    - Mise à jour en cours
    - Promotion en ASD-STAN ensuite
  - RG 000 50 : [Titre à définir] devrait être un document-chapeau sur l'expression de besoin, la définition et la justification de solution
    - Travaux en cours
- Dans un cadre plus large, des groupes de travail par des structures militaires telles que NATO STO-CSO/IST Study "Arch. Description and Evaluation", et EDSTAR EG-20 "System Architecture", sont à l'œuvre pour promouvoir des méthodes de description et d'évaluation des architectures : NAF V4 terms and concepts, ainsi que les normes ISO-42010 et 42030.

4.9 CADRES D'ARCHITECTURE (ARCHITECTURE FRAMEWORKS) UTILISES DANS LE MONDE DE LA DEFENSE : NAF, DODAF

4.9.1 Introduction

Avant de s'engager sur les produits et services livrables, tous les besoins relatifs au développement, à la production, la validation, la qualification, la certification, l'emploi et l'utilisation d'un système opérationnel donné doivent être capturés, rendus explicites, justifiés et évalués. Cette activité amont (Feasability, concept exploration, cf. schéma 2.3) doit s'attacher à couvrir les besoins de toutes les parties prenantes, sur le contour de la solution, comprenant à la fois le système d'intérêt et les systèmes en support (cf. schéma 1.1).

Il s'agit ainsi, durant cette phase d'architecture de haut niveau (Architecting), de définir et partager, avec l'ensemble des parties prenantes, une représentation de la solution future. Cette description de haut niveau est particulièrement recommandée dans le cadre des systèmes de systèmes pour lesquels la description des capacités (capabilities) ou des services (capacités offertes à une tierce partie) attendus est primordiale. Plus généralement, il convient de définir un cadre partagé de description d'architecture, en support à cette activité.

Le standard ISO/IEC/IEEE 42010 :2011 « Systems and software engineering — Architecture description » définit le terme « architecture framework » (« cadre d'architecture » en français) de la façon suivante :

> "Architecture framework: conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders."

En pratique, les cadres d'architecture adressent diverses problématiques :

- L'organisation en entreprise : FEAF, GAF, E2AF, etc.
- Les formalismes : NATO A.F. (NAF), DoDAF, MODAF, etc.
- Les processus : PEAF, etc.
- Les méthodes et activités : TOGAF, ABM, etc.
- Les langages et notations : UPDM, ArchiMate®, etc.

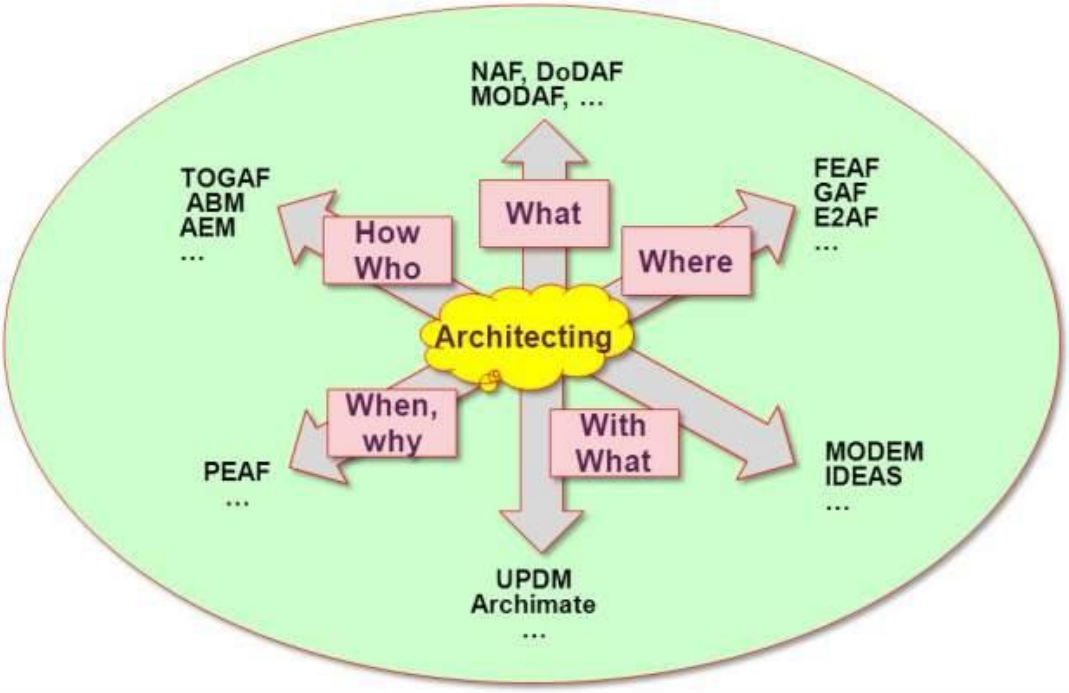


Schéma 4.15 : Divers cadres d'architecture pour différentes préoccupations

Il est donc nécessaire de combiner des cadres d'architecture pour mettre en place un environnement de travail.

Les « frameworks » reposent de plus en plus sur des méta-modèles de manière à :

- Formaliser les termes et concepts fondateurs.
- Donner des bases pour l'interopérabilité entre les environnements de travail.

4.9.2 Domaine d'emploi

D'un point de vue historique, le framework conçu par John Zachman chez IBM en 1987 est considéré comme pionner en la matière. Sa motivation était de s'attaquer aux problèmes créés par la complexité croissante des systèmes et au manque d'alignement entre le métier et les solutions techniques. Ce framework reste une référence ; en revanche, dans le domaine militaire, d'autres cadres d'architecture se sont rapidement imposés : tout d'abord avec C4ISR-AF, puis DoDAF (US Department of Defense Architecture Framework), MODAF (British Ministry of Defence Architecture Framework), NAF (NATO Architecture Framework), AGATE (Atelier de Gestion de l'ArchiTEcture des systèmes d'information et de communication développé par le DGA ; mais maintenant abandonné au profit du NAF), etc.

Le site du standard ISO/IEC/IEEE 42010[32] maintient une liste de ces frameworks, dont les principaux utilisés dans le monde de la défense pour la description d'architecture. Voir le lien vers Survey of Architecture Frameworks: www.iso-architecture.org/ieee-1471/afs/frameworks-table.html .

32 Nota : http://www.iso-architecture.org/ieee-1471/afs/frameworks-table.html

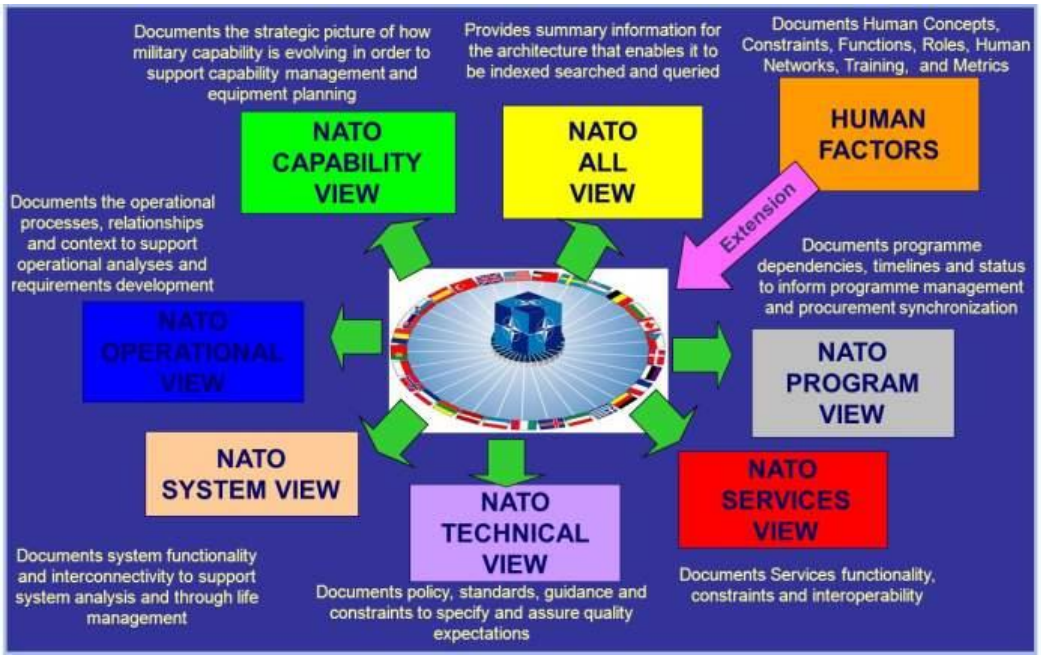


Schéma 4.16 : NAF V3 et extension Facteurs Humains

Le NAF est dérivé du C4ISR-AF, ainsi que le DoDAF dans une certaine mesure, et partage l'essentiel du méta-modèle avec MODAF. Ces trois frameworks (NAF, DoDAF et MODAF) sont de loin les plus utilisés dans le monde de la défense. En France, la recommandation de la DGA est l'emploi du NAF (depuis l'abandon d'AGATE).

Les frameworks permettent de configurer un environnement pour travailler les architectures (« Architecting » en anglais) avec la mise en place :

- De référentiel d'architecture (portfolios, librairies),
- De méthode(s) et processus pour l'architecture, en lien avec les autres processus de l'entreprise,
- Des moyens (humains, techniques [outils, langages] et organisationnels) pour couvrir l'architecture.

La démarche d'architecture permet de formaliser et évaluer des vues d'architecture, ainsi que de faire un bilan de risques et opportunités. Ceci constitue une base pour la gouvernance des développements et l'exploitation des systèmes/produits. En particulier, l'architecture définit les différents éléments architecturaux (par exemple les processus, l'information échangée, les services, standards, etc.) contenus dans les vues et proposent les formalismes les plus adaptés pour les décrire, souvent basés sur des notations de modélisation telles que BPMN (Business Process Model and Notation) et UML (Unified Modeling Language).

Les liens et les dépendances possibles entre les éléments sont également établis par les frameworks. Ainsi, par exemple, les processus métier peuvent être reliés aux fonctions logicielles/matérielles les supportant, ce qui permet d'identifier l'impact de la modification d'un processus sur le système technique et vice-versa. Ce mécanisme est

à la base de l'intérêt que présentent les outils basés sur les frameworks d'architecture dans l'aide à la décision et à la gestion de l'évolution des systèmes.

4.9.3 Application du NAF dans SESAR : European ATM Architecture (EATMA)

Dans SESAR[33] (Single European Sky ATM Research), la description de l'architecture ATM européenne est décrite dans des centaines de documents produits par des dizaines de projets travaillant en parallèle. Les objectifs stratégiques (feuille de route), les processus opérationnels, l'information, les fonctions système et d'autres éléments architecturels sont décrits dans des documents séparés mais interdépendants, dont la cohérence doit être maintenue.

Face à la difficulté d'assurer la cohérence globale du programme, l'initiative « European ATM Architecture (EATMA) » a été lancée en 2012 : son objectif est d'orienter le développement du programme vers une approche de plus en plus dirigée par les modèles en se fondant sur un sous ensemble de la norme NAF adapté aux besoins SESAR. Cette approche sera renforcée lors de la nouvelle organisation qui est en train de se mettre en place pour le futur programme SESAR 2020.

Les modèles intégrant EATMA sont développés à partir des documents existants et des interviews d'experts opérationnels/techniques ou managers. Pendant la modélisation, un accent particulier est porté sur la vérification des liens parmi les différents éléments de l'architecture afin d'identifier des manques ou des incohérences dans les documents, qui sont alors corrigés.

Le modèle EATMA est stocké sur une base de données accessible à toutes les parties prenantes. Ainsi, le contenu d'EATMA est exploitable informatiquement via la programmation de requêtes[34] permettant de :

- Développer un portail Web[35] offrant des points de vue d'accès à l'information (navigation du contenu, recherche/filtrage information) adaptés aux différents profils utilisateurs (managers, architectes, opérationnels, etc.).
- Générer des rapports personnalisés aux différents profils utilisateurs, et à terme générer automatiquement les livrables SESAR (partiale ou totalement).
- Développer des applications qui réalisent automatiquement des tests de cohérence du contenu EATMA.
- Développer d'éventuelles applications spécifiques à l'aide à la décision et au pilotage du programme.

Dans la figure ci-dessous, nous montrons à titre d'exemple deux éléments EATMA modélisés par deux projets différents : un processus opérationnel modélisé avec la

---

[33] Nota : *SESAR est un programme européen visant à moderniser la gestion du trafic aérien (ATM) à l'horizon 2020 et au-delà.*

[34] Nota : *Dans un langage du type SQL, dans le cas de l'outil MEGA utilisé dans SESAR*

[35] Nota : https://www.atmmasterplan.eu/architecture/

notation BPMN (« Provide Tactical Separation Assurance ») et l'entité d'information aéronautique « ATCClearance » modélisée avec un diagramme de classes UML.

Pour gérer un conflit, le contrôleur peut avoir besoin d'envoyer une clearance à l'avion, ce qui est représenté dans le processus BPMN comme un échange d'information (élément encerclé en bleu). Ce message est une instance de l'entité « ATCClearance » définie dans le diagramme de classes UML d'information aéronautique. Ce sous-ensemble du modèle d'information nous indique quels sont les types de clearance et montre que certains types de clearance sont liés à d'autres entités comme la trajectoire 4D.

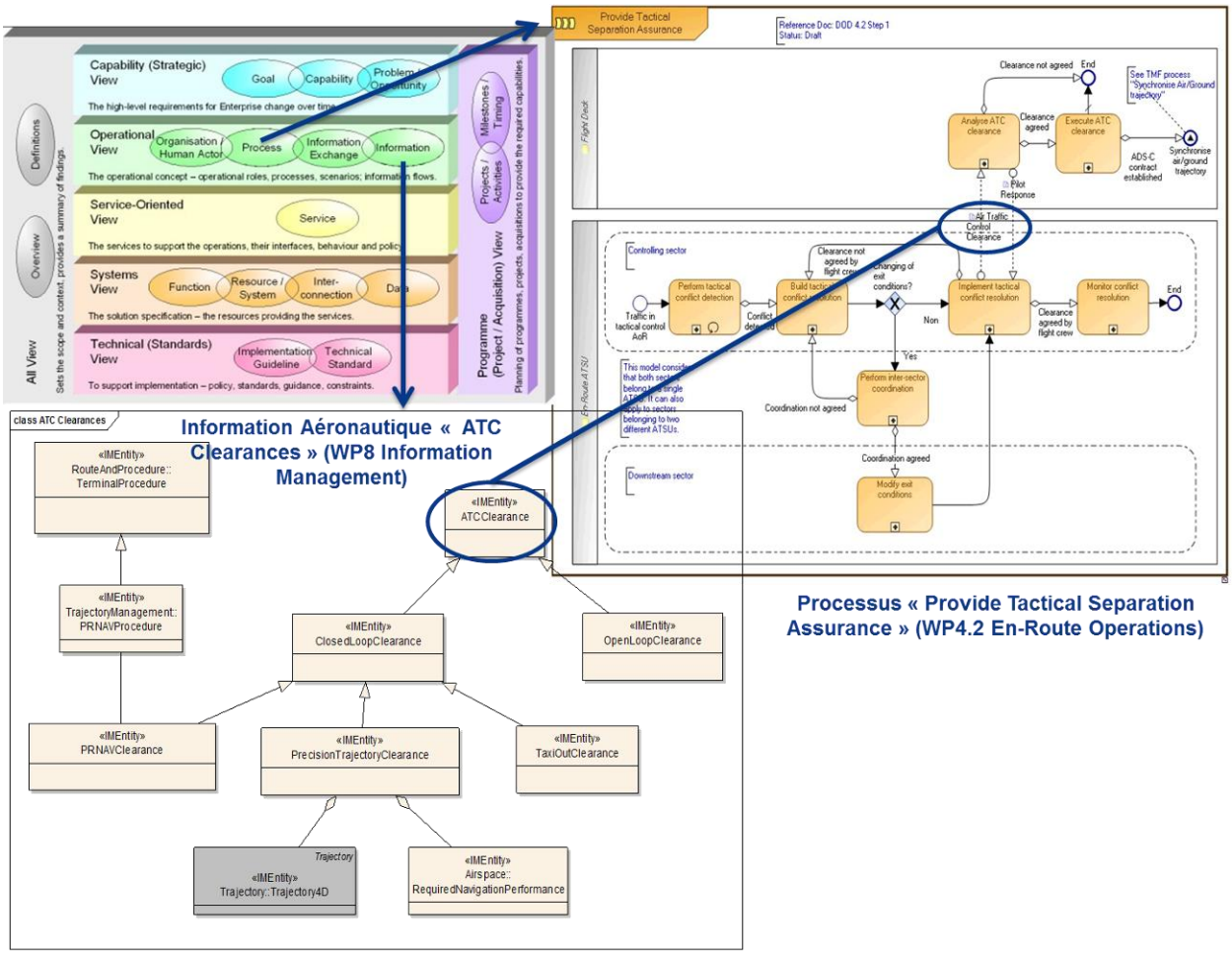


Schéma 4.17 : Exemple d'éléments modélisés dans EATMA

Ainsi, le responsable du processus de séparation tactique de conflits peut faire une requête sur la base EATMA pour voir si l'entité clearance a été déjà créée. Si c'est le cas, il peut s'en servir directement pour créer un nouveau message de type « ATCClearance » et le lien entre le message et son type (entité) fera partie du modèle. Sinon, il vient de découvrir qu'une information est manquante, et il devra se coordonner avec le projet responsable de l'information aéronautique, afin de définir cet élément dans le modèle et mettre à jour le document. La mise à jour du document se ferait

automatiquement, si celui-ci pouvait être généré à partir du modèle, ce qui est à terme le but recherché.

Pour continuer avec l'exemple, les petites boîtes dans le diagramme du processus représentent des activités opérationnelles (ex. « Perform tactical conflict detection »). Ces activités sont des éléments du modèle qui peuvent être liées à des éléments « systèmes » modélisés par d'autres projets dans d'autres vues de l'architecture. Des requêtes peuvent alors servir à déterminer quels systèmes (fonctions logicielles, ressources humaines) sont nécessaires pour supporter une activité opérationnelle telle que « Perform tactical conflict detection ».

Finalement, les éléments stratégiques de la feuille de route de l'ATM[36] (ex. : évolutions opérationnelles, objectifs de performance) font également partie d'EATMA et des liens avec les processus/activités opérationnelles sont modélisés. Avec les bons outils exploitant le modèle, il est possible pour la SJU[37] de suivre l'alignement entre les éléments des vues stratégique, opérationnelle et technique de l'architecture, ce qui facilite la gouvernance du programme.

En définitive, la cohérence et les impacts des changements dans l'architecture et donc son évolution peuvent être plus facilement maîtrisés grâce à des descriptions architecturales basées sur des modèles reposant sur des standards tels que le NAF, à condition d'adapter et d'outiller la démarche proprement.

4.9.4 Statut sur les cadres d'architecture

Il faut signaler que malgré les bénéfices d'une telle approche permettant le partage d'un référentiel commun et offrant la possibilité d'exploiter les éléments architecturaux afin de mieux piloter l'évolution des systèmes représentés :

- Les cadres d'architecture sont fortement orientés vers la maitrise de l'acquisition des systèmes à forte dominance fonctionnelle et informationnelle. Les points de vue physiques (poids, masse, etc), « non-fonctionnels » (sécurité, sureté de fonctionnement, performance), et techniques (software, hardware) sont peu ou pas représentés.
- Bien trop souvent le travail d'architecture se limite à la description. Les pratiques d'évaluation telles que proposées dans la norme ISO-42030 (« Architecture Assessment », en draft actuellement), ou par des méthodes comme ATAM (origine : Software Engineering Institute - SEI), sont faiblement abordées.
- Les méthodes sont encore peu formalisées.
- Les outils supportant les principaux frameworks tels que le NAF/DoDAF/MoDAF sont encore peu nombreux, assez coûteux et peu compatibles.
- En outre, l'adoption des « architecture frameworks » reste complexe car elle exige une forte implication des parties prenantes et un investissement à long-terme. De fait, leur utilisation ailleurs que dans le monde de la défense reste pour

---

[36] Nota : https://www.atmmasterplan.eu/

[37] Nota : *SJU : SESAR Joint Undertaking, organisme européen créé en 2007 destiné à piloter le plan directeur européen pour la gestion du trafic aérien.*

l'instant principalement limitée à des organisations de grande taille (multinationales, institutions gouvernementales/internationales).

4.9.5 Organisation dans le domaine de la défense française

Pour s'engager dans un processus d'amélioration continu, au niveau de la DGA, un Groupe de Travail DGA-Industrie-Académiques œuvre sur :

- Le retour d'expérience de projets pour statuer les avancés, les besoins et les recommandations.
- La recommandation de l'emploi des cadres d'architecture.
- Les recommandations sur l'évolution du NAF.

Note : Un sous-groupe va proposer un chapitre Méthode pour la description et l'évaluation d'architecture pour le prochain NAF V4.0. Ce travail sera mené en lien avec diverses actions :

- ISO JTC1/SC7 « Architecture Guidance Study Group ».
- EDSTAR "System Architecture" Expert Group.
- NATO SCO/IST "Architecture Description and Evaluation".

4.9.6 Perspectives

Aujourd'hui, on assiste à une volonté de convergence des cadres d'architecture. Des groupes de travail ont œuvré pour bâtir des fondations unifiées facilitant l'outillage et l'interopérabilité des frameworks (voir schéma 4.19) :

- IDEAS s'est attaché à définir les bases pour l'échange de description d'architecture : interopérabilité de données.
- MODEM propose une unification de termes et concepts principaux pour la description d'architecture : interopérabilité sémantique « minimum ».

Les versions supérieures à V2.0.3 sont basées sur IDEAS et devraient migrer sur MODEM à court terme.

NAF, à partir de la version 4, sera bâti sur IDEAS et MODEM.

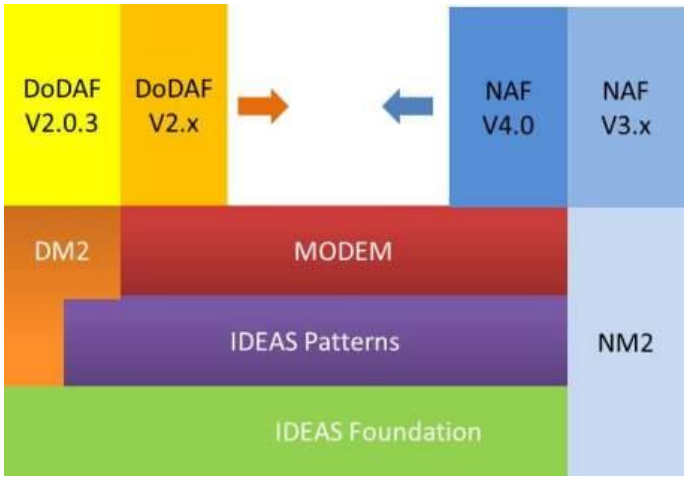


Schéma 4.18 : Nouvelles fondations pour les A.F

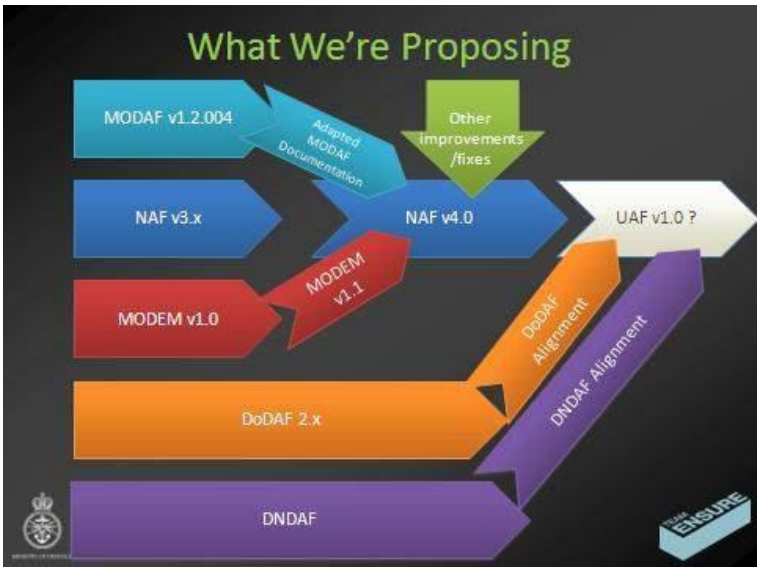


Schéma 4.19 : Convergence des cadres d'architecture (Présentation de Ian Bailey à la conférence OTAN SCO/IST Toulouse, mai 2013)

Depuis cette publication de Ian Bailey (schéma 4.19), le MoD UK a annoncé l'abandon du MoDAF, au profit de NAF V4 . Plus globalement, une convergence des cadres d'architecture est ciblée, à un horizon temporel non défini, vers un cadre d'architecture unifié « UAF ».

Outre le cadre d'application actuel essentiellement limité aux systèmes de systèmes dans des domaines tels que la défense ou l'ATM, il y a des perspectives pour que les cadres d'architecture soient utilisés pour comprendre l'évolution des lignes de produits. En effet, de telles approches peuvent faciliter la description des interactions d'une ligne de produit avec l'environnement et les contributeurs externes. Cette prise en compte élargie des services et des opérabilités peut aider à mieux cerner les aspects stratégiques et les impacts des changements extérieurs sur la ligne de produits.

4.9.7 Recommandations sur les cadres d'architecture

Recommandations :

- **R4.9.1 :** Soutenir les initiatives destinées à stabiliser le contexte normatif (cf. ISO 'Architecting Guidance' Study Group, NATO STO-CSO/IST Study,, …),
- **R4.9.2 :** Promouvoir des initiatives destinées à améliorer l'interopérabilité entre les cadres d'architecture et les autres outils de l'ingénierie des système (en particulier dans l'approche Model-Based System Engineering),
- **R4.9.3 :** Recommander/favoriser le développement de méthodes bien documentées (« modes d'emploi »), pour faciliter l'adoption des cadres d'architecture et guider leur adaptation aux besoins de chaque projet, y compris au-delà du domaine de la défense, car l'utilisation des cadres d'architecture nous semble un bon moyen pour caractériser, et capturer/éliciter les besoins des parties prenantes, pour des systèmes complexes (gestion du trafic aérien, insertion des drones, gestion de flottes, opération d'un système de lancement spatial, …).
- **R4.9.4 :** Assurer la traçabilité/alignement des éléments capturés dans le cadre d'architecture, avec l'architecture technique et les exigences, ainsi que la gestion de leur co-évolution.

4.10 RECOMMANDATIONS GENERALES RELATIVES AUX NORMES

Recommandations :

- **R4.10** : Créer, ou renforcer au niveau du GIFAS et/ou du BNAE, une structure centrale consacrée à l'analyse et à l'évolution des normes, permettant, d'obtenir une base de référence pour la conformité aux standards, normes, et documents normatifs en ingénierie système (ARP4754A/ED79, ISO/EN9100, RG Aero, …), pour application par les industriels français. Les missions de cette structure seraient, entre autres :
  - d'analyser l'impact des nouvelles normes, en ingénierie système (mais aussi au-delà),
  - de s'assurer, par analyse, qu'il n'y a pas de régression des normes,
  - de dé-risquer les pièges normatifs, notamment en provenance des Etats-Unis,
  - d'établir un dictionnaire « inter-normes »,
  - à la manière de nos concurrents non européens, d'être proactifs dans le processus d'évolution des normes / d'implémentation de nouvelles normes, afin de conserver ou d'améliorer notre avantage compétitif.

5. SPECIFICATIONS ET INGENIERIE DES EXIGENCES

Dans ce chapitre on regroupe toutes les activités nécessaires à l'établissement et à la consolidation des spécifications : analyse opérationnelle et fonctionnelle, architecture fonctionnelle et design, capture et ellicitation des exigences. Ce chapitre a pour but de capitaliser les principaux constats, difficultés et bénéfices liés à l'ingénierie des exigences depuis une dizaine d'années, aussi bien du côté des avionneurs que des systémiers et équipementiers. Le retour d'expérience énoncé dans ce chapitre concerne principalement le domaine de l'aviation civile, mais les recommandations ont fait l'objet d'un consensus avec les autres domaines concernés (militaire, spatial).

5.1 CONTEXTE DE L'INTRODUCTION DE L'INGENIERIE DES EXIGENCES

5.1.1 Ingénierie des exigences dans le domaine spatial. Bref rappel historique

Historiquement, l'introduction de spécification par exigence s'est faite dans le spatial pour la spécification de grands programmes (exemple : Hermès). Cette démarche a été structurée et renforcée en particulier au travers des normes ECSS, et en particulier de la norme ECSS-E-ST-10-06C « Space engineering – Technical requirements specification ». Depuis, l'ESA a imposé l'usage de DOORS sur le programme ATV, et les programmes ultérieurs.

A l'initiative d'ASTRIUM, l'ingénierie des exigences s'est imposée sur tous les programmes dont cette société avait la charge. Côté lanceurs, un mode très structuré de gestion des exigences a été mis en place par Airbus DS, puis maintenant par Airbus Safran Launchers, sur le programme Ariane 5 ME (Midlife Evolution, programme aujourd'hui arrêté), et maintenant sur le programme Ariane 6. Sur les programmes de satellites, Airbus DS déploie aussi une ingénierie des exigences très structurée.

5.1.2 Ingénierie des exigences pour les applications militaires en France: un bref historique

Dans le domaine militaire, la complexité des systèmes considérés, en particulier pour la gestion des variantes, a conduit avant l'apparition de standards contraignants, à mettre en place une approche de spécification par les exigences (exemple : Mirage 2000).

L'introduction et la généralisation de l'ingénierie des exigences en France, dans le domaine de la défense, pourrait se décrire en 3 étapes : naissance et premières instances méthodologiques dans les années 80, puis premières instances concrètes et premiers outillages dans les années 90, avant une généralisation au début des années 2000.

5.1.2.1 Naissance et introduction dans les années 80

Les contrats français avec l'Administration utilisaient généralement au début des années 80 le terme "caractéristiques". Les spécifications comportaient alors un chapitre regroupant les caractéristiques techniques et de performances, que les maîtrises d'œuvre industrielles s'engageaient à tenir, de façon contractuelle.

Certaines de ces caractéristiques faisaient d'ailleurs l'objet de marges de tolérances, pour définir ce qui était acceptable.

Par exemple, le cours de monsieur J. Villepelet (Directeur Technique de Thomson-CSF, Division Systèmes), à l'ENSTA, Ecole Nationale Supérieure des Techniques Avancées, sur la méthodologie des systèmes sol-air, daté de 1981, détaille bien une démarche d'ingénierie des systèmes (qui ne porte pas encore ce nom) : il y est question de caractéristiques de performances, pas encore formulées comme des exigences (ce terme n'était pas utilisé).

Vers 1988-1989 sont apparues les matrices de vérification avec leur méthode associée (IADT[38]). Les exigences ne sont pas encore identifiées individuellement et la matrice IADT renvoie par exemple à des paragraphes.

5.1.2.2 **Premières instances concrètes dans les années 90**

1994 est l'année du lancement du NCOSE[39], qui est resté national pendant 4 ans avant de devenir international. C'est sous cette influence américaine, soutenue par l'apparition d'outils de gestion des exigences, que petit à petit cette ingénierie des exigences s'est imposée.

Ce terme d'exigence résulte de la traduction de "requirement", il recouvre ce qu'on appelait caractéristiques techniques et de performances, mais aussi parfois d'autres contraintes programmatiques ou de réalisation.

Par exemple, c'est en 1994 que le premier volet de MIST, la méthode d'ingénierie des systèmes de Thomson-CSF, est publié. Il ne couvre alors que la partie "descendante" du V. Le complément arrive en 1997; il comporte d'ailleurs une fiche sur la qualité d'une exigence (dérivée d'une publication NCOSE).

5.1.2.3 **Premiers outillages et généralisation au début des années 2000**

Il a fallu attendre la fin des années 1990 pour voir des contrats avec l'Administration intégrant des exigences, identifiées et numérotées.

Les outils et leur usage se généralisent également : RDD 100, par exemple, est présent dans le paysage quasi-quotidien dès 97 sur certains contrats. Les premiers tests concrets de DOORS remontent également à 97, et son déploiement explicite avec la DGA est avéré dès 99.

---

[38] Nota : IADT : Inspection, Analyse, Démonstration, Test.

[39] NCOSE: National Council of Systems Engineering

5.1.3 Dans l'aéronautique civile

Afin d'assurer une maîtrise des aspects sûreté, un certain nombre de normes et de recommandations applicables aux processus de développement ont été établis au cours des 20 dernières années pour le développement des aéronefs, les principales évolutions ont été les suivantes :

- A partir de 1992, la norme DO-178B pour les logiciels embarqués a introduit les notions de :
  - Traçabilité des éléments de spécifications entre niveaux système et logiciel
  - Vérification des exigences de haut et bas niveaux
  - Exigence dérivée
  - Activités d'assurance en développement graduées en fonction de la criticité du logiciel
- En 1996, l'ARP 4754, intitulée « Considérations sur la certification des systèmes de bord (pour le civil) à haute intégration ou complexes » a repris les concepts de la DO-178 en les étendant aux systèmes embarqués et à l'avion lui-même en insistant particulièrement sur les notions de :
  - Recueil et formalisation des exigences
  - Validation des exigences et des hypothèses spécifiques pour assurer que les exigences spécifiées soient suffisamment précises et complètes
  - Limitation du risque de présence de fonctions indésirables dans le système par la traçabilité des exigences depuis les fonctions attendues de l'avion jusqu'à leur implémentation dans du matériel ou du logiciel.
- Simultanément, la norme EN 9100 a décrit le système d'assurance qualité dans l'aéronautique et le spatial afin de garantir la satisfaction du client par :
  - La validation des exigences et du produit final par les parties prenantes
  - L'Identification des caractéristiques clés
  - La mise en place d'un système de revues formelles et d'un système de surveillance

La prise en compte de ces nouveaux besoins pour la certification des systèmes complexes et la maîtrise des développements a conduit les entreprises du domaine à définir des processus de développement fondés sur l'ingénierie et la gestion des exigences.

La sensibilisation s'est faite à l'occasion de programmes nouveaux (exemple : A340-500/600, A380, A400M ou A350) ou lors de modifications substantielles de produits existants (exemple : A320 neo). L'expérience de plus d'une décennie dans l'application de l'Ingénierie des exigences a mis en évidence de nouvelles activités à réaliser, dans le cadre d'un développement d'un aéronef, par l'ensemble des entités participants au développement, depuis l'avionneur jusqu'aux équipementiers en charge du développement du logiciel et du matériel.

Le processus de développement d'un produit complexe tel qu'un avion, vu dans un cadre ARP4754 peut être représenté de façon simplifiée par une succession de niveaux de développement pour lesquels des activités d'ingénierie des exigences similaires s'appliquent.

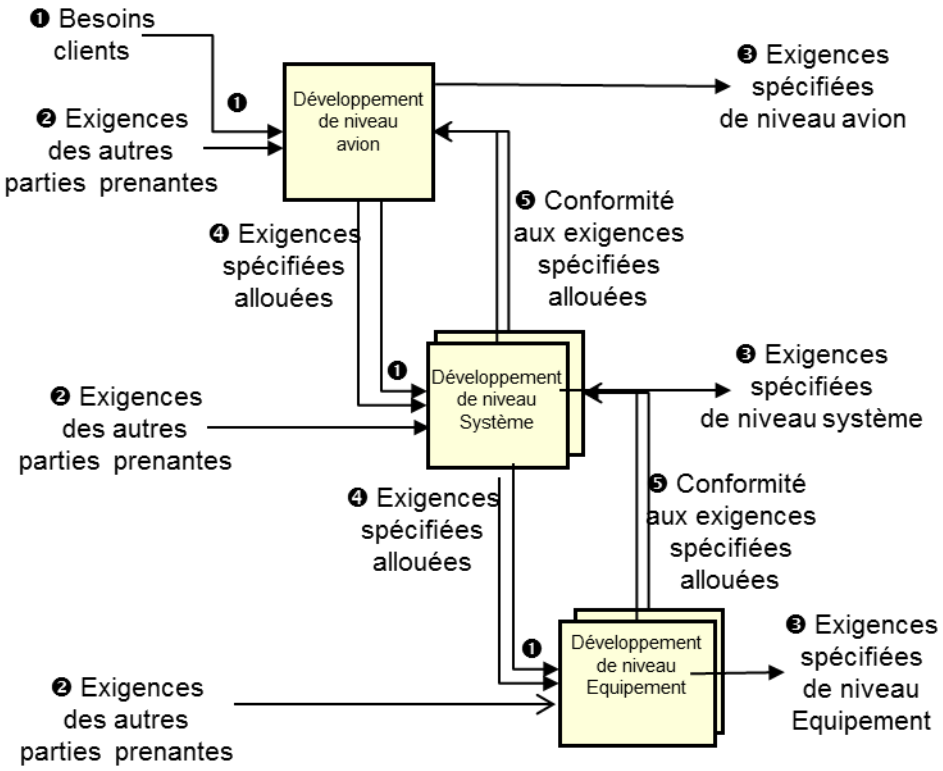


Schéma 5.1 : succession de niveaux de développement (dans un cadre ARP4754)[40]

A chaque niveau de conception, le processus doit considérer en entrée:

❶ Les exigences allouées par le niveau supérieur
❷ Les exigences des autres parties prenantes qui peuvent contraindre le produit à concevoir.

Chaque niveau de conception produit:

❸ Un ensemble d'exigences spécifiant le produit du niveau considéré
❹ Plusieurs ensembles d'exigences spécifiant la contribution attendue du produit de niveau inférieur
❺ Une justification de la conformité de la conception aux exigences allouées par le niveau supérieur

On notera que certaines exigences n'ont pas de lien de traçabilité avec le niveau au-dessus. En règle générale, ces exigences dérivées viennent de règles de l'art ou bien

[40] Nota : *La notion de système employée dans le schéma 5.1 diffère un peu de celle généralement employée jusqu'ici. Du point de vue de l'avion, on appelle système tout sous-système majeur, de niveau immédiatement inférieur au niveau avion proprement dit.*

de choix de conception et/ou d'architecture. De ce fait, elles n'ont pas nécessairement de lien de traçabilité avec le niveau du dessus.

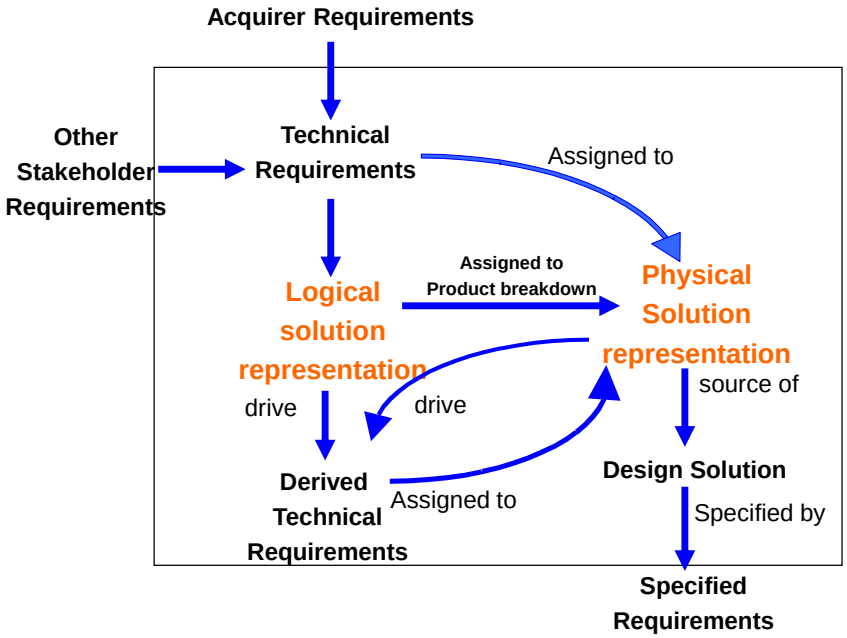


Schéma 5.2 : Requirement Flowdown (dans un cadre EIA632)

5.2 ANALYSES OPERATIONNELLE ET FONCTIONNELLE

L'Analyse Opérationnelle et l'Analyse Fonctionnelle procèdent d'une même démarche permettant de capter les besoins opérationnels et d'en dériver une décomposition fonctionnelle jusqu'à son allocation sur une architecture système.

Dans ce qui suit « système » désignera ce sur quoi porte l'analyse. C'est aussi bien un aéronef, une plateforme, qu'un sous-système ou un système au sens aéronautique des ATA 2 digit, ou un équipement.

5.2.1 La démarche

Quoique fondamentalement itérative comme toute activité de design, il est possible de mettre en avant une séquence logique en 3 phases :

- **Contexte opérationnel**

Identifier les limites (services rendus, interfaces…) du système étudié,

Caractériser son environnement opérationnel,

Définir des paramètres clés pour son analyse.

- **Analyse Opérationnelle[41]**

  Typiquement, en passant en revue le cycle de vie complet du système, identifier et caractériser les Cas d'Utilisation (Use Cases) importants. Il s'agit d'identifier les principaux services attendus et leurs interactions avec l'environnement opérationnel.

  Définir des Scénarios opérationnels qui affinent ces Cas d'Utilisation en précisant la séquence des interactions entre le système et les différents constituants de son environnement.

- **Analyse Fonctionnelle**

  En écho aux opérations et scénarios, identifier les Fonctions et les raffiner (i.e. les décomposer).

  Décrire les Flots ou les Flux (Flows) entre les (sous-)Fonctions. Ces flots couvrent les données échangées bien évidemment mais pas seulement (ex : alimentation électrique, phénomène physique…)

  Si besoin est, compléter par une description comportementale de l'enchainement et/ou de la mise en parallèle des (sous-)Fonctions.

  Itérer la décomposition fonctionnelle jusqu'à pouvoir la mettre en regard d'une Architecture système.

  Allouer les (sous-)Fonctions aux composants du système.

  Il est important de garder en tête que ce processus est en interaction permanente avec les autres contingences du développement (réutilisation - « reuse », faisabilité, contraintes de Sûreté de Fonctionnement et de certification…).

  Différents formalismes sont capables de supporter cette analyse. De nos jours, des outils matures existent et facilitent le travail.

  L'intérêt des outils est à signaler car ils permettent d'assurer la cohérence de la définition (en fait du modèle). Pour certains, il est possible d'instrumenter le modèle et de le simuler dynamiquement. Les Scénarios fournissent alors de bons Cas de Tests (Test Cases) à cette activité de validation. Un cas intéressant est celui de l'instrumentation de modes de défaillance et de la réalisation d'Analyse Dysfonctionnelle.

  Tout ceci participe alors du MBSE (Model-Based System Engineering)[42].

  Il est habituellement question de DMU fonctionnelle lorsque les outils sont capables de coupler ce type de modélisation avec de la modélisation physique 3D.

---

[41] Nota : *On notera bien qu'Analyse Opérationnelle et Analyse Fonctionnelle, même si elles procèdent d'une même démarche et sont en continuités sont séparées, et souvent conduites avec des acteurs différents.*

[42] Nota : *Le MBSE et la démarche associée est décrite dans le chapitre 10, consacré aux approches futures.*

5.2.2 L'analyse fonctionnelle dans le processus de gestion des exigences

Les exigences et le design fonctionnel sont intimement liés tout au long de la démarche.

- Dans les étapes amont, l'analyse des besoins opérationnels va permettre de capturer les exigences opérationnelles.

- La décomposition fonctionnelle va, quant à elle, répondre aux besoins opérationnels (performances de haut niveau, Dispatch opérationnel…) et conduire la manière de cascader les exigences.

- Les exigences de Sûreté vont contraindre cette même décomposition fonctionnelle de façon à ce qu'elle se projette sur des concepts d'architecture physique viables, avec des performances atteignables pour chacun des systèmes envisagés.

Point important : on associe les exigences fonctionnelles aux fonctions et de-là aux composants qui les hébergent. Ce faisant les fonctions sont en quelque sorte les « contenants » des exigences fonctionnelles qui permettent de structurer les spécifications. On notera que certaines exigences ne peuvent être rattachées qu'aux produits, par exemple la masse d'un calculateur.

Dès lors qu'on a affaire à un système complexe, il nous semble largement préférable de s'appuyer sur une analyse fonctionnelle, pour structurer les exigences (voir recommandation R5.2.2.1). Ce point de vue est partagé par plusieurs standards (ISO 15288, ARP 4754, ECSS,…).

- Constat : Une analyse fonctionnelle n'est **pas systématiquement réalisée** formellement en amont du travail d'élaboration des spécifications. Lorsque celle-ci est réalisée, le travail itératif de définition des exigences peut commencer jusqu'à l'atteinte de la maturité fonctionnelle.

- Constat : Dans les cas où le contenu et les attendus de l'analyse fonctionnelle sont **insuffisamment partagés** entre le client (par exemple : avionneur) et le fournisseur (par exemple : systémier, ou sous-systémier), cela peut entrainer des itérations dans des phases où la définition devrait être gelée.

- Constat : La recopie d'exigences d'un programme précédent, lorsqu'elle se fait sans référence aux fonctions nécessite un travail de retro-engineering ultérieur.

- Constat : Parfois, la progression de la maturité des fonctions, dans la cascade de la chaîne de valeur, est insuffisamment jalonnée (par des revues ou des « Maturity Gates », par exemple). On peut alors rater des opportunités d'optimisation du design (par « sur spécification »), ou bien prendre des risques d'évolution tardive de certaines exigences, conduisant à des modifications majeures et non anticipées du design.

- Constat : En cas de **modification** postérieure à la RDP/PDR (Revue de Définition Préliminaire / Preliminary Design Review), l'analyse fonctionnelle, lorsqu'elle existe, n'est pas toujours mise à jour. L'analyse d'impact « haut niveau » n'est ainsi pas réalisée. A fortiori, lorsque cette analyse fonctionnelle n'existe pas, l'architecture n'est ainsi pas robuste aux changements.

Recommandations :

➔ **R5.2.2.1 Systématiser l'analyse fonctionnelle**, analyse qui doit être agréée entre le plateformiste / donneur d'ordre (e.g.: l'avionneur) et le fournisseur/sous-systémier (« systémier », en langage d'avionneur), si possible **coréalisée** en phase plateau (proposition ou PDR au plus tard). Cette analyse fonctionnelle, et les impacts dus aux modifications postérieures à la RDP/PDR devront être mis à jour autant que nécessaire, jusqu'à la fin du développement, voire même tout au long du cycle de vie du système.)

➔ **R5.2.2.2** Lier les **exigences** soit aux fonctions, soit aux interfaces qu'elles s'échangent, les **prioriser** en conséquence.

5.3 INGENIERIE DES EXIGENCES

5.3.1 Activités d'ingénierie des exigences

5.3.1.1 Gestion des exigences

L'ingénierie des exigences peut requérir de nombreuses activités en fonction du niveau de rigueur de développement souhaité (DAL). Celles-ci peuvent se révéler très coûteuses en termes de documentation:

- Définition des exigences,
- Validation des exigences,
- Allocation et dérivation des exigences sur une architecture,
- Vérification de la définition du produit en regard des exigences,
- Vérification du produit lui-même en regard des exigences (tests),
- Gestion des non-conformités de la définition au regard des exigences (« design compliance », en anglais),
- Gestion différenciée des exigences en fonction de leur nature : Fonctionnelles ou non fonctionnelles, de type produit ou non-produit (organisationnelles, processus, ou projet),
- Gestion des exigences des systèmes contributeurs (« enabling systems »), par exemple :
    - Peinture porte-avions, vs tenue des pneus à l'appontage (exemple sur un système non soumis à la certification et à l'ARP 4754),
    - système de transport A380.
- Gestion de configuration des exigences et de leur évolution,
- Gestion des échanges de données d'exigences (y compris données de justification, de validation et de vérification), avec les fournisseurs,
- Analyse d'impact dans un référentiel d'exigences,
- Gestion de la qualité des exigences.

5.3.1.2 Exigences : quantité, type

L'ED79/ARP4754 identifie la nécessité de considérer des exigences de types variés (>10, voir en annexe B les types d'exigences, selon l'ARP4754A) à chaque niveau de développement (aéronef, système, item).

De plus, il a souvent été jugé nécessaire de capturer les exigences relatives aux aspects industriels ou économiques, qui n'ont pas d'impacts sur les exigences de sécurité ou de certification.

- Constat : On constate une inflation du nombre d'exigences à gérer, dans le développement d'un aéronef ou d'un système.

- Exemples :

  - Avion A350 : plusieurs centaines de milliers d'exigences gérées par Airbus (depuis le niveau avion jusqu'au niveau de spécification vers des fournisseurs)
  - EC175 : Avionique HELIONIX : plusieurs dizaines de milliers d'exigences.
  - Système de prélèvement d'air développé en 2003 -> 1600 exigences, système équivalent développé en 2013 -> 2600 exigences.
  - Système porte (Latécoère) (fonctionnalités équivalentes) : 800 exigences (techno 2000), 1200 (techno 2012)
  - Système d'air complet : 16 000 exigences
  - Spécification suite Avionique ATR > 6000 exigences
  - Spécification du besoin FMS A400M > 10000 exigences
  - Pour un avion militaire, non soumis à l'ARP4754 (ex : Rafale), le nombre d'exigences est supérieur à celui d'un avion commercial (300 000)
  - Il n'y a pas consensus sur la façon de structurer les exigences, de les structurer en niveau, et sur la part de liberté laissée au fournisseur.

- On peut identifier un certain nombre de causes à l'origine de cette inflation :

  - Le nombre des parties prenantes (« stakeholders »)[43],
  - La granularité de plus en plus fine des spécifications portant sur les sous-systèmes à développer,
  - La terminologie utilisée par chaque spécialité (qui cache parfois, sous des mots différents, des similitudes),
  - Le nombre de sous-systèmes pour un niveau d'architecture donné et le nombre de niveaux d'ingénierie (liés à la complexité et/ou à l'organisation) qui multiplient la gestion des interfaces
    – note : L'ampleur réelle de l'expansion du nombre d'exigences entre niveaux d'ingénierie n'a pas fait l'objet d'études approfondies.

---

[43] Nota : *On constate par exemple une tendance à mieux refléter les besoins de SLI (Support Logistique Intégré), et de MCO, dans les exigences. C'est également le cas pour les exigences de SSI (Sécurité du (des) Système(s) et de l'Information).*

- Sur-spécification :
    - Mélange d'exigences de spécification et d'exigences de définition (solution technique). Ces dernières exigences étant sans lien avec le besoin fonctionnel ou opérationnel,
    - Absence de partage des Use Cases fonctionnels et opérationnels dimensionnant,
    - Surdimensionnement des exigences pouvant amener la solution en limite de faisabilité,
    - Exigences sans lien avec le besoin fonctionnel ou opérationnel,
    - Mélange des exigences « produit » et des exigences de type « processus/projet »,
    - Répétition d'exigences, d'un niveau à l'autre.

- Y-a-t-il trop d'exigences ? C'est parfois une critique formulée, en particulier par le management. La vraie question n'est pas celle du nombre d'exigences générées, mais plutôt celle de la capacité des parties prenantes à gérer efficacement ces exigences.

- Constat : les activités de Validation et de Vérification à conduire en face des exigences de Produit, de Processus ou de Projet, n'ont pas été suffisamment différentiées, conduisant à une charge de V&V jugée improductive.

- Constat : Difficulté à prioriser et jalonner les exigences conduisant à une absence de lissage de la charge de travail sur la spécification des exigences et le V&V associé.

- Constat : Lorsque, sur certains programmes, la traçabilité n'a pas été assurée dans le processus d'allocation, il a parfois été nécessaire de conduire des activités de traçabilité ou de documentation des exigences a posteriori du développement.

- Constat : Difficulté du travail de synthèse des exigences à réaliser, à partir des exigences exprimées par l'ensemble des parties-prenantes

- Constat : Le réalisateur (logiciel et matériel) comprend de moins en moins la finalité de ce qu'il lui est demandé de réaliser.

- Constat : Certain donneurs d'ordre (exemple : Boeing) demandent aux fournisseurs de justifier la moindre exigence de performance ou de dimensionnement et de la raffiner aux niveaux exigences système /équipement.

- Constat : On manque de temps et de moyens pour challenger les exigences. De plus, dans les pratiques actuelles, lors d'un processus d'appel d'offre, le fournisseur potentiel ne se considère généralement pas en situation de challenger les exigences émises par le client. Il nous semble donc utile de souligner l'intérêt de déployer une démarche d'ingénierie des systèmes globale, visant à optimiser globalement les performances et les coûts, en incluant les achats et les processus de négociation contractuelle. A titre d'exemple, dans le cadre de la préparation d'une revue amont (SRR ou SysRR, PDR), on pourrait demander au fournisseur choisi (à l'issue du processus d'appel d'offre) de challenger les exigences que le donneur d'ordre vise à rendre applicables.

Recommandations :

➔ **R5.3.1.1** Promouvoir à tous les niveaux un processus visant à challenger les exigences, dans une perspective **d'optimisation globale** des systèmes, sur l'ensemble de leur chaîne de valeur.

➔ **R5.3.1.2 Généraliser le principe d'une revue d'exigences de type SRR**, au cours de laquelle on pourra acter, entre le client et le fournisseur, les éventuelles solutions alternatives proposées par le fournisseur, en lieu et place des exigences initialement demandées. On notera qu'une telle approche exige d'être innovant sur le plan contractuel.

➔ **R5.3.1.3** Identifier (« taguer ») les exigences qui n'ont pas d'impacts sur les exigences de sécurité ou de certification et dont la gestion doit se faire hors référence ARP4754 car elles ne nécessitent pas le même niveau de documentation. Exemples :

- ➔ Gérer les exigences « spécifiques » du produit selon l'arbre de décomposition produit (PBS)
- ➔ Gérer les exigences Processus & Projet selon le WBS

➔ **R 5.3.1.4** Rechercher le meilleur compromis entre les exigences exprimées en langage naturel, et celles faisant appel à d'autres moyens de spécification (modèles par exemple). Dans ce dernier cas, ne le faire que lorsque leur formalisme a été formellement établi auparavant et est non-ambigu.

➔ **R5.3.1.5 Limiter et justifier les exigences décrivant des solutions plutôt que le besoin**.

➔ **R5.3.1.6** Assurer la bonne qualité rédactionnelle (syntaxique et sémantique) des exigences. Au besoin la contrôler a posteriori (par diffusion de bonnes pratiques, relectures ou utilisation d'outils.)

➔ **R5.3.1.7** Renforcer les moyens (méthode, formation, outil,…) supportant l'activité de synthèse des exigences[44] des parties prenantes pour couvrir les duplications et réduire les risques de contradictions.

➔ **R5.3.1.8** Agréer une **enveloppe/** plage de performance, plutôt qu'une valeur déterminée (notion de **flexibilité**).

➔ **R5.3.1.9** Promouvoir la recherche d'opportunités, et valoriser les gains de performance, par rapport aux valeurs cibles, sous forme de primes (incentives).

➔ **R5.3.1.10** Proposer des sujets de recherche permettant de comprendre/ modéliser la mécanique d'inflation des exigences en fonction de la complexité et définir les critères permettant d'identifier le nombre optimum de niveau d'ingénierie requis pour maîtriser la complexité.

---

[44] Nota : *L'activité de synthèse des exigences regroupe la qualité de leur rédaction, leur validation, leur montée en maturité, leur mise en cohérence, la suppression des doublons et des contradictions, l'analyse de leur capacité à être vérifiée, …*

5.3.1.3 **Qualité des exigences.**

Evaluer la qualité correspond à analyser les critères suivants :

- ***Exactitude*** *(« Correctness»): mon exigence est-elle correcte ?*
  Le libelle de l'exigence est-il compréhensible par les parties prenantes ?
  - Courte
  - Simple
  - Non ambigüe
  - La terminologie est comprise/agréée par les parties prenantes

  Cette analyse est à mener sur chaque exigence et peut être assistée par un outil d'« authoring », permettant d'écrire des exigences de bonne qualité du premier coup.

- **Cohérence** (« Consistency ») : les exigences sont-elles cohérentes ?

  Pas de conflits entre exigences :
  - De configuration/version (mauvaise version prise en entrée)
  - Absence d'exigences redondantes ou contraires
  - Absences de conflits de valeurs numériques (valeurs, unités, dimensionnement).

  Cette analyse est à mener sur un ensemble d'exigences, et doit être évaluée dans une cascade complète.

- **Complétude (« Completeness»):** La complétude est la capacité d'un ensemble d'exigences à satisfaire les intérêts des clients, utilisateurs, … dans tous les modes opératoires et phases du cycle de vie pour l'environnement opérationnel défini.

  Cette analyse est à mener sur un ensemble d'exigences et doit être évaluée dans une cascade complète.

Gérer la qualité des exigences peut se faire de deux manières non concurrentes :

A. Sur l'ensemble des exigences : Analyser la qualité après écriture (« Quality Analysis »)
B. A la volée : Assister le rédacteur pour écrire du premier coup une bonne exigence (« Requirement Authoring »)

Le Cas d'Utilisation/Use Case ci-dessous formalise la manière de gérer une analyse Qualité sur un ensemble d'exigences :

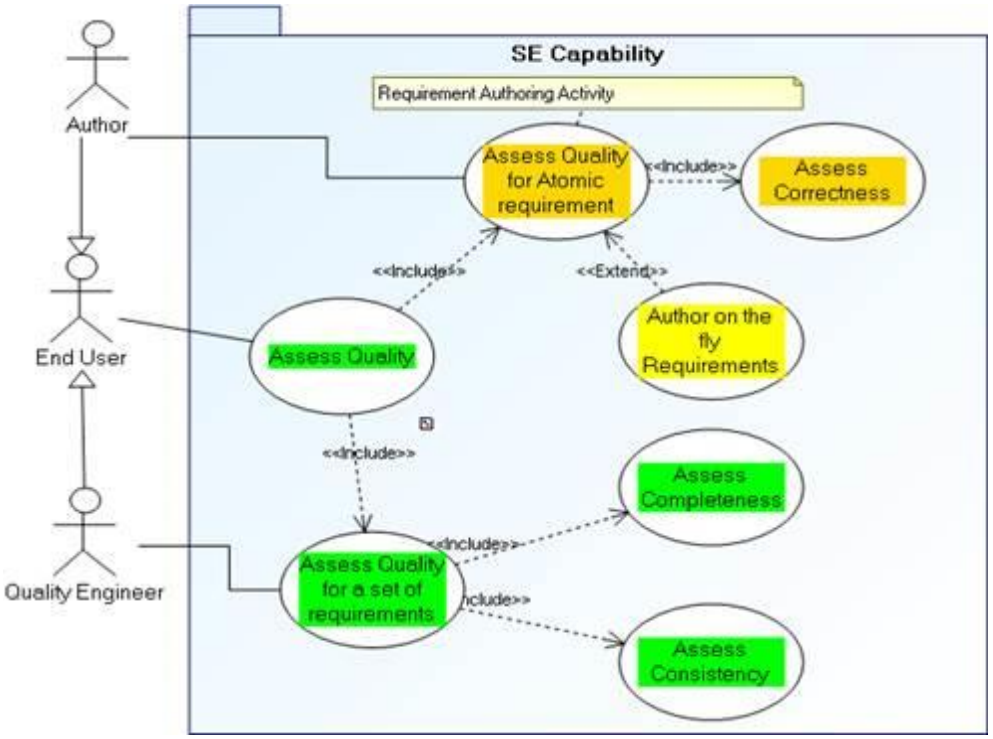


Schéma 5.3 : Analyse Qualité sur un ensemble d'exigences

5.3.1.4 Mise en œuvre d'une approche qualité basée sur les ontologies

Afin de répondre aux critères de qualité définis ci-dessus, il est possible de mettre en oeuvre des ontologies.

La définition d'une **ontologie**[45] repose sur le fait de partager une terminologie, définir des concepts des règles sémantiques et syntaxiques

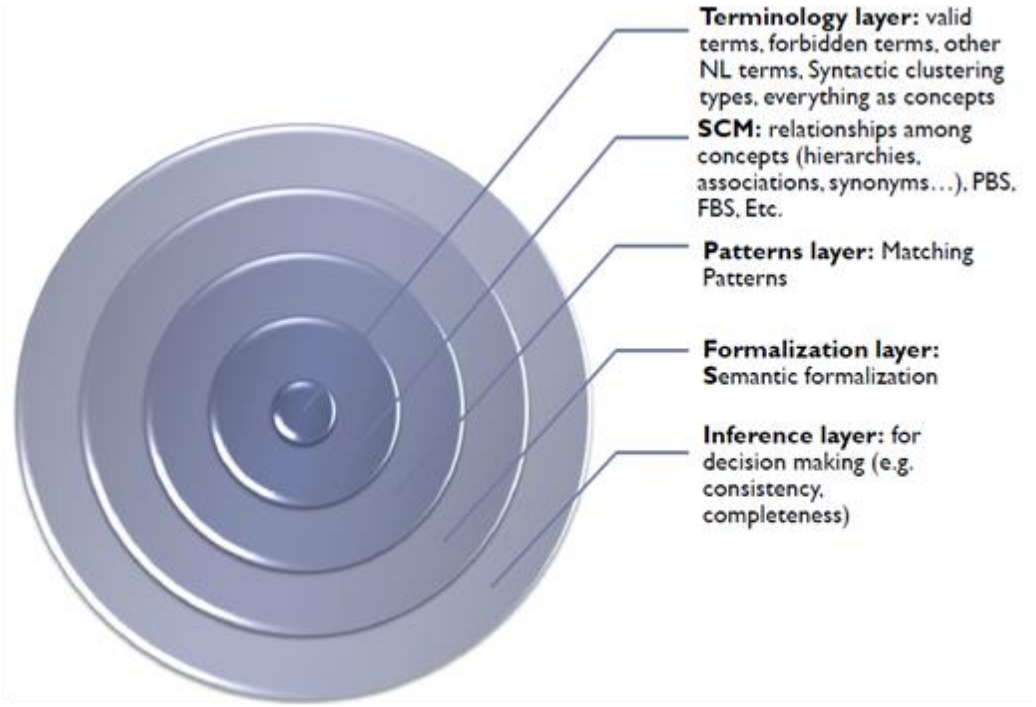
Une ontologie correspond à la spécification des concepts ("specification of a conceptualization" selon GRUB 95).

L'utilisation d'une ontologie permet d'exprimer de manière explicite la connaissance implicite au sein d'une entreprise ou d'une communauté pour un domaine donné.

---

[45] Nota: *Ontologie : Au sens premier il s'agit du domaine philosophique qui se concentre sur l'étude de l'être. En ingénierie des systèmes, ou en informatique, une ontologie est une représentation partagée et consensuelle, sur un domaine donné. Le but est de définir un ensemble de connaissances, sur ce domaine, et d'expliciter le vocabulaire définissant les termes nécessaires à la connaissance liée à ce domaine.*

Une ontologie est définie selon les couches suivantes :



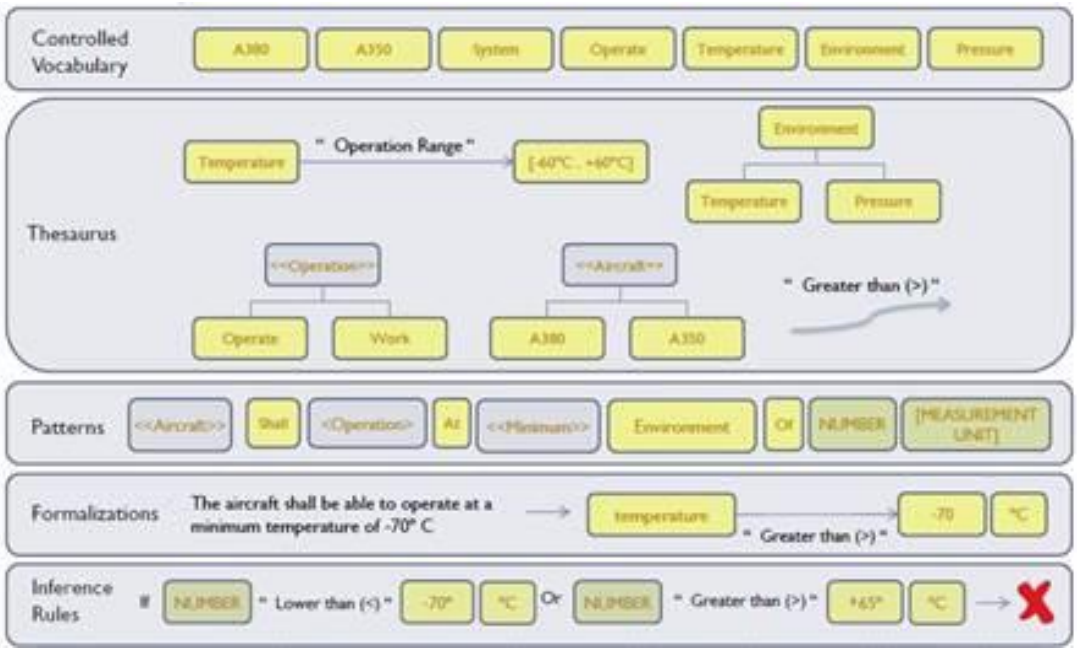


Schéma 5.5 : Constitution d'une ontologie

5.3.1.5 Activités nécessaires à la définition des ontologies en contexte industriel

1. Gérer l'ontologie de manière incrémentale et pour chaque domaine,
2. Commencer par l'analyse individuelle avec des règles simples et enrichir les règles progressivement,
3. Définir une terminologie de manière itérative,
4. Dès que la base de terminologie est complète, définir les règles liés à la terminologie
5. Définir un thesaurus (modèle entre les concepts et la terminologie associée) agréé par les parties prenantes,
6. Définir les règles liées au domaine (exemple : Take Off operations est reliée à une vitesse, une condition de piste, …).
7. Définir des patterns (liant les différents concepts)) en commençant par les classes d'exigences obligatoires (« mandatory ») → Point de départ pour les activités d'assistance à l'écriture.

Références:

GRUB 95 Gruber, Thomas. "Toward Principles for the Design of Ontologies Used for Knowledge Sharing", International Journal Human-Computer Studies Vol. 43, Issues 5-6, November 1995, p.907-928.

ISO/IEC TR 24766-- Systems and software engineering -- Guide for requirements engineering tool capabilities

5.3.2 DAL et exigences

Selon l'ARP4754/ED79, le niveau de rigueur du processus de développement est donné par le niveau d'assurance de développement.

- Le niveau de rigueur de processus de développement des fonctions est donné par le niveau d'assurance de développement de ces fonctions appelé FDAL.
- Les objectifs à suivre pour le développement des items en fonction de l'IDAL sont décrits dans les DO-254 / ED-80 et DO-178 / ED-12.
- Les objectifs pour l'intégration des items logiciel et matériel sont du ressort de l'ARP4754A / ED79A.
- Constat : Les notions de FDAL (Functional Design Assurance Level) et de IDAL (Item Design Assurance Level) sont insuffisamment partagés.
- Constat : Difficulté d'interpréter et appliquer le **juste niveau de rigueur** des processus et méthodes de développement associées à des niveaux de DAL (Design Assurance Level).

.

Recommandations :

➔ **R5.3.2.1** Définir une réponse méthodologique graduée en fonction du risque permettant d'alléger ou de renforcer les processus d'Ingénierie des exigences et de V&V de façon cohérente pour le développement d'un produit complexe.

5.3.3 Le jalonnement du processus de validation des exigences, dans une démarche de développement incrémentale

Dans un monde idéal, on pourrait s'attendre à disposer d'un jeu d'exigences complet et validé, avant de définir la solution. Dans la réalité, les processus de spécification et de définition s'effectuent de manière concourante, ce qui nécessite de conduire une démarche rigoureuse de validation et d'analyse de la maturité des exigences (dont les analyses d'impact en cas d'évolution.)

- Constat : Appliqué **trop tard**, le processus de validation engendre des risques de re-conception ou ré-industrialisation, voire de non certification.

  Par manque de ressources, ou afin de répondre aux jalons contractuels, les activités de traçabilité et de validation des exigences ne sont parfois pas totalement réalisées juste après les activités de capture / écriture des exigences. Ceci peut en particulier être fait pour privilégier le respect des contraintes de process assurance et de certification, au détriment de la maturité technique. Dans ces cas, la validation complète des exigences n'intervient que tardivement, ce qui engendre des risques de reprises de conception.

- Constat : Appliqué **trop tôt,** ce processus est source d'inefficacité, car on itère (en conception, justification, vérification) autour d'exigences non figées, tout en déroulant un processus coûteux. *Une des résultantes classiques est la multiplicité des batchs de logiciels qui sont développés, validés, vérifiés, pour répondre à des besoins fonctionnels mouvants.*

Recommandations :

➔ **R5.3.3.1:** *Formaliser, dans les **processus de développement** des entreprises et les formations d'ingénierie des systèmes, ce principe de **développement incrémental, en s'appuyant sur une analyse fonctionnelle partagée entre les différents intervenants.***

➔ **R5.3.3.2:** *Associer à chaque exigence **un critère de maturité** permettant d'évaluer un risque d'instabilité.*

5.3.4 Les relations client / fournisseurs

5.3.4.1 **Vision partagée du développement**

- Constat : de nombreuses divergences de points de vue entre donneur d'ordre et fournisseur peuvent apparaître au cours du développement, notamment en termes d'attendus par rapport à l'ARP4754. Chacun ayant sa propre interprétation du document. *Les contrats sont souvent signés assez tôt. De ce fait, il est normal que certains attendus sur le processus n'aient pas été identifiés explicitement dès la signature du contrat.*

- Exemples :

  - Quels efforts de traçabilité entre spécifications, documents de validation, de vérification ?

  - Quelles spécifications doivent faire l'objet de revues de validation approfondie au sens ARP ?

  - Quels sont les documents fournis aux autorités de certification ?

  - Quels sont les % de validation / vérification requis à tel jalon ?

  - Comment doivent être gérées les déviations ?

  - Comment seront gérées les demandes et acceptations de modifications ?

  - Comment doivent être déclinées les exigences d'indépendance ?...

Recommandations :
➔ **R5.3.4.1:** Concevoir et mettre en place des **formations** / e-learning, et des « Engineering Procedures », partagées entre donneurs d'ordre et fournisseurs de tous rangs qui expliquent ce qui est attendu (en particulier au titre de l'ARP4754).

➔ **R5.3.4.2 :** Partager et négocier, dès le début du projet les **attendus** en matière de **processus d'ingénierie système** (dont l'ingénierie des **exigences),** et de **certification** système. Prévoir explicitement de négocier au cours du projet les attendus qui peuvent apparaître.

5.3.4.2 **Documents d'interfaces**

- Constat : Même si beaucoup de nos grands programmes gèrent leurs interfaces avec une grande rigueur, il existe encore des cas où les « Interface Control Documents » (ICD), réalisés entre donneur d'ordre et un ou plusieurs fournisseurs, ne sont pas gérés avec une rigueur suffisante. Dans ces cas, des exigences fondamentales pour la définition du système peuvent se retrouver noyées au milieu de données informelles, sans une gestion de configuration suffisante. Dans ces cas, c'est souvent au fournisseur de « faire le tri » et de décider des exigences à incorporer aux spécifications.

  Ces documents ne sont, ni des documents de rang donneur d'ordre, ni de rang fournisseur, ils ont dans un « entre-deux ».

Recommandations :
➔ **R5.3.4.3 :** Traiter toujours les ICD avec la même rigueur que les spécifications. Identifier, tracer, et valider les différentes exigences d'interface de toute nature : fonctionnelles, physiques, … nécessaires. Le planifier (au niveau d'un SOW par exemple), et le faire suffisamment en amont pour une approbation lors des jalons programmes appropriés (par exemple : à la PDR pour les ICD fonctionnels, à la CDR pour les ICD de câblage, …)

➔ **R5.3.4.4 :** Formaliser et partager les modèles de données associés à chaque interface. En assurer la cohérence, tout au long des développements et du cycle de vie des produits (en particulier : gestion en configuration).

➔ **R5.3.4.5 :** Promouvoir l'utilisation du Model Based System Engineering, car c'est un des moyens les plus adaptés pour gérer les interfaces de manière efficace et non ambigüe (en particulier : éviter les ambigüités liées à une description textuelle).

5.3.4.3 **Frontières et Délégation**

Exigence de l'ARP4754 : L'avionneur doit pouvoir vérifier que les hypothèses (« Assumptions ») prises par les fournisseurs sont valides, en particulier pour la gestion des interfaces entre sous-systèmes.

- Constat :

a/ Pour certains projets, les donneurs d'ordres (plateformiste, avionneur) délèguent la bonne implémentation et le suivi des hypothèses, voire des interfaces entre sous-systèmes, aux fournisseurs dès lors qu'ils sont reconnus comme étant des fournisseurs ayant un bon niveau de maturité.

b/ D'autres, dans des contextes de projets différents, ne donnent pas cette délégation et s'assurent directement de la cohérence (en particulier pour

contrôler les interfaces)[46]. Certains fournisseurs perçoivent cette attitude comme le fait que le donneur d'ordre fait de l'ingérence et cherche à s'assurer par ses propres moyens que le fournisseur réalise le travail proprement à son niveau.

c/ Dans certains cas, ce travail de cohérence est fait conjointement. A titre d'exemple, en phase amont, typiquement jusqu'à la PDR, l'avionneur et les fournisseurs travaillent en plateau, pour faciliter ce travail de mise en cohérence.

- Constat : Il y a un **manque de délégation** quant à l'application des normes de certification, avec pour conséquence la **multiplication des audits** du type ARP / DO à tous les niveaux avionneurs, systémiers, sous-systémiers, et équipementiers. Chacun y allant de son propre format d'audit et de la sa propre définition des attendus. Conséquence dérivée : l'augmentation exponentielle des activités d'**assurance des processus**, coûteuses.

Recommandations :
➔ **R5.3.4.6 :** Définir dès le début du projet, les périmètres de responsabilité et de délégation, les pratiques industrielles adaptées, et les jalonnements/synchronisations/réconciliations à appliquer, en matière de gestion des exigences et de contrôle des interfaces, tenant compte des risques identifiés, de la maturité avérée du fournisseur, et du niveau de criticité des éléments sous-traités. Ceci peut d'ailleurs se généraliser à l'ensemble du périmètre Ingénierie des Systèmes.

➔ **R5.3.4.7 :** Mettre en place, pour l'ARP 4754A et la DO 178 / DO 254, un système d'agrément et de qualification des processus de type DOA / DOID[47], qui repose sur des critères objectifs, et régulièrement enquêtés/évalués.

[46] Note : *Un moyen privilégié de le faire étant de compiler dans une base unique tout ou partie des exigences multi-niveaux.*
[47] Nota : *DOA : Design Organisation Approval ; DOID : Design Organisation Interface Document*

5.3.4.4 **Gestion des changements**

Constats :

- Certains donneurs d'ordres refusent de faire évoluer leur spécification contractuelle, alors même que des modifications importantes de la définition sont demandées, rendant la traçabilité au niveau fournisseur difficile. On notera cependant que d'autres donneurs d'ordres appliquent une gestion de configuration et un processus de gestion des modifications rigoureuses.

- Sur certains programmes, trop d'évolutions sont demandées par « Mémos », sans traçabilité rigoureuse au niveau des fonctions et exigences (exemple : l'exigence XX devient l'exigence YY)

- En cas d'évolution, le gain attendu n'est pas toujours expliqué ni justifié.

- Il y a un manque de coordination dans le temps entre les différents niveaux de spécification.

- La notion de Baseline documentaire n'est pas toujours formalisée (mono et multi niveaux).

Exemple de la concurrence : Boeing propose un "Requirement Manager" dans l'organisation de l'avionneur en charge de gérer les demandes d'évolution des

Recommandations :
➔ **R5.3.4.8 :** Etablir en commun entre les industriels, le **jalon contractuel** à partir duquel il convient de **gérer les modifications** au travers d'un processus rigoureux.

Nota : Cette recommandation s'applique aussi bien au cas de développement hardware classique (type cycle en V, « document centric ») qu'aux développements dans des technologies telles que les technologies de l'information ou les télécommunications, où l'on privilégie les méthodes « agiles », les approches « data centric », ... Le point principal est dans tous les cas de ***bien établir contractuellement les obligations des parties****, et les mécanismes d'évolution associés.*

➔ **R5.3.4.9 :** Chaque **demande de modification doit être exprimée avec au moins la même rigueur que la Baseline d'exigences initiale** (en précisant en particulier la situation des exigences « avant » et « après » la demande de modification).

➔ **R5.3.4.10 :** Pour chaque demande de modification, il est recommandé de **partager** la **valeur attendu**e avec toutes les parties prenantes, et de conduire une **analyse d'impact rigoureuse et exhaustive** sur **les baselines de spécification, et la définition du produit/système.**

➔ **R5.3.4.11 :** Agréer entre les parties prenantes un processus de **réconciliation** pour maintenir une Baseline d'exigences multi-niveaux, avec a minima une mise à jour à l'occasion de jalons majeurs.

Nota : Selon les cas, la baseline peut contenir des éléments prenant différentes formes : base de données outillée (DOORS, Reqtify, …), documents consignant des exigences textuelles, ensemble de données et de modèles, éléments de CAO, PLM, etc.

exigences en remontée des fournisseurs (pour une meilleure compréhension du besoin, voire un challenge).

5.3.4.5 La documentation technique et les instructions clients

- Constats :
  - On note une inflation des documents associés au processus de développement (Exemple : plus de 2500 documents livrés sur le CPIOM A350) :
    - En entrée : Nombreuses directives applicables (ABD, BAC, BMA, EP…) à tiroirs, nécessitant la fourniture de matrices de conformité.
    - Dans certains cas, absence de filtre sur les documents réellement applicables (ex. envoi de documents avionneurs aux équipementiers) ; avec comme conséquence l'absence de focus, la déresponsabilisation, et le risque d'erreur.
    - En sortie: Documents de type livrables : Spécifications, Définitions, Plans, Justifications, etc.…
  - Les architectures documentaires sont de plus en plus complexes, et rendent difficile la compréhension du fonctionnement du système et de sa définition.
  - Un effort considérable est consacré à l'analyse des documents applicables tels que les exigences sur les processus, les normes techniques, … et leur gestion de configuration (révisions fréquentes, cohérence,…). Cette activité est impérative, mais, en l'absence de filtre, sa valeur ajoutée associée est souvent faible, même si ce type d'analyse a permis par le passé de lever des risques.
  - Les demandes clients conduisent fréquemment à la production de documents redondants (exemple dans les plans qui demandent à chaque fois la description du système/sous-système), qui conduisent à des pertes de temps dans leur écriture, ou pire à des incohérences.

Recommandations :
➔ **R5.3.4.12 : Définir et agréer en début de programme les documents applicables** et leur contenu.

➔ **R5.3.4.13 :** Systématiser la **revue des documents applicables**, en mettant l'accent sur le contenu, la cohérence et l'utilité.

➔ **R5.3.4.14 :** Appliquer aux **changements de documents** applicables le **même processus de gestion de la configuration et de contrôle** qu'aux exigences (notion de « Avant » -« Après ».)

➔ **R5.3.4.15 :** Limiter l'écriture de documents redondants, en regroupant les parties communes dans des documents chapeaux auxquels on fera référence, et qui seront plus facile à gérer en configuration.

5.3.4.6 **L'organisation d'entreprise pour supporter le processus V&V**

- Constat : Dans le cadre de nouveaux partages industriels de l'Entreprise étendue, la relation entre avionneur/plateformiste et systémiers/sous-systémiers ou entre, systémiers/sous-systémiers et équipementiers a évoluée :

  - Pour l'A350, Airbus a fait le choix de s'appuyer sur un nombre restreint de systémiers auxquels il délègue une partie de son rôle d'avionneur (par exemple validation des DDP - Déclaration de Design et des Performances). Exemple: RSP (Risk Sharing partners) / NSP (New System Policy)

- Constat : Les nouveaux partages industriels entrainent une remise en cause des **organisations** traditionnelles et la définition ou redéfinition de certains **rôles et responsabilités**, tout au long du processus de développement, et notamment des activités d'intégration et de V&V : ingénieur en chef, architecte système, spécialiste en capture d'exigences et traçabilité, Responsabilité Assurance des Processus, fonctions support (qualification, fiabilité, sûreté de fonctionnement, calculs, simulations…) ; rôles qui existaient dans le domaine militaire (Dassault) .

  - On notera en particulier, le rôle de l'ingénieur en chef (ou autorité technique) qui assure la responsabilité complète (TCQ) du produit à réaliser.

  - Il doit s'appuyer sur des rôles indépendants (par exemple sûreté de fonctionnement, certification) lors des revues de V&V.

- Constat : Le développement de systèmes/sous-systèmes ne correspond plus strictement au découpage ATA et s'intéresse en premier lieu aux fonctions à réaliser qui peuvent réclamer la contribution de plusieurs ATA (exemple la décélération d'un aéronef qui s'appuie sur les becs et volets (ATA 27), le système de freinage (ATA 32) et le système de propulsion pour les inverseurs de poussée (ATA 7x). L'avionique modulaire a introduit de nouvelles exigences et interfaces entre le système lui-même (ATA 42) et les fonctions qu'il supporte.

- Constat : La recherche d'optimisation globale au niveau d'un système peut être contrariée dans des schémas d'organisation historiquement optimisée d'un point de vue local : Exemple : optimisation masse d'éléments de pointe avant, sans prise en compte du "bracketing" (support d'attache).

- Constat : La recherche d'optimisation de niveau système peut conduire le systémier à reporter sur l'équipementier la recherche de solutions techniques qui permettent de répondre à certaines conditions particulières de niveau système. La solution proposée peut ne pas être consistante avec d'autres solutions du même type retenues sur l'ensemble de l'avion. Ce qui remet en cause la capacité d'intégration limitée à un niveau système.

- Constat : Les processus d'ingénierie des exigences de V&V associé sont bien acceptés par les concepteurs systèmes/sous-systèmes électriques et électroniques (au sens large), mais beaucoup moins par les concepteurs en mécanique. Ainsi, dans la pratique, le processus complet (traçabilité, validation et vérification avec indépendance) n'est pas appliqué systématiquement à tous les niveaux équipements. Nous en venons à définir des notions d'équipements « complexes » (en gros, contenant de l'électronique) et « simples », et des niveaux de validation associés.

- Constat : Le processus de revues de validation avec indépendance est très consommateur de temps (1h pour 5 à 10 exigences avec 2 à 4 participants). Certes, la qualité et la rigueur en sont renforcées. Ceci est d'autant plus intéressant que la question de l'acceptabilité du rapport bénéfice/coût est posé par certains acteurs.

- Constat : Il y a quelques années on mettait en Assurance des Processus des anciens avec expérience, aujourd'hui on a tendance à faire appel à de la sous-traitance avec des niveaux d'expérience plus légers, ce qui conduit parfois à de la surenchère sur des problèmes de forme plus que de fond, et des coûts inutiles …

- Maturité des systèmes / gains du processus V&V

Exemple vs concurrence : est-on meilleurs que la concurrence ?

- LA DO160 impose des tests spécifiques unitaires (thermique, vibration, humidité,…) mais aucun essai combiné qui peut être plus contraignant.

- Les stratégies de test et de maturité (HALT…) viennent compléter ces tests de vérification de niveau équipement.

- Il est nécessaire de définir des tests de robustesse de niveau système s'appuyant non seulement sur les modes dégradés et les modes opérationnels, mais également sur les marges et les dispersions.

Recommandations :
➔ **R5.3.4.16 :** *Il est fondamental de valider les exigences le plus en amont possible. Le coût (coût financier, shift de planning) d'une correction apportée en amont sera toujours moindre que celui d'une correction plus aval.*

➔ **R5.3.4.17** *L'Assurance de Développement ne doit pas être le déroulement d'un processus de contrôle purement formel, déroulé par du personnel qualité, sans acquis technique. Elle doit être conduite par du personnel de préférence in situ, et techniquement expérimenté, à même d'accompagner du point de vue méthodologique les ingénieurs chargés du design.*

5.3.4.7 **Certification**

- Constat : Certains donneurs d'ordre demandent une traçabilité complète de toutes les exigences vers le cas de test et le résultat du test, incompatible avec les méthodes et outils existants.

- Constat : Sous la pression des clients et des autorités de certification, il y a une propension à faire plus de processus que de technique ("dashboards", revues, preuves…)

Recommandations :
➔ **R5.3.4.18** Arrêter l'inflation du coût des activités nécessaires pour la certification par exemple en mettant un frein aux demandes d'évolutions de l'ARP4754 ou 4761.

5.4 ANNEXE AU CHAPITRE 5 :

Bénéfices attendus	Constat	Cause probable
Une meilleure maturité du produit à l'entrée en service, donc au bénéfice du client final	Obtenu mais avec une augmentation des coûts NRC	Sur-contrainte imposées ou auto imposées
Une meilleure maîtrise et une meilleure stabilité de la définition système	De nombreux exemples montrent des réductions des coûts de développement dues à la diminution des reprises de conception. D'autres exemples montrent qu'il n'y a pas encore une maturité suffisante pour montrer le gain.	Il est dans de nombreux cas trop tôt pour pouvoir montrer un retour d'expérience concluant.
Des designs plus optimisés car plus intégrés	Partiellement réalisé, encore du potentiel	Découpage ATA et organisations existantes par mono-spécialités
Des couts récurrents mieux maitrisés	Partiellement réalisé,	Bridage de l'innovation par manque de confiance dans la relation
Des temps de développement raccourcis	Partiellement obtenu, des efforts sont nécessaires pour la cohérence temporelle entre définition et industrialisation	Manque d'outils de simulations et de maîtrise du concurrent engineering
Optimisation globale	La chaine de valeur complète n'est pas intégrée pour avoir un produit efficient	Pas de phase de développement dédiée à la revue commune des exigences dans les processus. Méconnaissance de l'environnement opérationnel.
Evolutions de produits facilitées	On ne sait plus revenir en arrière…	
Avantage concurrentiel important	Les industriels français du secteur ont un réel savoir-faire dans la maitrise des développements de systèmes complexes, mais avec un effort trop important	Objet du présent rapport en général

Table 5.1 : Etat des bénéfices attendus et de la situation constatée

6. PROCESSUS, METHODES POUR L'INTEGRATION LA VERIFICATION, LA VALIDATION, ET LA QUALIFICATION (IVV&Q)

Globalement, les objectifs poursuivis dans l'IVV&Q (Intégration Vérification, Validation, et Qualification, sigle valide en français comme en anglais) sont d'effectuer les opérations d'assemblage et de test des composants, équipements, sous-ensembles, sous-systèmes et systèmes, jusqu'au plus haut niveau de l'arbre des produits (PBS), en s'assurant de la

conformité de la construction du système de plus haut niveau, à partir de ses composants. L'objectif final est la qualification en condition opérationnelle[48].

On notera que ces activités sont très consommatrices en ressources (coûts, délais), et qu'à ce titre elles doivent être très soigneusement organisées (stratégie et optimisation des logiques, plans détaillés d'IV&V, …) au niveau de l'entreprise, mais aussi au niveau de l'entreprise étendue (« supply chain »). Elles constituent un gisement important d'innovation et de réduction des coûts[49].

• Constat : Lorsque la stratégie de IVV&Q n'est pas partagée (rôle des simulations, des plateformes, des essais au banc, et des essais en vol) chez les différents intervenants, les efforts des parties prenantes ne sont pas synchronisés, et cela génère, des risques (liés aux éventuels « trous de vérification »), des redondances, des surcoûts, et des actions correctrices.

6.1 FINALITE ET OBJECTIFS DU PROCESSUS D'INTEGRATION

L'objectif de l'intégration est d'effectuer les opérations d'assemblage[50] et de tests d'intégration et de non régression des composants, équipements, sous-ensembles, sous-systèmes, et systèmes, jusqu'au plus haut niveau de l'arbre des produits (PBS), en s'assurant que la construction de ce système de plus haut niveau, à partir de ses composants et constituants est conforme à ce qui a été prévu et planifié lors de la phase de conception (conformité à la logique d'intégration).

Selon, l'ARP 4754, l'intégration consiste en: "1/ The act of causing elements of a system/item to function together. 2/ The act of gathering a number of separate functions within a single implementation."

Ce processus est très étroitement imbriqué avec le processus de vérification. Selon les domaines et les industriels, les frontières de ces deux processus peuvent varier légèrement.

---

48 Nota : *La qualification opérationnelle permet de s'assurer que le système ou produit livré répond aux besoins opérationnels du client. Il ne faut pas la confondre avec la qualification environnementale, applicable dans le domaine aéronautique civile, qui consiste à s'assurer de la conformité du produit, vis-à-vis des exigences environnementales. Pour l'aéronautique civile, l'équivalent de la qualification opérationnelle est le « route proving », procédure au cours de laquelle les compagnies aériennes de lancement (« launch customer ») participent à la démonstration des capacités opérationnelles de l'avion.*

49 Nota : *C'est en particulier le cas chez Space-X, qui a modifié les processus d'IVV&Q traditionnels. Une présentation AIAA de l'IS chez Space-X, par John Muratore est fournie en annexe C.*

50 Nota : *Certains industriels feront la distinction entre le processus d'assemblage et le processus d'intégration, d'autres au contraire les considèrent comme un seul processus (c'est ce que fait aussi l'ISO 15288).*

6.2 FINALITE ET OBJECTIFS DU PROCESSUS DE VERIFICATION

Le processus de vérification a pour finalité de s'assurer, tout au long du processus d'intégration, que les exigences spécifiées (exigences aux différents niveaux fonctionnels et physiques, exigences d'interfaces), sont bien satisfaites. A ce titre, le processus de vérification sera chargé de bâtir la stratégie et la logique de vérification, de choisir les différentes méthodes de vérifications et de planifier les activités associées.

6.2.1 Bâtir la Logique de Vérification

Les principales étapes sont :

- Définir la stratégie de vérification.
    - Cette étape précise comment organiser la vérification du(des) produit(s), vis-à-vis des exigences[51], en partant de la définition et en décrivant la succession des justifications théoriques et expérimentales nécessaires.
    - Les critères de vérification sont déterminés par le risque perçu, la sécurité / sûreté et la criticité du système ou de l'élément concerné.
    - Nominalement, les éléments de niveau inférieur sont vérifiés en premier.
    - Différentes solutions sont comparées au travers de contraintes et de critères de vérification.
- Les types de vérification les plus courants sont les suivants:
    - Le contrôle (vérification de propriétés qui nécessite un examen, une observation),
    - Les études d'ingénierie (simulations, calculs…) lorsque la vérification dans les conditions réelles ne peut pas être atteinte ou ne rentre pas dans des coûts acceptables,
    - La démonstration (à utiliser, par exemple, quand les exigences sont exprimées de façon statistique ou pour démontrer la similitude avec un autre produit),
    - Les essais (réalisés à l'aide de plateformes d'essais).
    - De manière pratique, en aéronautique civile, il peut arriver que des essais spécifiques soient remplacés par du retour d'expérience d'utilisation opérationnelle d'un système (sur un autre aéronef) par exemple, pour peu qu'on démontre que le domaine opérationnel est bien couvrant par rapport au besoin.
- Identifier les besoins liés à l'environnement de vérification.

[51] Nota : On parle parfois, de manière abusive de vérification des exigences. Stricto sensu, ce terme est inapproprié.

- Bâtir la logique de vérification détaillée et la mettre à jour autant que nécessaire.
    - Les points ouverts relatifs à la vérification sont tracés et leur résolution est planifiée dans la logique de vérification.
    - La structure du futur dossier de justification de la définition (DJD) est précisée.
- Résoudre les problèmes liés à la logique.

6.2.2 Démontrer la Faisabilité de la Vérification

Principales étapes:

- Identifier les besoins permettant de démontrer la faisabilité de la vérification.
    - Dans certains cas, il peut s'avérer nécessaire de faire des calculs préliminaires pour prévoir les résultats d'essais et / ou rendre possible l'analyse de ces essais.
- Evaluer la faisabilité de la vérification.
    - Cette étape vise à confirmer que les choix d'ingénierie (définition, intégration, opérations de vérification…) sont compatibles avec les objectifs et les contraintes de la vérification.
- Approuver le plan de vérification des exigences.
    - Le plan de vérification des exigences intègre dans sa logique des éléments de planification issus du processus Programme / Project Planning.
    - Selon la taille du projet/programme, le plan de validation des exigences peut renvoyer à d'autres plans, comme par exemple le plan général des essais ; la rédaction de ces plans nécessite la contribution des métiers d'ingénierie concernés.

6.2.3 Réaliser la Vérification

Principales étapes:

- Accepter l'environnement de vérification.
    - Les moyens, préalablement définis et qualifiés, sont eux-mêmes vérifiés de façon à confirmer leur aptitude à être utilisés pour la vérification.
- Mettre en œuvre les méthodes de vérification.
    - Des méthodes de vérification standards sont ou doivent être décrites dans des instructions et / ou des guides méthodologiques.
- S'assurer que les opérations de vérification sont menées conformément au plan de vérification.
    - Pour une maîtrise correcte du processus, il est recommandé de maintenir et de mettre à jour la traçabilité de la vérification des exigences du système et de ses éléments.
- Analyser les résultats des opérations de vérification et les problèmes rencontrés.
    - En cas de problème, tous les niveaux impactés de l'architecture sont identifiés et ces impacts sont analysés.
    - En cas de remise en cause de la logique de vérification, retourner à l'étape «Bâtir la Logique de Vérification».

6.2.4 Démontrer que la Vérification est Réussie

Principales étapes:

- Statuer sur et justifier la réalisation correcte de la vérification. Principales conditions:
  - A tous les niveaux et pour tous les éléments, chaque exigence a été vérifiée.
  - Tous les problèmes relatifs à la vérification sont réglés.
- Elaborer et maintenir le dossier de justification industriel
  - Tracer les preuves de l'application du plan de vérification des exigences, analyser les résultats et justifier les écarts.
  - Etablir le dossier de justification industriel (comprenant le dossier de justification de la définition) en remontant depuis le niveau le plus bas de l'architecture.

Pour réaliser ces étapes, on pourra s'appuyer sur des revues internes (de type « Maturity Gates ») et/ou des revues de programme avec participation (éventuelle) du client.

L'objectif global du processus de vérification est de démontrer, au travers de son déroulement, que le produit ou sous-système ou système intégré livré est conforme au jeu d'exigences qui lui sont applicables, et de ce fait répond aux fonctions attendues. On notera que ce processus se décline de manière similaire, quelle que soit la nature du livrable (produit, ou équipement, ou sous-système ou système intégré, de type avion, ou même service).

Aussi, une finalisation satisfaisante de ce processus constitue une des bases de l'acceptation contractuelle par le client[52], du produit ou service à livrer.

Plus précisément les objectifs de la vérification sont :

- De s'assurer, tout au long du développement et de l'intégration que le produit, ou ses parties sous test, présente(nt) des garanties de bon fonctionnement (telles que sûreté, sécurité, intégrité), et permet(tent) en l'état de sa (leur) vérification, de garantir que le produit final livré tiendra ses performances et exigences essentielles,
- D'assurer que le produit est conforme au design validé/accepté avec le client, qu'il ne comporte pas de défaut, et est au travers de la tenue des exigences, acceptable pour l'usage attendu,

---

[52] Nota : *Le processus de vérification contribue à la démonstration client, au même titre que les preuves de validation*.

- De démontrer que les performances effectives sont en accord avec les spécifications de performances, et qu'ainsi le produit est compatible de sa mission.

Dans le cas d'une évolution du système conçu, entrent dans les activités de vérifications les analyses d'impact et tous les tests consacrés à la démonstration de non-régression.

6.3 ACTIVITES DE VERIFICATION

Les activités associées au processus de vérification sont :

- la planification,
- l'exécution des tests et essais d'intégration et de vérifications diverses (tests physiques, tests logiciels, simulations, démonstrations par analyses et/ou notes de calcul, études de comportement statistique, revues de design, inspections, démonstrations mixant des moyens divers, …),
- le reporting (rapports de tests et essais, rapports d'avancement, …),
- le contrôle, et la démonstration de fin de vérification (« verification closeout » en anglais).
- Pour l'aéronautique civile, on peut ajouter que l'activité de vérification n'est close que lorsqu'il y a acceptation finale par les autorités de certification.
- De même, dans le domaine spatial ou défense, l'activité de vérification n'est close que lorsqu'il y a acceptation finale des autorités de qualification.
- Le processus, et ses différentes activités, sont illustrés sur le schéma suivant :

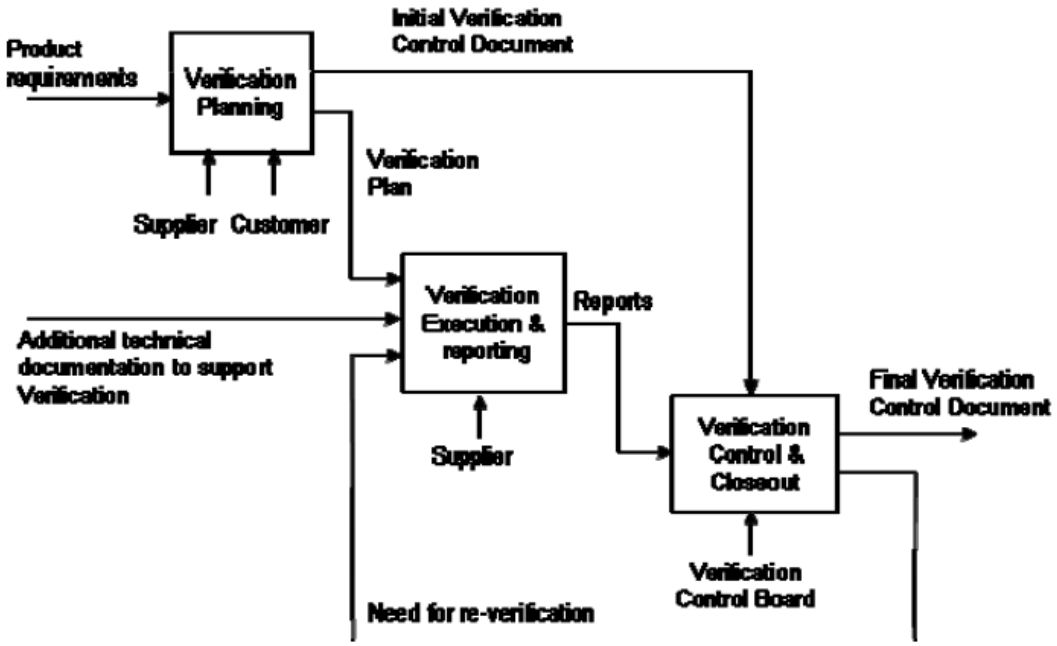


Schéma 6.1 : Processus et activités de Vérification (selon ECSS-E-ST-10-02C)

6.4 STRATEGIE ET PLANIFICATION DE LA VERIFICATION

Afin d'atteindre au mieux les objectifs de vérification, il est recommandé que la logique de vérification soit établie dès les phases amont du cycle de développement, et qu'elle fasse l'objet de revues et d'accords entre client et fournisseurs, en amont du développement.

Un moyen puissant d'y parvenir est d'analyser très en amont les exigences, sous l'angle de la vérification, et de prendre en compte :

- La particularité du design envisagé, et les contraintes éventuelles (e.g.: faisabilité de certaines démonstrations potentiellement très complexes/coûteuses, ou dangereuses, risque d'explosion combinatoire du nombre d'états du système à vérifier, etc…),
- L'état des solutions candidates, vis-à-vis de la vérification (maturité des solutions ; par exemple, pour une solution déjà éprouvée sur un système opérationnel, la preuve par l'usage peut contribuer à la vérification, à condition de l'accompagner d'une démonstration rigoureuse),
- La disponibilité, l'accessibilité, et la maturité des moyens et outils de vérification (par exemple : complexité des moyens de tests, nécessaires à la vérification, problématiques de sûreté associées aux épreuves de vérification, coûts, …),
- Les méthodologies de vérification et de test,
- Les spécificités liées aux essais en vol, aux tests à feu, aux démonstrations en orbite, …

- Les spécificités liées au type de produit : Typiquement, démonstration de l'aptitude minimale au vol dans l'aéronautique, civile et militaire, avant d'effectuer le premier essai en vol (e.g. : tests minimaux exigés pour un premier vol, en particulier vis-à-vis de la "Safety Of Flight"), alors que bien souvent, pour les missiles, les lanceurs et les satellites, on se doit de couvrir entièrement le domaine de vol, avant le premier essai en vol.

- L'acceptabilité des écarts de configuration, par rapport à la définition série, en fonction des attendus de l'essai,

- Les contraintes programmatiques,

- Les coûts et les délais.

Pour bâtir son approche, le concepteur doit s'interroger sur les trois étapes suivantes :

- Qui ou quoi ? : Quels sont les produits, ou équipements, ou sous-systèmes ou systèmes intégrés, ou services, objets du processus de vérification ? Quelles sont les exigences à vérifier ?

- Comment ? : Comment conduire la vérification ? Quelle sont les méthodes à utiliser ? Comment mettre en œuvre les méthodes imposées par les spécifications, lorsqu'il y en a ?

- Quand ? : Comment et quand appliquer la stratégie de vérification choisie ?

Cette approche se construit usuellement de manière itérative, en s'appuyant sur les constats de faisabilité (contraintes techniques, coûts, délais, ….), et au travers d'un processus d'agrément entre fournisseur et client.

6.5 METHODES DE LA VERIFICATION

La vérification est conduite en faisant appel à plusieurs types de méthodes. Classiquement on distingue[53] les :

- Tests :

  La vérification par test consiste à vérifier la tenue des exigences et l'atteinte des performances du produit sous test. Elle peut être réalisée soit dans l'environnement opérationnel, soit grâce à des modèles de simulation représentatifs de cet environnement opérationnel du produit sous test, soit éventuellement sur un environnement mixant éléments réels et simulateurs.

  La représentativité de l'environnement simulé dépend du cas et de l'étape de vérification. Suivant les cas, cela peut être conduit à l'aide de simulations purement numériques, ou bien aller jusqu'à un essai en vol, ou toute situation intermédiaire jugée adaptée.

[53] Nota : L'ISO 15288 parle d'IADT : Inspection, Analyse, Demonstration, and Test.

On notera tout d'abord que le choix des modèles de tests adaptés, et des moyens de mise en œuvre associés est une activité de la plus haute importance et généralement très complexe, qui doit être engagée assez tôt dans le développement avec des moyens suffisants, pour éviter des retards souvent très coûteux dans les phases aval, liés à l'indisponibilité des moyens de test[54].

On notera ensuite les autorités de certification demandent que les exigences critiques de sûreté (« safety critical » requirements), chaque fois que c'est possible, soient vérifiées par test.

On notera également que la vérification des logiciels comportera une étape de vérification sur machine cible (environnement hardware identique à celui du produit final).

[54] Nota : *La conformité des moyens de tests, et du produit sous test sera assurée avant le démarrage des campagnes de tests, au travers d'une revue d'aptitude au test (« Test Readiness Review » en anglais).*

- Analyses, démonstration, et modèles :

  La vérification par analyse consiste à conduire des évaluations théoriques, semi-empiriques ou empiriques, en mettant en œuvre des techniques agréées avec le client, et ayant fait l'objet d'une validation préalable (ex. : modèles, …).

  Rattachées à cette catégorie, on trouve les vérifications par similitudes, qui consistent à s'appuyer sur un produit similaire, déjà vérifié/validé/qualifié sur un autre système (« service experience » dans l'ARP4754), et une règle de similitude éprouvée entre ce produit et le produit à vérifier.

- Revues de design :

  La vérification par revue de design consiste en la mise à disposition des membres de revue d'éléments de preuve (documents de design, descriptions techniques, schémas et dessins, tests antérieurs, …) montrant sans ambiguïté que l'exigence (les exigences) à vérifier est (sont) bien remplie(s). Après examen de ces éléments, les membres de revue se prononcent sur l'acceptabilité de la vérification.

- Inspections.

  La vérification par inspection consiste en la détermination directe de caractéristiques physiques ou non du produit sous test (au travers d'inspections visuelles, ou autre). Elle peut porter sur des caractéristiques de construction, sur la conformité d'éléments à un dessin ou à un document de design (taille et forme de pièces par exemple), ou sur la bonne déclinaison de standards (aussi bien pour des pièces mécaniques que pour des logiciels – pour ces derniers, au travers de revues de code, et d'analyse de conformité à des standards de codage, …)

Suivant la maturité, la faisabilité et le besoin de confiance, on choisira au cas par cas la méthode la plus adaptée[55]. Dans tous les cas, les vérifications envisagées et le processus à dérouler seront définis dans le plan de vérification (PV ou VP en anglais).

Certaines normes, telles l'ARP4754A, imposent également que des exigences critiques soient vérifiées par une combinaison de plusieurs méthodes (revue + essai par exemple).

On notera également, que pour des systèmes à haut niveau de criticité, il est parfois demandé un niveau d'indépendance entre les activités de conception, et les activités de vérification (tests ou autre).

---

[55] Nota : *Par exemple, pour le développement d'un avion civil, il est communément admis qu'on ne fera pas de test physique spécifique pour démontrer sa capacité à amerrir et à flotter. La démonstration sera conduite par simulations numériques et analyse. Lorsque c'est pertinent, un retour d'expérience sur un/des cas de vol présentant des similitudes pourra être utilisé, comme élément de vérification*.

6.6 NIVEAUX ET ETAPES DE LA VERIFICATION

La vérification est un processus incrémental, de type « bottom-up » (allant de bas en haut), qui s'étale tout au du développement (revue de design, intégration, et remontée du V), et qui est mis en œuvre, tout au long de la chaîne de valeur (du composant, jusqu'au niveau système/plateforme).

Le principe de subsidiarité privilégie de vérifier ce qui peut l'être au niveau le plus bas et le plus amont. On évitera de démarrer la vérification d'un produit, tant que la vérification des produits de plus bas niveau qui le constituent, n'est pas totalement acquise.

On distinguera différents niveaux de vérification, en fonction du niveau de décomposition du système ; typiquement on trouvera des activités de vérification au niveau composant, au niveau équipement, au niveau sous-système, au niveau système, au niveau avion, ….

De même la vérification s'effectuera en plusieurs étapes, sanctionnées par de grandes revues. Ces étapes peuvent être différentes suivant le système /la plateforme considéré.

6.7 EXECUTION DE LA VERIFICATION, ET REPORTING ASSOCIE

Comme déjà dit au paragraphe précédent, la vérification est un processus incrémental, qui doit être conduit de manière rigoureuse. Ainsi, il est nécessaire de mettre en place une organisation spécifique, en charge de l'assurance de la Vérification, supervisée de bout en bout, par une autorité de vérification, instance de décision de haut niveau[56].

Cette organisation peut d'ailleurs être étendue à l'ensemble des activités d'intégration, vérification et validation (IV&V en anglais). Naturellement, elle devra être adaptée, en fonction de la nature et de la taille du programme considéré.

Cette organisation doit s'assurer du bon déroulement des plans de vérification, détaillant l'ensemble des activités et s'assurera de la bonne gestion les points de rendez-vous au niveau des plannings.

L'équipe en charge de la vérification doit ensuite mettre en place un système de rapports d'essais (« Test report » en anglais), de rapports d'analyses, de rapports de revues de design et de rapports d'inspections (selon la méthode de vérification utilisée), gérer les anomalies, et non-conformités constatées en essais et plus généralement en vérification (au travers de « Problem Reports » ou de Rapports de Non-Conformité ou NCR[57]), piloter leur instruction par les équipes de design, et consigner les résultats de vérification dans des documents (VCD, « Verification Control Documents » en anglais[58]) , soumis à revue par l'Autorité de Vérification.

---

[56] Nota : *Par exemple, les ECSS ESA demande a mise en place d'un « Verification Control Board » (VCB en anglais). Un équivalent existe, au niveau de l'avion, pour les vols de certification, dans le contexte CS 25.*

[57] Nota : Le vocabulaire diffère beaucoup d'une entreprise à l'autre.

[58] Nota : Dans le domaine de l'aviation civile (chez Airbus en particulier) on parlera de Certification Cards (CRD), au lieu de VCD.

Globalement, cette équipe synthétise l'ensemble des activités et résultats de vérification, au travers d'un Rapport de Vérification Global (VR), également soumis à revue par l'Autorité de Vérification.

Aujourd'hui, il nous semble raisonnable de préconiser une implémentation, sous forme de base de données informatique, pour l'ensemble des données et documents de vérification.

Cette base de données, si elle est mise en place doit être étroitement coordonnées avec celle décrivant la déclinaison et l'arborescence des exigences, lorsqu'elle existe.

C'est au vu de l'ensemble du processus, et au travers d'une revue dédiée que le l'autorité de vérification pourra in fine statuer sur le succès de la vérification.

6.8 CONTROLE, ET DEMONSTRATION DE FIN DE VERIFICATION (CLOSEOUT)

Dans le domaine spatial, le succès de la vérification sera contrôlé, grâce à la traçabilité des données et documents du processus de vérification, et sanctionné par un revue indépendante (des équipes de vérification), pilotée par le l'autorité de vérification (« VCB »), et faisant intervenir des experts extérieurs au programme. Cette revue s'assurera de :

- La complétude de la documentation et des données associée à la vérification
- L'exhaustivité de la vérification des exigences (taux de couverture = 100%)
- La tenue de l'ensemble des performances attendues et des exigences quantitatives, et qualitatives.

Dans le domaine de l'aéronautique civile, l'évènement qui sanctionne ce close-out, et la capacité de l'aéronef à être mis en service commercial, est l'obtention du Type Certificate (TC).

En amont du TC, le succès de cette vérification est, entre autres, assuré par les résumés de vérification[59] (« verification summary », dans l'ARP4754A), et par la déclaration des exigences non atteintes, lorsqu'elles sont acceptables (id est : rapport d'anomalie, analyse d'impact associée, déclaration d'acceptabilité et dérogation permanente – « disposition » et « waiver » respectivement, en anglais.)

[59] Nota : *La notion de VCB n'est pas explicitement utilisée, en aéronautique civile, mais au travers des revues, et du rôle affecté à des ingénieurs système, assurant un contrôle indépendant, la fonction associée est tout de même bien assurée.*

6.9 DOCUMENTS ASSOCIES A LA VERIFICATION

Ces documents sont les rapports d'essais, les rapports d'analyses, les rapports de revues de design et les rapports d'inspections.

On trouve également, dans la liste de documents à fournir et gérer, les rapports de Non-Conformité (NCR), permettant gérer les non conformités constatées en vérification, et les rapports de Contrôle de la Vérification (VCD, « Verification Control Documents » en anglais) permettant de consigner les résultats de vérification.

On trouve enfin, au sommet, le Rapport de Vérification Global (VR) qui assure la synthèse de l'ensemble des activités et résultats de vérification, et le(les) rapports des revues de fin de vérification, publiés par les membres de revues et le l'autorité de vérification.

Spécifique aéronautique civile : Le plan de vérification, les procédures et les résultats de la vérification, la matrice de la vérification et le résumé de la vérification : données de vérification définies dans le plan de certification.

6.10 CONFORMITE ET WITNESSING

Constat : Depuis quelques années, on constate dans le monde de l'aéronautique civile une propension de la part des avionneurs à renforcer le contrôle des activités de vérification menées par leurs systémiers et équipementiers, notamment en termes de conformité. Ainsi, se généralisent des notions directement inspirées des exigences de la FAA :

- Etat de conformité (Statement Of Conformity) des équipements et des bancs
- Autorisation à essai (Autorisation For Test)
- Witnessing : le client ou un délégué officiel assiste à tout ou partie des essais

Ces activités s'accompagnent souvent de procédures administratives lourdes, d'un formalisme documentaire et d'obligations de mettre en place des réseaux de délégués assermentés, autant de contraintes qui s'avèrent coûteuses pour toutes les parties, et consommatrices en délai. Lorsque de tels processus sont appliqués, on note ainsi un surcoût de 10 à 20% des activités de vérification.

On propose que l'industriel ait une délégation pour conduire les activités de démonstration de conformité et de witnessing, Pour cela, une délégation officielle, auditée, devrait permettre aux systémiers de procéder aux activités de vérification et de conformité en toute autonomie.

6.11 VALIDATION

Ce paragraphe s'attache à la partie aval du processus de Validation[60], la partie relative à la validation des exigences ayant été traitée au chapitre 5. Il s'agit ici de validation des équipements, sous-systèmes, systèmes …. vis-à-vis de leur conformité aux usages attendus (« we did the right thing »). A ce titre, ces activités sont complémentaires des activités d'« early validation », qui à la descente du V , dans la cascade des spécifications, ont consisté à s'assurer que les exigences spécifiées captureraient au mieux l'usage attendu des différentes fonctions et produits.

En effet, si le processus de Vérification a permis de s'assurer qu'à tous les niveaux de la remontée du cycle de développement, les exigences spécifiées sont bien satisfaites, il n'a pas pour autant apporté la démonstration que les différents composants, équipements, sous-ensembles, sous-systèmes et systèmes, jusqu'au plus haut niveau de l'arbre des produits (PBS), sont conformes à l'usage attendu.

Pour cela, il convient d'apporter des preuves que l'utilisation opérationnelle des produits et fonctions vérifiés, dans le(les) environnement(s) opérationnel(s) prévu(s) est conforme à l'attendu, au travers de la démonstration sur des scenarii d'usage.

Les tests, analyses, démonstrations, et modèles, revues, et inspections, conduites pour apporter ces preuves, ainsi que leur recueil constituent les activités de la partie aval du processus de validation.

---

[60] Nota : *Soit la partie en haut et à droite du cycle en V.*

6.12 QUALIFICATION

Cependant, au plus haut niveau, la validation par le concepteur ne suffit pas, car il appartient à l'acquéreur du produit ou du système de s'assurer que le produit ou le système développé satisfait son besoin opérationnel, et les exigences règlementaires qui lui sont applicables.

En règle générale, des tests conduits sur des prototypes (par exemple : aéronef, lanceur, missile, …), dans un environnement représentatif de l'opérationnel, associés à des démonstrations par analyse, calculs, simulations et modèles permettront de démontrer l'atteinte de l'état qualifié[61].

Cette atteinte sera bien souvent sanctionnée au travers d'une revue de qualification.

On notera comme déjà mentionné dans le texte chapeau du chapitre 6, que dans l'aéronautique civile, la certification englobe les dossiers de qualification (environnementale), et les dossiers de vérification. L'équivalent de la qualification opérationnelle est le « route proving », procédure au cours de laquelle les compagnies aériennes de lancement (« launch customer ») participent à la démonstration des capacités opérationnelles de l'avion.

6.13 RECOMMANDATIONS ASSOCIEES AU PROCESSUS D'INTEGRATION, DE VERIFICATION, DE VALIDATION, ET DE QUALIFICATION

Recommandations :

➔ **R6.13.1 :** Afin de dérisquer le processus, on préconise d'établir la stratégie de d'intégration, vérification, et validation, dès les phases amont du cycle de développement. La négocier et la partager, en amont entre client et fournisseur, en particulier au travers de revues (typiquement PDR).
➔ **R6.13.2 :** Dès le lancement de projet, agréer entre donneur d'ordre et fournisseur les **contenus fonctionnels des livrables** en cohérence avec leur utilisation (système, équipement, logiciel). Telle fonction devant être disponible pour telle application (banc sol, banc volant, banc d'intégration, 1er vol…)
➔ **R6.13.3 : Accepter (en négociation) la notion de développement incrémental dans le processus** de développement. Définir, dès la négociation du contrat, en commun plateformiste/donneur d'ordre - fournisseur (« avionneur – systémier »), les jalons de développement (revues et/ou Maturity Gates) auxquels telle ou telle fonction est attendue. On doit envisager le développement incrémental d'un sous-système dans le cas où il existe un risque technique lié au sous-système et qu'il convient de le lever dans un premier temps. Il faut aussi envisager le développement incrémental dans le cas où le développement complet du sous-système serait trop long et interdirait de facto de commencer plus tôt l'intégration (risque planning, même s'il n'y a pas de risque particulier sur le plan technique.).

---

61 Nota : *La qualification, et le processus associé ne font pas consensus chez les différents industriels. On peut voir la qualification comme une phase ultime du close-out de vérification, et du processus de validation. Cette notion est décrite dans les ECSS ESA.*

Recommandations (suite) :

➔ **R6.13.4 :** La vérification s'appliquant à un état de définition du produit, la démonstration a longtemps reposé sur des jeux de tests intensifs du produit final. La maîtrise des boucles amont et la connaissance de l'environnement opérationnel, au travers de l'obtention de modèles recalés par rapport aux phénomènes physiques mis en jeu, devra apporter la possibilité de **minimiser les jeux de tests** sur le produit physique **au profit de vérification sur des modèles**. L'utilisation de vérification sur modèle et calculs est par ailleurs incontournable pour des démonstrations inatteignables par test sur le produit physique (exemple : démonstration de ditching d'un avion, démonstration de tenue à l'éclatement moteur, tenue au max V dive, …).
➔ **R6.13.5 :** Conditionner l'écriture et la validation des exigences à leur capacité à être vérifiées.
➔ **R6.13.6 :** Planifier en amont, afin d'assurer au mieux la disponibilité, l'accessibilité, et la maturité des moyens et outils de vérification. En particulier, on recommande de privilégier, lorsque c'est possible (représentativité), l'usage de modèles, permettant de démarrer la vérification plus en amont, d'être économiquement plus efficace, d'être plus facilement maintenable et adaptable au contexte, et d'être souvent plus représentatif du contexte de vol, et plus couvrant (e.g. : simulation de cas de pannes.)
➔ **R6.13.7 :** Il est important de maîtriser l'ingénierie de Vérification. On préconise la mise en place de moyens permettant de gérer l'ensemble des outils et plateformes de tests, des données de vérification, de la documentation, et des indicateurs associés (dont la traçabilité vis-à-vis des exigences). Ces moyens devront être gérés en configuration, et leur pérennité devra être assurée sur le cycle de vie.
➔ **R6.13.8 :** Nous préconisons, au niveau de chaque entreprise et chaque programme, de gérer l'ensemble des données et documents de vérification, sous forme de base de données informatique. Cette base de données, si elle est mise en place, doit être étroitement coordonnées avec celle décrivant la déclinaison et l'arborescence des exigences, lorsqu'elle existe.
➔ **R6.13.9 :** on préconise que le succès de la vérification soit contrôlé, grâce à la traçabilité des données et documents du processus de vérification, et sanctionné par un revue indépendante (des équipes de vérification), et faisant intervenir des experts extérieurs au programme. Cette revue s'assurera de la complétude de la documentation et des données associées à la vérification, de l'exhaustivité de la vérification des exigences (l'objectif visé est l'atteinte d'un taux de couverture de 100%), et de la tenue de l'ensemble des performances attendues et des exigences quantitatives, et qualitatives.
➔ **R6.13.10 :** On propose que l'industriel ait une délégation pour conduire les activités de démonstration de conformité et de surveillance (witnessing), Pour cela, une délégation officielle, auditée, devrait permettre aux systémiers et équipementiers de niveau 1 et 2 de procéder aux activités de vérification et de conformité, avec une plus grande autonomie.
➔ **R6.13.11 :** On recommande de mettre en place, conjointement avec les autorités de certification, une réflexion inspirée du « lean engineering », visant à diminuer la documentation (suppression de la documentation difficilement exploitable, de type « waste »), et de remonter de manière plus simple les preuves nécessaires à la certification.
➔ **R6.13.12 :** Pour les produits conçus pour être réutilisables, établir leur contexte d'IV&V de façon à faciliter la réutilisation ultérieure avec un effort de vérification minimal.
➔ **R6.13.13 :** On préconise de capitaliser le savoir dans les modèles/les plateformes d'essais/les bancs et les processus, permettant de démontrer la validité de ces moyens d'IV&V.
➔ **R6.13.14 :** Utiliser au mieux la Validation amont (par exemple avec des outils de simulation technico opérationnelles) pour clarifier les besoins du client, définir au plus tôt le périmètre d'usage, réduire la complexité liée à la multiplicité des contraintes et des usages (en utilisant une approche par scénarios par exemple), et simplifier ainsi la vérification aval.

7. PROCESSUS, METHODES ET OUTILS SPECIFIQUES POUR LA CERTIFICATION

L'ED79/ARP4754 est reconnue par les principales autorités de certification (EASA, FAA,) comme une méthode de développement acceptable permettant de démontrer la conformité à la CS/FAR 25.1309(b), lorsqu'il s'agit de certifier des systèmes complexes sur les avions commerciaux (MTOW>12.5 tonnes ; voir extraits de la CS 25, en annexe B). Pour la FAA, l'ED79/ARP4754A est également reconnue comme une méthode de développement pouvant être applicable pour les avions légers (PART23), les hélicoptères (PART27/PART29), les moteurs (PART33) et les « propellers » (PART35)62. Des discussions sont également en cours avec l'EASA, sur ces mêmes sujets.

Globalement, les autres autorités de certifications (canadienne, brésilienne, japonaise, russe, et chinoise) suivent les préconisations de la FAA et de l'EASA.

L'objectif est de s'assurer que le risque d'erreur pouvant se produire au cours du développement reste cohérent avec la démonstration quantitative de la probabilité de panne des systèmes.

La rigueur des exigences d'assurance de développement des systèmes sera en relation directe avec la conséquence la plus sévère de panne du système intégré dans l'avion.

En 1999, les JAA publient la NPA 25F291, Les standards ED79/ARP 4754 sont considérés comme un support à la démonstration de conformité à la CS/FAR 25.1309(b), et il est clairement déclaré qu'il n'y avait pas l'intention de contraindre l'avionneur à utiliser ces standards. (Voir extrait « introduction to NPA 25F291 » ci-dessous) :

> Considerable effort has been put into developing Aerospace Recommended Practices (ARP 4754 and 4761) for carrying out Safety Assessments for airborne systems and equipment particularly for highly integrated or complex aeroplanes. While this work is considered worthwhile, the ARP documents merit recognition in the AMJ as a useful means of demonstrating compliance with the requirements of JAR 25.1309. It was never the intention that the applicant be in any way constrained to using the reference ARP's to demonstrate compliance.

Schéma 7.1 : extrait de « introduction to NPA 25F291 »

Cette évolution règlementaire a été introduite par les Joint Aviation Authorities (JAA) dans le JAR 25 à l'amendement 16 en Mai 2003 et ensuite reprise par EASA dans l'édition initiale du CS25.

En Juillet 2011, lors de l'évolution 11 du CS25, l'EASA fait référence à l'issue A de l'ARP4754/ED79

En Septembre 2011, la FAA publie l'Advisory Circular AC 20-174 qui reconnait l'utilisation de l'ED79/ARP4754A comme un moyen acceptable pour minimiser les erreurs de développement de système complexe.

Les autorités de certification ont continué à développer ces standards et exigent, pour toute nouvelle certification, une vue détaillée des méthodes de développement (décrites dans des plans). Cette vue détaillée est systématiquement comparée au contenu de ces standards.

---

62 Nota : *FAA Advisory Circular AC20-174*

Cependant des méthodes alternatives peuvent être proposées mais l'autorité demandera à identifier les différences (démarche « comply or explain »).

Les méthodes de développement ainsi que les moyens de démonstration de conformité doivent faire partie du programme de certification (comme attendu par la règlementation EASA/FAA Part 21). Toutefois il ne faut pas perdre de vue que la preuve de déclinaison par l'avionneur et ses fournisseurs, des recommandations du standard ARP4754/ED79 ne constitue pas, en soi, la preuve de conformité aux règlements de certification applicable.

Pour les autorités de certification, la preuve d'adhésion à ces standards d'assurance de développement doit être complétée aussi par des audits (de niveau avion, systèmes, et équipements), qui viennent s'ajouter aux réunions techniques de certification et aux audits Logiciels & Matériels, déjà prévus au titre des DO 178 et DO 254.

Le volume et la profondeur des preuves attendues vont bien sûr dépendre du niveau d'expérience du concepteur. Ainsi, on peut penser que l'autorité de certification sera-t-elle probablement plus exigeante avec un fournisseur peu ou pas expérimenté qu'avec un fournisseur ayant déjà démontré une expérience appropriée, sur des systèmes ou sous-systèmes de nature comparable.

Cette adhésion est demandée pour tous les niveaux d'un système (en partant au niveau avion jusqu'au niveau logiciel/composant électronique complexe en passant par les couches systèmes multiples, systèmes, équipement, carte électronique).

Il est important de rappeler que cette demande ne doit pas s'appliquer aux systèmes non-complexes (« simple systems » au sens de la CS 25).

Le juste niveau de rigueur doit s'appliquer afin que l'impact des ressources nécessaires pour cette assurance de développement reste compatible avec l'objectif de sûreté (safety) attendu.

Une focalisation excessive sur l'adhésion aux processus peut être en soi une source d'erreur (trop de ressources mises sur l'assurance processus au détriment du fond). Durant les diverses étapes de revue de la conception, le jugement de l'ingénieur doit rester toujours un moyen acceptable de conformité lorsque le niveau de complexité le permet.

Recommandations :

➔ **R7.1 :** On recommande en particulier que les personnes en charge de l'assurance processus, du côté des industriels développeurs, comme du côté de l'autorité de certification, aient une expérience opérationnelle antérieure.

➔ **R7.2 :** Faire un effort en amont, au niveau de la taylorisation des plans, afin d'optimiser le ratio ressources impliquées dans les processus d'IS – ressource globale du programme (cf. recommandation R5.3.4.2, et recommandation générale R8).

➔ **R7.3 :** Adapter les efforts mis sur la sûreté, afin de renforcer la démonstration au niveau mission, et de ne traiter que le juste besoin au niveau des équipements. On notera que c'est un point fort de l'ARP4754A.

➔ **R7.4 :** Obtenir des autorités une meilleure reconnaissance de l'approche basée sur les modèles pour la maitrise du développement des systèmes complexes (Attention toutefois : il ne serait pas souhaitable de se laisser entrainer dans le concept de l'outil certifié, car cela ne ferait que déplacer le problème, sans alléger quoi que ce soit !)

➔ **R7.5 :** Evaluer la nécessité, pour les fonctions (ou chaînes fonctionnelles) sensibles (par exemple critiques au niveau SdF), et à caractère transverse, de mettre en place un rôle, ou un responsable pour ces fonctions (ou par chaine fonctionnelle), avec une vision end-to-end.

8. L'IS DANS L'ENTREPRISE ETENDUE

Les enjeux associés aux tâches de conception et design, à l'environnement de design virtuel, aux flux d'échanges de données techniques ne se limitent pas aux frontières de l'entreprise. On attend un gain majeur, en termes de réduction des risques, de maîtrise de la complexité et d'efficacité, de la mise en place de processus et de moyens permettant de transférer des jeux d'exigences, des modèles, et des définitions complexes, des éléments de vérification et de justification, mettant en œuvre de nombreux paramètres de nature diverses (géométriques, mécaniques, électriques, …), au travers de l'entreprise étendue.

A contrario, cela ne dispensera pas, bien au contraire, de clairement et précisément définir les limites contractuelles et légales, les interfaces entre les entreprises impliquées, ainsi que la gestion des droits de PI, de la confidentialité des données transférées, et des lois et règles afférents au contrôle des exportations (Export Control rules, CIEMG, ITAR rules, …). Ainsi, une évolution en conséquence de la gestion contractuelle et une sensibilisation des juristes à traiter précisément ces questions sont des prérequis au développement de l'IS dans l'entreprise étendue.

8.1 DEFINITION DE L'ENTREPRISE ETENDUE

Une entreprise étendue est un ensemble d'entreprises ou plus généralement d'acteurs (entreprises, agences, administrations locales ou nationales, entités de recherche, …) associés dans la réalisation d'un ou plusieurs projets communs. Elle fonctionne sur la base de contrats (contrats cadres par exemple), de partenariats, ou d'alliances (par exemple, dans le domaine de la R&T : IRT, pôles de compétitivité, accords-cadres, etc…).

Pour certaines phases de réalisation d'un projet (phase d'écriture des spécifications par exemple), l'entreprise étendue pourra s'appuyer sur des ressources mises à disposition et colocalisées, fonctionnant en commun sur un mode dit « mode plateau ».

A ce titre, les acteurs impliqués se posent la question du développement de processus et de méthodes communes, pour conduire les activités d'ingénierie des systèmes de cette entreprise étendue.

8.2 ETAT DE L'ART

8.2.1 Avions d'affaire Falcon

Chez Dassault-Aviation, le développement des avions d'affaire a connu depuis le Falcon 2000 des évolutions importantes dans les processus mis en œuvre du fait de l'entreprise étendue.

Tout d'abord l'utilisation d'une DMU (Digital Mock-Up) a permis de concevoir de façon entièrement numérique et de s'affranchir des plans papier. Centrée cellule et aménagement, cette évolution a été rendue possible en plateau physique par la contribution des différents partenaires industriels sous forme d'un modèle 3D du sous-système/équipement de leur responsabilité.

Cette démarche a été étendue pour le Falcon 7X, les revues d'aménagement ont pu être menées via un Virtual Reality Center, incluant les aspects ergonomie et maintenabilité, accélérant ainsi la validation de la conception. La mise en place d'un plateau virtuel a permis ensuite aux différents partenaires d'accéder depuis leurs sites à la base de donnée commune hébergée par le maître d'œuvre, et ainsi d'optimiser la prise en compte des évolutions de conception post CDR. Le couplage fort entre bureau d'études et production a permis de réaliser le 1er avion de série sans prototype préalable.

Le programme suivant, le Falcon 5X, a mis en œuvre une ingénierie collaborative sur plateau physique puis virtuel, non seulement sur les aspects aménagement 3D, mais également sur les aspects systèmes. Dans un cadre de modélisation fonctionnelle et logique établi par le maître d'œuvre, les partenaires industriels ont contribué à modéliser, dans la même base de données, la part des fonctions leur incombant ainsi que les interfaces fonctionnelles puis physiques échangées. Cette convergence outillée a permis de stabiliser assez rapidement la définition des interfaces entre constituants et surtout d'en réduire le taux d'erreur au niveau de la liasse de câblage.

8.2.2 Rénovation du système de combat de l'ATLANTIQUE 2

Autre exemple chez Dassault-Aviation, celui de l'Atlantique 2 (ATL2), pour lequel la DGA a demandé une rénovation du système de combat. Cet exemple se caractérise principalement par le fait qu'il s'agit d'un avion ancien, plus de 30 ans, donc pour lequel la conception n'avait bénéficié, à l'époque, ni des processus ni des outils d'ingénierie des systèmes. Autre caractéristique, les systèmes « legacy » existants (en fait des sous-systèmes) étaient quasiment indépendants l'un de l'autre, et chaque industriel concerné pouvait développer son sous-système directement sous la maîtrise d'ouvrage étatique, sans réel besoin d'un architecte système global.

Sur la base de cet existant, le projet de rénovation du système de combat s'est trouvé confronté, d'une part, à des équipes jeunes n'ayant pas vécu la conception initiale de l'ATL2 mais néanmoins demandeuses d'un référentiel de définition outillé ; d'autre part, à des évolutions techniques interconnectant beaucoup plus les sous-systèmes entre eux et nécessitant de facto la présence d'un architecte ; et enfin à une contrainte coût/délai obligeant les industriels à converger rapidement entre eux sur une conception tout en minimisant le risque de régression sur les fonctions non touchées.

A l'instar des avions civils, la mise en place d'un plateau de travail multipartenaire et l'application d'un processus d'ingénierie système collaborative autour d'une base de données commune ont contribué grandement à la réussite du challenge. Avec pour principaux drivers :

- un accord préalable sur les données rendues visibles de tous (établir la zone de partage dans l'atelier système),
- l'attribution explicite d'un propriétaire pour chaque donnée (définir qui a le droit de modifier, indépendamment de qui a la visibilité),
- l'obligation de « réconcilier » les interfaces entre partenaires (vérifier explicitement que les sorties de l'un deviennent les entrées de l'autre)
- la mise en place de revues structurées selon des chaînes fonctionnelles, avec pour participants les différents industriels contributeurs.

8.2.3 Contraintes apportées par l'ingénierie collaborative pour les systémiers et sous-systémier

Du point de vue du systémier (sous-systémier), cette démarche l'ingénierie collaborative, si elle a des vertus, nécessite concrètement aujourd'hui d'adopter, sans négociation, les méthodes et outils du maître d'œuvre. Une conséquence est qu'il faut alors, pour le systémier, effectuer deux fois les activités de gestion de configuration, dans la plateforme commune et dans la sienne. Se pose aussi la question du maintien ou non de cette plateforme collaborative en vie série.

Recommandations :

➔ **R8.2.1 :** Afin de mettre en place une démarche collaborative, il est recommandé de travailler ensemble au niveau des processus, afin d'acquérir une compréhension commune (harmonisation du vocabulaire), avant de vouloir harmoniser ces processus et d'échanger méthodes et outils.

➔ **R8.2.2 :** Mettre à profit la phase d'architecture, afin de mettre en place les processus d'ingénierie collaborative, ainsi que les méthodes et outils associés. Bien le refléter dans les contrats. Afin d'y parvenir, il peut être utile de faire un mapping complet des méthodes et outils de chaque partie prenante, avant de statuer sur ce qu'on échange et en vue de quelle finalité.

8.3 R&T

8.3.1 Projet ISC2 : Projet Collaboratif des Systèmes Complexes (ISC2) de System X

L'extrême hétérogénéité des besoins et des contraintes impactant la définition d'un système conduit en pratique chaque partenaire industriel à définir des solutions d'ingénierie au cas par cas. Une conséquence de cette situation est la prédominance de solutions d'ingénierie ad hoc et d'outils de spécifications totalement informels qui ne permettent pas une fluidification optimale des échanges. Cette problématique d'autant plus importante dans le cas de transferts de responsabilité entre MOA et MOE.

L'objectif du projet ISC, dont les travaux sont réalisés par l'Institut de Recherche Technologique SystemX, est de faciliter la collaboration entre les parties prenantes d'un projet (différence entre les métiers, cycles de vie, environnement de développement, zones géographiques…) pour assurer la cohérence globale et l'efficience du système.

Le projet ISC met en œuvre de nouvelles pratiques d'ingénierie collaborative pour permettre :

- à l'ingénierie dirigée par les modèles de passer à l'échelle
- la mise en place d'une entreprise étendue

Cinq thématiques sont traitées :

- Ingénierie des modèles et collaboration : fédération de modèles, exposition contrôlée d'éléments de modèles, cohérence des modèles fédérés, traçabilité, synchronisation et réconciliation de modèles
- Evaluation d'architectures : analyse, vérification et optimisation d'architectures
- Prise de décision: Modèles de décision, hypothèses et argumentation
- Co-simulation
- Réutilisation d'architecture, de modèles et de composants.

L'utilisation d'une plateforme partagée d'évaluation permet de supporter les processus collaboratifs innovants

Projet lancé en 2015 en partenariat entre l'IRT SystemX et Dassault Aviation, DCNS, la DGA, et Thales.

8.3.2 Projet MOISE de l'IRT Saint-Exupéry

8.3.2.1 Introduction

Le projet MOISE (MOdels and Information Sharing for System engineering in Extended entreprise) est un projet de R&T géré et financé par l'IRT Saint-Exupéry à Toulouse (nous ne reviendrons pas ici sur le mode de financement des IRT). De nombreuses entreprises, notamment du secteur aérospatial, participent au projet, assurant ainsi la pertinence des sorties obtenues.

MOISE traite de l'Ingénierie System Orientée Modèles (Model Based System Engineering en anglais) et spécifiquement de l'ingénierie collaborative dans la partie amont du développement.

MOISE s'applique à identifier et définir, à partir de méthodes et outils existants, des moyens de partage de modèles en entreprise étendue. Il ne s'agit donc plus d'échanger des données (ici des modèles), mais de les partager.

8.3.2.2 Objectifs du projet

Consacré à l'ingénierie collaborative dédiée modèles, le projet MOISE traite de la partie amont du cycle de développement. Il inclut l'ingénierie des exigences, la définition et la vérification de l'architecture système, jusqu'à la spécification détaillée des équipements. Le projet couvre donc le « pourquoi », le « quoi » et le « comment ».

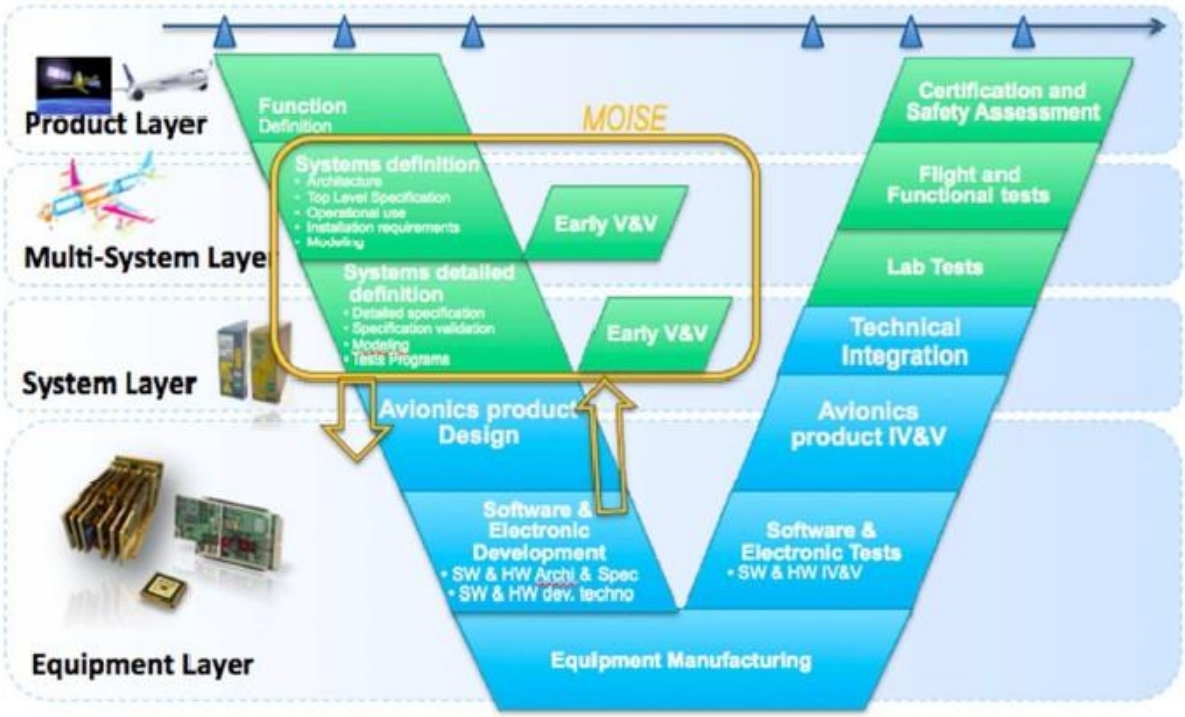


Schéma 8.1 : Description du projet MOISE (courtoisie Frédéric Paci)

L'architecture du système, telle que définie dans le cadre du projet MOISE, consiste en l'ensemble des décisions de conception en interaction avec les différents métiers, mais ne couvrent en aucun cas les travaux spécifiques à chacun. L'architecture du système devant servir de support aux décisions, elle doit permettre des analyses prenant en compte les données de ces différents métiers. Pour supporter cela, le projet MOISE utilise la notion de « point de vue » qui devient ainsi fondamentale.

Le projet MOISE implique des acteurs de divers secteurs d'activité. L'ambition est d'aboutir à une standardisation des échanges de données d'ingénierie dans un contexte d'évolution des standards de certification (ARP4754A, ECSS, ISO26262…), en tirant pleinement profit des possibilités offertes par l'ingénierie des systèmes basée modèles.

Pour adresser les enjeux économiques de maîtrise des coûts et délais, le projet MOISE vise à étudier l'introduction progressive de techniques de formalisation interopérables concernant les exigences et l'architecture de systèmes tout au long du cycle de développement.

Pour les membres industriels participant au projet il est essentiel de disposer de méthodes, outils et plateforme d'ingénierie systèmes collaborative de référence.

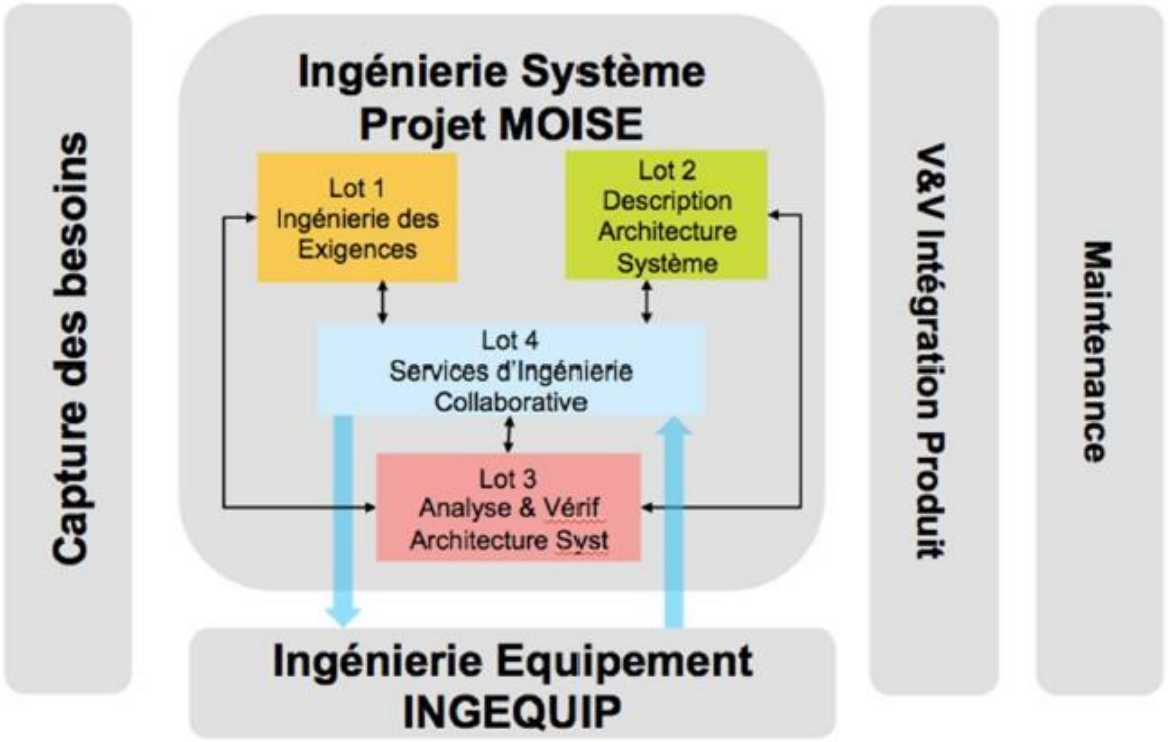
8.3.2.2.1 Verrous technologiques

Cinq verrous ont été identifiés. Il a été déterminé que l'atteinte des objectifs du projet MOISE était conditionnée par l'ouverture des cinq verrous suivants :

- **V1 :** Cohabitation d'exigences textuelles et modélisées dans le processus d'ingénierie des exigences – TRL2 vers TRL4
- **V2 :** Définition et utilisation de points de vue sur une architecture globale (fonctionnelle et physique) pour formaliser les exigences, en particulier les exigences non fonctionnelles – TRL3 vers TRL5
- **V3 :** Approche collaborative dans la construction des modèles d'architecture en respect des recommandations des autorités de certification et de la confidentialité des acteurs de l'entreprise étendue – TRL2 vers TRL4
- **V4 :** Multi modèles, multi formats (architectures issues d'outils différents), multi points de vue : comportemental - synchrone versus asynchrone, temporel/temporisé - ordonnancement, performance, modèles métier (masse, coût, énergie, …). – TRL3 vers TRL5
- **V5 :** Problème de passage à l'échelle dans le processus (prendre en compte l'ensemble des acteurs de l'entreprise étendue, éviter les ruptures liées au changement de société) et dans le grand volume de données à traiter qui va être partagé au niveau de l'architecture via les modèles. – TRL3 vers TRL4

8.3.2.2.2 Lotissement

Pour clarifier l'organisation du projet et en faciliter la gestion, il a été divisé en quatre lots :



- **Lot 1 : Ingénierie des exigences**
- **Lot 2 : Description d'architecture**
- **Lot 3 : Analyse, vérification et validation d'architecture**
- **Lot 4 : Infrastructures de services collaboratifs**

Schéma 8.2 : Lotissement du projet MOISE

8.3.2.2.3 Résultats attendus :

- Des guides méthodologiques de modélisation et d'analyse, des propriétés à vérifier/concepts d'architecture/patrons génériques, des bibliothèques ou canevas de description de processus d'ingénierie, des règles et des métriques associés à un processus d'ingénierie collaborative basé sur l'utilisation de modèles,

- L'identification des éléments caractéristiques des modèles d'architecture et simulation permettant des échanges entre métiers, disciplines et acteurs de l'entreprise étendue, dans le but de définir un (ou plusieurs) standard(s) d'échanges.

- Un ensemble de maquettes d'outils logiciels intégrés à la plateforme technique de l'IRT, permettant de démontrer la faisabilité des concepts et méthodes précédents, sur des cas d'utilisation industriels et un cas d'utilisation commun.

8.4 LA PROPRIETE INTELLECTUELLE DANS L'INGENIERIE COLABORATIVE

Bien que les avantages de l'ingénierie collaborative soient multiples, tel que la réduction du temps de développement en réduisant les erreurs et les itérations, l'intégration de plusieurs métiers et l'amélioration des échanges de données techniques, ce concept présente quelques limitations notamment en terme de la gestion de la propriété intellectuelle.

D'après une étude mené par PwC Innovation et Performance réalisée à la demande de l'Observatoire de la propriété intellectuelle de l'INPI (Institut National de la Propriété Industrielle), une démarche de l'ingénierie collaborative soulève pour les différents partenaires plusieurs défis clés liés à la propriété intellectuelle (également notée PI), parmi lesquels :

- le périmètre de la collaboration,
- La gestion du savoir-faire et les droits de PI antérieurs au projet,
- l'attribution aux partenaires de la PI issue de la collaboration,
- la réparation de la propriété et l'exploitation de la PI générée par le projet.

Afin de mieux appréhender cette problématique, il est recommandé de :

- Intégrer la gestion de la propriété intellectuelle au cœur du processus de développement : La construction d'un partenariat se déroule nécessairement en plusieurs étapes, depuis l'identification des thèmes de collaboration jusqu'à la définition du cadre de commercialisation des résultats : dans ces conditions, généralement, plusieurs accords successifs sont négociés. Une bonne gestion de la PI suppose donc de définir à quel moment tel ou tel aspect (confidentialité, exploitation…) doit être traité et quelles sont les compétences, notamment juridiques, à mobiliser. La formalisation de tels processus contribue à rendre plus efficace le montage de projets collaboratifs,

- Définir un modèle de valorisation de la propriété intellectuelle adapté aux enjeux de la collaboration : Les questions de propriété et surtout d'exploitation sont au cœur des enjeux de PI, dans le cadre de partenariats. Une définition claire des objectifs de la collaboration est un préalable indispensable à la négociation des droits correspondants. Le choix du mode d'exploitation en découle en partie : plusieurs modèles sont envisageables, une certaine souplesse est possible, l'enjeu pour les partenaires étant de trouver un compromis respectant les intérêts de chacun,

- Développer une culture interne de la propriété intellectuelle : Si la PI est majoritairement perçue comme un enjeu majeur, la « culture PI » n'est pas encore suffisamment diffusée au sein des organisations. Bien entendu, cet enjeu doit être décliné de façon différenciée selon la taille de l'entité, l'organisation et les moyens. Les boîtes à outils existent, qu'il s'agisse de formation, de dispositifs d'incitation, d'outils de pilotage…, mais une plus large diffusion et un meilleur partage d'expérience seraient souhaitables.

9. MBSE, ET SIMULATION.

9.1 L'EXPERIENCE DE THALES DANS LE MBSE

Ce retour d'expérience décrit comment la modélisation et la simulation ont été déployées chez Thales dans un projet destiné au marché avionique commercial, pour réaliser le processus d'ingénierie des exigences.

> "Le Model-based systems engineering (MBSE) est l'application formalisée de modélisation supportant les activités de spécifications des exigences système, de conception, d'analyse, de vérification et de validation commençant dès la phase de conception et se poursuivant pendant le développement et jusque loin dans les phases du cycle de vie."
> *"Model-based systems engineering (MBSE) is the formalized application of modelling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases."*
> INCOSE SE Vision 2020 (INCOSE-TP-2004-004-02), Sept 2007

Depuis près de 10 ans, Thales s'est engagé dans la voie du Model-based systems engineering (MBSE). Après des campagnes d'évaluations, au travers de projets pilote et d'essais comparatifs, une méthode, appelée ARCADIA, a été développée ainsi qu'un outil de modélisation, Capella, mettant en œuvre cette méthode[63].

Le projet décrit ci-après concerne:

- La mise à niveau d'un avion par l'ajout de nouvelles capacités opérationnelles exigées par l'Organisation de l'Aviation Civile Internationale (OACI) pour développer des procédures d'approche aux instruments des aéroports,

- La capture et la validation des exigences au sens de la norme SAE ARP4754A/ED-79A : ce retour d'expérience met l'accent sur la capture du besoin opérationnel et sur la formalisation de l'analyse du système au moyen d'une validation au plus tôt (early validation) basée sur la modélisation et la simulation.

---

[63] Nota : *Pour obtenir de plus amples informations sur ARCADIA et Capella, vous pouvez visiter le site web PolarSys* https://www.polarsys.org/node/236.

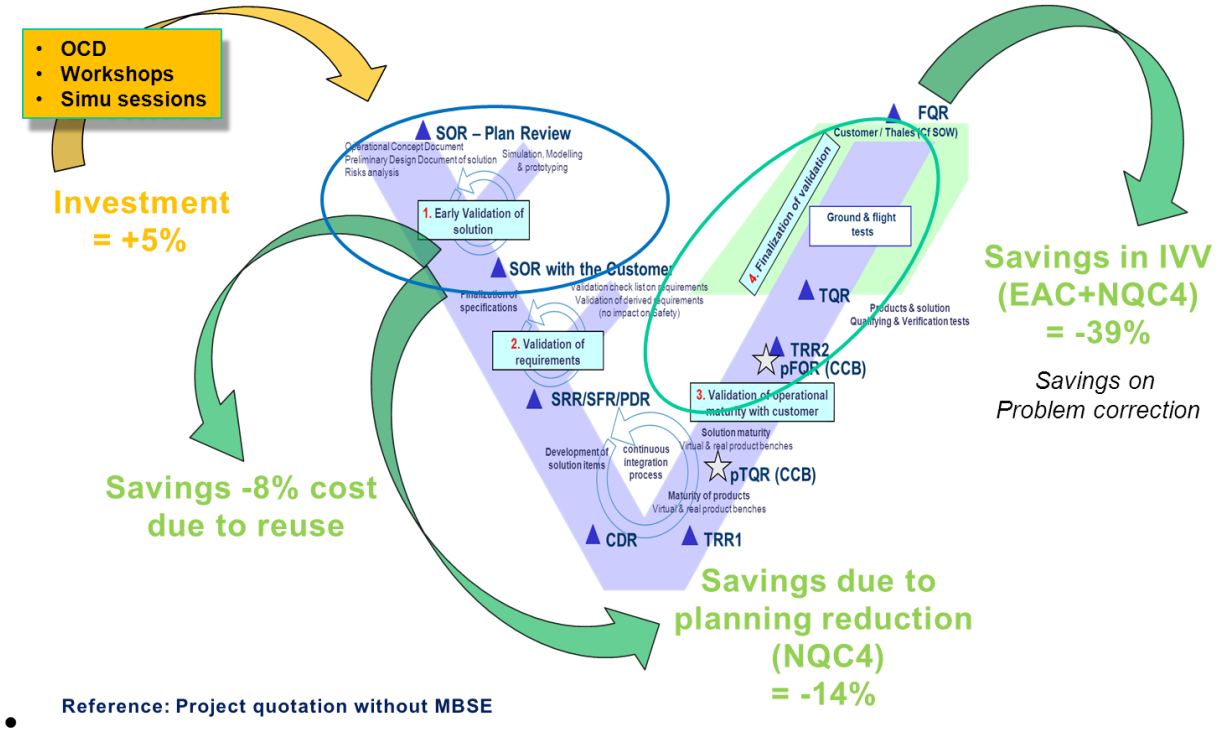


Figure 9.1 : Economies réalisées grâce à la Validation au plus tôt

Avant d'entrer dans des détails méthodologiques, nous voudrions mettre en avant les bénéfices, d'un point de vue financier, d'adopter une validation au plus tôt (Figure 9.1). L'investissement fait dans les phases amont a été significativement rentabilisé dans les phases aval. Notre objectif final étant d'éviter les reprises dans la phase de développement (rework) soumise à l'assurance produit et à la certification; et dont les coûts dus à ces reprises sont élevés dans un contexte de certification. Cet objectif a pu être atteint grâce à une meilleure compréhension des besoins opérationnels et un dérisquage de la solution technique par une approche de co-ingénierie impliquant aussi bien l'ensemble de nos équipes d'ingénierie que les représentants du Client et de l'organisme de certification.

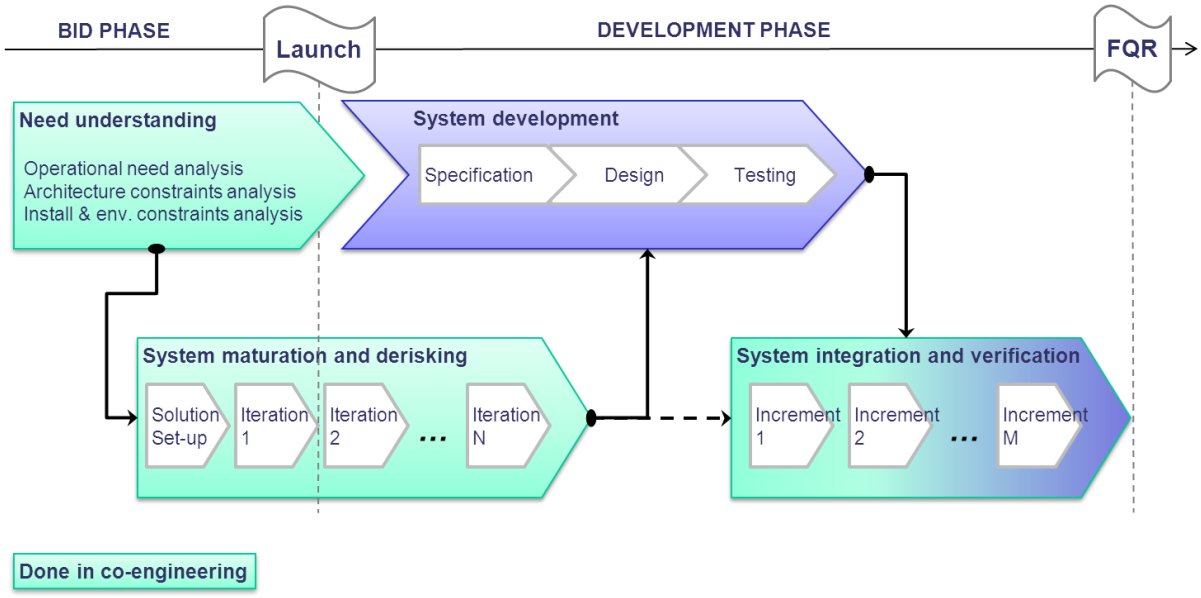


Figure 9.2 : Processus d'ingénierie

Notre processus d'ingénierie comprend les activités suivantes (Figure 9.2):

- L'activité de « compréhension des besoins » qui précise les besoins opérationnels. Les scénarios opérationnels, qui seront exécutés lors de la vérification du système, sont préalablement éprouvés dans un environnement virtuel (simulation) afin d'être agréés par le Client et capturés dans des diagrammes de séquence (modélisation).

- L'activité de « Levée de risques et maturité du Système » doit permettre de stabiliser les spécifications du système. Les architectures système candidates sont évaluées par rapport aux exigences Client et à nos contraintes industrielles. L'utilisation de points de vue technologie multiples (au sens de l'ISO/IEC/IEEE-42010) permet de développer et d'évaluer ces architectures basées sur des modèles de données (modélisation). Typiquement, l'analyse de ces points de vue est effectuée pour l'évaluation de la sûreté de fonctionnement (safety) et pour l'allocation des ressources des calculateurs. Une fois l'architecture optimum choisie, le résultat de cette activité de dérisquage est un ensemble d'exigences de safety et d'exigences fonctionnelles qui ont été validées sur un banc d'intégration système virtuel (simulation).

- Les activités de développement, d'intégration et de vérification du Système sont conduites avec une approche plus classique. Les modèles précédents, aussi appelés modèles de spécification dans la terminologie aérospatiale, sont maintenus, tout comme les moyens de simulation associés, en vue d'une analyse d'impact sur des changements du système ou de l'avion. Les modèles de conception tels que définis par la RTCA DO-331 ne seront pas détaillés ci-après.

MODÈLE : une représentation abstraite d'un ensemble donné des aspects d'un système/fonction/composant qui est utilisé pour l'analyse, la simulation et/ou la génération de code et qui a une syntaxe et une sémantique bien définies et non-équivoques.
MODEL: An abstract representation of a given set of aspects of a system/function/item that is used for analysis, simulation and/or code generation and that has an unambiguous, well defined syntax and semantics.

ARP4754A/ED-79A

Avant de discuter comment les modèles peuvent être utilisés, il est utile d'introduire les différents types de modèles que nous utilisons :

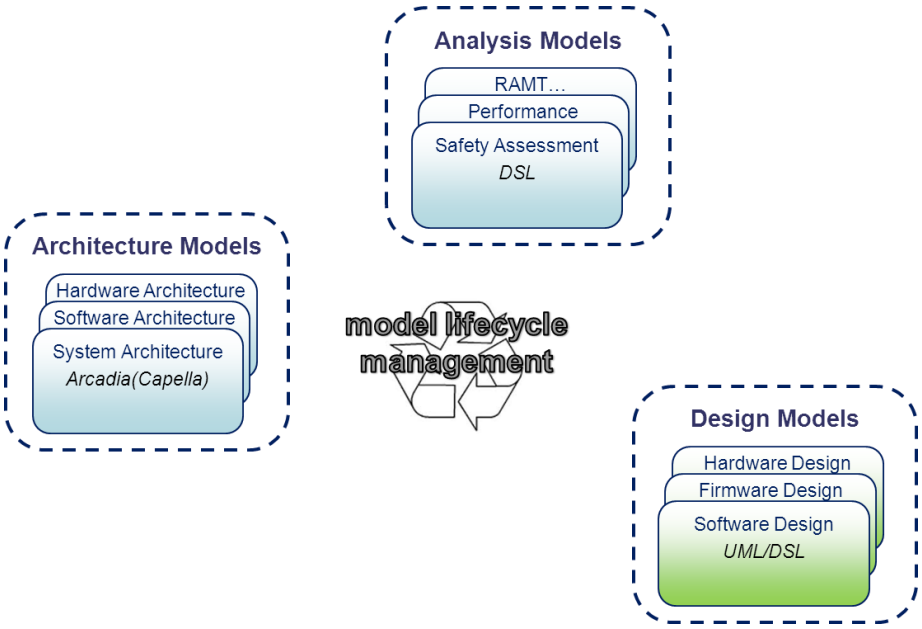


Figure 9.3 : Typologie de modèles

Les types de modèles suivants sont nécessaires pour atteindre les objectifs d'une approche MBSE (Figure 9.3) :

- Les modèles d'architecture qui structurent la Solution incluant le système d'intérêt (system-of-interest) et les systèmes contributeurs (enabling systems). Ils traitent des concepts et des principes du domaine qui sont hérités des meilleures pratiques. Pour le projet décrit ici, ils sont développés avec la méthode ARCADIA et l'outil de modélisation Capella.

- Les modèles d'analyse qui supportent les ingénieries de spécialité telles que la safety, la sécurité (security), la puissance de calcul et la maintenance. Ils utilisent des langages spécifiques au domaine (DSL – Domain Specific Language) comme AltaRica pour l'évaluation de la safety.

- Les modèles de conception qui fournissent une description détaillée de la façon dont les éléments du Système sont mis en œuvre. À titre d'exemple, dans le domaine logiciel, le langage UML est largement utilisé pour la génération du code et la maintenance. Les DSL sont aussi très appréciés.

La suite de ce retour d'expérience ne traite que des modèles d'architecture.

Actuellement, la plupart des exigences sont spécifiées en langage naturel (textuel). Cela devrait perdurer tant (i) que la syntaxe de modélisation ne permet pas de capturer les besoins avec le bon niveau de sémantique et (ii) qu'une telle syntaxe et sémantique ne puissent être formellement partagées qu'entre utilisateurs avertis et compétents.

En attendant, on peut tirer profit des techniques de modélisation pour structurer les exigences et naviguer entre spécification, architecture et conception.

À moyen et long terme, notre ambition est toujours d'élargir le périmètre du MBSE à l'ensemble du processus d'ingénierie des exigences. Ceci exige d'améliorer la sémantique des langages de modélisation de système, ou de compléter les notations semi-formelles avec des parties de spécification formellement définies. Ceci exige aussi de meilleures façons d'identifier et de gérer les exigences dans un modèle système.

En conclusion, les modèles d'architecture sont plus utilisés aujourd'hui en support du processus d'ingénierie des exigences que comme spécifications formelles. Procéder ainsi est déjà un grand pas (progrès) comparé à l'approche textuelle et documentaire classique.

10. PARTICULARITES LIEES AUX SYSTEMES DE SYSTEMES

10.1 SYSTEME DE SYSTEMES: DEFINITION ET CARACTERISATION

Un système de systèmes résulte de l'intégration d'un nombre fini d'éléments, systèmes indépendants et opérables en tant que tels, mis en relation sur une période de temps donnée pour atteindre un objectif particulier[64].

Au-delà de cette définition, il est admis qu'un système de systèmes présente les propriétés suivantes, connues sous le nom de critères de Maier[65] :

- indépendance opérationnelle des éléments constituants (chaque système possède son cadre d'utilisation propre),
- indépendance managériale des éléments constituants (acquisitions diverses, utilisations indépendantes),
- développement incrémental sur la base des éléments constituants (définition et conception évolutives),
- distribution géographique des éléments constituants,
- comportement émergent résultant de la mise en relation des éléments constituants.

Un système de systèmes délivre ainsi des capacités qui lui sont propres, par la collaboration de systèmes autonomes mais en interaction. Ce regroupement de systèmes peut inclure aussi bien des systèmes existants, que des systèmes partiellement développés, voire même à développer.

Du point de vue de l'ingénierie des systèmes, les systèmes isolés tout comme les systèmes de systèmes sont à considérer comme des systèmes, c'est-à-dire un ensemble de constituants, des relations et un « tout » qui surpasse la somme des constituants. En revanche, tous les systèmes ne sont pas des systèmes de systèmes, pour lesquels il s'agit de prévoir, analyser, organiser et intégrer les capacités individuelles d'un ensemble de systèmes - déjà en service, encore en développement, voire à développer - pour créer une capacité nouvelle du système de systèmes, plus large que la somme des capacités individuelles[66].

---

64 Nota : *D'après Jamshidi, 2009, 'System of systems engineering - innovations for the 21st century', J.Wiley & Sons*

65 Nota: *Maier, 1998, 'Architecting principles for systems-of-systems', Systems Engineering, Vol. 1, No. 4*

66 Nota: *D'après Department of Defense, October 14, 2004, 'System of Systems Engineering', Defense Acquisition Guidebook*

Les systèmes de systèmes prennent différentes formes. On identifie ainsi les systèmes de systèmes types[67] :

- Virtuels.
    - L'absence d'élément central de contrôle, de finalité globale prédéfinie, laisse la place à des comportements émergents de grande ampleur ;
    - par exemple : le Global Information Grid (GIG, initiative du Département de la Défense des Etats-Unis) ;
- Collaboratifs.
    - Les constituants interagissent de façon plus ou moins prévue pour remplir un objectif convenu ;
    - par exemple : internet et des communautés d'intérêt ;
- Contractualisés.
    - Les objectifs, les moyens consommés et le contrôle de la collaboration sont partagés, mais chaque constituant préserve son indépendance (propriété, objectifs propres, capacité d'évolution, financement…) ;
    - par exemple : système de défense anti-missile balistique ;
- Dirigés.
    - Le système de systèmes est constitué et mis en œuvre sur des objectifs spécifiques, y compris dans le long terme, par un donneur d'ordre identifié. Chaque constituant préserve sa capacité d'action propre, mais le cadre principal d'emploi est celui du système de systèmes constitué ;
    - par exemple : système de combat terrestre mettant en œuvre plusieurs véhicules , moyens de communication, et armes.

Il s'agit donc de travailler la maîtrise des capacités de niveau système de systèmes, tout en préservant l'autonomie technique et managériale des systèmes constituants.

---

[67] Nota : *Source MITRE, Systems Engineering Guide, 2014*

10.2 LE CONTEXTE. QUELQUES EXEMPLES DANS LE MONDE DE L'AERONAUTIQUE ET DE L'ESPACE

10.2.1 Le contexte

La notion de système de systèmes apparaît vers 1995, dans les domaines de la Défense (défense anti-missile, opérations interarmées), des technologies de l'information (Internet, systèmes bancaires réseau-centrés), ou encore du contrôle du transport aérien.

Depuis quelques années, sous le double effet des progrès des moyens de communication, qui facilitent la mise en relation des systèmes, et de la pression sociétale vers le développement durable, qui milite pour la réutilisation des moyens en place en même temps que pour l'optimisation globale des capacités, les initiatives en faveur des systèmes de système se multiplient, particulièrement en Europe.

Citons par exemple les initiatives de la Commission Européenne (FP7, projets 2011) DANSE Designing for Adaptability and evolutioN in System of systems Engineering, COMPASS Comprehensive Modelling for Advanced Systems of Systems, ROAD2SoS Roadmaps for System-of-Systems Engineering, T-AREA-SoS Trans-Atlantic Research and Education Agenda on Systems of Systems , dont un des objets est d'identifier les axes principaux de recherche.

10.2.2 Exemple des Opérations Aériennes, SESAR

Le projet de recherche SESAR, Single European Sky Air traffic management Research, volet technologique du Ciel Unique Européen lancé à l'initiative de la Commission européenne, vise quatre objectifs majeurs :

- restructurer l'espace aérien afin d'augmenter la capacité et d'améliorer l'efficacité globale du système de gestion du trafic aérien,
- accroître le niveau de sécurité d'un facteur 10 dans un contexte de doublement du trafic d'ici 20 ans,
- diminuer l'impact sur l'environnement de l'activité aérienne,
- développer l'efficacité économique du système.

Lancé en 2006, le programme SESAR est entré dans sa troisième phase : le déploiement, qui vise la mise en service progressive, entre 2015 et 2025, des éléments définis et développés dans les deux phases précédentes sur l'ensemble des acteurs du monde du trafic aérien, pour satisfaire six fonctionnalités majeures :

- Extended Arrival Management and Performance Based Navigation in high density TMAs,
- Airport Integration and Throughput,
- Flexible Airspace Management and Free Route,
- Network Collaborative Management,
- Initial Trajectory Information Sharing,
- Initial System Wide Information Management.

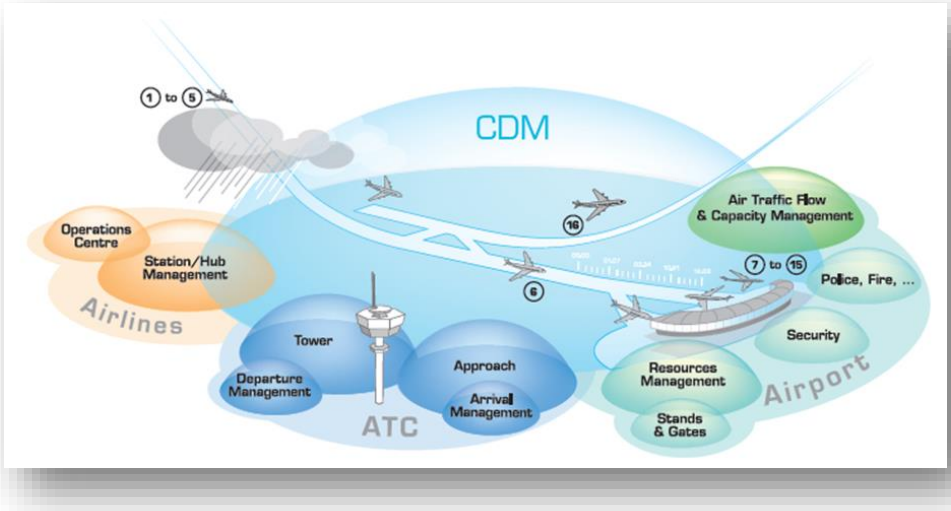


Figure 10.1 : Principaux systèmes et capacités du monde du trafic aérien.

Il s'agit bien de faire travailler plusieurs systèmes ensemble et d'obtenir une synergie vers des objectifs communs, objectifs capacitaires et/ou de performance.

10.2.3 Programme de défense développé en coopération européenne.

De nombreux programmes de défense sont développés en, coopération européenne, et ont vu la mise en place d'une entité transnationale agissant comme maître d'ouvrage.

Ainsi un même programme voit-il coopérer différents MoD, aux exigences parfois dissemblables, et une entité de gestion de projet, qu'il convient de gérer comme autant de parties prenantes (« stakeholders ») indépendantes.

Ces différents MoD devront eux-mêmes assurer l'insertion de ce même nouveau système en développement dans un ensemble de forces, et de concepts d'emploi qui peuvent être différents.

Dans un tel contexte, il est souvent difficile de hiérarchiser les exigences et les prises de décision. Une approche système de systèmes est bien adaptée pour conduire les analyses et guider le processus de développement.

10.2.4 Exemple de l'Observation de la Terre, Agence Spatiale Européenne

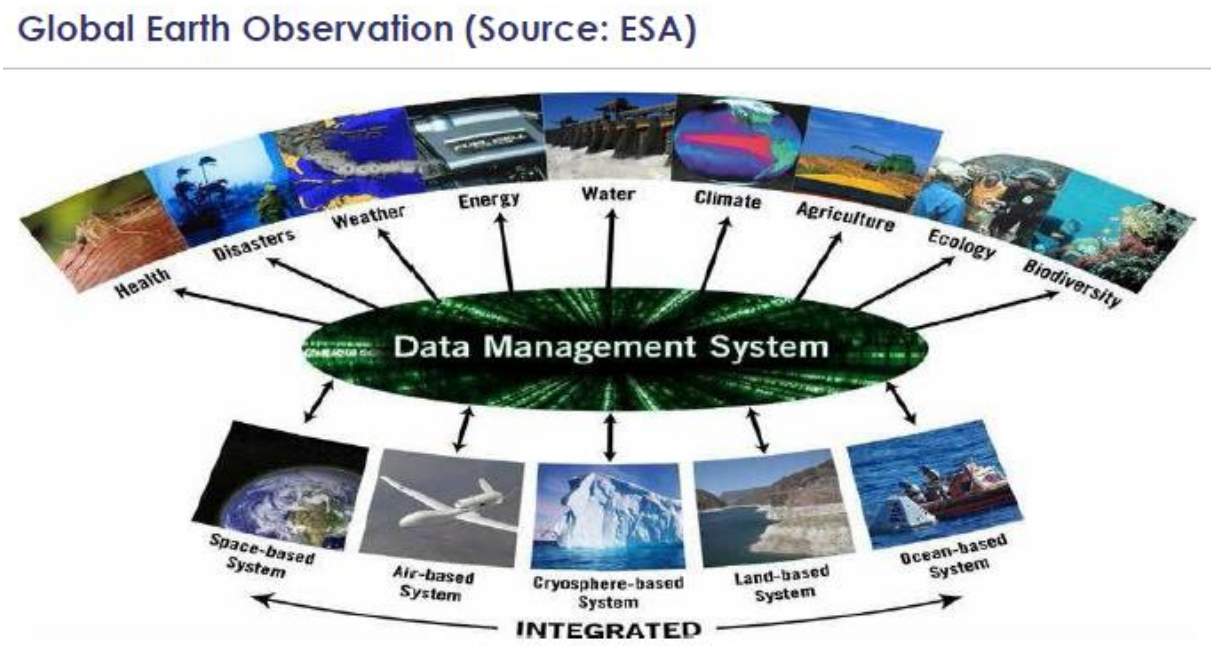


Figure 10.2 : Global Earth Observation System.

10.3 LES ENJEUX POUR LA DISCIPLINE INGENIERIE DES SYSTEMES

Dans le déploiement de la démarche d'Ingénierie des Systèmes, la première difficulté avec les systèmes de systèmes est perceptible dans la communauté des parties prenantes des systèmes constituants. Pour cette communauté, l'intégration dans un système de systèmes se matérialise par des contraintes et des obligations supplémentaires, de la complexité additionnelle. Ainsi, la participation à un système de systèmes est rarement vue comme une opportunité ![68]

La seconde difficulté réside dans l'énoncé même des objectifs de l'ingénierie. Il s'agit de changer le paradigme de l'ingénierie des systèmes traditionnelle, qui s'attache à construire le système adapté, pour construire une ingénierie de systèmes de systèmes, centrée sur la définition de la bonne combinaison de systèmes et leurs interactions pour satisfaire un ensemble de besoins changeants. Cela implique principalement :

- la prise en compte élargie de l'environnement de la solution, de façon à assurer une bonne compréhension mutuelle des enjeux (doctrine, concept d'opération, …) et des contextes par les parties prenantes,

- une orientation 'service' pour l'expression du concept d'opération et son instanciation sur les systèmes concernés.

Pour plus de détails, voici quelques différences clés entre système et système de systèmes dans leurs environnements [69] :

---

[68] Nota: *D'après Rebovich, G., (2009), Enterprise Systems of Systems*

[69] Nota : *Source MITRE, Systems Engineering Guide, 2014*

Contexte	Système	Système de systèmes
Management et Contexte		
Implication des parties prenantes	Un ensemble de parties prenantes clairement identifié	Plusieurs ensembles de parties prenantes, aux niveaux systèmes et système de systèmes, avec des intérêts et des priorités variées. Il peut arriver que certains décisionnaires n'aient pas d'intérêt dans le SdS
Gouvernance	Management de programme et budgets cohérents	Un niveau de complexité supplémentaire dû aux gestions de programmes et budgets à la fois pour le système de systèmes et les systèmes pris isolément. Le système de systèmes n'a pas 'autorité' sur les systèmes
Environnement Opérationnel		
Objectifs opérationnels	Conçu et développé pour satisfaire les objectifs opérationnels	Invoqué pour satisfaire une série d'objectifs opérationnels, en utilisant les systèmes dont les objectifs opérationnels ne sont pas nécessairement alignés sur ceux du système de systèmes
Réalisation		
Acquisition	En phase avec les jalons d'acquisition, les exigences documentées, le programme suit un plan d'ingénierie système	Un niveau de complexité supplémentaire dû aux multiples décalages des cycles de vie des systèmes impliqués (nouveau développement, en développement, ou déjà en place), de leurs jalons d'acquisition.
Tests et Evaluation	Les tests et l'évaluation du système sont en général réalisables	Réaliser les tests est plus complexe, car cela nécessite des points de synchronisation des systèmes à des stades de développement différents, met en jeu de nombreux éléments peu stables et peut avoir des conséquences inattendues
Ingénierie et Conception		
Périmètre et Interfaces	Se limite au périmètre du seul système	Se concentre sur l'identification des systèmes qui contribuent aux objectifs globaux et qui permettent les échanges de données, le contrôle, la réalisation des fonctions du système de systèmes, tout en préservant les capacités des systèmes individuels
Performances et Comportement	Performances du système pour satisfaire les objectifs spécifiés	Performance du système de systèmes pour satisfaire les objectifs opérationnels globaux tout en ménageant l'atteinte des objectifs de chaque système

Tableau 10.1 : Différences clés entre système et système de systèmes dans leurs environnements.

L'approche d'ingénierie SdS diffère donc de l'approche d'ingénierie des systèmes habituelle. Elle s'appuie sur les systèmes candidats à la constitution du SdS et doit contraindre leur développement ou évolutions, dans l'objectif de réaliser les capacités attendues du système de systèmes. Elle consiste essentiellement en :

- la définition de l'interopérabilité des systèmes (règles et moyens),
- la négociation des évolutions des systèmes constituants tout au long de leur cycle de vie, en faveur d'une optimisation des performances du système de systèmes,
- une bonne connaissance des systèmes constituants et de leur usage,
- la vérification et la validation de la réalisation des capacités requises durant le développement,
- la vérification et la validation régulières de la réalisation de ces capacités durant les phases opérationnelles malgré les évolutions des systèmes constituants,
- des itérations pour ajuster le besoin, les capacités fournies, le processus.

10.4 STANDARDS

La dernière édition de la norme System Life Cycle Processes standard (ISO/IEC/IEEE 15288) adresse clairement la problématique des systèmes de systèmes : elle leur dédie une annexe (Annexe G) intitulée 'Application of system life cycle processes to a system of systems'. Y sont discutés les principaux points d'attention à apporter sur les processus d'ingénierie, en fonction de la catégorie de système de systèmes concernée (virtuel, collaboratif, contractualisé, dirigé).

De même, les standards ISO-IEC de la série 42xxx (en cours de rédaction pour les 42 020 'Architecture processes' et 42 030 'Architecture evaluation'), dédiée à l'architecture système, prennent soin de considérer les deux points de vue, système et système de systèmes.

10.5 LES RECOMMANDATIONS

Recommandations :

➔ **R10.1 :** Même s'il ne s'agit pas à proprement parler d'une recommandation, nous jugeons utile de rappeler que, au-delà de la maîtrise de la complexité l'approche SdS constitue un changement de paradigme : On est ainsi conduit à analyser la situation de chacune des parties prenantes et leurs interactions, sur des systèmes constituants aux cycle de vie indépendants et non nécessairement coordonnés, avant de pouvoir conduire une démarche de type analyse fonctionnelle et de capture des exigences. Ce paradigme Système de Systèmes fonctionne bien également pour traiter les systèmes complexes, même si tous les critères de Maier ne sont pas clairement satisfaits.

➔ **R10.2 :** Identifier clairement l'ensemble des parties prenantes, et leur rôle. Prendre en compte l'ensemble de leurs contraintes, qu'elles soient organisationnelles ou techniques, pour alimenter les études de compromis et les prises de décision.

➔ **R10.3 :** Favoriser le travail collaboratif entre les parties prenantes, expliciter et capturer les données techniques et programmatiques (cadres d'architectures et modélisation).

➔ **R10.4 :** Identifier clairement les rôles d'architecte et/ou d'ingénieur système à chacun des niveaux système de systèmes et systèmes, expliciter les différences d'approches entre ces deux niveaux d'ingénierie.

➔ **R10.5:** Rechercher les compromis équilibrés entre ces deux niveaux.

➔ **R10.6 :** Rechercher les architectures ouvertes, favorisant l'usage de standards et un couplage dynamique des systèmes.

11. PROCESSUS, METHODES ET OUTILS POUR LA GESTION DES EVOLUTIONS ET FAMILLES DE PRODUITS

11.1 LA VOLONTE DE STANDARDISATION OU DE REUTILISATION ("REUSE") : REUTILISATION « OPPORTUNISTE » ET APPROCHE LIGNE DE PRODUIT

Le besoin haut niveau est de fournir des systèmes ou équipements disposant de fonctionnalités et performances maîtrisées, pour des coûts de plus en plus bas, offrant une plus grande fiabilité, le tout démontré dans un délai de mise à disposition de plus en plus court.

Il convient de préciser que la réutilisation ne se limite pas au système ou équipement seul, mais à l'ensemble des moyens mis en œuvre dans le développement d'origine, tels que la documentation, les processus, les méthodes, les outils ou modèles, les moyens de fabrication, les formations, et le personnel de l'entreprise, etc. Cela doit ainsi permettre de réduire, pour le nouveau projet, les efforts de développement, d'industrialisation, et de fabrication, ainsi que les risques d'anomalie ou de non-conformité.

Deux stratégies différentes coexistent pour l'atteinte de cet objectif :

- La réutilisation (re-use) 'opportuniste' qui consiste à s'approprier un existant pour un nouveau projet,

- l'approche ligne de produit, qui organise la dérivation à partir d'une ligne de développement produit, de l'instance du produit adaptée à un nouveau projet.

La première approche consiste à accepter le risque de déviations techniques (voire certaines limitations opérationnelles). Les notions de déviations permanentes ou de régressions sont étudiées pour être jugées acceptables au regard du besoin d'un marché.

La seconde approche vise à promouvoir une amélioration, notion de "Product Improvement" apportant une vraie valeur ajoutée du produit à satisfaire un ou plusieurs besoins, dans une démarche rigoureuse QCDR (Qualité-Coût-Délai-Risques). L'aspect gain de coût peut être une résultante positive dès lors que la quantité d'équipements (OEM) fabriqués rejoint un modèle économique proche d'une "production en série" où les investissements industriels deviennent rentables sur le long terme et que les défauts de qualité et de fiabilité sont fortement réduits. Le gain économique s'inscrit dans une stratégie d'entreprise à long terme.

11.2 LA REUTILISATION « OPPORTUNISTE »

La notion de standardisation ou de "reuse" (réutilisation) repose sur l'idée d'utiliser les moyens ou éléments physiques (d'un système ou d'un équipement), développés lors de projets précédents, au profit d'un nouveau projet dans un but d'améliorer les caractéristiques de ce dernier en termes de coût et de planning.

Cette notion impose que le concept de réutilisation soit parfaitement maîtrisé et ne nécessite presque aucune activité de recherche et de développement.

Pour cela, il est nécessaire de considérer des prérequis ou recommandations pour garantir la réussite de la bonne application de ce type de "reuse" pour un développement donné de système ou d'équipement aéronautique ou spatial.

La réponse à ce besoin nécessite une investigation précise et rigoureuse du référentiel des exigences et des interfaces pour assurer la réussite du développement du système ou de l'équipement opérant dans un environnement différent de ceux initialement pris en compte.

Il est donc indispensable que le choix de la réutilisation, et de ses conséquences soient évalués au plus tôt dans le développement du nouveau projet. Cette phase doit être synchronisée avec la contractualisation du projet entre les parties prenantes, sous condition de convergence de choix de la réutilisation entre les différents niveaux d'exigences et de l'architecture système. La grande part de la validation de design par le client doit être acquise dès cette étape du projet.

Chez les systémiers et équipementiers de l'aéronautique civile, cette réutilisation est de plus en plus demandée par des programmes non européens, avec pour premier objectif des modèles économiques très agressifs imposant de très faibles coûts de développement et de faible prix de revient (RC – Recurring Cost) qui s'appuient sur des produits (concepts) plus ou moins anciens, mais tirant bénéfice d'un retour d'expérience en terme de fiabilité pour des conditions d'utilisation connues associées à des applications reconnues (porteurs Airbus ou Boeing).

Les hélicoptéristes en général et certains avionneurs régionaux fondent leurs nouveaux développements sur cette approche. Les programmes A320neo chez Airbus ou 737MAX chez Boeing illustrent aussi cette nouvelle approche du marché du monocouloir où la concurrence s'est accélérée entre le duopole Airbus-Boeing et les nouveaux entrants.

Une réutilisation réussie est dépendante du marché ou du programme sur lequel elle est décidée ; les facteurs clés sont une architecture figée, des communalités / compatibilités / interopérabilités identifiées entre les différentes applications et un processus suffisamment bien documenté. La condition préalable est que le personnel affecté à cette réutilisation connaisse le détail du produit ou de l'équipement et de l'application sur lequel elle est portée, disposant de la documentation de la conception à la qualification du produit lors de son(ses) développement(s) antérieur(s).

La difficulté de la réutilisation réside souvent dans la transposition des fonctions compatibles des interfaces entre produit ou équipement, système et avion (ex. : mécanique, connectique, liaison CAN, protocole de maintenance, …) pouvant conduire à des limitations au début du développement, lesquelles sont à analyser et à lever au cours du projet moyennant des investissements spécifiques.

Le fait de réutiliser un produit ne dispense en rien de refaire (ou a minima de revoir) le travail de spécification du produit intégré au système. Les exigences applicables au produit doivent correspondre exactement aux besoins connus du système, ou ceux-ci doivent être revus et renégociés, pour s'adapter au produit proposé, afin d'éviter des infaisabilités futures.

Recommandation R11.1 : En cas de réutilisation, la revalidation des exigences entre les différents niveaux de spécifications est impérative.

Si la validation des exigences de spécifications multi-niveaux n'est pas simplifiée avec la réutilisation, et n'offre donc pas d'économie en début de projet, une **réutilisation permet en revanche une vérification allégée des exigences** ce qui en fait l'essentiel des gains en développement. Il est devenu en effet admis de présenter aux autorités de certification une démonstration de conformité d'une solution de réutilisation, sur la base d'une **similarité ou d'une analyse** du produit d'origine dont la conformité fut démontrée par essai. La réduction du nombre d'essais dans la phase de vérification permet une économie significative sur les dépenses de développement et une réduction importante du cycle de développement.

Le **retour d'expérience** peut être aussi utilisé pour conforter l'acceptation des analyses par similarité et de fiabilité en complément des essais imposés pour une application donnée. La réutilisation peut être utile dans certains DAL lorsque la double vérification est requise. Le retour d'expérience est cité dans l'ED79/ARP4754A/ED79a comme élément possible de démonstration.

Recommandation R11.2 : Il est souhaitable de négocier en amont avec les autorités de certification, l'acceptabilité de preuves de vérifications, obtenues dans un autre contexte (autre programme, autre autorité de certification, …) dès lors qu'on peut démontrer que ces preuves sont couvrantes, vis-à-vis du besoin du programme en cours de certification.

Certains avionneurs dans leurs directives insistent sur l'intérêt de s'appuyer sur leur retour d'expérience (« best practices and lessons learnt »), comme support à la certification. Ceci est d'ailleurs attesté par l'ARP 4754A (chapitre 6.5.1, page 83 : « … Service history may be used to support certification of new/modified item or system… »).

Ainsi le retour d'expérience permet a posteriori d'étendre la durée de vie de produits ou d'équipements, et s'inscrit progressivement sur les programmes "Legacy" ou nouvelles générations bénéficiant des évolutions incrémentales (A320neo ou 737MAX). Par exemple, on peut dans certains cas se permettre d'étendre la durée de vie d'un équipement de 30 000 à 50 000 heures, sans qu'il y ait ni modification de sa définition, ni test de fatigue additionnel, sur la seule base d'une analyse du retour d'expérience.

Le bénéfice économique s'étend alors jusqu'aux compagnies aériennes qui améliorent leur rentabilité grâce, par exemple, aux intervalles augmentés de maintenance, aux réductions du nombre d'incidents en service critique (condition Aircraft On Ground – AOG).

11.3 LA DEMARCHE LIGNE DE PRODUITS

Beaucoup d'industriels ont déjà eu l'occasion d'appliquer des démarches locales de réutilisation.

Ces démarches devenant de plus en plus fréquentes, il est alors nécessaire de définir une véritable **stratégie d'entreprise** autour de la création de ligne de produits, **afin de répondre aux besoins des marchés.**

Le développement doit ainsi pouvoir s'appuyer sur une **plateforme de produits** qui offre des **configurations multiples** sur diverses applications, adaptées au besoin des marchés. Cette approche, la terminologie associée (parties fixes et variables, options et variantes par exemple), l'organisation et les processus, doivent faire l'objet de **plans de communication et de formation** dans l'entreprise, pour une large partie de ses métiers, pas seulement les métiers techniques mais en premier lieu les métiers du marketing, et également ceux de la vente, des achats, de l'industrialisation, et de la gestion de projets

A titre d'exemple, les équipementiers dans l'aéronautique civile développent de plus en plus des **jeux de spécifications génériques**[70] dans le but de répondre à plusieurs applications et de couvrir la majorité des environnements opérationnels connus. Ces **jeux de spécifications** intègrent les notions **d'enveloppe d'exigences fonctionnelles et d'enveloppe de contraintes**[71], associant aussi parfois le principe **d'exigences paramétrables** pour le systémier.

Le développement d'une ligne de produit est un **projet à part entière** qui impose certaines considérations.

L'approche ligne de produit s'inscrit dans une démarche d'amélioration du produit sur les aspects qualité et maturité tenant compte du retour d'expérience et de corrections réalisées dans le temps (modifications itératives dans un processus de développement continu ou d'amélioration continue).

Une ligne de produit, selon l'AFIS, est un ensemble de produits ayant des éléments communs tels que leur prise en compte dans une stratégie de développement globale va apporter des gains significatifs grâce à la capitalisation : réduction des coûts, réduction du temps de développement et du temps de test, augmentation de la qualité …

Réciproquement, afin de pouvoir s'adapter à une grande variété de besoins, les différents produits de la Ligne de Produits se distinguent par des caractéristiques variables (ou variabilités).

Les principes d'une organisation en ligne de produit ne sont pas détaillés dans ce rapport. Ils font l'objet d'un guide produit par l'AFIS : L'ingénierie Système d'une Ligne de Produits (éditions Cépaduès, sous la direction d'Alain Le Put).

---

70 Nota : *Jeux de spécifications génériques, parfois appelées « règles », chez certains industriels.*

71 Nota : *Aussi appelés « key design drivers »*

11.4 RECOMMANDATIONS COMMUNES AUX DEMARCHES DE REUTILISATION

Recommandations :

➔ **Recommandation R11.1 : En cas de réutilisation, la revalidation des exigences entre les différents niveaux de spécifications est impérative.**..

➔ **Recommandation R11.2 :** La mise en œuvre d'une réutilisation requiert au plus tôt une analyse détaillée des compatibilités / incompatibilités fonctionnelles. L'objectif principal est d'identifier toutes les limitations ou déviations possibles, de les **accepter ou de pouvoir les lever moyennant des investissements spécifiques**.

➔ **Recommandation R11.3[70] :** Afin de rester dans une approche « gagnant-gagnant », lorsqu'on effectue une analyse des exigences de haut niveau, il peut être fructueux de comparer et de partager, entre client et fournisseur(s), dès les phases amont, une solution conçue ad hoc pour répondre au besoin exprimé, une solution de réutilisation opportuniste, et une solution issue d'une ligne de produits existants (solution de type réutilisation ou « re-use »), plus attractive économiquement, même si elle répond de manière moins parfaite à ce besoin.

➔ **Recommandation R11.4 :** Il est souhaitable de négocier en amont avec les autorités de certification, l'acceptabilité de preuves de vérifications, obtenues dans un autre contexte (autre programme, autre autorité de certification, …) dès lors qu'on peut démontrer que ces preuves sont couvrantes, vis-à-vis du besoin du programme en cours de certification.

[72] Nota : *Cette recommandation a été remontée dans une recommandation "Top Ten » ([R10]).*

12. L'INGENIERIE DES SYSTEMES DANS LES ENTREPRISES AERONAUTIQUES, DE DEFENSE ET SPATIALES

12.1 ORGANISATION INTERNE

L'organisation de l'ingénierie doit prendre en compte trois dimensions et en organiser la gouvernance transverse, afin de maintenir la dynamique d'amélioration et la cohérence des moyens.

La première dimension concerne l'organisation des projets (travaux sur les Produits, Appels d'Offres, Programmes) qui concerne l'exécution des travaux, et met en place les postes clés de Management de Lots d'Ingénierie et d'Architecte Projet, en sus des ingénieurs projets et experts nécessaires à la tenue des performances (safety, security, facteurs humains, thermique, CEM, algorithmie, etc.)

La deuxième dimension concerne l'organisation de la performance des individus et des équipes, souvent identique à l'organisation hiérarchique des équipes. Cette dimension s'assure du déploiement des processus, méthodes et outils, de la formation, de l'allocation des individus aux équipes Projet. Elle s'assure également de la définition et de l'exécution des plans d'amélioration de la performance, en s'appuyant sur des mesures de performance et des analyses causales des difficultés rencontrées.

La troisième dimension est celle de l'organisation du support aux équipes afin de faciliter le déploiement des processus, méthodes et outils, et de fournir formation et accompagnement pour les Projets.

Dans les entreprises de taille moyenne à grande, ces trois organisations sont instanciées de multiples fois dans les domaines couverts par l'entreprise et la mise en place d'une gouvernance d'ensemble est nécessaire pour mettre de la cohérence dans les pratiques, éviter les duplications d'effort, faciliter les coopérations entre équipes et les mouvements de personnes.

Cette gouvernance s'applique sur au moins quatre axes :

- Le référentiel de l'entreprise en tant que processus, méthodes, outils ainsi qu'en terme de définition des rôles
- L'animation et la mise en cohérence des plans d'amélioration, afin de maintenir la dynamique du changement et de coordonner les grands thèmes de la transformation
- L'animation et la mise en cohérence des actions de R&T préparant les futures pratiques en évitant les divergences et les redondances
- La mise en place d'une autorité technique transverse, indépendante des axes Projets, et décisionnelle dans les phases clés de ces Projets, en particulier dans les Appels d'Offres et les investissements dans l'innovation.

Sachant que la performance vient avant tout de la qualité des individus, et de la capacité à développer une culture commune, il est recommandé de structurer l'analyse de la population en familles professionnelles et métiers clés dans les familles, grille support de l'analyse de l'évolution en responsabilité des individus dans ces familles, support de l'analyse de la mobilité, support de l'analyse des parcours de formation. Un référentiel de compétence mis en relation avec cette découpe et avec les plans de charge permet les analyses quantitatives et qualitatives d'évolution des populations d'ingénieurs.

Enfin, une politique de Certification peut-être mise en place (type INCOSE), qui offre la possibilité d'identifier une communauté de personnes particulièrement intéressées par les aspects processus et méthodes et de les faire rayonner dans l'entreprise afin d'aider à la mise en place des améliorations et du support.

12.1.1 Exemple chez un systémier aéronautique

Chez le systémier A, les organisations programmes / projets d'une part, et conception système d'autre part, sont intimement liées. En règle générale, chaque développement d'un système (entre 2 et 5 ans), se déroule au sein d'une organisation en plateau regroupant :

- Un responsable programme
- 1 équipe d'ingénieurs système pilotée par le chef de projet système, celui-ci occupant les rôles d'architecte / intégrateur, mais aussi d'animateur projet (objectifs Qualité / Coût / Délais)
- Des concepteurs équipements, qui sont également chefs de projet dans leur périmètre (planning et budget)
- 1 ingénieur en chef (Design Authority) en charge de la validation technique des revues et documents, de la maîtrise des risques techniques, et de la capitalisation. Cette responsabilité, qui ne correspond pas toujours à une activité à temps plein, appartient en général au département système de l'entreprise.

- Des métiers support (Safety, SW, simulations, vérification/qualification/essais, Assurance Qualité développement, …)

Cette organisation a le mérite d'optimiser les coûts, de responsabiliser les concepteurs, au détriment, parfois, d'un mélange des genres (conception technique <-> gestion de projet).

Une grande difficulté est également de dédier des ressources métiers aux projets R&T, ressources trop souvent absorbées par les projets en développement (non séparation des départements).

En termes de profil, les ingénieurs système ont en général exercé une spécialité au sein de projets (conception mécanique ou électronique, simulations, essais…), les plus expérimentés étant appelés à piloter un projet global. Il n'y a pas de réel cycle de formation ni habilitation, seulement des modules de formation internes accessibles à tous.

Les ingénieurs en chefs, eux, sont peu nombreux, ils ont au moins 15 ans d'expérience.

12.1.2 Exemples de Dassault Aviation

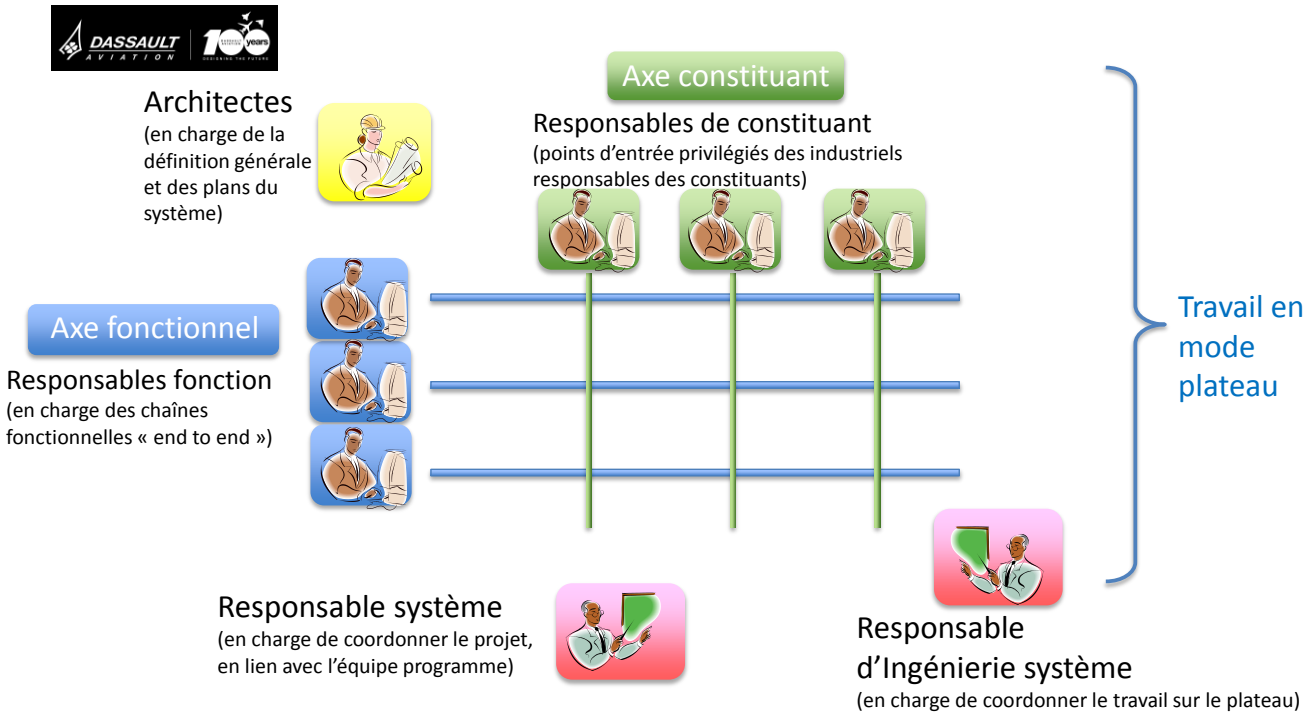


Figure 12.1 : Organisation du développement système chez Dassault

.

12.1.3 Recommandation

Recommandation **R12.1 :** L'ingénierie des systèmes introduit une vision transverse des processus et de l'entreprise, différente de celle portée par l'organisation traditionnelle en métiers (spécialités techniques, programmes, assurance qualité, industrialisation, production, et services). Afin d'être en mesure d'appréhender la complexité des systèmes futurs et d'être innovantes, nos sociétés se doivent de mettre en place de nouvelles organisations, permettant de déployer au mieux cette dimension transverse.

12.2 METIERS ET CARRIERES

Recommandation **R.12.2** : Identifier, formaliser, et maintenir les métiers de l'ingénierie des systèmes dans nos entreprises, et prévoir une gestion prévisionnelle des compétences associées (, reconnaissance, management des compétences, ..).

12.3 ETAT DES LIEUX FORMATIONS PRISES EN COMPTE PAR NOS ENTREPRISES

Recommandation **R.12.3** : Promouvoir la généralisation des formations d'ingénierie des systèmes dans l'ensemble des écoles d'ingénieurs et des universités.

Recommandation **R.12.4** : Généraliser les formations continues d'ingénierie des systèmes, au sein de nos entreprises.

Recommandation **R.12.5** : Si l'on confie des tâches d'ingénierie des systèmes à des acteurs de la supply chain, ou à des prestataires externes, s'assurer que ces sociétés assurent des formations d'ingénierie des systèmes à leur personnel, et qu'elles mettent à disposition du personnel convenablement formé.

12.4 POSITION VIS-A-VIS DES CERTIFICATIONS DE PERSONNES EN INGENIERIE DES SYSTEMES

L'intérêt de la certification est très variable suivant les types de business et les métiers. Il n'y a pas de tendance massive chez nos clients (DGA, ESA, …) et chez nos grands systémiers.

A contrario, pour certains clients, exports par exemple, la certification INCOSE peut être vue comme une garantie sur les personnes mises en face d'eux sur les contrats.

12.1 RECOMMANDATIONS SUR L'INGENIERIE DES SYSTEMES DANS LES ENTREPRISES AERONAUTIQUES, DE DEFENSE ET SPATIALES

Recommandations :

➔ **Recommandation R12.1 :** L'ingénierie des systèmes introduit une vision transverse des processus et de l'entreprise, différente de celle portée par l'organisation traditionnelle en métiers (spécialités techniques, programmes, assurance qualité, industrialisation, production, et services). Afin d'être en mesure d'appréhender la complexité des systèmes futurs et d'être innovantes, nos sociétés se doivent de mettre en place de nouvelles organisations, permettant de déployer au mieux cette dimension transverse.

➔ **Recommandation R12.2 :** Identifier, formaliser, et maintenir les métiers de l'ingénierie des systèmes dans nos entreprises, et prévoir une gestion prévisionnelle des compétences associées (, reconnaissance, management des compétences, ..).

➔ **Recommandation R12.3 :** Promouvoir la généralisation des formations d'ingénierie des systèmes dans l'ensemble des écoles d'ingénieurs et des universités.

➔ **Recommandation R12.4 :** Généraliser les formations continues d'ingénierie des systèmes, au sein de nos entreprises.

➔ **Recommandation R12.5 :** Si l'on confie des tâches d'ingénierie des systèmes à des acteurs de la supply chain, ou à des prestataires externes, s'assurer que ces sociétés assurent des formations d'ingénierie des systèmes à leur personnel, et qu'elles mettent à disposition du personnel convenablement formé.

13. SITUATION DE LA CONCURRENCE

13.1 FEEDBACK SUR LE RAPPORT DE LA FAA SUR LE BOEING 787

Le 31 janvier 2013, l'administration américaine fédérale de l'aéronautique (FAA - Federal Aviation Administration) et la division Avion commercial de Boeing ont établi un groupe d'audit commun (CSRT - Critical Systems Review Team) en charge de réaliser une revue détaillée des systèmes critiques du Boeing 787 tant sur les aspects conception que fabrication et assemblage de l'avion[73]. Le groupe d'audit a remis son rapport le 16 août 2013 qui a été rendu public et est accessible sur le site de la FAA.

- L'examen a démontré que le Dreamliner est sûr et est aussi fiable que d'autres avions Boeing lors de leur mise en service (sic).

- Le FAA a publié sept recommandations, quatre pour Boeing et trois pour elle-même visant à améliorer la manière de surveiller la conception et la fabrication de nouveaux avions.

- L'examen, conduit par les experts techniques de l'Administration Fédérale d'Aviation et de Boeing, valide le rôle de supervision joué par la FAA tout en notant que la FAA et Boeing n'ont pas exercé assez de contrôle de qualité sur les sous-traitants pendant le développement 787.

- Les changements recommandés pour Boeing se concentrent sur l'amélioration des flux d'information, des normes de conception, de l'expression des attentes entre la société et ses fournisseurs et la nécessité de rendre plus mature le processus de contrôle lors des jalons programme.

- La liste de points remontés par le groupe d'audit se rapporte en grande partie à la manière dont la chaîne d'approvisionnements du 787, fortement externalisée, a été contrôlée.

- Dans certains cas les exigences de conception n'ont pas été déclinées complétement et précisément depuis Boeing vers son fournisseur de premier niveau puis de celui-ci vers les fournisseurs de second niveau.

- Le rapport d'audit attire l'attention sur les problèmes de communication et de vérification tout au long de la chaine de fournisseurs.

- L'audit a identifié que l'ambiguïté de certaines formulations d'exigence, par Boeing, vers ses fournisseurs, a conduit ces fournisseurs à supposer, de façon incorrecte, qu'ils avaient répondu à toutes les exigences avec succès.

---

[73] Nota : *Cet audit a été décidé, antérieurement à la découverte des problèmes de batteries du 787. Cette initiative était consécutive au retard pris par Boeing, entre la certification et la mise en service du Dreamliner, et au questionnement sur cette certification FAA, qui en a découlé.*

14. RECOMMANDATIONS « TOP TEN »

Après classement et regroupement des recommandations, les dix recommandations « Top Ten » sont donc les suivantes, classées selon leur ordre d'importance perçue par les membres du groupe:

- **R1** : L'ingénierie des systèmes introduit une vision transverse des processus et de l'entreprise, qui **fédère les disciplines et les spécialités de l'organisation traditionnelle** (spécialités techniques, programmes, assurance qualité, industrialisation, production, achats, services, ...). Afin d'être en mesure d'appréhender la complexité des systèmes futurs et d'être innovantes, nos sociétés se doivent de mettre en place de nouvelles organisations, permettant de déployer au mieux cette dimension transverse.

- **R2** : Promouvoir l'utilisation du Model-Based System Engineering (MBSE), car c'est un des moyens les plus adaptés pour **partager et gérer de façon cohérente** : scenarii opérationnels, capacités, chaines fonctionnelles, propriétés non fonctionnelles, interfaces, etc. de manière efficace et non ambigüe (en particulier : éviter les ambigüités liées à une description uniquement textuelle).

- **R3** : **Mettre à profit les phases amont**, dont la phase d'architecture, **afin de mettre en place les processus d'ingénierie collaborative**, ainsi que les méthodes et outils associés. Bien le refléter dans les contrats. Afin d'y parvenir, il peut être utile de faire une mise en correspondance (« mapping ») complète des méthodes et outils de chaque partie prenante, avant de statuer sur ce qu'on échange, et en vue de quelle finalité.

- **R4** : **Utiliser au mieux la validation amont** (par exemple avec des outils de simulation technico-opérationnelle) pour, en particulier (liste non limitative), clarifier les besoins du client, définir au plus tôt les périmètres opérationnel, d'emploi et d'usage, réduire la complexité liée à la multiplicité des contraintes (en utilisant une approche par scénarii par exemple), et simplifier ainsi la vérification aval.

- **R5** : Identifier, formaliser, et **maintenir le métier de l'ingénierie des systèmes dans nos entreprises**, prévoir une gestion prévisionnelle des compétences associées (référentiel de connaissances, reconnaissance, management des compétences, recours aux normes, et système qualité, ...) et promouvoir les formations :
  - Dans l'ensemble des écoles d'ingénieurs et des universités,
  - Au sein de nos entreprises,
  - Parmi tous les acteurs de l'entreprise étendue (acteurs de la supply chain : fournisseurs et prestataires).
- **R6** : **Identifier** clairement l'ensemble des **parties prenantes, et leur rôle** en fonction de la phase du cycle de vie. Prendre en compte l'ensemble de leurs contraintes, qu'elles soient organisationnelles, techniques, ou autres (politiques, économiques, environnementales, sociétales, …), pour alimenter les études de compromis et les prises de décision.

- **R7** : **Définir**, partager, et négocier **la stratégie d'intégration, de vérification, et de validation**, dès les phases amont du cycle de développement, entre client et fournisseur. Ceci permet, entre autres, de mieux maitriser les risques et de réduire les coûts.

- **R8** : Mettre en place une **démarche collaborative**, au niveau de **l'entreprise étendue** ; en particulier (proposition non limitative) :

    - Partager et négocier, dès le début de l'avant-projet, conformément aux périmètres de responsabilité et processus de décision définis, les attendus en matière de processus d'ingénierie système collaborative (dont l'ingénierie des exigences), et de certification système. Les tracer dans le contrat. Prévoir explicitement de négocier au cours du projet les attendus, non encore mis en œuvre dans le contrat, qui peuvent apparaître.
    - Travailler ensemble au niveau des processus, afin d'acquérir une compréhension commune (harmonisation du vocabulaire, …). Une telle approche permettra de rendre compatibles les différentes méthodes et processus IS outillés des parties prenantes. L'ISO 15288 pourrait servir de standard de convergence.
    - Favoriser le travail collaboratif entre les parties prenantes, expliciter et capturer les données techniques et programmatiques (cadres d'architectures et modélisation).
    - Agréer, avant contractualisation, entre donneur d'ordre et fournisseur(s) les jalons de développement (revues et/ou « Maturity Gates »), les contenus fonctionnels des livrables, et leur jalonnement, en cohérence avec leur utilisation (système, équipement, logiciel). Telle fonction devant être disponible pour telle application (banc sol, banc volant, banc d'intégration, 1er vol…). Le traduire dans la négociation du contrat, en commun avionneur / plateformiste / donneur d'ordre - fournisseur (« avionneur – systémier »).

- **R9** : Mettre en place, conjointement avec les autorités de certification, une **réflexion visant à diminuer la documentation livrable** (suppression de la documentation livrable difficilement exploitable), et de remonter de manière plus simple les preuves nécessaires à la certification. Cette réflexion pourrait être portée dans un premier temps par un Groupe de Travail GIFAS, en lien avec l'EASA-FAA, et au besoin les autres autorités de certification (ministères de la défense européens, ou autres).

- **R10** : Afin de rester dans une approche « gagnant-gagnant », lorsqu'on effectue une analyse de la valeur des exigences de haut niveau, il peut être fructueux de comparer et de partager, entre client et fournisseur(s), une solution conçue ad hoc pour répondre au besoin exprimé, et une solution issue d'une **ligne de produits existants** (solution de type **réutilisation**) plus attractive économiquement, même si elle répond de manière moins parfaite à ce besoin.

15. RECOMMANDATIONS « DETAILLEES »

Voici la liste des 77 recommandations détaillées, exposées dans le corps du texte :

- Recommandation R2.9.1 : Malgré l'intérêt perçu sur la connexion entre la modélisation fonctionnelle et la modélisation physique, nous recommandons de bien réfléchir, au cas par cas, à la valeur ajoutée d'une telle connexion, la rentabilité de l'investissement, et la capacité de maintenir dans le temps une telle base de données intégrée.

- Recommandation R2.15.1 : L'ingénierie système en tant que spécialité est à développer. Même si des éléments existent dans nos entreprises, on se doit de renforcer la formation afin d'harmoniser le métier, et de fournir une compréhension commune du champ d'expertise, au sein d'une même entreprise.

- Recommandation R2.15.2 : Une formation type à l'ingénierie système pourrait être partagée entre les donneurs d'ordres (plateformistes), et les systémiers ou sous-systémiers, par exemple dans la perspective d'un projet en commun.

- Recommandation R4.9.1 : Soutenir les initiatives destinées à stabiliser le contexte normatif (cf. ISO 'Architecting Guidance' Study Group, NATO STO-CSO/IST Study …).

- Recommandation R4.9.2 : Promouvoir des initiatives destinées à améliorer l'interopérabilité entre les cadres d'architecture et les autres outils de l'ingénierie des système (en particulier dans l'approche Model-Based System Engineering),

- Recommandation R4.9.3 : Recommander/favoriser le développement de méthodes bien documentées (« modes d'emploi »), pour faciliter l'adoption des cadres d'architecture et guider leur adaptation aux besoins de chaque projet, y compris au-delà du domaine de la défense, car l'utilisation des cadres d'architecture nous semble un bon moyen pour caractériser, et capturer/éliciter les besoins des parties prenantes, pour des systèmes complexes (gestion du trafic aérien, insertion des drones, gestion de flottes, opération d'un système de lancement spatial, …).

- Recommandation R4.9.4 : Assurer la traçabilité/alignement des éléments capturés dans le cadre d'architecture, avec l'architecture technique et les exigences, ainsi que la gestion de leur co-évolution.

- Recommandation R4.10 : Créer, ou renforcer au niveau du GIFAS et/ou du BNAE, une structure centrale consacrée à l'analyse et à l'évolution des normes, permettant, d'obtenir une base de référence pour la conformité aux standards, normes, et documents normatifs en ingénierie système (ARP4754A/ED79, ISO/EN9100, RG Aero, …), pour application par les industriels français. Les missions de cette structure seraient, entre autres :
  - d'analyser l'impact des nouvelles normes, en ingénierie système (mais aussi au-delà),
  - de s'assurer, par analyse, qu'il n'y a pas de régression des normes,
  - de dé-risquer les pièges normatifs, notamment en provenance des Etats-Unis,
  - d'établir un dictionnaire « inter-normes »,
  - à la manière de nos concurrents non européens, d'être proactifs dans le processus d'évolution des normes / d'implémentation de nouvelles normes, afin de conserver ou d'améliorer notre avantage compétitif.

- Recommandation R5.2.2.1 : Systématiser l'analyse fonctionnelle, analyse qui doit être agréée entre le plateformiste / donneur d'ordre (e.g.: l'avionneur) et le fournisseur/sous-systémier (« systémier », en langage d'avionneur), si possible coréalisée en phase plateau (proposition ou PDR au plus tard). Cette analyse fonctionnelle, et les impacts dus aux modifications postérieures à la RDP/PDR devront être mis à jour autant que nécessaire, jusqu'à la fin du développement, voire même tout au long du cycle de vie du système.)

- Recommandation R5.2.2.2 : Lier les exigences soit aux fonctions soit aux interfaces qu'elles s'échangent, les prioriser en conséquence.

- Recommandation R5.3.1.1 : Promouvoir à tous les niveaux un processus visant à challenger les exigences, dans une perspective d'optimisation globale des systèmes, sur l'ensemble de leur chaîne de valeur.

- Recommandation R5.3.1.2 : Généraliser le principe d'une revue d'exigences de type SRR, au cours de laquelle on pourra acter, entre le client et le fournisseur, les éventuelles solutions alternatives proposées par le fournisseur, en lieu et place des exigences initialement demandées. On notera qu'une telle approche exige d'être innovant sur le plan contractuel.

- Recommandation R5.3.1.3 : Identifier (« taguer ») les exigences qui n'ont pas d'impacts sur les exigences de sécurité ou de certification et dont la gestion doit se faire hors référence ARP4754 car elles ne nécessitent pas le même niveau de documentation. Exemples :
  - Gérer les exigences « spécifiques » du produit selon l'arbre de décomposition produit (PBS)
  - Recommandation Gérer les exigences Processus & Projet selon le WBS

- Recommandation R5.3.1.4 : Rechercher le meilleur compromis entre les exigences exprimées en langage naturel, et celles faisant appel à d'autres moyens de spécification (modèles par exemple). Dans ce dernier cas, ne le faire que lorsque leur formalisme a été formellement établi auparavant et est non-ambigu.

- Recommandation R5.3.1.5 : Limiter et justifier les exigences décrivant des solutions plutôt que le besoin.

- Recommandation R5.3.1.6 : Assurer la bonne qualité rédactionnelle (syntaxique et sémantique) des exigences. Au besoin la contrôler a posteriori (par diffusion de bonnes pratiques, relectures ou utilisation d'outils.)

- Recommandation R5.3.1.7 : Renforcer les moyens (méthode, formation, outil,…) supportant l'activité de synthèse des exigences des parties prenantes pour couvrir les duplications et réduire les risques de contradictions.

- Recommandation R5.3.1.8 : Agréer une enveloppe/ plage de performance, plutôt qu'une valeur déterminée (notion de flexibilité).

- Recommandation R5.3.1.9 : Promouvoir la recherche d'opportunités, et valoriser les gains de performance, par rapport aux valeurs cibles, sous forme de primes (incentives).

- Recommandation R5.3.1.10 : Proposer des sujets de recherche permettant de comprendre/ modéliser la mécanique d'inflation des exigences en fonction de la complexité et définir les critères permettant d'identifier le nombre optimum de niveau d'ingénierie requis pour maîtriser la complexité.

- Recommandation R5.3.2.1 : Définir une réponse méthodologique graduée en fonction du risque permettant d'alléger ou de renforcer les processus d'Ingénierie des exigences et de V&V de façon cohérente pour le développement d'un produit complexe.

- Recommandation R5.3.3.1: Formaliser, dans les processus de développement des entreprises et les formations d'ingénierie des systèmes, le principe de développement incrémental, en s'appuyant sur une analyse fonctionnelle partagée entre les différents intervenants.

- Recommandation R5.3.3.2 : Associer à chaque exigence un critère de maturité permettant d'évaluer un risque d'instabilité.

- Recommandation R5.3.4.1 : Concevoir et mettre en place des formations / e-learning, et des « Engineering Procedures », partagées entre donneurs d'ordre et fournisseurs de tous rangs qui expliquent ce qui est attendu (en particulier au titre de l'ARP4754).

- Recommandation R5.3.4.2 : Partager et négocier, dès le début du projet les attendus en matière de processus d'ingénierie système (dont l'ingénierie des exigences), et de certification système. Prévoir explicitement de négocier au cours du projet les attendus qui peuvent apparaître.

- Recommandation R5.3.4.3 : Traiter toujours les ICD avec la même rigueur que les spécifications. Identifier, tracer, et valider les différentes exigences d'interface de toute nature : fonctionnelles, physiques, … nécessaires. Le planifier (au niveau d'un SOW par exemple), et le faire suffisamment en amont pour une approbation lors des jalons programmes appropriés (par exemple : à la PDR pour les ICD fonctionnels, à la CDR pour les ICD de câblage, …)

- Recommandation R5.3.4.4 : Formaliser et partager les modèles de données associés à chaque interface. En assurer la cohérence, tout au long des développements et du cycle de vie des produits (en particulier : gestion en configuration).

- Recommandation R5.3.4.5 : Promouvoir l'utilisation du Model Based System Engineering, car c'est un des moyens les plus adaptés pour gérer les interfaces de manière efficace et non ambigüe (en particulier : éviter les ambigüités liées à une description textuelle).

- Recommandation R5.3.4.6 : Définir dès le début du projet, les périmètres de responsabilité et de délégation, les pratiques industrielles adaptées, et les jalonnements/synchronisations/réconciliations à appliquer, en matière de gestion des exigences et de contrôle des interfaces, tenant compte des risques identifiés, de la maturité avérée du fournisseur, et du niveau de criticité des éléments sous-traités. Ceci peut d'ailleurs se généraliser à l'ensemble du périmètre Ingénierie des Systèmes.

- Recommandation R5.3.4.7 : Mettre en place, pour l'ARP 4754A et la DO 178 / DO 254, un système d'agrément et de qualification des processus de type DOA / DOID, qui repose sur des critères objectifs, et régulièrement enquêtés/évalués.

- Recommandation R5.3.4.8 : Etablir en commun entre les industriels, le jalon contractuel à partir duquel il convient de gérer les modifications au travers d'un processus rigoureux.

  Nota : Cette recommandation s'applique aussi bien au cas de développement hardware classique (type cycle en V, « document centric ») qu'aux développements dans des technologies telles que les technologies de l'information ou les télécommunications, où l'on privilégie les méthodes « agiles », les approches « data centric », ... Le point principal est dans

tous les cas de bien établir contractuellement les obligations des parties, et les mécanismes d'évolution associés.

- Recommandation R5.3.4.9 : Chaque demande de modification doit être exprimée avec au moins la même rigueur que la Baseline d'exigences initiale (en précisant en particulier la situation des exigences « avant » et « après » la demande de modification).

- Recommandation R5.3.4.10 : Pour chaque demande de modification, il est recommandé de partager la valeur attendue avec toutes les parties prenantes, et de conduire une analyse d'impact rigoureuse et exhaustive sur les baselines de spécification, et la définition du produit/système.

- Recommandation R5.3.4.11 : Agréer entre les parties prenantes un processus de réconciliation pour maintenir une Baseline d'exigences multi-niveaux, avec a minima une mise à jour à l'occasion de jalons majeurs.

  Nota : Selon les cas, la baseline peut contenir des éléments prenant différentes formes : base de données outillée (DOORS, Reqtify, …), documents consignant des exigences textuelles, ensemble de données et de modèles, éléments de CAO, PLM, etc.

- Recommandation R5.3.4.12 : Définir et agréer en début de programme les documents applicables et leur contenu.

- Recommandation R5.3.4.13 : Systématiser la revue des documents applicables, en mettant l'accent sur le contenu, la cohérence et l'utilité.

- Recommandation R5.3.4.14 : Appliquer aux changements de documents applicables le même processus de gestion de la configuration et de contrôle qu'aux exigences (notion de « Avant » -« Après ».)

- Recommandation R5.3.4.15 : Limiter l'écriture de documents redondants, en regroupant les parties communes dans des documents chapeaux auxquels on fera référence, et qui seront plus facile à gérer en configuration.

- Recommandation R5.3.4.16 : Il est fondamental de valider les exigences le plus en amont possible. Le coût (coût financier, shift de planning) d'une correction apportée en amont sera toujours moindre que celui d'une correction plus aval.

- Recommandation R5.3.4.17 : L'Assurance de Développement ne doit pas être le déroulement d'un processus de contrôle purement formel, déroulé par du personnel qualité, sans acquis technique. Elle doit être conduite par du personnel de préférence in situ, et techniquement expérimenté, à même d'accompagner du point de vue méthodologique les ingénieurs chargés du design.

- Recommandation R5.3.4.18 : Arrêter l'inflation du coût des activités nécessaires pour la certification par exemple en mettant un frein aux demandes d'évolutions de l'ARP4754 ou 4761.

- Recommandation R6.13.1 : Afin de dérisquer le processus, on préconise d'établir la stratégie de d'intégration, vérification, et validation, dès les phases amont du cycle de développement. La négocier et la partager, en amont entre client et fournisseur, en particulier au travers de revues (typiquement PDR).

- Recommandation R6.13.2 : Dès le lancement de projet, agréer entre donneur d'ordre et fournisseur les contenus fonctionnels des livrables en cohérence avec leur utilisation (système, équipement, logiciel). Telle fonction devant être disponible pour telle application (banc sol, banc volant, banc d'intégration, 1er vol…)

- Recommandation R6.13.3 : Accepter (en négociation) la notion de développement incrémental dans le processus de développement. Définir, dès la négociation du contrat, en commun plateformiste/donneur d'ordre - fournisseur (« avionneur – systémier »), les jalons de développement (revues et/ou Maturity Gates) auxquels telle ou telle fonction est attendue. On doit envisager le développement incrémental d'un sous-système dans le cas où il existe un risque technique lié au sous-système et qu'il convient de le lever dans un premier temps. Il faut aussi envisager le développement incrémental dans le cas où le développement complet du sous-système serait trop long et interdirait de facto de commencer plus tôt l'intégration (risque planning, même s'il n'y a pas de risque particulier sur le plan technique.).

- Recommandation R6.13.4 : La vérification s'appliquant à un état de définition du produit, la démonstration a longtemps reposé sur des jeux de tests intensifs du produit final. La maîtrise des boucles amont et la connaissance de l'environnement opérationnel, au travers de l'obtention de modèles recalés par rapport aux phénomènes physiques mis en jeu, devra apporter la possibilité de minimiser les jeux de tests sur le produit physique au profit de vérification sur des modèles. L'utilisation de vérification sur modèle et calculs est par ailleurs incontournable pour des démonstrations inatteignables par test sur le produit physique (exemple : démonstration de ditching d'un avion, démonstration de tenue à l'éclatement moteur, tenue au max V dive, …).

- Recommandation R6.13.5 : Conditionner l'écriture et la validation des exigences à leur capacité à être vérifiées.

- Recommandation R6.13.6 : Planifier en amont, afin d'assurer au mieux la disponibilité, l'accessibilité, et la maturité des moyens et outils de vérification. En particulier, on recommande de privilégier, lorsque c'est possible (représentativité), l'usage de modèles, permettant de démarrer la vérification plus en amont, d'être économiquement plus efficace, d'être plus facilement maintenable et adaptable au contexte, et d'être souvent plus représentatif du contexte de vol, et plus couvrant (e.g. : simulation de cas de pannes.)

- Recommandation R6.13.7 : Il est important de maîtriser l'ingénierie de Vérification. On préconise la mise en place de moyens permettant de gérer l'ensemble des outils et plateformes de tests, des données de vérification, de la documentation, et des indicateurs associés (dont la traçabilité vis-à-vis des exigences). Ces moyens devront être gérés en configuration, et leur pérennité devra être assurée sur le cycle de vie.

- Recommandation R6.13.8 : Nous préconisons, au niveau de chaque entreprise et chaque programme, de gérer l'ensemble des données et documents de vérification, sous forme de base de données informatique. Cette base de données, si elle est mise en place, doit être étroitement coordonnées avec celle décrivant la déclinaison et l'arborescence des exigences, lorsqu'elle existe.

- Recommandation R6.13.9 : on préconise que le succès de la vérification soit contrôlé, grâce à la traçabilité des données et documents du processus de vérification, et sanctionné par un revue indépendante (des équipes de vérification), et faisant intervenir des experts extérieurs au programme. Cette revue s'assurera de la complétude de la documentation et des données associée à la vérification, de l'exhaustivité de la vérification des exigences (l'objectif visé est

l'atteinte d'un taux de couverture de 100%), et de la tenue de l'ensemble des performances attendues et des exigences quantitatives, et qualitatives.

- Recommandation R6.13.10 : On propose que l'industriel ait une délégation pour conduire les activités de démonstration de conformité et de surveillance (witnessing), Pour cela, une délégation officielle, auditée, devrait permettre aux systémiers et équipementiers de niveau 1 et 2 de procéder aux activités de vérification et de conformité, avec une plus grande autonomie.

- Recommandation R6.13.11 : On recommande de mettre en place, conjointement avec les autorités de certification, une réflexion inspirée du « lean engineering », visant à diminuer la documentation (suppression de la documentation difficilement exploitable, de type « waste »), et de remonter de manière plus simple les preuves nécessaires à la certification.

- Recommandation R6.13.12 : Pour les produits conçus pour être réutilisables, établir leur contexte d'IV&V de façon à faciliter la réutilisation ultérieure avec un effort de vérification minimal.

- Recommandation R6.13.13 : On préconise de capitaliser le savoir dans les modèles/les plateformes d'essais/les bancs et les processus, permettant de démontrer la validité de ces moyens d'IV&V.

- Recommandation R6.13.14 : Utiliser au mieux la Validation amont (par exemple avec des outils de simulation technico opérationnelles) pour clarifier les besoins du client, définir au plus tôt le périmètre d'usage, réduire la complexité liée à la multiplicité des contraintes et des usages (en utilisant une approche par scénarios par exemple), et simplifier ainsi la vérification aval.

- Recommandation R7.1 : On recommande en particulier que les personnes en charge de l'assurance processus, du côté des industriels développeurs, comme du côté de l'autorité de certification, aient une expérience opérationnelle antérieure.

- Recommandation R7.2 : Faire un effort en amont, au niveau de la taylorisation des plans, afin d'optimiser le ratio ressources impliquées dans les processus d'IS – ressource globale du programme (cf. recommandation R5.3.4.2, et recommandation générale R8).

- Recommandation R7.3 : Adapter les efforts mis sur la sûreté, afin de renforcer la démonstration au niveau mission, et de ne traiter que le juste besoin au niveau des équipements. On notera que c'est un point fort de l'ARP4754A.

- Recommandation R7.4 : Obtenir des autorités une meilleure reconnaissance de l'approche basée sur les modèles pour la maitrise du développement des systèmes complexes (Attention toutefois : il ne serait pas souhaitable de se laisser entrainer dans le concept de l'outil certifié, car cela ne ferait que déplacer le problème, sans alléger quoi que ce soit !)

- Recommandation R7.5 : Evaluer la nécessité, pour les fonctions (ou chaînes fonctionnelles) sensibles (par exemple critiques au niveau SdF), et à caractère transverse, de mettre en place un rôle, ou un responsable pour ces fonctions (ou par chaine fonctionnelle), avec une vision end-to-end.

- Recommandation R8.2.1 : Afin de mettre en place une démarche collaborative, il est recommandé de travailler ensemble au niveau des processus, afin d'acquérir une compréhension commune (harmonisation du vocabulaire), avant de vouloir harmoniser ces processus et d'échanger méthodes et outils.

- Recommandation R8.2.2 : Mettre à profit la phase d'architecture, afin de mettre en place les processus d'ingénierie collaborative, ainsi que les méthodes et outils associés. Bien le refléter dans les contrats. Afin d'y parvenir, il peut être utile de faire un mapping complet des méthodes et outils de chaque partie prenante, avant de statuer sur ce qu'on échange et en vue de quelle finalité.

- Recommandation R10.1 : Même s'il ne s'agit pas à proprement parler d'une recommandation, nous jugeons utile de rappeler que, au-delà de la maîtrise de la complexité l'approche SdS constitue un changement de paradigme : On est ainsi conduit à analyser la situation de chacune des parties prenantes et leurs interactions, sur des systèmes constituants aux cycle de vie indépendants et non nécessairement coordonnés, avant de pouvoir conduire une démarche de type analyse fonctionnelle et de capture des exigences. Ce paradigme Système de Systèmes fonctionne bien également pour traiter les systèmes complexes, même si tous les critères de Maier ne sont pas clairement satisfaits..

- Recommandation R10.2 : Identifier clairement l'ensemble des parties prenantes, et leur rôle. Prendre en compte l'ensemble de leurs contraintes, qu'elles soient organisationnelles ou techniques, pour alimenter les études de compromis et les prises de décision.

- Recommandation R10.3 : Favoriser le travail collaboratif entre les parties prenantes, expliciter et capturer les données techniques et programmatiques (cadres d'architectures et modélisation).

- Recommandation R10.4 : Identifier clairement les rôles d'architecte et/ou d'ingénieur système à chacun des niveaux système de systèmes et systèmes, expliciter les différences d'approches entre ces deux niveaux d'ingénierie.

- Recommandation R10.5 : Rechercher les compromis équilibrés entre ces deux niveaux.

- Recommandation R10.6 : Rechercher les architectures ouvertes, favorisant l'usage de standards et un couplage dynamique des systèmes.

- Recommandation R11.1 : En cas de réutilisation, la revalidation des exigences entre les différents niveaux de spécifications est impérative...

- Recommandation R11.2 : La mise en œuvre d'une réutilisation requiert au plus tôt une analyse détaillée des compatibilités / incompatibilités fonctionnelles. L'objectif principal est d'identifier toutes les limitations ou déviations possibles, de les accepter ou de pouvoir les lever moyennant des investissements spécifiques.

- Recommandation R11.3 : Afin de rester dans une approche « gagnant-gagnant », lorsqu'on effectue une analyse des exigences de haut niveau, il peut être fructueux de comparer et de partager, entre client et fournisseur(s), dès les phases amont, une solution conçue ad hoc pour répondre au besoin exprimé, une solution de réutilisation opportuniste, et une solution issue d'une ligne de produits existants (solution de type réutilisation ou « re-use »), plus attractive économiquement, même si elle répond de manière moins parfaite à ce besoin.

- Recommandation R11.4 : Il est souhaitable de négocier en amont avec les autorités de certification, l'acceptabilité de preuves de vérifications, obtenues dans un autre contexte (autre programme, autre autorité de certification, …) dès lors qu'on peut démontrer que ces preuves sont couvrantes, vis-à-vis du besoin du programme en cours de certification.

- Recommandation R12.1 : L'ingénierie des systèmes introduit une vision transverse des processus et de l'entreprise, différente de celle portée par l'organisation traditionnelle en métiers (spécialités techniques, programmes, assurance qualité, industrialisation, production, et services). Afin d'être en mesure d'appréhender la complexité des systèmes futurs et d'être innovantes, nos sociétés se doivent de mettre en place de nouvelles organisations, permettant de déployer au mieux cette dimension transverse.

- Recommandation R12.2 : Identifier, formaliser, et maintenir les métiers de l'ingénierie des systèmes dans nos entreprises, et prévoir une gestion prévisionnelle des compétences associées (, reconnaissance, management des compétences, ..).

- Recommandation R12.3 : Promouvoir la généralisation des formations d'ingénierie des systèmes dans l'ensemble des écoles d'ingénieurs et des universités.

- Recommandation R12.4 : Généraliser les formations continues d'ingénierie des systèmes, au sein de nos entreprises.

- Recommandation R12.5 : Si l'on confie des tâches d'ingénierie des systèmes à des acteurs de la supply chain, ou à des prestataires externes, s'assurer que ces sociétés assurent des formations d'ingénierie des systèmes à leur personnel, et qu'elles mettent à disposition du personnel convenablement formé.

GLOSSAIRE, ET TRADUCTION DE TERMES US/UK

Nota : Ce glossaire s'inspire très fortement du glossaire de l'AFIS « Glossaire d'Ingénierie Système de Base ».

Agreement Processes : Processus d'alignement, amenant à un accord. Ils recouvrent les deux processus contractuels d'acquisition et de fourniture. On pourra parler de processus de gestion en français.

Architecting : Terme anglais non traduisible directement. On pourrait éventuellement le traduire en jargon d'ingénieur par « Architecturage » ou « Architectude ». L'architecting se centre sur la capture et la stabilisation des besoins et contraintes de haut niveau, au travers d'un processus collaboratif. Au besoin on pourra utiliser le mot architecture en français, même s'il ne rend pas bien le contenyu d' »architecting ».

Assumption(s): Hypothèse(s)

Bracketing : Support d'attache

Capability : Capacité

Common Cause Analysis : Terme anglais traduit par « analyses de causes communes ».

Concept design : Terme anglais traduit par « Conception » en français.

Dashboard : Tableau de bord

Design : Terme anglais traduit aussi par « Conception » en français.

Design Definition : Terme anglais traduit par « Définition » en français.

Development Assurance : Terme anglais couvrant l'ensemble des activités nécessaires à la maîtrise du développement technique de systèmes complexes.

Decommissioning, Dismantling, Disposal, Retirement: Dernière phase du cycle de vie d'un système recouvrant « Retrait du service » et « Démantèlement ».

Ditching (of an airplane) : Amerrissage (d'un avion).

Elicitation : Terme traduit souvent en français par « élicitation ». Ce mot est un anglicisme qu'on pourrait aussi traduire par « identification ».

Enabling Systems : Terme anglais traduit par « Systèmes de Soutien » ou « Systèmes Contributeurs », parfois nommés aussi « Systèmes Capacitants » (glossaire AFIS).

End-Product Terme anglais associé aussi à System of Interest, traduit par le « Système Principal » ou le « Système Réalisé », en français.

End User Utilisateur final, en anglais.

Engineering	Terme anglais traduit par « Ingénierie ».
Flow	Flot ou Flux
Functional Tree	« Arbre des Fonctions » ou « Arbre Fonctionnel », en anglais.
Handbook	Manuel en Français.
Integral Process	Terme anglais utilisé dans l'ED79/ARP4754, et traduit par « Processus support de l'IS ».
Intended Use	Terme anglais traduit par « Usage Attendu » (le Besoin Client).
Max V dive :	Taux de descente maximum (correspondant à une manœuvre d'urgence pour un avion).
Mitigate :	Terme anglais traduit par « minimiser, réduire » (pour les risques). S'utilise par exemple dans le plan de réduction des risques.
Problem Reports :	Rapport d'anomalie.
Product Assurance :	Terme anglais du domaine de la Qualité traduit par « Assurance Produit ».
Product Tree	« Arbre des Produits », en anglais. On utilise fréquemment le sigle PBS.
Safety	Terme anglais traduit par « Sûreté » ; cependant on garde bien souvent dans le texte ce terme anglo-saxon, pour éviter l'ambigüité existant en français entre Sûreté et Sécurité.
Security	Terme anglais traduit par « Sécurité » (exemple : Sécurité des Systèmes d'Information) ; recouvre la lutte contre la malveillance.

Space Sustainability : « Espace Durable » en français.

Stakeholders :	« Parties Prenantes », en anglais.
Standard :	Norme, en anglais.

Statement of Conformity : « Etat de conformité », en anglais.

Supply Chain :	Chaîne d'achat/fourniture (interne et externe), en anglais.
System Engineer :	Ingénieur Système ou Ingénieur des Systèmes.

Systems Engineering : Ingénierie des Systèmes.

System of Interest :	Terme anglais associé aussi à End-Product , traduit par le « Système Principal » ou le « Système Réalisé », en français.
Solution :	Ensemble constitué par le « Système Principal » ou le « Système Réalisé, et les « Systèmes de Soutien » ou « Systèmes Contributeurs », ou « Systèmes Capacitants ».

Time to Market : Date à laquelle un système doit être mis en service, afin de s'assurer une place privilégiée, ou pour le moins une place acceptable (selon les cas), sur le marché.

Tools Vendors : Sociétés de service en informatique, commercialisant des progiciels.

Type Certificate : Certificat de Type.

Virtual Digital Mock-Up : Terme anglais traduit par « Maquette de Conception Virtuelle ».

Use Cases : Terme anglais traduit par « Cas d'Utilisation ».

Verification closeout : Démonstration de fin de vérification

Waiver : Dérogation (sur le produit après certification, ou définition qualifiée).

Work Breakdown Structure : Terme anglais traduit par « Organigramme des Tâches ».

SIGLES & ACRONYMES

A5ME	Ariane 5 Midlife Evolution.
ABD	AirBus Directive.
ABM	Activity Based Methodology.
AF	Analyse Fonctionnelle.
AFIS	Association Française d'Ingénierie Système (« Chapitre Français » de l'INCOSE).
AESA	Agence Européenne de la Sécurité Aérienne (EASA en anglais).
AFNOR	Association Française de NORmalisation.
AGATE	Atelier de Gestion de l'ArchiTEcture des systèmes d'information et de communication. Ancien cadre d'architecture de la DGA.
AH	Adopted Handbook (ECSS).
AMDEC	Analyse des Modes de Défaillance, de leurs Effets, et de leur Criticité. Outil utilisé en Sûreté de Fonctionnement (SdF).
AOG	Aircraft On Ground.
ArchiMate®	Standard de langage ouvert pour l'Enterprise Architecture.
ARP	Aerospace Recommended Practice.
AS	Adopted Standard (ECSS).
ASE	Agence Spatiale Européenne (plus connue sous le sigle anglo-saxon d'ESA).
ASL	Airbus Safran Launchers.
ATA	Air Transportation Association of America. Le sigle ATA désigne usuellement les systèmes avions, les structures avions, et les systèmes moteurs, définis par la norme A4A (Arlines for America, anciennement ATA). Exemples : ATA27 : Flight Controls System, ATA34 : Navigation System.
ATAM	Architecture Tradeoff Analysis Method (développée par le SEI).
ATL2	Atlantique 2.
ATM	Air Traffic Management.

ATV	Automated Transfer Vehicle ; programme ESA de véhicule de service automatique de la station internationale ISS. Cinq missions ont été effectuées, au total.
BNAE	Bureau de Normalisation de l'Aéronautique et de l'Espace.
BMS	Business Management System.
BPMN	Business Process Model and Notation.
C4ISR	C4 (Computerized Command, Control, Communications, depuis 2007 ; anciennement Command, Control, Communications, Computers), Intelligence (renseignement militaire), Surveillance, and Reconnaissance.
C4ISR-AF	C4ISR Architectural Framework, maintenant devenu DoDAF.
CAD	Computer Aided Design, en français.
CAO	Conception Assistée par Ordinateur.
CCA	Common Cause Analysis (analyses de causes communes).
CDR	Critical Design Review.
CMA	Common Mode Analysis.
CMMI	Capability Maturity Model Integration. Voir SEI/CMMI.
CMS	Company Management System.
CNES	Centre National d'Études Spatiales (Agence française de l'Espace)
COMPASS	Comprehensive Modelling for Advanced Systems of Systems
CONOPS	Concept des opérations (traduit de l'anglais).
COTS	Commercial (or Component) Off-The-Shelf.
CPIOM	Core Processing Input / Output Module.
CRD	CeRtification carDs.
DAL	Development Assurance Level (auparavant : Design Assurance Level).
DANSE	Designing for Adaptability and evolutioN in System of systems Engineering.
DGA	Direction Générale de l'Armement.
DLR	Deutsches Zentrum für Luft und Raumfahrt (Centre de Recherche et Agence Allemande de l'Aéronautique et de l'Espace).
DOA	Design Organisation Approval.

DoD	Department of Defense. Ministère de la défense des Etats-Unis.
DoDAF	Department of Defense Architecture Framework.
DOID	Design Organisation Interface Document.
DOORS	Progiciel commercialisé par IBM, supportant l'activité de gestion/ingénierie des exigences (progiciel le plus répandu du marché).
DSL	Domain Specific Language.
EA	Enterprise Architecture.
EASA	European Aeronautic Safety Agency.
EATMA	European ATM Architecture.
ECSS	European Cooperation for Space Standardization.
ED	European Directive.
EDA	European Defence Agency (Agence de Défense Européenne).
EDSTAR	European Defence Standards Reference System.
E2AF	Extended Enterprise Architecture Framework.
EFB	Electronic Flight Bag.
ESA	European Space Agency (Agence Spatiale Européenne).
EUROCAE	European Organization for Civil Aviation Electronics. Organisation qui développe les standards ED, pendant européens des ARP américains.
EUROSPACE	Association des industriels européens du secteur de l'Espace.
FBS	Functions or Functional Breakdown Structure.
FDAL	Functional Development Assurance Level.
FEAF	Federal Enterprise Architecture Framework.
FFR	First Flight Review.
FMEA	Failure Modes and Effects Analysis.
FMECA	Failure Modes, Effects and Criticality Analysis.
FMES	Failure Modes and Effects Summary.
FRR	Flight Readiness Review.
FTA	Fault or Failure Tree Analysis (arbres de défaillance).

GAF	Governance Analysis Framework.
GIG	Global Information Grid (Département de la Défense des Etats-Unis).
HALT	Highly Accelerated Life Test.
HB	HandBook.
HPC	High-Performance Computing.
IADT	Inspection, Analysis, Demonstration, and Test, ou équivalent en français
ICD	Interface Control Document.
IDAL	Item Development Assurance Level.
IDEAS	Integrated Design Environment for Assessment of computer Systems.
ILS	Integrated Logistic Support.
IHM	Interface Homme-Machine.
INCOSE	International Council on Systems Engineering.
INPI	Institut National de la Propriété Industrielle.
Integrity	Progiciel supportant l'activité de gestion/ingénierie des exigences, distribué par PTC.
IRL	Integration Readiness Level.
IS	Ingénierie des Systèmes, ou Ingénierie Systèmes.
ISO	International Organization for Standardization. Voir: www.iso.org
ISS	International Space Station.
IV&V	Integration, Verification, and Validation.
IVV&Q	Integration, Verification, Validation, and Qualification.
LCC	LifeCycle Cost.
MAIT	MAnufacturing, Integration, and Tests.
MBSE	Model Based System Engineering (Ingénierie des Systèmes fondée sur les modèles).
MCO	Maintien en Condition(s) Opérationnelle(s).
MDA	Model Driven Architecture.
MDD	Model Driven Design.

MOA	Maîtrise d'Ouvrage.
MOD ou MoD	Ministry of Defence. Ministère de la défense (par exemple britannique ou allemand).
MODAF	MOD Architecture Framework (UK).
MODEM	MODAF Ontological Data Exchange Model.
MOE	Maîtrise d'Oeuvre.
MOISE	MOdels and Information Sharing for System engineering in Extended entreprise.
MRL	Manufacturing Readiness Level.
NAF	NATO Architecture Framework.
NATO	OTAN en anglais (North Atlantic Treaty Organization).
NCO	Network Centric Operation.
NCOSE	National Council of Systems Engineering, précurseur de l'INCOSE.
NCR	Non Conformance Report (Rapports de Non-Conformité).
NEC	Network Enabled Capability.
NIH	Not Invented Here (syndrome du « non inventé ici »).
NRC	Non Recurring Cost.
NSP	New System Policy.
OCDE	Organisation de Coopération et de Développement Economiques. Voir www.oecd.org
OMG	Object Management Group.
OT	Organigramme des Tâches.
OTAN	Organisation du Traité de l'Atlantique Nord.
PBS	Product Breakdown Structure.
PCT	Patent Cooperation Treaty, système de brevets internationaux.
PDM	Product Data Management.
PDR	Preliminary Design Review.
PEAF	Pragmatic Enterprise Architecture Framework (free to use framework).
PI	Propriété Intellectuelle.

PLM	Product Lifecycle Management.
PME	Petite et Moyenne Entreprise.
Polarion	Progiciel, supportant l'activité de gestion/ingénierie des exigences, distribué par Siemens.
PRA	Particular Risks Analysis.
PSSA	Preliminary System Safety Analysis.
QCDR	Qualité-Coût-Délai-Risques.
QR	Qualification Review.
RC	Recurring Cost.
RDP	Revue de Définition Préliminaire (équivalent en français de PDR).
ROAD2SoS	Roadmaps for System-of-Systems Engineering.
RSP	Risk Sharing Partners.
RTCA	Radio Technical Commission for Aeronautics. Organisation qui développe des standards, tels la DO 254.
SADT	Structured Analysis and Design Technique.
SAE	Society of Automotive Engineers. Organisation qui développe les standards ARP (ARP 4754, ARP4761, …).
SdF	Sûreté de Fonctionnement.
SdS	Système de Systèmes.
SE BoK	System Engineering Body of Knowledge (BoK).
SEI	Software Engineering Institute.
SEI/CMMI	Software Engineering Institute / Capability Maturity Model Integration.
SESAR	Single European Sky ATM Research.
SJU	SESAR Joint Undertaking.
SLI	Support Logistique Intégré.
SoS	System of Systems.
SRL	System Readiness Level.
SRR	System Requirement Review.
SSA	System Safety Analysis.

SSI	Sécurité du (des) Système(s) et de l'Information.
ST	Standard.
STANAG	Standardization Agreements.
SysML	Systems Modelling Language. Voir www.sysml.org
SysRR	System Requirement Review.
T-AREA-SoS	Trans-Atlantic Research and Education Agenda on Systems of Systems.
TC	Type Certificate.
TM	Technical Memorandum.
TOGAF	The Open Group Architecture Framework.
TPE	Très Petite Entreprise.
TRL	Technology Readiness Level.
UML	Unified Modelling Language.
UPDM	Unified Profile for the Department of Defense Architecture Framework (DoDAF) and the Ministry of Defence Architecture Framework (MODAF).
V&V	Verification and Validation.
VCB	Verification Control Board.
VCD	Verification Control Document.
VSE	Very Small Entities.
WBS	Work Breakdown Structure (Organigramme des Tâches).
ZSA	Zonal Safety Analysis.

BIBLIOGRAPHIE

DOCUMENTS AFIS ET DOCUMENTS PUBLIES PAR L'AFIS :

Pages html du site web AFIS (http://www.afis.fr, *en partie accessible à un public non membre)*

« Pourquoi l'Ingénierie Système ? » Fiche AFIS 2005 (cf. site AFIS).

« Principaux concepts de l'Ingénierie Système» Fiche AFIS 2005 (cf. site AFIS).

« Processus de l'Ingénierie Système» Fiche AFIS 2005 (cf. site AFIS).

« Le déploiement de l'IS » Fiche AFIS 2005 (cf. site AFIS).

« Découvrir et comprendre l'Ingénierie Système », ouvrage collectif d'un Groupe de Travail AFIS, sous la direction de Serge Fiorèse et Jean-Pierre Meinadier. AFIS, 2009

« Recommandations pour l'élaboration d'un référentiel d'exigences techniques » Fiche AFIS 2001 GT Ingénierie des Exigences (cf. site AFIS).

« Glossaire de Base de l'Ingénierie Système – version Expérimentale », v1.2 AFIS Octobre 2004.

« Glossaire AFIS » Septembre 2011

« Ingénierie Système : La vision AFIS pour les années 2020 – 2025 », Livre Blanc AFIS, ouvrage collectif sous la direction du Conseil d'administration de l'AFIS.

« Introduction au penser Système », ouvrage collectif sous la direction de Brigitte Daniel Allegro (2014).

« Bonnes pratiques en expression du besoin », ouvrage collectif sous la direction de Gauthier Fanmuy (2014).

« Bonnes pratiques en ingénierie des exigences », ouvrage collectif Groupe Technique Ingénierie des Exigences (GTIE) et CT PG.

« Bonnes pratiques en maîtrise des interfaces », ouvrage collectif sous la direction de Gilles Meuriot.

« Bonnes pratiques en prise de décision multicritères », ouvrage collectif sous la direction de Gilles Meuriot.

« L'ingénierie Système d'une Ligne de Produit », sous la direction d'Alain Le Put (2014). (*traduction anglaise publiée par l'INCOSE début 2016*). (éditions CEPADUES).

AFIS 5ème Conf Annuelle d'Ingénierie Système, 2009 : "Vision 2020, The Globalisation of Systems Engineering", Ralf Hartmann, Astrium Satellites,

DOCUMENTS INCOSE ET DOCUMENTS PUBLIES PAR L'INCOSE ET ORGANISMES ASSOCIES :

Pages html du site web INCOSE (http://www.incose.org , *en partie accessible à un public non membre)*

"Systems Engineering Vision 2020", v 2.03, INCOSE, 2007

"A World in Motion - Systems Engineering Vision 2025", INCOSE, 2014

"INCOSE System Engineering Handbook : A Guide for System Life Cycle Processes and Activities", INCOSE-TP-2003-002-03.2.2 , San Diego, CA, USA: International Council on Systems Engineering (INCOSE), October 2011.

INCOSE SE Lean enablers (194 "do's and don'ts" and organized into six Lean Principles)

"Guide to the Systems Engineering Body of Knowledge" (SEBoK) v1.3.2, BKCASE, April 14, 2015

"System Engineering for Dummies®", Cathleen Shamieh (IBM limited Edition, published by Wiley & Sons Inc., with the support of INCOSE ; ISBN : 978-1-118-24414-2) ; existe aussi en édition française : « Ingénierie Système pour LES NULS® », édition limitée IBM (2012)

AUTRES DOCUMENTS :

« A Guide to the Project Management Body of Knowledge" (PMBoK® Guide), PMI Standard Committee, Duncan W., Project Management Institute. Aujourd'hui 5ème édition (cinq éditions: 1996, 2000, 2004, 2009, 2013). ISBN 97861693558966769

"NASA System engineering Handbook", Shishko R., NASA/SP-6105, National Aeronautics and Space Administration (NASA) Washington DC (1995 original edition), NASA/SP-2007-6105 (2007 revision 1).

"Ingénierie et intégration des systèmes" J.P. Meinadier, Hermès ed. Paris 1998

"Le métier d'intégration des systèmes" J.P. Meinadier, Hermès/Lavoisier ed. Paris 2002

"The Engineering Design of Systems – Models and Methods", D. Buede, Wiley-Interscience Publication, 2000

"Systems Engineering Guidebook – A process for Developing Systems and Products", J. Martin, 1st ed. Boca Raton, FL, USA: CRC Press, 1997

"The art of systems architecting". FL, Maier, M. et E. Rechtin, 3rd ed. Boca Raton, USA: CRC Press 2009

"Systems engineering and analysis." Blanchard, B. S. et W. J. Fabrycky. Prentice-hall international series in industrial and systems engineering. 4th ed. Englwood Cliffs, NJ, USA: Prentice-Hall. 2005 .

"Systems Engineering", 3rd ed. Hull, M. E. C., Jackson, K. et Dick, A. J. J. , Springer London 2010.

“Requirements engineering”. Van Lamsweerde, A. , Wiley, New York, NY 2009.

« Ingénierie des systèmes complexes » Alain Faisandier, Techniques de l’Ingénieur, Fiche Pratique Référence 0269

« Cours Ingénierie Système - Approche processus », Philippe Meyne, ENSTA ParisTech

« Ingénierie Système - Quelques concepts, place dans les Entreprises, problématiques de formation», Alain Faisandier, Directeur de MAP système, Directeur Technique de l'AFIS, Colloque AIP-PRIMECA Avril 2011

« What is ISO/IEC 15288 and Why Should I Care? », Garry Roedler, US Head of Delegation for JTC1/SC7/WG7, US TAG TG7 Lead, Principal Systems Engineer, Lockheed Martin Management and Data Systems, September 2002

« Overview of the System Engineering Process », Ed Ryen, PE ; Maintenance – ITS, North Dakota Department of Transportation, March 2008

« Pratique de l’analyse fonctionnelle », Robert Tassinari, Dunod, Paris 1997

« Cours d’Analyse Fonctionnelle », Michel Bigand, Centrale Lille

« Cours d’Analyse Fonctionnelle du Besoin », Jean-Marie Virely et all., ENS Cachan

AFAV (Association Française pour l'Analyse de la Valeur) site: http://www.afav.eu

“A review of systems engineering standards and processes”, Guey-Shin Chang, Horng-Linn Perng, Jer-Nan Juang, National Applied Research Laboratories, 3F, No. 106, Ho-Ping E. Road, Sec. 2, Taipei 10622, Taiwan ; Journal of Biomechatronics Engineering Vol. 1, No. 1, (2008) 71-85

“Toward Principles for the Design of Ontologies Used for Knowledge Sharing”, Thomas Gruber, International Journal Human-Computer Studies Vol. 43, Issues 5-6, November 1995, p.907-928.

Wikipedia: WikiProject Systems/List of systems engineering books

NORMES

Normes principales:

EIA/ANSI 632 “Processes for Engineering a System” (1994, Avril 1998, publiée en janvier 1999 et confirmée en 2003)

IEEE 1220 “Standard for Application and Management of the Systems Engineering Process” (1994, et Janvier 1999)

ISO 9001 v 2000 et 2008 (avec l’approche par processus)

ISO/IEC 15288 « Systems Engineering – System Life-Cycle Processes » (2002,2008, et nouvelle version 2015)

ISO-IEC 19760 “Systems and software engineering - Guide for Application of ISO-IEC 15288” (2003)

ISO/IEC TS 24748-1 (First edition 2016-05-01) “Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management”

ISO/IEC TS 24748-2 (First edition 2011-09-01) “Systems and software engineering — Life cycle management —— Part 2: Guide to the application of ISO/IEC 15288 (System life cycle processes)”

ISO/IEC 26702 “Systems and software engineering - Application and Management of the Systems Engineering Process” (2007)

ISO/IEC 29110 “Systems and Software Engineering - Lifecycle Profiles and Guidelines for very Small Entities (VSEs)” (norme composée de cinq parties ISO/IEC TR 29110-1 à ISO/IEC TR 29110-5)

ISO/IEC TR 24766 - “Systems and software engineering -- Guide for requirements engineering tool capabilities”

EN 1325-1:1996 – “Value management, value analysis, functional analysis vocabulary — Part 1: Value analysis and functional analysis”

EN 12973:2000 – "Value management"

NF X 50-100 : Analyse Fonctionnelle — Caractéristiques fondamentales — 1996.

NF X 50-151 : Analyse de la Valeur, Analyse Fonctionnelle — Expression fonctionnelle du besoin et cahier des charges fonctionnel — 1991.

FD X 50-101 : Analyse Fonctionnelle — L’Analyse Fonctionnelle outil interdisciplinaire de compétitivité — 1995.

NF EN 1325-1 : Vocabulaire du Management par la Valeur, de l’Analyse de la Valeur et de l’Analyse Fonctionnelle — 1 : analyse de la valeur et Analyse Fonctionnelle —

“Capability Maturity Model Integration (CMMI) for Development”, version 1.2 . Software Engineering Institute, 2007

Enfin, pour les PME, on peut simplifier l'approche et utiliser, pour le déploiement de l'IS, le standard ISO/IEC 29110 "Systems and Software Engineering - Lifecycle Profiles and Guidelines for Very Small Entities (VSEs)" (norme composée de cinq parties ISO/IEC TR 29110-1 à ISO/IEC TR 29110-5), qui est promue par l'AFIS.

Normes pour nos domaines spécialisés

Normes du BNAE (Bureau de Normalisation de l'Aéronautique et de l'Espace) :

RG. Aero 00040A (norme AFNOR FD X 50-410) « Recommandation générale pour la spécification de management de programme », Bureau de Normalisation de l'Aéronautique et de l'Espace (BNAE) 1999.

RG. Aero 00077 « Management de programme – Guide pour le management de l'ingénierie système », BNAE 2005., promue en norme européenne: ASD-STAN EN 9277 (décembre 2012, édition A)

RG 000 120 : Recommandation générale pour l'acquisition et la fourniture de systèmes ouverts.

RG 000 08 : Guide pour l'élaboration de la spécification technique de besoin.

Dans le domaine spatial, on trouve les ECSS (European Cooperation for Space Standardisation) développées avec le support de l'ESA (agence spatiale européenne), avec une série complète de normes pour l'ingénierie système. Dernière mise à jour complète le 22 mai 2014 + parution de la norme ECSS-E-ST-10-24C « Space engineering - Interface management » au 1er juin 2015).

Pour l'aéronautique civile, on trouve :

Règlements de Certification EASA CS25 (« Large Aircraft » - Avions commerciaux), CS23 (Avions légers), CS29 (« Large Rotorcraft » - Hélicoptères), CS27 (« Small Rotorcraft » - Hélicoptères légers), CS33 (Moteurs).

La recommandation Eurocae ED-79A/ RTCA ARP 4754A « System Development Process »

La recommandation Eurocae ED-135/ RTCA ARP4761, qui explique comment décliner les exigences de sûreté («safety»).

La recommandation Eurocae ED-12C/ RTCA DO-178C "Software considerations in airborne systems and equipment certification".

La recommandation Eurocae ED-80 / RTCA DO-254 "Design Assurance Guidance for Airborne Electronic Hardware" ; La réunion du matériel DO-254 et du logiciel DO-178B forment un système embarqué qui est régi par un standard dédié ED-79/ARP4754. L'ensemble forme une approche cohérente des méthodes de développement des systèmes embarqués pour les applications aéronautiques.

La RG AERO 00044 " Guide d'application de l'ARP 4754A"

Pour le domaine militaire, on trouve :

MIL-STD-499, “Military Standard: System Engineering Management” (17 Jul 1969). Abandonnée

MIL-STD-499A (Notice 1), “Military Standard: System Engineering Management” (27 Feb 1975). Appliquée à l’Air Force, mais devenu un standard de fait. Abandonnée

MIL-STD-499B (Draft), “Military Standard: System Engineering Management” (24 Aug 1993) Ce document en draft, daté du 24 Août 1993, et préparé par le MIL-STD-499B Joint Office of the Secretary of Defence (OSD)/ Services /Industry Working Group n’a jamais été approuvé.

En 1994 le secrétaire à la défense américain, William Perry publia un mémorandum supprimant le recours à des normes spécifiques sur les programmes d’acquisition du département de la défense (DoD). Ce même mémorandum poussa les fournisseurs d’équipements militaires à adopter des pratiques commerciales en accord avec le standard EIA 632 IS (Standard Intérimaire), puis avec le standard IEEE 1220 (Version d’essai) en lieu et place de la MIL-STD-499A. De ce fait la MIL-STD-499B n’a jamais été approuvée, et la MIL-STD-499A a été annulée sans remplacement en 1995.

“MOD Architecture Framework”, UK MOD, version 1.2.004 MODAF, UK Ministry of Defence, 2010

“DOD Architecture Framework”, DOD, version 2.02 DODAF

L'Agence de Défense Européenne (EDA), par le biais du Groupe d’Experts N°20, propose une sélection de bonnes pratiques, normes et standards pour l’Architecture et l’Ingénierie Système, dans un rapport de novembre 2014, disponible en ligne: https://edstar.eda.europa.eu/docs/librariesprovider7/standards-docs/edstar---eg-20---system-architecture---final-report_after-jmc-edstar-presentation.pdf?sfvrsn=2 . Un outil en ligne, regroupant les bonnes pratiques et recommandations des experts, quant à une sélection de normes applicables à un domaine technique, est également disponible: https://edstar.eda.europa.eu/standards .

ANNEXE A : EXTRAITS DE LA CS 25

CS 25.1309 Equipment, systems and installations
(See AMC 25.1309)
The requirements of this paragraph, except as identified below, are applicable, in addition to specific design requirements of CS-25, to any equipment or system as installed in the aeroplane.
…/…
(b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that -
(1) Any catastrophic failure condition
(i) is extremely improbable; and
(ii) does not result from a single failure; and
(2) Any hazardous failure condition is extremely remote; and
(3) Any major failure condition is remote.
…/…

AMC 25.1309 - System Design and Analysis
1. *PURPOSE*.
a. This AMC describes acceptable means for showing compliance with the requirements of CS 25.1309.
These means are intended to provide guidance to supplement the engineering and operational judgement that must form the basis of any compliance demonstration.
b. The extent to which the more structured methods and guidelines contained in this AMC should be applied is a function of systems complexity and systems failure consequence. In general, the extent and structure of the analyses required to show compliance with CS 25.1309 will be greater when the system is more complex and the effects of the Failure Conditions are more severe. This AMC is not intended to require that the more structured techniques introduced in this revision be applied where traditional techniques have been shown to be acceptable for more traditional systems designs. The means described in this AMC are not mandatory. Other means may be used if they show compliance with CS 25.1309.
../..
3. *RELATED DOCUMENTS*.
The following guidance and advisory materials are referenced herein:
…/…
b. *Industry documents.*
…/…
(2) Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754A/EUROCAE ED-79A, Guidelines for development of civil aircraft and systems
…/…
5. *DEFINITIONS.*
…/…
f. *Complex.* A system is Complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods.
…/…
i. *Development Assurance.* All those planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis.
j. *Error.* An omission or incorrect action by a crewmember or maintenance personnel, or a mistake in requirements, design, or implementation.
…/…
s. *System*. A combination of components, parts, and elements, which are inter-connected to perform one or more functions.
…/…
6. *BACKGROUND*
…/…
c. *Highly Integrated Systems.*
(1) A concern arose regarding the efficiency and coverage of the techniques used for assessing safety aspects of highly integrated systems that perform complex and interrelated functions, particularly through the use of electronic technology and software based techniques. The concern is that design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for more complex systems. Thus, other assurance techniques, such as development assurance utilising a combination of process assurance and verification coverage criteria, or structured analysis or assessment techniques applied at the aeroplane level, if necessary, or at least across integrated or interacting systems, have been applied to these more complex systems. Their

systematic use increases confidence that errors in requirements or design, and integration or interaction effects have been adequately identified and corrected.
(2) Considering the above developments, as well as revisions made to the CS 25.1309, this AMC was revised to include new approaches, both qualitative and quantitative, which may be used to assist in determining safety requirements and establishing compliance with these requirements, and to reflect revisions in the rule, considering the whole aeroplane and its systems. It also provides guidance for determining when, or if, particular analyses or development assurance actions should be conducted in the frame of the development and safety assessment processes. Numerical values are assigned to the probabilistic terms included in the requirements for use in those cases where the impact of system failures is examined by quantitative methods of analysis. The analytical tools used in determining numerical values are intended to supplement, but not replace, qualitative methods based on engineering and operational judgement.
…/…
9. *COMPLIANCE WITH CS 25.1309.*
…/…
b. *Compliance with CS 25.1309(b).*
…/…
(1) *General.* Compliance with the requirements of CS 25.1309(b) should be shown by analysis and, where necessary, by appropriate ground, flight, or simulator tests. Failure Conditions should be identified and their effects assessed. The maximum allowable probability of the occurrence of each Failure Condition is determined from the Failure Condition's effects, and when assessing the probabilities of Failure Conditions appropriate analysis considerations should be accounted for. Any analysis must consider:
…/…
(iii) The possibility of requirement, design and implementation errors.
…/…
(3) *Availability of Industry Standards and Guidance Materials.* There are a variety of acceptable techniques currently being used in industry, which may or may not be reflected in Documents referenced in paragraphs 3b(2) and 3b(3). This AMC is not intended to compel the use of these documents during the definition of the particular method of satisfying the objectives of this AMC. However, these documents do contain material and methods of performing the System Safety Assessment. These methods, when correctly applied, are recognised by the Agency as valid for showing compliance with CS 25.1309(b).
…/…
(4) *Acceptable Application of Development Assurance Methods.* Paragraph 9b(1)(iii) above requires that any analysis necessary to show compliance with CS 25.1309(b) must consider the possibility of requirement, design, and implementation errors. Errors made during the design and development of systems have traditionally been detected and corrected by exhaustive tests conducted on the system and its components, by direct inspection, and by other direct verification methods capable of completely characterising the performance of the system. These direct techniques may still be appropriate for simple systems which perform a limited number of functions and which are not highly integrated with other aeroplane systems. For more complex or integrated systems, exhaustive testing may either be impossible because all of the system states cannot be determined or impractical because of the number of tests which must be accomplished. For these types of systems, compliance may be shown by the use of Development Assurance. The level of Development Assurance should be determined by the severity of potential effects on the aeroplane in case of system malfunctions or loss of functions. Guidelines, which may be used for providing Development Assurance, are described for aircraft and systems in Document referenced in paragraph 3b(2), and for software in Documents referenced in paragraph 3a(3). (There is currently no agreed Development Assurance standard for hardware.) Because these documents were not developed simultaneously, there are differences in the guidelines and terminology that they contain. A significant difference is the guidance provided on the use of system architecture for determination of the appropriate development assurance level for hardware and software. EASA recognises that consideration of system architecture for this purpose is appropriate. If the criteria of Document referenced in paragraph 3b(2) are not satisfied by a particular development assurance process the development assurance levels may have to be increased using the guidance of Document referenced in paragraph 3a(3).

ANNEXE B : LES TYPES D'EXIGENCES, SELON L'ARP4754A

Types of Requirements

The requirements associated with a given function define the way the function acts in its environment and include the definition of the user/machine interface. The types of requirements detailed below should be considered at various phases of the development activities (i.e., aircraft, system and item). There may be requirements that address strictly business or economic issues and do not impact safety or certification requirements.

Safety Requirements

The safety requirements for aircraft and system-level functions include minimum performance constraints for both availability and integrity of the function.

These safety requirements should be determined by conducting a safety assessment consistent with the processes in section 5.1. Safety requirements for aircraft and system functions are determined by identifying and classifying associated functional Failure Conditions. All functions have associated failure modes and associated aircraft effects, even if the classification is "No safety effect." Safety related functional failure modes may have either contributory or direct effects upon aircraft safety.

Requirements that are defined to prevent failure conditions or to provide safety related functions should be uniquely identified and traceable through the levels of development. This will ensure visibility of the safety requirements at the software and electronic hardware design level.

Functional Requirements

Functional requirements are those necessary to obtain the desired performance of the system under the conditions specified. They are a combination of customer desires, operational constraints, regulatory restrictions, and implementation realities. These requirements define all significant aspects of the system under consideration. Regardless of the original source, all functions should be evaluated for their safety related attributes.

Customer Requirements

Customer requirements will vary with the type of aircraft, the specific function or the type of system under consideration. Requirements may include those associated with the operator's intended payload, route system, operating practices, maintenance concepts, and desired features.

Operational Requirements

Operational requirements define the interfaces between the flight crew and each functional system, the maintenance crew and each aircraft system, and various other aircraft support people and related functions or equipment. Actions, decisions, information requirements and timing constitute the bulk of the operational requirements. Both normal and non-normal circumstances need to be considered when defining operational requirements.

Performance Requirements

Performance requirements define those attributes of the function or system that make it useful to the aircraft and its operation. In addition to defining the type of performance expected, performance requirements include function specifics such as: accuracy, fidelity, range, resolution, speed, and response times.

Physical and Installation Requirements

Physical and installation requirements relate the physical attributes of the system to the aircraft environment. They may include: size, mounting provisions, power, cooling, environmental restrictions, visibility, access, adjustment, handling, and storage. Production constraints may also play a role in establishing these requirements.

Maintainability Requirements

Maintainability requirements include scheduled and unscheduled maintenance requirements and any links to specific safety-related functions. Factors such as the percent of failure detection or the percent of fault isolation may also be important. Provisions for external test equipment signals and connections should be defined in these requirements.

Interface Requirements

Interface requirements include the physical system and item interconnections along with the relevant characteristics of the specific information communicated. The interfaces should be defined with all inputs having a source and all output destinations defined. The interface descriptions should fully describe the behavior of the signals.

Additional Certification Requirements

Additional functions, functional attributes, or implementations may be required by airworthiness regulations or may be necessary to show compliance with airworthiness regulations. Requirements of this type should be defined and agreed upon with the appropriate certification authorities.

Derived Requirements

At each phase of the development activity, decisions are made as to how particular requirements or groups of requirements are to be met. The consequences of these design choices become requirements for the next phase of the development. Since these requirements result from the design process itself, they may not be uniquely related to a higher-level requirement and are referred to as derived requirements.

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 to safety analyses) at progressively higher system levels until it is determined that no further impact is propagated.

For example, derived requirements may result from the decision to select a separate power supply for equipment performing a specific function. The requirements for the power supply, including the safety requirements, are derived requirements. The Failure Condition resulting from the fault or failure of the function supported by the power supply determines the necessary development assurance level.

Derived requirements may also result from architecture choices..

ANNEXE C : PRESENTATION DE JOHN MURATORE SUR L'INGENIERIE CHEZ SPACE X