Propositions pour « l'Ingénierie Sûre »

Léa Dumont
Sonovision-Itep / Ligeron®
11, rue Bernard Palissy
33700 Mérignac
Lea.dumont@ligeron.com

Gaëtan Blaison
Sonovision-Itep / Ligeron®
Les Algorithmes, Bâtiment Euclide
91194 Saint Aubin cedex
Gaetan.blaison@ligeron.com

Résumé

L'ingénierie sûre pourrait se définir comme une approche modernisée de l'ingénierie, visant à limiter le nombre d'itérations, notamment dans les processus de conception. Le retour d'expérience des projets met en évidence de nombreux exemples qui montrent la nécessité de décloisonner les métiers et de mieux partager les données, tout en anticipant davantage les analyses de Sûreté de Fonctionnement.

L'objet de cet article est de présenter des propositions, raccrochées aux différents processus de l'ingénierie, en partant de l'expression du besoin jusqu'à la mise en service du système. Par le partage des données et des outils, l'ingénierie sûre tend à considérer au même niveau l'analyse des dysfonctionnements par rapport à l'analyse du fonctionnement, et que chaque acte de conception sous tend une analyse des risques.

Le besoin de rechercher de nouvelles voies d'économies sur les projets ainsi que l'émergence de nouvelles générations d'outils informatiques sont deux facteurs conjoncturels qui permettent de positionner l'ingénierie sûre comme une opportunité, d'améliorer la compétitivité sur les projets et les organismes qui les gèrent. En outre, cette réflexion sur l'ingénierie sûre permet d'apporter un nouveau regard sur les métiers de la sûreté de fonctionnement.

Summary

Safe engineering could be defined as a modernized approach to engineering, to limit the number of iterations, especially in the design process. The return of project experience highlights many examples that show the need to open up trade and better share data, while anticipating further analysis of dependability.

The purpose of this paper is to present proposals to hook different engineering processes, starting from the expression of need until the commissioning of the system. By sharing data and tools, safe engineering tends to see the same level of analysis of malfunctions from the analysis of the operation, and that each act of conception underlies a risk analysis.

The need to seek new ways to save money on the projects and the emergence of new generations of tools are two economic factors that allow safe engineering position as an opportunity to improve competitiveness on projects and agencies that manage them. In addition, this reflection on the safe engineering can bring a new look at the trades for dependability.

1. Contexte

Depuis plusieurs années, les métiers de la sûreté de fonctionnement agissent de plus en plus sur les phases amont des projets. Chacun sait que plus les analyses de sûreté de fonctionnement sont menées au plus tôt de la conception, plus elles seront efficaces.

Mais aujourd'hui il semble nécessaire de dépasser cette idée en imaginant que les processus de conception et de sûreté de fonctionnement ne doivent faire plus qu'un.

Il suffit de partir des constats suivants :

- Les processus de la SdF, du Soutien Logistique Intégré, de l'Ingénierie Système, de la sécurité ont de nombreux outils en commun.
- Le principe de précaution utilisé par défaut, conduit généralement au surdimensionnement des systèmes.
- Les temps de développement sont de plus en plus courts.
- On a besoin aujourd'hui de plus de flexibilité dans les projets. Les fonctions, les plannings, les performances peuvent évoluer fortement en cours de projet.
- La SdF est encore perçue comme une contrainte dans les relations client - fournisseur.
- Les recommandations issues des analyses de SdF peuvent remettre en cause une conception déjà figée.
- L'analyse du Facteur Humain est une donnée d'entrée fondamentale pour la conception des Interfaces Homme Machine et de la Documentation Technique Utilisateur, et plus généralement pour la conception du système.
- De nouveaux concepts sont à prendre en compte, comme l'éco-conception ou la HQE.
- Le plan de validation du produit ou du système prend rarement en compte les résultats des analyses SdF.

- L'optimisation des coûts d'exploitation-maintenance et les coûts de démantèlement sont primordiaux dans les choix d'acquisition.

Au-delà de ces différents constats, le cloisonnement encore très présent des métiers et des données dans les projets conduit le plus souvent à :

- des reprises tardives de la conception, ou tout simplement à une non prise en compte des recommandations issues de la SdF par les fabricants du système,
- des modifications contractuelles et matérielles, avec des conséquences significatives sur les plannings et les budgets,
- des retards de mise en exploitation[1], ou des coûts d'exploitation exorbitants,
- une incompréhension par les managers de la valeur ajoutée de la sûreté de fonctionnement,
- de trop nombreuses itérations de conception.

2. Objectifs

L'objet de cet article est de récapituler les diverses propositions qui peuvent être faites pour rapprocher les études de SdF des études de conception, et de le fédérer sous un même concept : « l'Ingénierie Sûre ».

Le principe est de fournir quelques indications clés qui permettraient au Chef de Projet d'orienter les processus de développement vers une intégration de la sûreté de fonctionnement dès les premières esquisses du produit.

Pour commencer, proposons une définition pour l'**ingénierie sûre** :

*Ensemble des tâches et processus qui concourent à définir, concevoir, exploiter, démanteler un système **dans un nombre d'itérations optimisé au plan technico-économique**, tout en répondant à l'ensemble des contraintes (sécurité, disponibilité, environnements, coûts …).*

La différence avec l'ingénierie classique est de considérer que le nombre d'itération optimisé est une performance aussi importante que les autres (coûts, délais, performances système).

Le corolaire d'une telle définition est que l'ingénierie sûre doit être un axe majeur de gain de productivité, principalement en phase étude. Ce gain de productivité est recherché en s'intéressant principalement à la mise en cohérence des différents outils, et au partage des données par tous les métiers du projet.

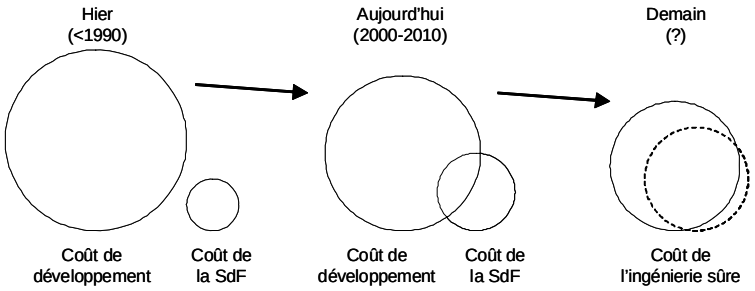

Figure 1 : Evolution des coûts d'étude et développement

L'originalité de la démarche repose sur deux changements principaux :

1- Révision profonde de l'organisation des équipes d'ingénierie. Les concepteurs doivent faire des analyses SdF. Réciproquement, les analystes SdF doivent avoir l'esprit concepteur.

2- Rationalisation poussée du partage des données par construction d'un modèle global du système, unique, et évolutif.

3. Démarche

Force est de constater que les nouvelles générations d'outils logiciels permettent de contribuer au partage des données. Les progrès dans l'interfaçage des outils logiciels, dans les outils de modélisation, dans les réseaux et dans la puissance des ordinateurs rendent possible la mise en pratique de l'ingénierie sûre.

Quelques exemples montrent que les premières bases d'application existent déjà :

- Il est possible de faire des synthèses automatiques d'AMDEC à partir de modèles UML / SysML [2]. Il peut aider le concepteur à identifier par lui-même les éléments de fiabilité.
- Les modèles ALTARICA permet de passer d'un Bloc Diagramme Fonctionnel à un graphe d'état rapidement [4]. On sait que les graphes d'états sont très utiles aux études de disponibilité et à la prise en compte des évènements

[1] Des exemples récents existent. De grandes installations internationales affichent une disponibilité maîtrisée, en se basant sur le fait que chacun de ces constituants est fiable. Le prolongement de la période de mise en service démontre souvent le contraire.

(erreur humaine, agressions externe). Ces modèles offrent la possibilité de présenter efficacement tous les scénarios de fonctionnement et de dysfonctionnement. En outre les modèles ALTARICA peuvent être interconnectés pour modéliser des modèles plus complexes. Il est possible également d'y injecter des modèles simplifiés qui contiennent les exigences SdF alors, que la globalité du système n'est pas encore définie.

- L'outil System Designer de Dassault System, ex BPA DAS, permet de faire une analyse dysfonctionnelle d'un système en modélisant ses comportements. Ces modèles permettent de faire des simulations d'injections de fautes et d'évaluer de manière précise la propagation des effets.

Ainsi, le schéma qui suit montre comment les différents outils au service de l'ingénierie peuvent contribuer à la construction linéaire, convergente, et quasiment non itérative, du référentiel de conception.

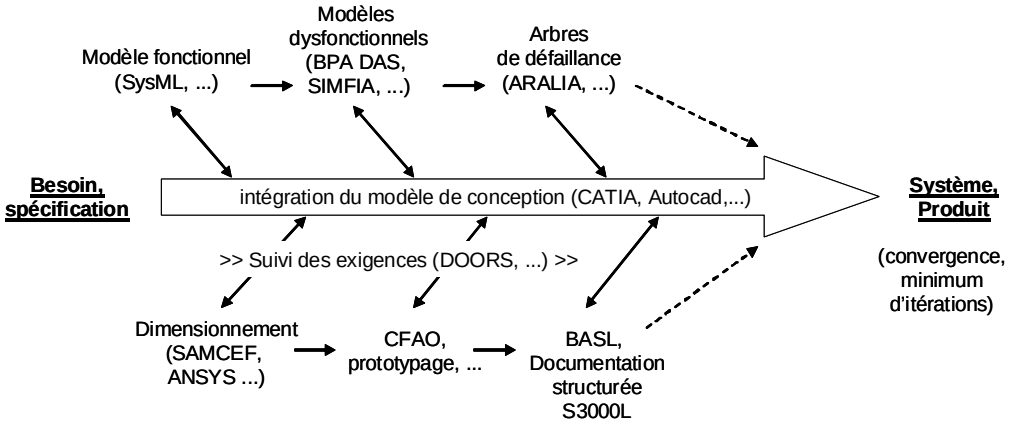

Figure 2 : Intégration et convergence des outils informatiques

Dans un tel schéma, un des principes important est l'unicité des données, principe largement connu dans l'exploitation des bases de données. Par ailleurs, on n'exclut pas l'existence de petites itérations autours de chacun des outils, pourvu que l'ensemble du référentiel de conception itère peu.

Ainsi, la démarche proposée pour l'ingénierie sûre repose sur l'inventaire des processus et métiers de l'ingénierie système [7], croisée avec les référentiels de données que l'on utilise couramment dans les projets de développement.

Le schéma ci-dessous, présente de manière simplifiée, les principales données à partager à mettre en interface, pour limiter le nombre d'itérations dans les études.

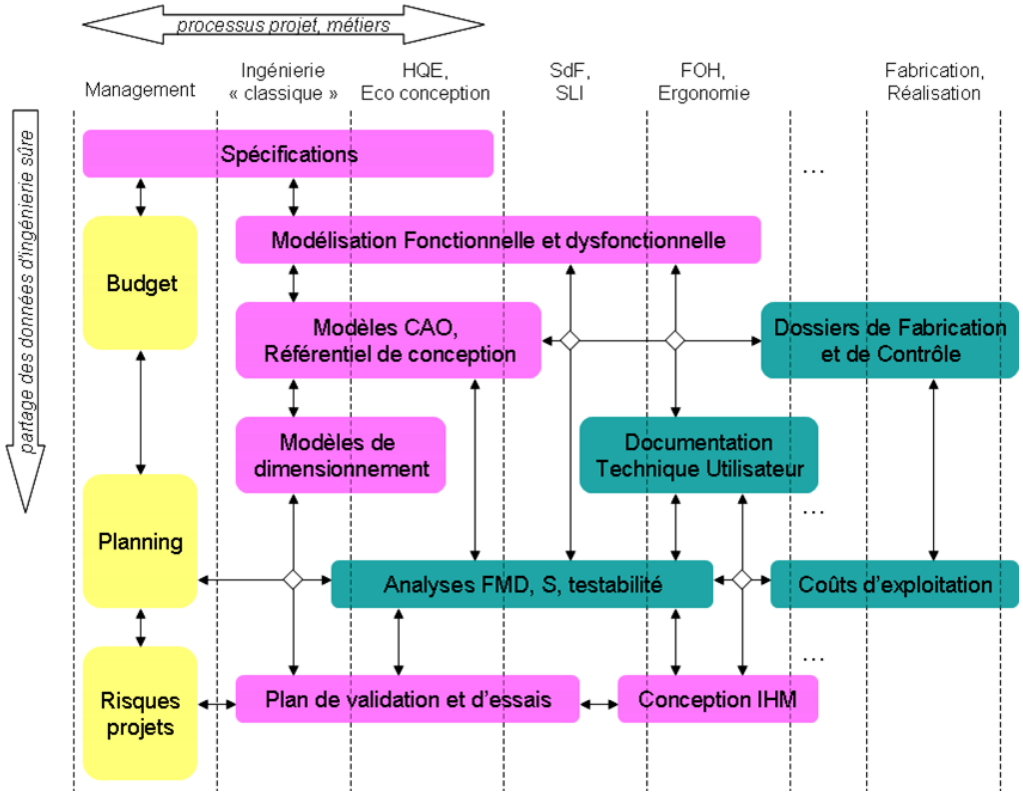

Figure 3 : Partage des données et principales interfaces de l'ingénierie sûre

Les paragraphes qui suivent décrivent des propositions et des principes pour l'ingénierie sûre, pour les principaux processus projet concernés. Il faut considérer que cette liste de principes et de propositions est non exhaustive. Sans doute, le lecteur en identifiera d'autres.

Toutefois, nous prenons soin d'orienter la liste des processus du management de projet de l'amont vers l'aval, c'est-à-dire de l'expression du besoin jusqu'à la mise en exploitation, sachant que certains processus du projet fonctionnent en parallèle.

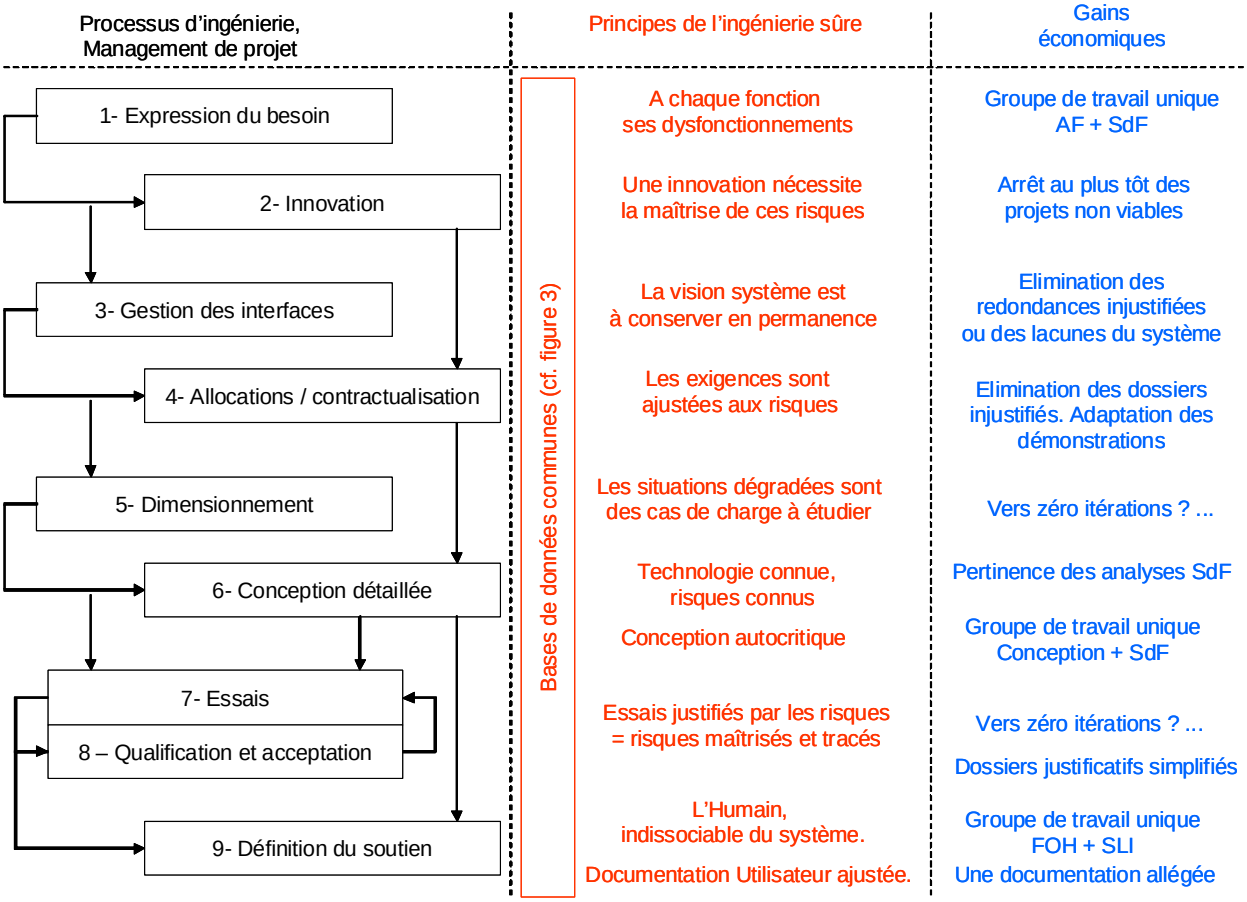

Figure 4 : Workflow de l'ingénierie sûre

3.1. Processus d'expression du besoin

On le sait, l'expression du besoin doit, autant que possible, faire abstraction de solutions techniques. La seule manière d'y parvenir est d'exprimer le besoin sous forme de fonctions et de performances (cahier des charges fonctionnel, spécifications fonctionnelles, STB).

Dès qu'une fonction est spécifiée, l'ingénierie sûre doit envisager et étudier ses dysfonctionnements. A partir d'un outil d'analyse fonctionnelle partagé pour l'ensemble du projet, on peut très tôt identifier les modes de défaillance fonctionnels (arrêt, intempestif, dégradé …). Il est également possible de paramétrer de manière quasi automatique les liens entre les AF, les AMDEC et les APR [1]. Cela permet, conjointement à l'APR de proposer, si besoin, des fonctions de sécurité dédiées à la réduction des risques.

Un cahier des charges « dysfonctionnel », complétant la STB, peut permettre d'identifier et de spécifier les fonctions importantes pour la sécurité.

Fonction de sécurité
N°F :
Libellé : Limiter la consigne d'accélération

Evènement(s) redouté(s) à maîtriser par cette fonction

N°ER	Position d'Utilisation	Libellé de L'ER	Causes possibles	Conséquences, Gravité
	Moteur en régime …, Véhicule en roulage …	incohérence entre la volonté du conducteur et la consigne de couple	panne électrique ou panne mécanique …	ERn°xy : « Accélération Intempestive »
	…			

Caractéristiques de la fonction de sécurité

N°C	Critère	Niveau	Flexibilité
	Temps de réponse …		
	Détection …		
	Automatique / Manuel …		
	Temps de blocage de la rampe d'accélération	? 2 secondes	Impératif
	Ecart maximum entre la consigne d'accélération conducteur et l'accélération moteur, sur 2 s …	? 1 $m.s^{-2}$	Impératif

Niveau de Sécurité attendu :

Prévention :	L'ER xx passe de P = …. à P' = … L'ER yy passe de P = …. à P' = …
Protection :	L'ER xx passe de G = …. à G' = … L'ER yy passe de G = …. à G' = …

Etats autorisés et interdits

Rappel des états de fonctionnement nominaux :

Etats dégradés autorisés :

Etats interdits :

Figure 5 : exemple de canevas de spécification « dysfonctionnelle »

On a coutume de commencer les APR après la diffusion des STB, pratiquement dans le creux du cycle en « V ». Dans ce cas les fonctions de sécurité sont identifiées tardivement, ce qui engendre une nécessaire itération de mise à jour des STB.

Ainsi, la démarche d'analyse dysfonctionnelle conjointe à l'expression du besoin doit permettre de limiter les itérations sur la STB du système. Plus globalement, cette démarche doit permettre de décliner plus naturellement les exigences de sécurité dans les STB des équipements (exemple : cf. article [5]).

Enfin, si la modélisation fonctionnelle initiale est effectuée directement dans un outil formel connu tel que SysML, elle pourra être transmise directement à l'équipe SdF pour l'étude des dysfonctionnements.

3.2. Processus d'innovation

Une idée ne présente d'intérêt que si elle est réaliste, et tout particulièrement, si elle n'engendre pas de risques. Mise en œuvre dès le stade R&D-faisabilité, les premières analyses SdF pourront aider à écarter une solution présentant un niveau de risque inacceptable, ou, à minima, définir ces conditions de mises en œuvre nécessaires à la réduction du risque.

Par exemple, dans un projet concernant la recherche de filières innovantes pour le traitement isotopique de matières, une question d'intérêt a été posée par les concepteurs, qui proposaient de récupérer les condensats après évaporation (voir schéma suivant).

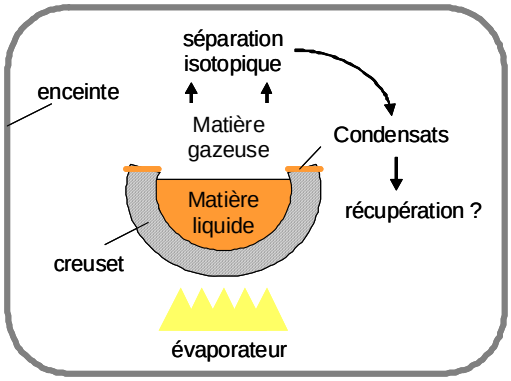

Figure 6 : Exemple d'un projet d'innovation

Après une réunion de projet faisant intervenir les différentes compétences du projet, il a été identifié que :

- Au plan de la rentabilité économique du procédé, l'idée était excellente,

- Au plan de la complexité des démonstrations de sûreté, l'idée était à proscrire.

Dans cet exemple on comprend que si l'analyse préliminaire de la sûreté avait été plus tardive, on aurait lancé le développement d'une solution non viable, avec les conséquences financières que l'on peut imaginer.

Un deuxième principe peut être retenu. Il s'agit de l'adaptation des analyses APR et AMDEC, en fonction du degré d'innovation. Dans l'article [1] on va jusqu'à :

- supprimer les AMDEC sur les fonctions les moins innovantes,
- se limiter à une AMDEC fonction pour les fonctions moyennement innovante,
- réserver l'AMDEC complète (fonction + produit) uniquement aux fonctions très innovantes.

3.3. Processus de gestion des interfaces (internes et externes)

La somme des études SdF ne fait pas la SdF du système. Cette affirmation semble évidente pour l'ingénieur SdF système. La réalité des projets montre qu'elle n'est pas toujours prise en compte.

Dans un premier exemple, assez classique, deux ponts roulants équipant un atelier de préparation d'objets à haut niveau d'intégration avaient été livrés accompagnés de dossiers de SdF. La SdF était démontrée sur chacun des deux équipements. Pourtant, une erreur humaine à conduit à une collision entre un palonnier vide et un colis, faute d'étude système. Cet exemple montre en outre la nécessité d'engager des études de Facteur Humain au niveau système, en amont de la conception.

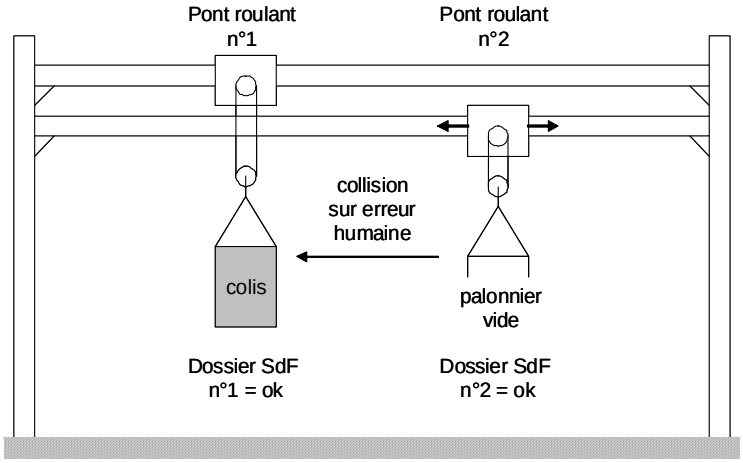

Figure 7 : Exemple d'un atelier de préparation d'objets à haut niveau d'intégration

Dans un deuxième exemple, la conception des fonctions de sécurité d'un système vaste et complexe a nécessité le déploiement des exigences de sécurité dans plusieurs STB, vis-à-vis de fournisseurs industriels distincts.

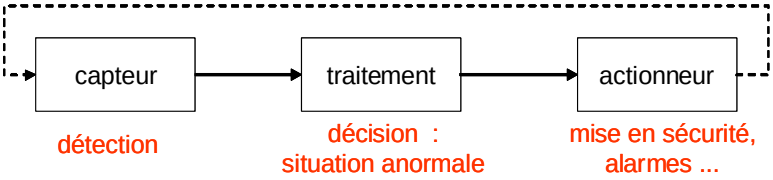

Figure 8 : Conception d'une fonction de sécurité, dans l'esprit de la norme NF-EN-61 508 [6]

Le capteur est développé par un premier fournisseur industriel, le traitement par un second fournisseur, l'actionneur par un troisième fournisseur. Mais au cours des contrats de développement il est constaté que l'actionneur a été spécifié au fournisseur n°2 et au fournisseur n°3. La fonction de sécurité comprend désormais 2 barrières alors que le risque à couvrir n'en exigeait qu'une seule.

Ces deux exemples justifient la nécessaire intégration des études SdF en amont du déploiement des exigences. Le principe que l'on peut proposer est d'intégrer les acteurs SdF dans les décisions suivantes :

- validation des STB des sous ensembles,
- validation des propositions d'évolution (lien à la gestion de configuration),
- franchissement des premières revues de conception.

Concernant les interfaces externes, le domaine d'action privilégié de l'ingénierie sûre est la conception des Interfaces Homme – Machine (IHM) et des automatismes qui les régissent. Il est raisonnable de considérer que la spécification et la conception des IHM et des automatismes doit considérer les analyses SdF comme une donnée d'entrée essentielle.

Par exemple, certains constructeurs automobiles font découler les spécifications de diagnostics moteur et allumages voyants directement des AMDEC [3].

3.4. Processus d'allocations et contractualisation

Tous les contrats de développement ne requièrent pas le même niveau d'exigence dans le détail des études. Cela dépend essentiellement des caractéristiques du produit. Cette réflexion est à privilégier face au réflexe traditionnel du « copié-collé » des spécifications SdF.

Exemple 1 : Emission de consultations pour des contrats de développement concernant un projet d'installation de recherche. A chaque dossier de consultation est jointe la même spécification générale de SdF. Une fois les offres remises, on constate que le total des propositions financières pour les lots d'études de SdF est très supérieur au budget initialement alloué à la SdF.

Exemple 2 : Exigence d'analyse AMDEC du mobilier d'un bâtiment :

- Cette exigence n'a pas de véritable sens si le bâtiment étudié est la salle de repos d'une gare.
- Au contraire, l'exigence prend une importance toute autre si le bâtiment étudié est un hôpital.

Ces deux exemples montrent qu'il est essentiel d'adapter le niveau d'exigence de SdF en fonction de la nature des sous-ensembles, de leur technologie, de leur complexité, de leur degré d'innovation (§ 3.2) et du contexte de risque. Cet effort d'adaptation sera facilement rentabilisé par la suite.

3.5. Processus de dimensionnement

Le temps consacré au dimensionnement d'un système peut être optimisé au juste besoin en prenant en compte l'avis de la SdF. Il est très courant que les analyses SdF soient enclenchées alors que le système est déjà dimensionné. On constate alors que de nombreux cas de charge n'ont pas été pris en compte.

Une proposition concrète est de faire relire la liste des cas de charge et conditions aux limites par l'équipe SdF, pour vérifier qu'on intègre les cas de charges représentatifs des situations normales, dégradées ou accidentelles. La relation entre l'équipe SdF et l'équipe de calcul devient une relation d'échange « gagnant – gagnant » car n'oublions pas que les calculs de dimensionnements alimentent les démonstrations déterministe attendues dans les dossiers de sécurité.

En prolongeant le raisonnement, sur des projets d'envergure plus restreinte, il est envisageable que les ingénieurs calculs mettent en œuvre eux même les outils de la SdF. Par exemple, l'application des approches Résistance-Contrainte peut être prise en compte directement par les ingénieurs calculs, plutôt que mise en œuvre à postériori par la SdF.

3.6. Processus de conception détaillée

Les acteurs de la SdF doivent être pleinement intégrés dans les équipes de conception et dimensionnement. A l'extrême, on pourrait envisager qu'un concepteur réalise lui même ses propres analyses de SdF.

Réciproquement, il faut garantir que les ingénieurs SdF maîtrisent bien les technologies. Bien souvent, analyser le système comme un simple assemblage de « boites noires » (blocs élémentaires qui réalisent des fonctions), ne suffit pas à appréhender les modes défaillances spécifiques ou les états dangereux particuliers.

Ces deux aspects posent la question du recrutement et de la formation des ingénieurs SdF. Il semble de plus en plus nécessaire que les ingénieurs aient une double compétence technologies + sûreté de fonctionnement.

3.7. Processus de spécification et réalisation des essais

La SdF doit permettre d'identifier les essais les plus démonstratifs et les alternatives en cas d'échec. Cette évidence pour un ingénieur SdF est souvent occultée par les chefs de projet.

Ainsi, les marges de performances et les coûts ne doivent pas être les seuls critères retenus pour décider de conduire des essais de qualification. La hiérarchisation des risques en est un autre. Le principe est d'effectuer les essais prioritairement sur les processus et produits présentant des niveaux de risque important, comme exemple :

- L'utilisation d'un matériel innovant engendrant des contraintes nouvelles sur les opérations.
- Les essais de fiabilité (essais accélérés, essais tronqués), sur des composants critiques pour la sécurité ou la disponibilité.
- Les barrières de sécurité, qui sont prévues pour être rarement sollicitées (en principe). Seuls des essais permettront de vérifier leur réelle efficacité, si les modèles ne sont pas suffisamment démonstratifs.
- Les modalités d'utilisation du système, lorsqu'elles présentent de fortes contraintes sur le facteur humain (coactivité, possible surcharge cognitive, gravité élevée en cas d'erreur, etc.).

- Les procédures de traitement des situations dégradées, qui même si elles sont peu fréquentes, sont très accidentogènes, en particulier en l'absence d'entraînement des opérateurs.

La réalisation d'essais coûte cher. Sur certains projets, elle représente une part importante du coût de développement, parfois aggravé fortement lorsqu'on découvre tardivement qu'une démonstration de sécurité requiert des essais supplémentaires.

Il est donc essentiel que le programme d'essais de qualification et que toute spécification d'essai soit rédigés conjointement avec les acteurs de la SdF. La logique classique de constitution d'un programme d'essai est de prendre en compte en priorité les essais de démonstrations des performances, lorsque les justifications théoriques ne suffisent pas ou lorsque les modèles de calculs sont en limite de représentativité. En complément de cela, l'ingénierie sûre préconise d'y ajouter les essais suivants :

- Démonstration de robustesse du système vis-à-vis des situations accidentelles, à condition que leur probabilité soit significative.
- Démonstration d'aptitudes à la mise en sécurité, lors de situations dégradées, à condition que leur probabilité soit significative.
- Démonstration d'aptitude à la maintenance, pour les interventions les plus fréquentes ou mettant en œuvre des moyens ou des situations complexes.
- Eventuels essais de fiabilité, éventuels essais de confirmation des modes de défaillance ou de testabilité.

Si a première vue cette approche tend à augmenter le coût des essais par le nombre et leur diversité, elle permettra également d'éliminer les essais non justifiés, et de limiter les itérations multiples par la découverte tardive de nouveaux besoins d'essais. Il n'est pas exclus qu'elle permette également au chef de projet d'affiner le plan de développement en identifiant plus facilement des alternatives en cas d'échec de la démonstration d'une performance.

3.8. Processus de justification de la conception et d'acceptation des produits et du système

Cette intégration de la SdF dans les processus de conception détaillée et les processus d'essai (voir paragraphes précédents) apporte une aide significative à la traçabilité et au suivi des exigences :

- Tel essai provient de quelle exigence ?
- Telle exigence provient de quelle analyse de risque ?
- L'essai est il concluant ?
- Le risque est il couvert ?

Cette traçabilité (cf. exemple Figure 9) est utile voire nécessaire notamment dans l'élaboration du DJD système ou dans l'établissement des dossiers de sécurité soumis aux autorités qui valident la mise en exploitation.

En outre, il est fréquent que les acteurs de la SdF soient consultés pour traiter les demandes d'évolution ou de dérogation. Dans ce cas, les APR et AMDE peuvent constituer une source d'aide à la décision pour l'acceptation des produits : Si la dérogation (ou l'évolution) touche un paramètre important pour la sécurité (ou la disponibilité) : une analyse technique approfondie sera nécessaire pour décider son application. Dans le cas contraire, la décision pourra reposer sur une analyse simplifiée, ou au seul regard des coûts et des délais.

L'AMDEC, le catalogue des paramètres de sécurité, sous forme de base de données peuvent constituer un outil efficace d'aide à la décision.

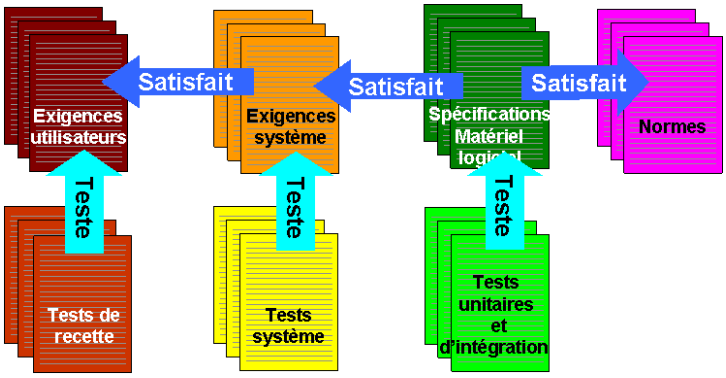

Figure 9 : Traçabilité des exigences, proposées par l'application DOORS

3.9. Processus de Définition du Soutien, prise en compte du Facteur Organisationnel et Humain

La documentation doit être spécifiée et adaptée en fonction des résultats des analyses du Facteur Humain[2]. La documentation est souvent surdimensionnée, alors qu'elle pourrait contenir uniquement un juste nécessaire en complément des IHM.

Les voies permettant de limiter les coûts de rédaction de la documentation technique d'utilisation et de maintenance pourraient être les suivantes :

- Assurer que les rédacteurs n'aient pas à refaire l'analyse fonctionnelle. La meilleure solution serait de leur faire partager les outils de modélisation fonctionnelle pour qu'il puisse décrire facilement les opérations à réaliser.
- Définir préalablement à qui serviront les documents (chef d'équipe, responsable du poste de conduite, opérateur métier X, Y ou Z …) afin de les adapter à leurs futurs destinataires. Si pour un document donné, on ne parvient pas à identifier les destinataires, il est peut-être raisonnable de ne pas commencer sa rédaction.
- Justifier les consignes et les modes opératoires par rapport à des risques identifiés. Les analyses de risques en opération, les évènements type « erreur humaine » dans les arbres de défaillance, les autres analyses FOH, doivent être à considérer comme les principales sources de prescriptions.
- Garder une place pour les formations : il est parfois préférable de former les opérateurs par la pratique, de les entraîner, plutôt que de les surcharger de consignes et de modes opératoires.
- Considérer, que sur un système à supervision centralisée, un grand nombre d'informations et de consignes peuvent être déjà disponibles sur les écrans. Sauf pour le traitement des situations dégradées (coupures d'énergies par exemple), il n'est pas toujours nécessaire de redonder les écrans avec une documentation (qui elle-même contient des copies d'écrans).

Pour terminer sur cet aspect, n'oublions pas qu'un grand nombre d'erreurs humaines relevées dans l'accidentologie ont pour origine les consignes contradictoires. Lorsque l'IHM dit le contraire du mode opératoire, quelle décision prendre ? La mauvaise, si on se réfère à Murphy.

D'autre part, le système de soutien, conçu pour maintenir le système principal en état tout au long de sa durée de vie, ne peut pas faire abstraction de l'organisation des futurs exploitants.

Le Système de Gestion de la Sécurité et plus généralement, le système de management QSE, qui intègre les exigences réglementaires, définit une organisation, des processus et des règles qui, si elles ne sont pas analysées transversalement, provoquent un cloisonnement naturel entre les métiers.

Il devient alors logique de considérer que les concepteurs du système de soutien (équipe « SLI ») intègrent l'analyse de facteur humain, jusqu'à l'organisation du futur exploitant.

4. Conclusions

La plupart de ces principes sont déjà appliqués sur de nombreux projets. Mais quelle entreprise les applique tous et de manière intégrée ? Le développement des outils de l'ingénierie système va dans le sens d'intégrer la SdF, cela facilite et facilitera l'intégration de tous les principes exposés dans cet article.

Ce qui fait que ces principes ne sont pas mis en œuvre de manière globale peut s'expliquer par le fait que les modèles classiques d'organisation et de logique de déroulement des projets s'opposent sur certains aspects à l'application de ces principes. Aussi, mettre en œuvre une véritable ingénierie sûre implique sans doute :

- La proposition de nouvelles logiques de déroulement avec de nouveaux jalons de projet.
- La création de nouvelles fonctions dans l'organigramme des acteurs du projet.
- Une rénovation des approches de contractualisation et de sous-traitance des études de SdF ?
- La mise en place de nouveaux systèmes documentaires (revoir la structure des STB et des DJD par exemple ?), redistribuer l'accès aux informations avec des bases de données simples et interconnectables.
- Une nouvelle approche dans le recrutement et la formation des ingénieurs (concepteurs et responsables SdF ?).
- Autres ?

Une telle démarche peut sans nul doute générer des gains économiques pour les projets. Il reste aujourd'hui à mettre en place les indicateurs qui permettraient des les évaluer.

Si aujourd'hui le présent article permet d'éveiller la conscience des responsables qui mettent en place de nouveaux projets, avec cette nouvelle vision des processus de SdF, alors il s'agira d'un premier résultat concret.

Il reste beaucoup à construire en matière d'ingénierie sûre. Elle devra notamment permettre d'apporter des éléments de réponse à une question essentielle des décideurs : quel est le retour sur investissement des études de SdF ?

[2] Rappelons que ces analyses, qui doivent être lancées très tôt dans le projet, alimentent d'autres processus, comme la conception du système, les études de sécurité, l'analyse du concept d'exploitation.

Remerciements à M. Tony HUTINET.

5. Références

[1] M. PILLET, V. OZOUF, 2008, Paramétrez les champs de vos AMDEC Produits grâce à l'APR, 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement

[2] P. DAVID, V. IDASIAK, F. KRATZ, 2008, Etude pour une meilleure intégration des données de conception dans les analyses de fiabilité, 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement

[3] F. PETIT, N. BONNET, 2001, La conception sûre des systèmes embarqués ; Les systèmes GMP, Phoebus n°17, Editions Préventique

[4] R. BERNARD, P. BIEBER, A. GRIFFAULT, M. ZEITOUN, 2008, Raffinement ALTARICA pour l'étude des systèmes à différents niveaux de détail, 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement

[5] F. RIEUNEAU, P. BEAUCHARD, 2001, La conception sûre des systèmes embarqués ; Les systèmes GMP, Phoebus n°17, Editions Préventique

[6] Norme NF EN 61508, 2002, Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmable relatifs à la sécurité, AFNOR

[7] EIA STANDARD - EIA632, 1999, Processes for Engineering a System, ANSI

[8] E. PAGE, J. VAN DER VLIET, 2008, La mise en œuvre de l'approche systémique dans la conception sûre de systèmes complexes, 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement