Une expertise de Sûreté de Fonctionnement en maîtrise d'ouvrage : pourquoi ?

Hervé Du Baret

Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Une expertise de Sûreté de Fonctionnement en maîtrise d'ouvrage : pourquoi ?

DU BARET Hervé
DGA Maîtrise de l'Information
BP 7 - 35998 RENNES CEDEX 9
herve.du-baret-de-lime@intradef.gouv.fr

Résumé — L'objectif de cet article est de justifier le besoin d'expertise de Sûreté de Fonctionnement (SdF) dans une maîtrise d'ouvrage. Dans un premier temps, on analyse les relations entre maîtrise d'ouvrage (MOA) et maîtrise d'œuvre industrielle (MOI), les spécificités du métier SdF et des systèmes acquis. Cette analyse permet d'identifier des facteurs liés à l'organisation, au métier SdF et aux spécificités éventuelles des systèmes acquis justifiant le besoin d'expertise technique chez un MOA et d'en préciser les différentes missions. Un ensemble de conditions indispensables à l'efficacité de l'expertise SdF en MOA sont également établies.

Mots-clefs — maîtrise d'ouvrage, maîtrise d'œuvre, sûreté de fonctionnement, expertise

Abstract— This paper explains why a RAMS (Reliability, Availability, Maintainability, Safety) expertise in a contracting authority is needed. It analyses the relationships between the contracting authority and the prime contractor, the specificities of the RAMS job and of the systems procured. This analysis identifies factors that generate the need for a RAMS expertise in a contracting authority. A set of conditions essential to the contracting authority RAMS expertise effectiveness are highlighted.

Keywords — contracting authority, contractor, dependability, safety, expertise

I. INTRODUCTION

A. *Contexte*

Le particulier fait régulièrement l'expérience de l'intérêt de disposer d'un minimum d'expertise technique lorsqu'il achète des produits industriels complexes (automobile, produits high-tech, …). Cette expertise lui permet d'acquérir un produit répondant au mieux à son besoin et à son budget, et de réaliser au meilleur prix les éventuelles réparations. Cependant, aucun particulier ne demande l'AMDEC de son automobile et ne réalise des audits de SdF chez les équipementiers ! L'expertise en SdF des maîtrises d'ouvrages (MOA) qui réalisent des acquisitions de systèmes complexes (système d'armes, centrale de production d'énergie, système de transport…) auprès de maîtres d'œuvre Industriels (MOI) est évidemment beaucoup plus approfondie que celle du particulier.

Cependant, on peut s'interroger sur le besoin et la plus-value d'une expertise SdF d'un MOA face à des industriels spécialisés dans la conception et la fabrication de familles de systèmes analogues, depuis parfois plusieurs décennies et disposant de moyens plus significatifs. Le risque est grand pour l'expert SdF de n'être qu'une mouche du coche qui « Pique l'un, pique l'autre, et pense à tout moment - Qu'elle fait aller la machine » (La Fontaine), et de n'être qu'un coût pour le projet et une contrainte supplémentaire pour l'industriel…

La plus-value de la SdF à la conception est parfois discutée en interne MOI. Pourquoi rajouter une couche d'analyse SdF en MOA ? Comment l'expertise SdF en MOA peut-elle contribuer à la maîtrise des risques des systèmes ? L'apport de la SdF en MOA peut apparaître comme une interrogation au carré.

B. *Problématique*

On se place dans le cas où un opérateur (énergie, transport, défense…) a choisi de de ne pas conduire en propre l'étude et la réalisation d'un ou plusieurs systèmes complexes. Il choisit de l'acquérir auprès d'un MOI, avec développement ou sur étagère.

Dans le cas des industries de défense, certaines activités autrefois étatiques (ex : DCN, GIAT…) ont été externalisées sur la base de considérations de politique industrielle (gestion de l'innovation, dualité civile-militaire, accès aux marchés étrangers…) [1]. La problématique retenue ici n'est pas de se demander si le MOA a intérêt ou non à externaliser une activité donnée. L'expertise SdF d'une MOA doit considérer ce choix comme une donnée d'entrée. La question qu'on se pose dans cet article est : le MOA ayant décidé d'externaliser le développement et la réalisation de systèmes complets, est-ce qu'une expertise technique en SdF reste nécessaire chez le MOA ?

Cet article a deux objectifs :

- Justifier le besoin d'expertise SdF auprès de la Direction Technique d'une maîtrise d'ouvrage. L'expertise technique en MOA peut représenter une part significative du coût des projets . Dans un contexte de maîtrise budgétaire, qu'elle soit publique ou privée, il est nécessaire d'analyser précisément les éléments justifiant une expertise technique afin de la dimensionner au plus juste.
- Aider le nouvel expert SdF en MOA à comprendre les enjeux de son activité.

S'interroger sur le « pourquoi » de l'expertise SdF en MOA permet également de répondre à la question « pour quoi », et ainsi de définir les principales missions de l'expert SdF en MOA et d'orienter l'expertise sur des activités sur lesquelles elle a potentiellement le plus de valeur ajoutée. Cette analyse permet également d'identifier les conditions d'une plus-value de l'expertise SdF.

L'enjeu est d'optimiser le coût et l'efficacité de cette expertise, et au final d'améliorer les performances de SdF des systèmes dans des contraintes fixées de coût et de délai.

C. *Périmètre*

1) Périmètre de l'expertise

L'expertise SdF considérée ici correspond à une activité spécialisée exercée en soutien des manageurs du projet du MOA.

Le besoin d'expertise de SdF en MOA est envisagé sur l'ensemble des phases du cycle de vie des systèmes (études amont, développement, vie opérationnelle…).

2) Périmètre de la SdF

La SdF est « l'ensemble des aptitudes (fiabilité, maintenabilité, disponibilité, sécurité) d'un produit qui lui permettent de disposer des performances fonctionnelles spécifiées, au moment voulu, pendant la durée prévue et sans dommage pour lui-même et son environnement » [2]. Il faut rappeler que cet objectif très ambitieux n'est pas rempli par les seuls spécialistes SdF. La performance SdF d'un système est la résultante de l'ensemble des activités de conception et de réalisation, le métier SdF apportant des outils et méthodes en support des activités de développement dans le but de construire et évaluer les performances SdF du système.

La SdF considérée ici couvre l'ensemble des performances « FMDS » (Fiabilité, Maintenabilité, Disponibilité, Sécurité), c'est-à-dire à la fois les aspects « dependability » (FMD) et « safety » (S) des anglo-saxons. Elle comprend les aspects systèmes et composants (mécanique, électronique, logiciel…).

La SdF couvre les deux démarches complémentaires suivantes :

- une approche « processus » (probabiliste) consistant à mettre en œuvre une démarche d'identification et de maîtrise des risques de niveau système (APR, AMDEC, arbres de défaillances…) et composants (évaluation de fiabilité des composants mécaniques, électroniques, électriques, logiciels…)
- une approche « produit » (déterministe) consistant à respecter un ensemble de règles de conception relatives au nombre de barrières de sécurité, aux marges, aux règles de sélection de composants, d'isolement des signaux électriques, aux contrôles périodiques de bon fonctionnement, à la sécurité positive…

La réf. [3] précise ces deux approches.

D. *Démarche*

Dans un premier temps, on analyse les relations entre MOA et MOI, les spécificités du métier SdF et les éventuelles spécificités des systèmes acquis par le MOA.

Cette analyse permet d'identifier les facteurs à l'origine ou amplifiant le besoin d'expertise en SdF chez le MOA, les principales missions de cette expertise, puis des missions secondaires. Des conditions d'efficacité de cette expertise sont ensuite identifiées.

La Fig. 3 présente de façon synthétique les facteurs et missions identifiés et décrits dans le corps du texte, et leur articulation. Afin de faire le lien entre le corps du texte et la Fig. 3, les [Facteurs] et [Missions] sont décrits de façon synthétique entre crochets.

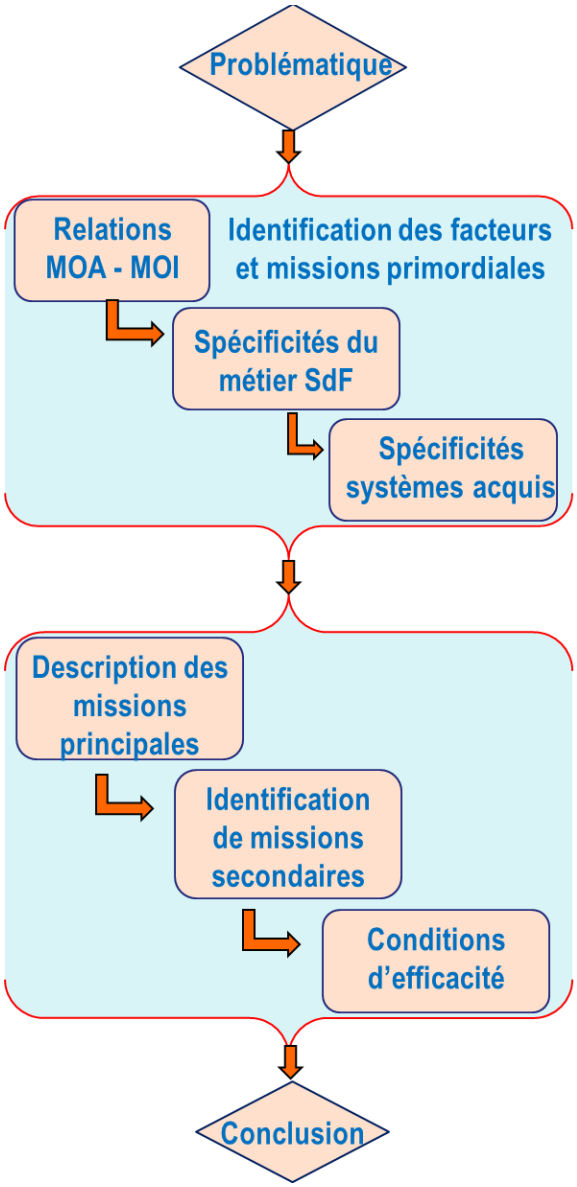


Fig. 1. Démarche suivie

Cet article s'appuie sur l'expérience de l'auteur en MOA, sur des articles des congrès λμ et RAMS et sur des échanges avec des spécialistes de SdF et d'autres activités d'ingénierie.

II. CONTEXTE MAITRISE D'OUVRAGE (MOA) / MAITRISE D'ŒUVRE INDUSTRIELLE (MOI)

A. *Finalités d'une MOA*

On retient les définitions suivantes [4] :

Maître d'ouvrage (MOA) : « organisme étatique ou industriel, client, qui, ayant passé le(s) marché(s) couvrant la globalité des travaux, sera le propriétaire de l'ouvrage ou agira pour le compte de l'acquéreur et en assumera les risques. Le maître d'ouvrage est l'acteur responsable, dans le réseau d'acquisition, de la définition des besoins (spécifiés en termes techniques et contractuels) et de la maîtrise de la réalisation confiée au maître d'œuvre afin de respecter les objectifs de performance, de coûts et de délais contractuels »

Maîtrise d'œuvre (MOE) : « personne physique ou morale qui, pour sa compétence technique, est chargée, par le maître d'ouvrage ou par la personne responsable du marché, de

l'exécution des travaux (ou de les faire exécuter) dans le respect des délais, des coûts, des ressources et de la qualité attendue ».

On désigne ici par MOI le maître d'œuvre d'un projet industriel.

De ces définitions, il ressort un premier facteur [Mission spécifique MOA] de nature organisationnelle qui est à l'origine des deux missions essentielles d'un MOA : [Spécifier] et [Qualifier].

B. Existence d'activités MOA de nature MOI

Un MOA peut acquérir « clé en main » l'intégralité d'un système complexe auprès d'un unique MOI, par exemple une usine de production d'énergie. Cependant, il est souvent amené à intégrer plusieurs systèmes complexes entre eux constituant un SdS (Système de Systèmes). Exemples : un porte-avion, avions embarqués, armements et base de soutien; installations fixes et matériel roulant ferroviaire… Pour cette part d'activité d'intégration de systèmes, le MOA est alors amené à conduire des activités qui sont par nature celles d'un MOI.

Il apparaît ainsi un second facteur [MOA $\neq$ 100%] de nature organisationnelle qui génère la mission intitulée [Concevoir le SdS].

C. Divergence d'intérêt

1) Tension entre coût d'acquisition et prix de vente

Les intérêts du MOA et du MOI sont globalement convergents, en particulier sur l'objectif de réalisation du système opérationnel dans le respect du calendrier fixé. Cependant, il apparaît une divergence légitime d'intérêts :

- Le MOA souhaite disposer d'un système répondant au strict besoin, fiable et sûr, sur l'ensemble du profil de vie, pour un coût complet minimum. Le MOA recherche des mutualisations (technologies, équipements, outils de développement, de fabrication, maintenance…) avec les autres systèmes qu'il opère.
- Le MOI souhaite réaliser une marge sur le contrat en cours et assurer la pérennité des marges de l'entreprise: il recherche un prix de vente aussi élevé que le marché le permet et tente de réduire les coûts du projet en cours et des projets futurs. Dans le cas où le contrat de suivi en service fait l'objet d'un contrat séparé de l'acquisition, l'intérêt du MOI est de maximiser le prix de vente complet du système. Le MOI recherche des mutualisations avec les autres développements qu'il conduit, éventuellement au profit d'autres clients.

2) Exposition au risque différente

Comme indiqué dans la définition du §II.A, c'est le MOA qui assume les risques de l'ouvrage : il est opérationnellement et juridiquement en première ligne ; il devra assumer les conséquences du non-respect des performances attendues (perte de confiance des clients, dédommagement des victimes, perte de crédibilité…) occasionnées par un système qu'il opère. Il peut exister des mécanismes de compensation en faveur du MOA (assurance, recours vers le fournisseur…), mais qui ne couvrent en général pas l'intégralité du préjudice subi ; de plus, la recherche de responsabilités entre le concepteur et l'utilisateur n'est pas toujours concluante.

Cette divergence d'intérêt peut conduire à une prise en compte des besoins du MOA par le MOI différente de celle attendue par le MOA. Il apparaît ainsi un troisième facteur [Divergence intérêts MOA-MOI] de nature organisationnelle qui renforce le besoin d'expertise en SdF vis-à-vis de la mission [Qualifier].

D. Contrôle externe règlementaire

Dans la plupart des secteurs d'activité ayant un impact sur la sécurité des personnes, des biens et la protection de l'environnement, la règlementation impose un contrôle de l'évaluation de sécurité du MOI par un organisme externe (par exemple, dans le domaine ferroviaire, les OQA, Organisme Qualifié Agrée). Ce contrôle externe apporte alors au MOA une confiance dans le niveau de sécurité du système qu'il acquiert. Le MOA peut également faire l'objet d'un contrôle externe pour ses activités éventuelles de MOI (cf. §II.B), ainsi que pour la conduite des opérations du système. L'existence de ces contrôles externes limite le besoin d'expertise SdF en MOA. Cependant, ces contrôles externes couvrent uniquement les aspects sécurité, pas les autres performances (en particulier pour la SdF : la fiabilité et la disponibilité).

La simple analyse du contexte MOA-MOI fait apparaît un besoin d'expertise technique, qui n'est pas propre à la SdF. Le MOA doit spécifier les performances techniques du système et le qualifier, en étant conscient de ses intérêts communs et divergents avec le MOI.

III. ANALYSE DES SPECIFICITES DU METIER SDF

L'analyse du besoin d'expertise SdF en MOA nécessite de comprendre les spécificités de la SdF par rapport aux autres activités d'ingénierie.

A. Une performance-clé…parmi d'autres

De façon générale, les performances-clé du système nécessitent une attention particulière (de la part du MOA comme du MOI) lors de l'ensemble du cycle de vie des systèmes.

Bien que « fonction de contrainte » plutôt que « fonction principale » au sens de l'analyse fonctionnelle, la SdF est une activité de conception particulièrement critique d'un projet dans la mesure où elle contribue à la sécurité, à la réussite de mission et au coût complet (via les coûts des réparations liées aux défaillances). Cela est d'autant plus le cas que les systèmes acquis par le MOA présentent des enjeux élevés en matière de fiabilité, disponibilité et sécurité.

Il faut cependant être conscient que :

- La SdF est une performance du système découlant de l'ensemble des activités de conception, le métier SdF fournissant « seulement » une démarche et un ensemble d'outils pour garantir cette performance (cf. §I.C.2).
- Dans certains secteurs (exemple : la pyrotechnie), la SdF est apparue alors qu'il existait déjà une forte culture de sécurité et une règlementation (une approche « produit », cf. §I.C.2). Elle a été rendue nécessaire par l'introduction d'éléments électroniques et logiciels. Dans ces secteurs, la SdF couvre uniquement le volet « processus » de la sécurité du système.
- Les études de performance peuvent contribuer également à la réussite de la mission ou à la sécurité. Exemple: la démonstration de sécurité des véhicules autonomes repose davantage sur les performances des

capteurs et algorithmes que sur la maîtrise des défaillances apportée par la SdF classique [5].

Il apparaît ainsi que la SdF est une discipline répondant à des enjeux critiques et nécessitant à ce titre une attention particulière. Cependant, le besoin d'expertise SdF en MOA identifié dans cet article ne doit pas être limité aux seuls experts SdF, mais doit être élargi à l'ensemble des disciplines contribuant aux performances de SdF.

B. Des concepts à adapter à chaque projet

Des notions normalisées et en apparence très simples de SdF telles que la fiabilité et la disponibilité nécessitent d'être adaptées au contexte d'utilisation. Exemples :

- Une performance de SdF doit être associée à une description précise du profil de vie et de la politique de maintenance.
- La notion de défaillance doit être définie précisément: par exemple, à partir de quel nombre de postes défaillants doit-on considérer qu'un réseau de communication est défaillant [6] ?
- La notion de fiabilité sur un profil de mission est souvent à privilégier par rapport à celle de MTBF [7], [8].
- Dans le cas de systèmes à stockage prépondérant, il faut distinguer la « disponibilité du parc » (part des équipements en état de marche lors des contrôles périodiques en stockage) de la « disponibilité opérationnelle » (part des équipements en état de marche lors de la sollicitation par l'utilisateur).
- Un objectif de pourcentage de disponibilité seul n'est en général pas suffisant ; il est souvent nécessaire de préciser les durées maximales acceptables des indisponibilités [6].
- Il faut se focaliser sur les performances-clés de SdF afin de traduire le besoin opérationnel, sans contraindre inutilement la conception ; par exemple, si les objectifs de fiabilité et disponibilité et la politique de maintenance ont été clairement définis, on peut en règle général se dispenser d'exigences de testabilité.

L'apparente simplicité des notions de SdF peut conduire à définir des exigences inappropriées. Il est essentiel de :

- clarifier ces notions, avec les parties prenantes (opérationnels, directions de projet, MOI), lors de la spécification des systèmes,
- s'assurer que les exigences sont correctement interprétées par le MOI pendant le développement.

Ce facteur [Concepts SdF à adapter] renforce le besoin d'expertise SdF en MOA vis-à-vis de la mission [Spécifier].

C. Une démarche à la mise en œuvre complexe

1) Une performance difficilement vérifiable par essais

Certaines caractéristiques et performances sont physiquement mesurables avec une précision élevée, et donc vérifiables sur un ou quelques exemplaires du système : masse, encombrement, consommation…

Les performances fonctionnelles sont souvent plus difficilement vérifiables dans tous les scénarios envisageables et pour un coût raisonnable. Il faut alors construire et valider des modèles complexes, rechercher un optimum entre les différents modes de démonstration (calculs, simulations, essais partiels ou essais système) et recaler les modèles sur les essais. Il est alors possible d'élaborer des plans de validation couvrant l'ensemble des scénarios de fonctionnement souhaités.

De façon générale, les performances de SdF peuvent être vérifiées par analyse ou par essais, dédiés ou non [8]. Dans le cas de systèmes complexes, les performances de SdF sont difficilement vérifiables car :

- Qualitativement : la SdF ne consiste pas à vérifier que le système remplit le nombre fini de fonctions pour lesquelles il a été conçu, mais de vérifier qu'il n'est pas susceptible de présenter des comportements imprévus. Il n'est pas possible de garantir l'exhaustivité des modes de défaillance et des scénarios accidentels du système.
- Quantitativement : La fiabilité étant une grandeur aléatoire et les objectifs de fiabilité étant en général élevés, les démonstrations de fiabilité nécessitent des retours d'expérience volumineux. On cherche à quantifier la probabilité d'événements rares. De plus, la fiabilité dépend très fortement du contexte d'utilisation. Ainsi, pour des systèmes complexes, les niveaux de fiabilité (et a fortiori les niveaux de sécurité) ne peuvent pas être constatés à un coût raisonnable par des essais lors de la qualification/réception. Seule l'exploitation des données opérationnelles de la totalité de la durée de vie du parc de systèmes permettra éventuellement de valider les évaluations prévisionnelles.

La SdF apparaît, dans des contraintes de coût acceptables, non vérifiable en qualification. Ainsi, la garantie de l'atteinte des performances de SdF repose principalement sur la mise en œuvre d'une démarche spécifique.

2) Une démarche à adapter aux systèmes considérés

Chaque secteur industriel présente une histoire, des risques, des technologies et des contraintes spécifiques. Le spécialiste SdF est un praticien qui doit, à partir d'une boîte à outils constituée d'un ensemble de méthodes génériques (APR, AMDEC, arbres de défaillances, fiabilité système, réseaux de Pétri…), construire une démarche SdF adaptée à son secteur industriel et au système considéré. Cela nécessite de choisir les bons outils et de les calibrer à l'application considérée.

3) Une nécessaire intégration de la SdF à la conception

La SdF est une activité de support à l'ensemble des activités de conception et d'industrialisation. Elle permet d'identifier, d'évaluer et de hiérarchiser les risques et de proposer des actions correctives.

Les défaillances peuvent provenir de n'importe quel élément en apparence anodin d'un système, parfaitement conçu, réalisé et utilisé par ailleurs. De ce fait, la démarche de SdF doit être mise en œuvre sur l'ensemble du système. Elle doit s'appuyer sur une connaissance approfondie du système (profil de vie, technologies mises en œuvre, logique de fonctionnement) et de son utilisation. L'expert SdF trouve auprès des concepteurs ces informations.

Un référentiel relativement lourd doit être décliné du système au composant. Au fur et à mesure qu'on descend dans l'arborescence produit du système, la visibilité sur l'origine du

besoin (ex : les événements redoutés du système) et sa compréhension diminuent. L'expert SdF apporte au concepteur l'explication du besoin SdF.

La singularité de la SdF provient de ce qu'elle utilise des techniques de nature différente des autres activités de conception et qu'elle s'intéresse aux dysfonctionnements des systèmes. Un concepteur n'envisage pas nécessairement la possibilité d'occurrence de défaillances dans les systèmes qu'il conçoit, ni la mise en place de mesures de protection, et donc le besoin de s'appuyer sur un spécialiste SdF. Les responsables de lot/ingénieurs en chef des MOI ont souvent une compétence limitée en SdF, ce qui conduit à une vérification de la documentation SdF insuffisante. Inversement, l'expert SdF n'a pas toujours des compétences techniques de conception du système considéré. Ainsi, l'intégration de la SdF à la conception est souvent insuffisante.

Une mauvaise intégration de la SdF à la conception génère principalement les risques suivants :

- des analyses de SdF qui ne s'appuient pas sur la définition en cours du système,
- des analyses SdF conduites en fin de développement, dans le seul but de répondre à une demande contractuelle sans améliorer la définition du produit.

4) Une mise en œuvre sur toute la durée du cycle de vie du système

La SdF doit être menée de façon « continue et itérative » [2] sur l'ensemble du cycle de vie du système. Elle doit être mise en œuvre dès l'expression de besoin (identification des objectifs de SdF et des normes pertinentes) et la conception préliminaire (identification des risques, choix d'architecture et de technologies et définition de la politique de maintenance), puis à chaque jalon de la conception détaillée afin de vérifier l'accessibilité puis l'atteinte des performances SdF spécifiées. La SdF doit également vérifier que les phases de fabrication et d'utilisation ne dégradent pas les performances de SdF. Enfin, la confiance dans les évaluations de SdF prévisionnelle étant toujours limitée, un suivi en service est nécessaire afin de s'assurer que les performances SdF sont respectées pendant la vie opérationnelle.

5) Une discipline en interaction avec d'autres activités transverses

La SdF est en interaction avec d'autres disciplines transverses. Elle fournit au SLI les données de fiabilité nécessaires au dimensionnement des stocks de pièces de rechange. Dans les structures dans lesquelles la SdF est rattachée au SLI, il y a un risque de négliger la contribution de la SdF à la réussite de mission et à la sécurité. Quand la SdF et le SLI sont respectivement rattachés à la conception et aux services de Support Client, un risque est que les données de fiabilité opérationnelle ne soient pas exploitées convenablement par le SLI.

Par ailleurs, la SdF contribue à la sécurité des systèmes. Les études de sécurité doivent prendre en compte les apports de la sécurité fonctionnelle (le volet « processus » de la sécurité) ; elles ne doivent pas se limiter aux sujets « historiques » de sécurité règlementaire (risque électrique, incendie, pyrotechnique), i.e. l'approche « produit ».

Il apparaît que la démonstration de l'atteinte des performances de SdF repose sur la mise en œuvre d'un ensemble de méthodes devant être adaptées à l'application envisagée et mises en œuvre tout du long du développement de façon coordonnée avec les autres activités du projet.

On verra au §V.C que ce facteur [Mise en œuvre complexe] renforce le besoin d'expertise SdF en MOA vis-à-vis de la mission [Qualifier].

IV. Analyse des specificites des Systemes acquis

On désigne ici par systèmes à Retex Représentatif Réduit (« R^3 ») des systèmes pour lesquels il n'est pas possible de disposer d'un retour d'expérience dans des conditions d'utilisation représentatives (en termes de définition, fabrication et utilisation) du système avant sa qualification et sa mise en service. Le retour d'expérience représentatif apporte une confiance dans l'atteinte des performances de SdF du système. Ce paragraphe présente plusieurs origines possibles d'un retour d'expérience représentatif.

A. Volume de production du système acquis

Dans le cas où le système acquis fait l'objet d'une production de grande série (seuil typique : 500 articles), il est possible de vérifier le bon fonctionnement d'un nombre significatif d'exemplaires. Le retex est valide dans la mesure où la capabilité du processus de fabrication est acquise [9]. Le coût de ces essais, même dans le cas où ils sont destructifs, peut être acceptable devant le coût du projet.

B. Eléments analogues en service

Des systèmes acquis par un MOA peuvent comporter des éléments relativement peu innovants présentant de grandes similitudes avec des éléments en service ayant fait l'objet de développements précédents.

C. Eléments testables avant réception

Certains systèmes, bien qu'innovants et réalisés en petite série, peuvent disposer d'une forme de retour d'expérience. C'est le cas des systèmes dont le fonctionnement peut être intégralement testé avant leur mise en service dans des conditions représentatives de leur emploi réel (ex : système de contrôle-commande d'une centrale nucléaire, système de freinage d'un TGV…). Cependant, pour certaines applications (ex : aéronef), du fait du coût et des risques liés aux essais, il peut être nécessaire de garantir des performances de SdF élevées avant la réalisation des essais de niveau système.

Exemple d'éléments non testables avant réception :

- Les éléments dits « one-shot », dont le fonctionnement est destructif, tels qu'un propulseur de lanceur/missile ne sont pas testables avant réception.
- Il faut être conscient des limites du retex apporté par les tests : le fonctionnement de certains équipements électroniques peut être testable avant réception, mais dans des conditions d'environnements mécanique, thermique ou électromagnétique qui ne sont pas complètement représentatives de l'emploi opérationnel.

D. Illustration

Trois natures de retour d'expérience ont été identifiées. Le schéma ci-dessous illustre le fait que l'existence d'un retour d'expérience représentatif diffère selon les systèmes considérés.

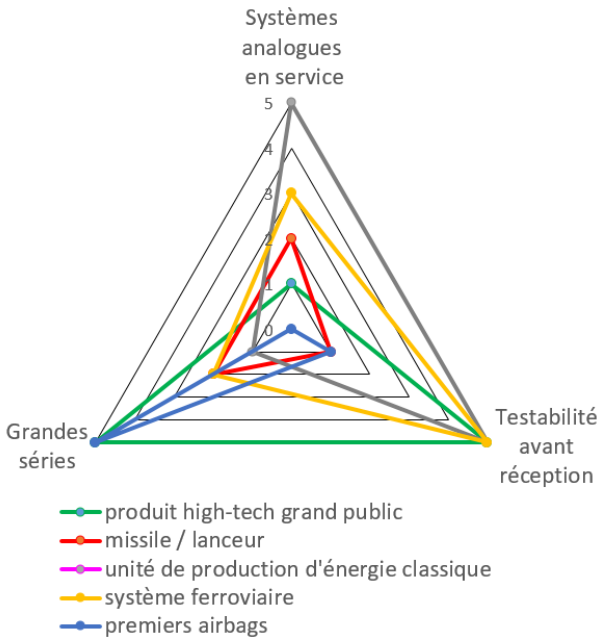


Fig. 2. Retex représentatif de diverses familles de systèmes

Il s'agit d'une première approche grossière par familles de systèmes, les retours d'expérience disponibles devant être analysés plus précisément pour chaque nouveau développement de système, et pour chaque élément du système.

Il existe des systèmes (dits ici R^3) bénéficiant de peu de retour d'expérience selon les trois natures identifiées. Il s'agit de systèmes innovants, fabriqués en en un nombre d'exemplaires limité, extrêmement coûteux et qui ne peuvent être intégralement testés avant tir. Les lanceurs spatiaux ou les missiles rentrent dans cette catégorie (triangle rouge de la Fig. 2).

E. Vérificabilité des systèmes R^3

De façon générale, les performances de SdF d'un système peuvent être obtenues par deux approches complémentaires, produit et processus (cf. §I.C.2). L'existence d'un retour d'expérience liés à des éléments analogues en service permet de :

- améliorer la confiance dans l'approche processus : exhaustivité des scénarios accidentels, données de fiabilité (taux de défaillance) des composants, équipements et systèmes,
- robustifier l'approche produit, en élaborant des règles de conception qui limitent les risques (et également la plus-value de l'approche processus).

L'existence de chacune des formes de retour d'expérience améliore la confiance dans les performances de SdF annoncées par un MOI.

En revanche, pour un système R^3, il n'existe pas d'architectures éprouvées et la confiance dans les données de fiabilité est limitée. Une approche « processus » renforcée est alors incontournable. Des méthodes de SdF spécifiques doivent être mises en œuvre pour garantir la maîtrise des défaillances systématiques de conception et de fabrication (analyse SdF du DJD, croissance de fiabilité, etc.) et assurer la conformité du produit réalisé à sa définition (ex : sécurité de réalisation [10]).

Ainsi, ce facteur « Système R^3 » renforce le facteur « Mise en œuvre complexe » et le besoin d'une expertise SdF vis-à-vis de la mission « Qualifier ».

Cependant, cette notion de retour d'expérience disponible ne se décline pas de façon homogène sur l'ensemble d'un système donné. On peut, pour certains éléments du système, bénéficier du retour d'expérience de systèmes antérieurs, voire d'un autre secteur (ex : équipements ou cartes électroniques de systèmes militaires réutilisant ou très similaires à des matériels civils mis en œuvre dans des environnements comparables) ou tester avant réception certaines fonctions, au moins partiellement. La présence de retour d'expérience peut permettre d'alléger l'expertise en MOA pour certains éléments du système.

V. MISSIONS DE L'EXPERTISE SDF EN MOA

Les facteurs à l'origine des principales missions de l'expertise SdF en MOA ayant été identifiés au chapitre précédent, ce chapitre développe les enjeux et difficultés de ces missions, ce qui génère des missions complémentaires.

On présente les missions de l'expertise SdF en MOA dans un ordre logique visant à montrer l'origine de chaque mission. Cette approche ne prend pas en compte le séquentiel des missions dans le cycle de vie des systèmes.

A. Concevoir le SdS

Dans le cas où le MOA acquiert différents systèmes qu'il intègre dans un SdF, il est amené à conduire des activités qui sont par nature celles d'un MOI (cf. §II.B). Cette activité de conception du SdS est alors une mission primordiale du MOA.

Le besoin de compétences chez le MOA dans certaines disciplines est alors évident. Par exemple, la précision d'un système d'armes dépendra de façon imbriquée des précisions des moyens de mesure au sol, sur la plateforme de tir et dans le projectile.

A première vue, l'activité de SdF liée à une intégration d'un faible nombre d'ensembles peut sembler relativement facile, la fiabilité d'un élément étant souvent une fonction simple de la fiabilité de ses différents constituants. Une direction de projets peut être tentée de réaliser une allocation de la performance SdF du système vers les sous-systèmes et une consolidation des performances SdF des sous-systèmes par des analyses « de coin de table ».

Une analyse approfondie est cependant nécessaire :

- L'identification des risques doit se faire au niveau du système complet, vis-à-vis des agressions et du fonctionnel, une chaîne de sécurité donnée pouvant être répartie sur plusieurs sous-systèmes. Les risques d'un système ne s'obtiennent par simple compilation des risques de ses sous-systèmes.
- La déclinaison des objectifs quantitatifs de SdF n'est pas toujours immédiate, les profils et durées de vie des sous-systèmes pouvant être différents.
- Une cohérence dans les démonstrations de SdF doit être assurée, afin d'obtenir un niveau de confiance comparable dans les justifications de SdF des différents sous-systèmes.

Une difficulté de l'expertise SdF dans cette mission provient de ce que cette activité d'ingénierie porte sur le sommet de l'arborescence du système, avec des sous-systèmes

de natures très différentes (dans le cas de systèmes de défense : plateformes navales, aériennes, télécommunications…). Chaque sous-système ayant un référentiel et des justifications de SdF spécifiques et volumineux, la maîtrise de la démonstration de sécurité de l'ensemble du système est difficile à acquérir par un seul expert SdF. Au-delà de l'aspect technique, chaque système étant piloté par une direction de projet dédiée (dans une organisation « en silo »), il peut être difficile d'obtenir une visibilité sur l'ensemble des justifications.

Les risques liés à une expertise SdF en MOA insuffisante vis-à-vis de cette mission de conception sont ceux de n'importe quel MOI : déclinaison et justification des exigences incorrectes /incomplètes et, à terme, une conception ne permettant pas d'atteindre les performances SdF attendues.

Cette mission « concevoir le SdS » est particulièrement délicate dans le cas de l'acquisition sur étagère d'un sous-système. Il est alors important d'identifier dans les justifications du MOI les conditions de validité des évaluations de SdF afin d'intégrer correctement les performances SdF du sous-système acquis sur étagère dans le système de niveau supérieur [11].

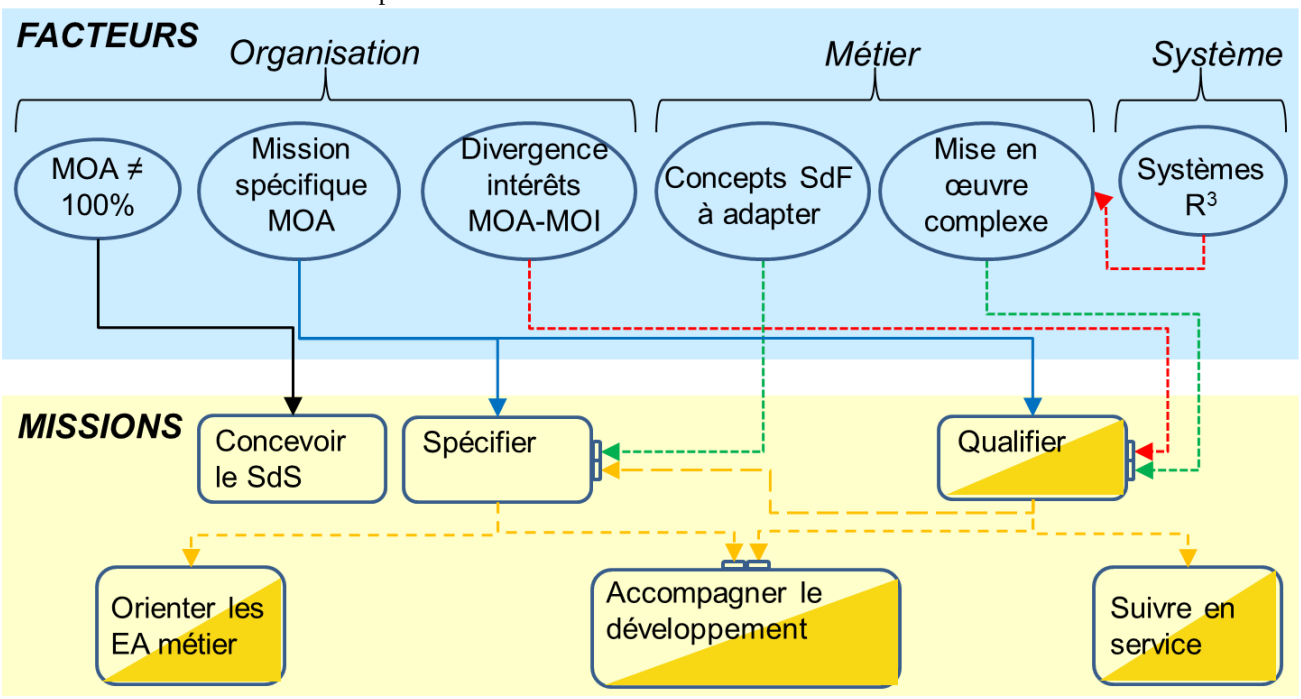
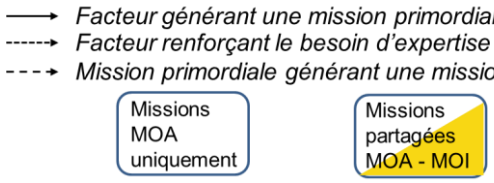


Fig. 3. Facteurs et Missions de l'expertise SdF en MOA

Légende



B. Spécifier

Le MOA doit spécifier les performances du système d'ensemble (cf. §II.B) et des sous-systèmes acquis auprès d'un MOI (cf. §II.A).

La spécification correspond à la traduction de l'expression de besoin en spécification technique (STB) du système. La spécification ne correspond pas aux tâches d'expression de besoin (utilisation attendue du produit, objectif de coût complet…), du ressort de l'utilisateur, ni de déclinaison des spécifications techniques vers les sous-systèmes et équipements, du ressort du MOI.

On a vu que spécifier était une mission essentielle du MOA, et que le facteur [Concepts SdF à adapter] renforçait le besoin d'expertise SdF en MOA sur cette mission. Cette mission requiert une connaissance de l'utilisation opérationnelle des systèmes acquis par le MOA, dont un MOI ne dispose pas toujours.

Par ailleurs, la qualification s'appuyant sur la mise en œuvre d'une démarche complexe (cf. §III.C), il importe d'inclure dans la spécification la démarche de SdF à mettre en œuvre. Cette démarche est spécifiée à travers le référentiel normatif applicable au contrat, et, quand les normes existantes apparaissent insuffisantes ou inadaptées, dans des exigences du CCTP (Cahier des Clauses Techniques Particulières).

Du fait du caractère non vérifiable des performances de SdF, amplifié dans le cas de systèmes R^3, et de la divergence d'intérêts entre MOA et MOI, les deux parties peuvent avoir des appréciations très différentes du plan de SdF qu'il est nécessaire de mettre en œuvre. Il en découle un besoin d'expertise de SdF en MOA afin de spécifier une démarche SdF appropriée, puis de vérifier le plan de management/SdF proposé par le MOI.

Une difficulté de la mission [Spécifier] est de définir une stratégie de qualification de la SdF appropriée au système développé : approche produit ou processus, la seconde pouvant être spécifiée de façon plus ou moins prescriptive. Cela peut être résumé de la façon suivante, inspirée de [3] :

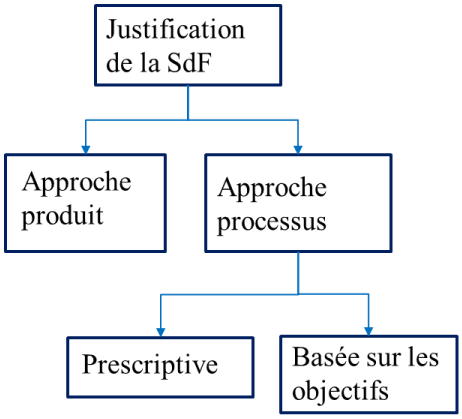


Fig. 4. Stratégie de qualification de la SdF

Dans le cas des systèmes R^3, l'approche SdF spécifiée est de nature « processus » plutôt que « produit » (cf. §IV.E), ce qui rend plus difficile la qualification (cf. §V.C), mais aussi la spécification.

Dans le cas où une approche processus de la SdF est mise en œuvre, il faut veiller à spécifier de façon précise sans être excessivement prescriptif : aux Etats-Unis en 1993, les normes MIL-HDBK, sans équivalentes civiles, ont été annulées par le DoD car les industriels s'attachaient davantage à respecter les normes qu'à concevoir des produits effectivement fiables et sûrs [12]. Cependant, la référence [7] montre que ce relâchement du référentiel normatif SdF des contrats a conduit à une régression des pratiques SdF des industriels.

Ainsi, les risques pour le MOA liés à la spécification sont:

- les exigences de performances de SdF ne traduisent pas correctement le besoin opérationnel,
- la démarche et les normes de SdF spécifiées dans le CCTP sont insuffisantes ou inappropriées, ou excessivement prescriptives. A terme, les performances SdF spécifiées ne sont pas atteintes.

Les activités de spécification de SdF constituent une mission primordiale de la SdF en MOA visant d'une part à formuler correctement le besoin technique, et d'autre part à définir le bon niveau d'exigences méthodologiques. Pourtant, un travers parfois observé est que l'activité de spécification ne représente qu'une part très marginale de cette activité, la qualification en occupant la principale du fait de la documentation volumineuse produite par le MOI à ce stade. Il est essentiel que les experts SdF du MOA soient consultés et que les exigences de SdF (STB et CCTP) ne soient pas simplement reconduites et adaptées de projets précédents.

La spécification est finalisée en phase contractualisation. L'expertise SdF du MOA doit alors permettre de vérifier que les activités SdF du MOI sont effectivement financées.

Ces deux premières missions [Spécifier] et [Concevoir le SdS] sont primordiales dans la mesure où elles sont de la seule responsabilité du MOA : il ne faut pas espérer que le(s) MOI comble(nt) les éventuelles lacunes du MOA dans ces deux missions.

C. Qualifier

La qualification est « l'ensemble des tâches qui concourent à fournir des preuves, en se basant sur des justifications théoriques et expérimentales, que le produit défini répond au besoin spécifié et est productible ». La qualification est prononcée par le MOA sur la base des justifications apportées par le MOI [13].

Dans le cas de systèmes standards réalisés en grandes séries, l'ensemble des activités de SdF (des études amont au suivi en service) sont conduites par un unique industriel. Une éventuelle mauvaise performance du système est constatée par l'industriel sur des premiers de séries non commercialisés. De plus, le retour d'expérience est remonté en boucle courte vers l'industriel et bénéficie à l'ensemble des acheteurs. L'acheteur s'appuie sur l'image de marque du constructeur. Le besoin de vérification des performances annoncées est alors limité. Ce n'est pas le cas des systèmes acquis par une MOA, le nombre d'exemplaires étant en général limité.

Dans le cas de systèmes acquis par un MOA, une performance vérifiable n'a pas besoin de faire l'objet d'une expertise approfondie chez le MOA. Du fait que la démonstration de la tenue des performances de SdF repose sur la mise en œuvre d'une démarche spécifique et de la divergence d'intérêts entre MOA et MOI, les deux parties peuvent avoir des niveaux d'exigences différents en termes de choix et d'approfondissement des méthodes de SdF à mettre en œuvre. Une vérification indépendante des analyses de SdF du MOI est nécessaire. Les facteurs [Mise en œuvre complexe] et [Divergence d'intérêts MOA-MOI] renforcent le besoin d'une expertise SdF en MOA vis-à-vis de la mission [Qualifier]. La qualification se prépare dès la phase de spécification, à travers la validation par le MOA du plan de SdF (cf. §V.B).

Dans le cas de systèmes R^3, on a vu qu'une approche SdF « processus » était à privilégier sur une approche « produit » (cf. §IV.E). Une approche processus est plus difficilement vérifiable qu'une approche produit : l'approche processus s'appuie sur des analyses complexes dont l'exhaustivité et l'exactitude sont discutables, tandis que l'approche produit concerne le respect de règles factuelles de conception. Ainsi, le facteur « système R^3 » renforce le besoin d'expertise SdF en MOA vis-à-vis de la mission « Qualifier ».

Les risques d'une expertise SdF en MOA insuffisante à ce stade sont :

- Les analyses sont insuffisamment approfondies, les hypothèses excessivement optimistes, la traçabilité et les justifications insuffisantes. Les analyses sont sous-traitées à des prestataires peu expérimentés. Ainsi, [14] illustre comment une maîtrise d'ouvrage ferroviaire qui n'a pas d'expertise technique et qui se contente pendant le développement de faire confiance aux promesses des industriels obtient des performances de SdF médiocres.
- La fiabilisation (croissance de fiabilité) du système est insuffisante.

On peut s'interroger sur la possibilité d'un MOA de vérifier les études SdF du MOI alors qu'il ne dispose pas de l'ensemble des données de conception/fabrication du système, et que ses ressources sont moindres que celles du MOI. De plus, il serait inefficace que le MOA vérifie l'intégralité des analyses du MOI. La référence [15] propose des pistes pour établir une démarche structurée permettant d'évaluer le niveau de confiance dans les performances de fiabilité/sécurité du système (ex : plan de vérification, points de vigilance) par une entité externe.

D. Accompagner le développement

La difficulté de vérifier les performances de SdF en fin de développement, plus particulièrement pour les systèmes R^3, rend nécessaire un suivi de l'ensemble du développement.

1) Evaluer le processus SdF

On a vu que la démarche de SdF devait être mise en œuvre par le concepteur (MOI) sur toute la durée du développement (cf. §III.C). On peut imaginer que le MOA ne vérifie qu'en fin de développement l'ensemble des activités de SdF conduites par le MOI et les équipementiers pendant l'ensemble du développement. A priori, cela permettrait de vérifier que les objectifs SdF sont tenus. Une expertise SdF en MOA apparaît cependant nécessaire pendant l'ensemble du développement :

- Il y a un risque que les exigences SdF de la STB aient été mal interprétées par le MOI (facteur [Concepts à adapter]) ou qu'un élément du référentiel normatif n'ait pas été pris en compte, ce qui aurait des conséquences lourdes en termes de coût/délai.
- Il est nécessaire d'identifier au plus tôt d'éventuelles faiblesses chez le MOI ou ses sous-traitants, éventuellement sur seulement certaines méthodes de SdF.
- La SdF permet d'identifier des points d'amélioration d'une conception donnée. La prise en compte de recommandations portant sur la définition du produit présente un coût significatif en fin de développement alors que le coût est davantage acceptable en début de développement. L'impact de la prise en compte d'une recommandation d'ordre méthodologique sur le niveau de fiabilité/sécurité étant souvent difficile à évaluer, ces recommandations ne sont en général pas prises en compte quand elles sont émises en fin de développement.
- Il faut veiller à ce que les nouvelles pratiques de développement (« agile », « design to cost »…) mises en œuvre afin de réduire les coûts et délais ne dégradent pas la qualité des analyses SdF [16] [17].
- Le travail d'expertise du MOA de l'ensemble de la documentation SdF en fin de développement introduirait un délai incompatible du planning du projet.
- Il faut principalement veiller à ce que le MOI, afin d'être conforme aux spécifications, ne surévalue pas les performances Sdf du système. Inversement il faut parfois s'assurer qu'il ne les sous-évalue pas dans le but de faciliter la négociation d'un marché ultérieur (ex : conception détaillée ou suivi en service).

Ainsi, la difficulté de qualifier une performance SdF génère le besoin d'une expertise approfondie de SdF dès la phase de conception préliminaire. Le principal risque d'une expertise SdF en MOA insuffisante pendant le développement est de disposer d'un système pour lequel on ne dispose pas de justifications satisfaisante de tenue des performances SdF.

2) Evaluer les choix de conception/technologies

Les besoins de SdF peuvent être déterminants dans les choix d'architecture (présence et types de redondances, de contrôles, implantation matérielle ou logiciel des différentes fonctions…) et de technologies. Au-delà des justifications insuffisantes (cf. §V.D.1), un processus SdF non satisfaisant peut aboutir à un système ne respectant pas les exigences de SdF du fait des raisons suivantes :

- Il arrive que les objectifs de SdF passent au second plan quand l'effort de conception se concentre excessivement sur l'atteinte des performances-clés du système.
- Le MOI propose des solutions réutilisables (en termes d'architectures, équipements ou composants) issues de son catalogue actuel et futur, mais qui ne répondent pas de façon optimale au besoin (en-deçà ou au-delà) du MOA. Inversement, certaines technologies prometteuses pour l'application considérée peuvent ne pas être envisagées par le MOI car coûteuses à court terme ou incohérentes avec la stratégie de l'entreprise. Si le besoin du MOA est spécifique, il y a un risque de se laisser imposer des choix techniques (architecture, technologies…) par le MOI ne répondant pas de façon optimale à la spécification.
- dans le cas où le développement d'un système et son maintien en condition opérationnel (ou soutien en service) font l'objet de contrats séparés, le MOI n'est pas incité à proposer une solution minimisant le coût global.

Les implications des choix de conception sur les scénarios accidentels, sur les fiabilités des composants, sur la politique de maintenance (contraintes liées aux contrôles) ne sont pas toujours immédiates. En phase de conception préliminaire, il est facile de d'affirmer l'accessibilité de performances SdF sur la base d'hypothèses approximatives ou incomplètes afin de favoriser un choix de conception. Une expertise SdF en MOA permet de valider (ou de remettre en cause) la conception préliminaire proposée par le MOI.

E. Suivre en service

De façon générale, l'objectif du suivi en service est de s'assurer que les performances non (ou partiellement) démontrées en qualification sont effectivement respectées et de faire évoluer si besoin la conception, la fabrication ou le profil de vie du système.

La confiance dans les évaluations de SdF prévisionnelle en fin de développement est toujours limitée, plus particulièrement dans le cas des systèmes R^3. Un suivi précis des faits techniques rencontrés pendant la vie opérationnelle du système est nécessaire pour confirmer/infirmer les performances de SdF opérationnelles et détecter d'éventuels signaux précurseurs d'accidents. Le guide [18] fournit des éléments pour tirer un maximum d'information de chaque fait technique.

L'évaluation de la SdF opérationnelle est un processus qui implique les opérateurs, le MOA et le MOI :

- Les opérationnels doivent rendre compte précisément de l'utilisation de l'ensemble des matériels du parc (profil de vie, environnements rencontrés, tests réalisés…) et des conditions d'apparition des défaillances.
- Le MOI, concepteur du système, dispose des données de conception permettant d'identifier les causes des « faits techniques » (les défaillances) et il lui appartient de conduire les évolutions de définition/fabrication rendues éventuellement nécessaires.

- L'évaluation des performances de SdF opérationnelle nécessite d'identifier la responsabilité de la cause de chaque fait technique : utilisateur ou concepteur. Le besoin d'expertise SdF chez le MOA provient du risque pour le MOA que le MOI minimise la gravité des faits techniques rencontrés (en particulier quand ils impactent la sécurité) ou attribue à tort la responsabilité d'un fait technique à l'utilisateur. (Cependant, MOA et MOI s'accordent en général sur la gravité de la plupart des faits techniques.)

Par ailleurs, les évaluations de SdF opérationnelles apportent des informations sur les modes de défaillance et leurs occurrences. Ainsi, elles permettent d'améliorer la qualité des analyses qualitatives et quantitatives de SdF des développements futurs. Il est donc important que l'expert SdF en MOA en ait connaissance.

F. Orienter les études amont

1) Orienter les études amont (architectures / technologies)

Les études amont peuvent répondre à un besoin de nouvelle capacité ou d'évaluation de l'intérêt de nouvelles technologies et architectures sur les applications du domaine et à les faire monter en maturité, via les niveaux TRL (cf. [19] pour les systèmes spatiaux). Par ailleurs, une étude amont peut être entreprise dans le but de répondre à un besoin SdF (exemple : remplacement de lignes pyrotechniques de lanceurs par des lignes optopyrotechniques afin d'améliorer la tenue aux environnements électromagnétiques et la contrôlabilité). Le lancement de programmes d'acquisition suppose que les technologies nécessaires sont disponibles et ont atteint un niveau de maturité suffisant (environ TRL 7).

Les études amont répondant souvent à des besoins spécifiques du MOA et n'étant pas toujours immédiatement concluantes et rentables, leur financement est principalement assuré par le MOA. Il est donc nécessaire de spécifier des études amont (vers les MOI ou équipementiers) et de faire une analyse critique des propositions industrielles.

La SdF peut apporter des outils utiles au concepteur contribuant à la montée en maturité des technologies (ex : AMDEC, essais aggravés). Une montée en maturité s'achève habituellement par des essais qui sanctionnent la qualité des travaux de R&D. Néanmoins, des analyse SdF conduites par le MOI peuvent contribuer à s'assurer que les risques sont correctement levés.

Dans le cas où des performances SdF font l'objet d'évaluations préliminaires, l'intérêt du MOI est de convaincre le MOA de la faisabilité d'un concept, mais aussi de s'assurer que les exigences (dont SdF) qui seront fixés en entrée de développement seront atteignables. Cela peut conduire l'industriel à surévaluer les différents risques (en particulier leurs probabilités).

Une expertise SdF en MOA est nécessaire en études amont portant sur une nouvelle architecture/technologies pour les mêmes raisons que vis-à-vis d'une architecture préliminaire en phase de développement (cf. §V.D.2).

2) Orienter les études amont (métier)

Les études amont métier recouvrent des activités très diverses : projets et GTR IMdR, suivi de thèses, normalisation, expérimentations, etc. L'objectif final est d'améliorer les spécifications (STB et CCTP).

Le retour d'expérience de la qualification des programmes peut conduire à identifier des pistes d'amélioration de la démarche de SdF mise en œuvre sur les systèmes acquis par le MOA. En fonction de la maturité de la solution, ces points peuvent être pris en compte directement dans les clauses des CCTP des futurs développements, dans des normes ou nécessiter des recherches complémentaires.

Du fait de la divergence d'intérêts entre MOA et MOI, les deux parties n'ont pas le même niveau d'exigences en termes d'amélioration des méthodes de SdF (approches produit et processus).

Dans le cas de systèmes faisant l'objet de normes établissant des règles de conception (approche « produit », cf. §I.C.2) spécifiques à la famille de systèmes acquis par le MOA, il est impératif que le MOA s'implique dans l'élaboration de ces normes. En effet, les règles de conception sont pertinentes pour un produit dans une application donnée. Le MOA doit veiller à ce que les exigences figurant dans les normes sont pertinentes dans le cas du système qu'il acquiert. Le risque est double :

- Les normes imposent des règles de conception n'apportant pas de plus-value dans l'application considérée, ce qui génère un surcoût significatif pour le MOA.
- Les produits acquis par le MOA dans les applications qu'il envisage présentent des risques qui ne sont pas pris en compte dans les normes. Un MOI pourra justifier une approche SdF « processus » peu approfondie en mettant en avant la conformité à des normes qui ne garantissent pas la fiabilité et/ou sécurité dans le cas considéré.

Les évaluations quantitatives de SdF prévisionnelles ne sont valides que dans la mesure où les défaillances de nature systématique (conception et fabrication) ont été éliminées avant le début de la vie opérationnelle. Dans le cas des systèmes R^3, il est très difficile de garantir que cette hypothèse est vérifiée. De ce fait, les systèmes R^3 nécessitent des méthodes SdF spécifiques visant à s'assurer de la prévention et de l'élimination des défaillances systématiques. La sécurité de réalisation [10] dont l'objectif est de montrer que la fabrication et l'utilisation du produit ne remettent pas en cause le niveau de sécurité évalué en conception est un exemple de méthode plus spécialement dédiée aux systèmes R^3. Il est impératif qu'une MOA acquérant de tels systèmes soit motrice dans le développement de ces méthodes.

Le bénéfice de l'implication d'une MOA dans les activités métier est moindre quand il s'agit de guides/normes de SdF traitant de méthodes génériques (AMDEC, arbres de défaillances…) pour lesquelles le MOA bénéficie de l'expérience de l'ensemble des domaines industriels (aéronautique, nucléaire…). Le MOA peut toutefois avoir un intérêt pour ces méthodes, d'une part en tant que MOI de SdS, d'autre part en tant que client des analyses conduites par un MOI. Un point d'attention particulier du MOA est alors de s'assurer qu'il disposera des données nécessaires pour se prononcer sur l'acceptabilité d'études SdF (exemple : comment une étude SdF basée un modèle MBSA est-elle validée par un MOA ?).

Par ailleurs, l'analyse menée dans cet article met en évidence des activités de l'expertise SdF en MOA différentes de celles d'une expertise SdF en MOI. Il semble que la plupart

des normes et guides de SdF se placent dans le cadre d'un industriel responsable de l'ensemble du cycle de vie des systèmes (dont la spécification) et n'approfondissent pas les rôles respectifs du MOA et du MOI et les missions spécifiques du MOA. Exemples de problématiques spécifiques à un MOA: faut-il spécifier une démarche Sdf produit ou processus (cf. §V.B)? Comment obtenir un niveau de confiance satisfaisant dans les évaluations de SdF du MOI avec des ressources et des informations sur la conception du système limitées ? De ce fait, la participation à des groupes de travail et de normalisation impliquant d'autres MOA, idéalement réalisant des acquisitions de systèmes analogues est souhaitable.

Le risque d'une absence d'expertise SdF en MOA en études amont est que les industriels reconduisent les activités SdF de projets en projets et limitent leurs efforts dans l'amélioration des méthodes existantes et la mise en œuvre de nouvelles méthodes, la réduction de risque apportée par un investissement dans ces normes étant jugée faible.

Il en ressort que l'implication d'une expertise SdF en MOA dans des GT et groupes de normalisation est nécessaire. Cependant, le champ d'application de la SdF étant très vaste, l'intérêt des activités métier de SdF dépend fortement de l'application envisagée. Il est essentiel de veiller à ce que les études amont de SdF d'un MOA découlent directement des points d'amélioration et limites constatées dans les justifications de SdF/Sécurité apportées par les industriels sur les systèmes acquis par le MOA.

VI. CONDITIONS D'EFFICACITE DE L'EXPERTISE SDF EN MOA

L'analyse conduite ci-dessus permet également d'identifier des conditions qui, si elles ne sont pas respectées rendent l'expertise SdF en MOA inefficace, voire contre-productive. Ces conditions portent sur les compétences des experts, les moyens techniques de l'expertise et l'organisation du MOA.

- Il existe une « culture SdF » chez le MOA (entretenue par des actions de sensibilisation des experts SdF). Les managers comprennent l'apport (et les limites) de la SdF.
- Dans le cas où le MOA a une activité de type MOI, des experts SdF sont identifiés et sollicités par les directions de projet quand une problématique liée à l'intégration de systèmes survient (en phase descendante et remontante du cycle en V).
- L'expertise SdF en MOA est impliquée sur l'ensemble des phases du cycle de vie des systèmes (et pas seulement la qualification), en particulier dans :
  - les études amont de montée en maturité de nouvelles architectures/technologies,
  - l'élaboration de la STB, avec les autres parties prenantes (opérationnels, équipe projet, MOI),
  - l'évaluation du plan SdF du MOI, celui-ci déterminant les justifications de SdF qui seront apportées,
  - le développement du système, à chaque jalon, afin de faire évoluer si besoin les fournitures, les analyses, voire le profil de vie ou la définition du système,
  - la vie opérationnelle du système. Les marchés de suivi en service doivent prévoir des analyses des défaillances et des évaluations de SdF opérationnelle par le MOI, qui seront soumises à l'expertise SdF du MOA.
- L'expertise SdF du MOA dispose d'une visibilité sur l'ensemble des activités d'ingénierie du projet considéré. Elle est intégrée aux équipes de projet (à la manière du SLI ou de la Qualité). Une proximité géographique avec les MOI et les équipementiers est souhaitable. L'intégration dans les équipes de projet permet de s'assurer de l'intégration des activités SdF du MOI aux autres activités de conception. La proximité géographique facilite la réalisation des audits de SdF jugés nécessaires.
- L'expert SdF MOA dispose d'une visibilité sur les développements de systèmes comparables (passés et en cours) et mène des actions de capitalisation. Il enrichit ainsi sa connaissance des méthodes de SdF, des modes de défaillance des composants, des valeurs quantitatives accessibles et dispose d'éléments de comparaison.
- L'expertise SdF du MOA est impliquée dans des études amont métier : participation à des congrès (a minima consultation des publications), animation de groupes de travail, de groupes de normalisation...
- Une implication de longue durée des experts SdF en MOA est souhaitable. En effet, l'expertise SdF en MOA nécessite une compréhension approfondie du fonctionnement des systèmes acquis ainsi qu'une maîtrise des activités SdF à chaque phase du cycle de vie. Cela nécessite une forte motivation personnelle et une reconnaissance par les Ressources Humaines du MOA de « parcours d'experts ».
- Les experts SdF du MOA ont eu une première expérience significative dans l'industrie. En effet, avant d'évaluer les activités SdF d'un MOI, il est nécessaire d'avoir conduit soi-même des analyses SdF et de comprendre les intérêts et contraintes respectifs des MOA et MOI. Un nouvel expert SdF en MOA sera d'abord affecté à des missions [Qualifier] afin d'avoir une visibilité complète d'une démarche SdF mise en œuvre sur un système. Par sa connaissance des systèmes, il sera alors en mesure d'intervenir progressivement sur des analyses de défaillances (mission [Suivre en service]). Il disposera alors du recul nécessaire pour être impliqué dans les missions [Spécifier] et [Orienter les EA métier].

On peut souligner que cette expertise ne nécessite en général pas l'acquisition de moyens coûteux (moyens d'essais, outils de modélisation…). Dans le cas où le MOI utilise des outils de modélisation de SdF, le MOA peut acquérir un bon niveau de confiance dans les évaluations de SdF du MOI sur la seule base de la vérification de la pertinence du modèle, de l'exactitude des hypothèses et des ordres de grandeurs des résultats.

VII. CONCLUSION

Les missions principales d'une expertise technique (pas uniquement SdF) en maîtrise d'ouvrage proviennent de ce que:

- Un maître d'ouvrage est souvent amené à intégrer plusieurs systèmes complexes entre eux. Le maître d'ouvrage doit alors conduire des activités qui sont par nature celles d'un maître d'œuvre.
- La traduction de l'expression de besoin en spécification technique de besoin est intrinsèquement de la responsabilité du maître d'ouvrage.

Des facteurs liés au métier SdF et aux systèmes acquis amplifient le besoin d'expertise spécifique de SdF en maîtrise d'ouvrage :

- Pour un système et une utilisation donnés, la définition des exigences SdF appropriées est souvent un exercice plus délicat qu'il n'y paraît. Il est essentiel de clarifier ces notions avec les parties prenantes lors de la spécification des systèmes et de s'assurer que les exigences sont correctement interprétées par les industriels pendant le développement.
- Les performances SdF ne sont pas vérifiables dans des contraintes de coût acceptables. Cela rend nécessaire la mise en œuvre d'un processus SdF complexe, adapté au secteur industriel et au système considérés et intégré aux autres activités de conception durant toute la durée du développement. La divergence d'intérêts entre MOA et MOI rend nécessaire une vérification approfondie par le MOA des activités du MOI pendant l'ensemble du développement.
- le besoin de mise en œuvre d'un processus SdF rigoureux est renforcé pour les systèmes, ou éventuellement seulement certains éléments des systèmes, pour lesquels il n'est pas possible d'acquérir un retour d'expérience représentatif (en termes de définition, fabrication et utilisation) avant la qualification et la mise en service.
- La confiance dans les évaluations de SdF prévisionnelles étant limitée, les performances SdF constatées pendant la vie opérationnelle doivent faire l'objet d'une attention particulière de la part du MOA.

Il apparaît qu'une expertise SdF en MOA est indispensable sur l'ensemble du cycle de vie des systèmes, particulièrement pour les systèmes, ou les éléments du système, à retour d'expérience représentatif réduit. Une MOA de tels systèmes doit s'impliquer dans les études amont métier afin d'améliorer les méthodes SdF visant la prévention et l'élimination des défaillances de nature systématique.

Les principaux risques d'une expertise SdF insuffisante en MOA sont:

- les études amont (architecture, technologies) visant à améliorer les performances SdF des systèmes futurs sont insuffisantes ou mal orientées,
- l'état de l'art des méthodes de SdF spécifiques aux systèmes acquis par le maître d'ouvrage ne progresse pas,
- le besoin de SdF du SdS constitué par l'intégration des systèmes acquis par le MOA n'est pas pris en compte,
- les performances SdF spécifiées ne traduisent pas correctement le besoin opérationnel,
- l'identification tardive de risques SdF génère des retards/surcoûts du projet,
- le système conçu ne respecte pas les exigences de SdF,
- le système conçu respecte peut-être les exigences de SdF, mais le plan SdF et/ou sa mise en œuvre ne permettent pas de garantir l'atteinte des performances SdF spécifiées,
- des performances de SdF insuffisantes ou en voie de dégradation pendant la vie opérationnelle ne sont pas identifiées et traitées,

Un ensemble de conditions indispensables à l'efficacité de l'expertise SdF en MOA a également été identifié.

A la suite de [15] et [20], cet article aborde le thème des objectifs et des méthodes de l'expertise de SdF en maîtrise d'. Ce thème est peu traité dans la littérature et mériterait d'être approfondi et partagé entre maîtrises d'ouvrages de différents domaines industriels.

REFERENCES

[1] La nouvelle architecture de l'industrie de la Défense en France – Evolution du rôle du maître d'ouvrage - Lazaric, Mérindol, Rochhia – Economie et institutions, n°12&13 -2008-2009

[2] Guide pour la maîtrise de la sûreté de fonctionnement - RG.Aéro 000 27, juillet 2015

[3] The Use of Safety Cases in Certification and Regulation, Prof. Nancy Leveson, MIT, November 2011

[4] Les fondamentaux de la gestion de projet, Afnor Editions, 2011

[5] Sécurité et véhicules autonomes : quels facteurs d'influence prendre en compte ? J. Rullier, V. Favre (SECTOR), λμ 2018

[6] ADMP-01 : Guidance for developping dependability requirements, OTAN - Edition B, Version 1 May 2022

[7] Evolutionary Reliability & Maintainability Strategy Improves Navy Ships, P. T. Dube, Naval Undersea Warfare Center, D. Greenhalgh, US Air Force Material Command (RAMS 2017)

[8] NF EN 60300-3-4 : Gestion de la sûreté de fonctionnement, Partie 3-4: Guide d'application – Spécification d'exigences de sûreté de fonctionnement, juillet 2008

[9] NF ISO 22514 (série), Méthodes statistiques dans la gestion de processus – Aptitude et performance

[10] Sécurité de réalisation : assurer la conformité du produit à sa définition en phase de réalisation - NF-C20-311, Février 2021

[11] Retour d'expérience en Sûreté de Fonctionnement d'un achat sur étagère – H. du Baret (DGA MI), λμ 2014

[12] "Perry Memo": Specifications & Standards - A New Way of Doing Business - William J. Perry, 29 June 94

[13] Recommandation générale pour la spécification de management de programme - RG.Aéro 000 40A, avril 1999

[14] Reliability and Maintainability as Key Driver for Rolling Stock Acquisition – R. van Baaren (ADSE Consulting and Engineering), W. Wijns, T. Smulders (Nederlandse Spoorwegen), RAMS 2017

[15] Bonnes pratiques de vérification de la SdF d'un système par une entité externe, H. du Baret, λμ 2018

[16] Multi-Discipline Agile Development and Reliability And Maintainability – C.C. Zanotti, A.J. Kaylor, K.L. Davidsen (Raytheon), RAMS 2017

[17] Risques et opportunités pour les lanceurs spatiaux de demain, S. Lombard, F. Farago (CNES), λμ 2016

[18] Guidance for Classification and Analysis of Dependability Events - ADMP-03 - Edition A, Version 1 May 2022

[19] Systèmes spatiaux — Définition des Niveaux de Maturité de la Technologie (NMT) et de leurs critères d'évaluation - NF ISO 16290, décembre 2014

[20] Points de vigilance récurrents dans la conduite d'une étude SdF, H. du Baret, λμ 2016