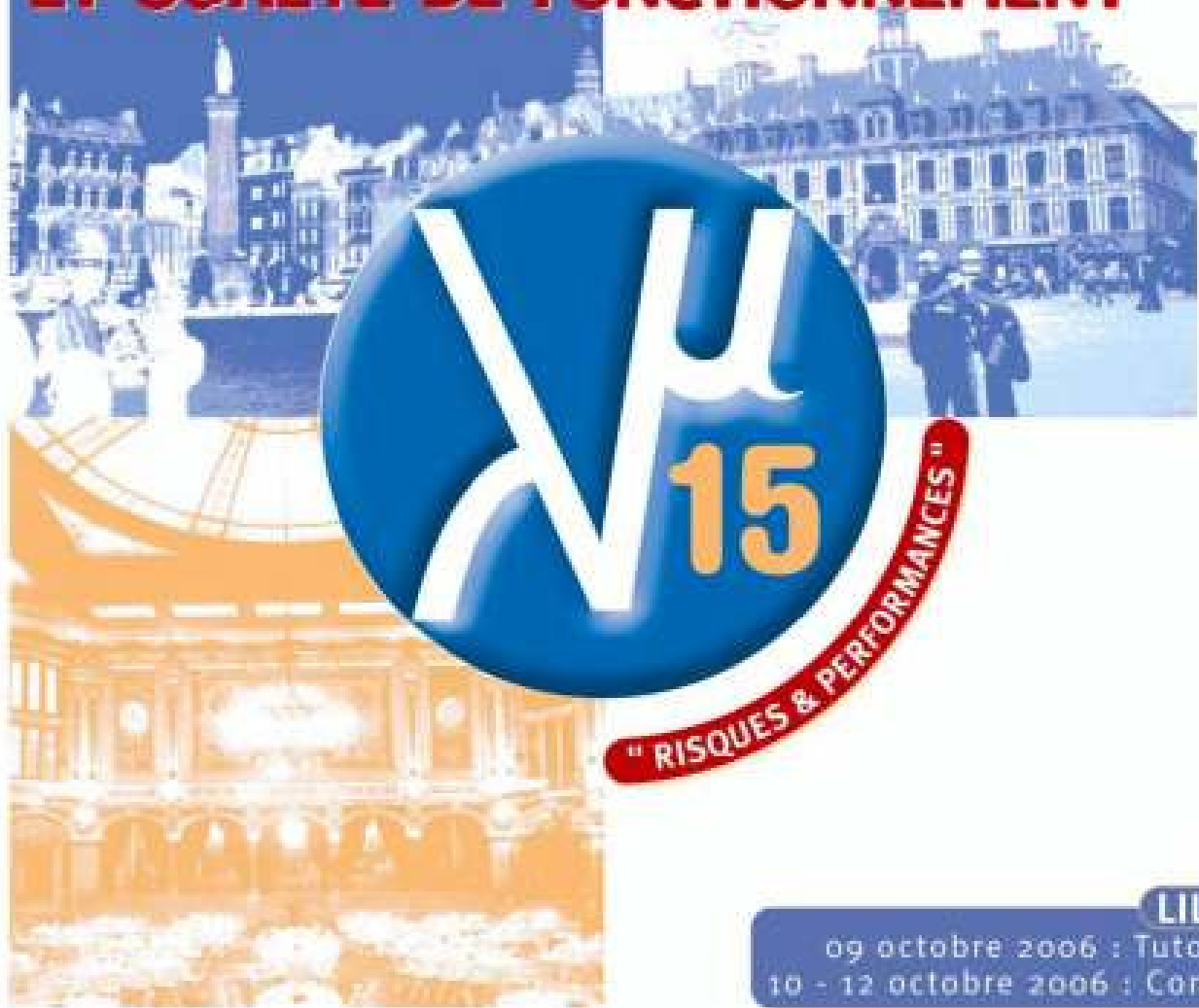


MAÎTRISE DES RISQUES ET SÛRETÉ DE FONCTIONNEMENT



LILLE

09 octobre 2006 : Tutoriels
10 - 12 octobre 2006 : Congrès

<http://imdr-sdf.asso.fr/lm15>

TEXTES DES CONFÉRENCES



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

L'INTÉGRATION DE LA DÉMARCHE SÛRETE DE FONCTIONNEMENT DANS LES PROJETS : CONCEVOIR SÛR À COÛTS OPTIMISÉS

INTEGRATION OF DEPENDABILITY PROCESS IN PROJECTS : SAFE DESIGN FOR OPTIMIZED COSTS

Claude FARGIER
5 du Grand Carroi
37270 Montlouis sur Loire
06 80 43 55 48
cfargier@wanadoo.fr

Résumé

La conception de produits critiques impose d'adopter une démarche de Sûreté de Fonctionnement. La plupart des entreprises ont aussi un système de management de la Qualité ISO 9001. Souvent ces deux approches vont être superposées, sans communication efficace entre les deux activités : les risques "produit" seront identifiés tardivement, lorsque des choix de conception sont faits. Les reprises d'études augmentent les coûts de développement et les délais. L'approche proposée ici intègre les deux démarches et fournit des outils de maîtrise des risques du projet lui même, pour une meilleure performance globale. Elle est applicable aux entreprises de toute taille et aux projets simples ou complexes.

Summary

The design of critical products requires the implementation of a dependability process. Most companies also have an ISO 9001 Quality Management System. In many cases, these two processes operate side by side, but without efficient communication between the two activities : the risks related to the product are identified too late, when design choices have been made. Resulting redesign activities significantly increase the development costs and jeopardise the project deadlines. The approach proposed here integrates both activities and provides means for project risk management, and therefore a better global performance. It may be used in large and small projects or companies.

Le processus projet

Les normes ISO 9001 et l'approche processus

La généralisation des systèmes de management de la Qualité basés sur les normes ISO 9001 version 2000 [1] a conduit les entreprises concevant leurs produits à formaliser leur processus de conception. Lorsque ces produits sont critiques vis à vis des aspects FMDS, ces mêmes entreprises mettent en place une démarche de Sûreté de Fonctionnement. Certains référentiels Qualité comme par exemple, la norme IRIS [2] récemment publiée par l'UNIFE dans le domaine ferroviaire, l'imposent d'ailleurs.

L'expérience des audits d'évaluation montre que dans de nombreux cas les activités de Conception et de Sûreté de Fonctionnement font l'objet de processus séparés confiés à des pilotes distincts pour assurer leur indépendance. Les deux processus sont souvent placés "en série". Les risques sont identifiés lorsque les choix de conception sont faits. La mise en place de mesures de réduction des risques peut conduire à des reprises d'études importantes et pénalisantes du point de vue des délais et des coûts.

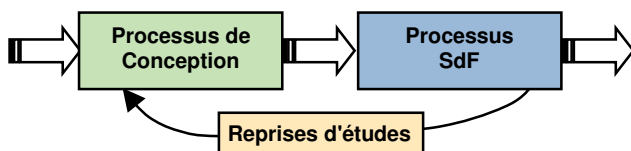


Fig. 1 : Les deux processus sont placés "en série".

Une meilleure performance est obtenue en plaçant les activités de Conception et de Sûreté de Fonctionnement "en parallèle" à l'intérieur du processus projet.

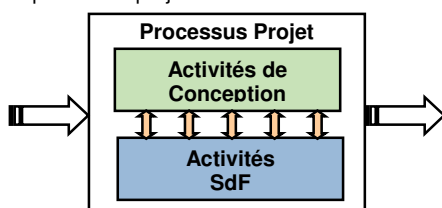


Fig. 2 : Les deux activités sont placées "en parallèle" pour une meilleure performance du processus projet

Les activités Sûreté de Fonctionnement se déroulent au fur et à mesure de l'avancement de la conception, les reprises d'études sont limitées, en importance et probabilité d'occurrence, les coûts de développement et les délais sont plus facilement maîtrisables. L'indépendance des activités de Conception et de Sûreté de Fonctionnement est assurée dans un fonctionnement matriciel du projet : le chef de projet est le pilote de l'ensemble du processus, mais le membre de l'équipe chargé de la Sûreté de Fonctionnement possède un rattachement hiérarchique indépendant des Concepteurs.

La mise en place de la nouvelle organisation projets

Deux situations se présentent :

- L'entreprise n'a pas de démarche Sûreté de Fonctionnement et doit s'en doter.
- L'entreprise a une démarche Sûreté de Fonctionnement mais elle intervient lorsque les choix de conception sont faits, comme présenté à la Fig. 1.

Dans les deux cas, l'évolution de l'organisation fait appel au reengineering des processus.

" Le Reengineering est une remise en cause fondamentale et une redéfinition radicale des processus opérationnels" [3]

Le reengineering est fréquemment utilisé dans le domaine du management de la Qualité , pour mettre en place une organisation transversale performante orientée vers la satisfaction des clients du processus. Il s'appuie sur :

- Les attentes des clients du processus
- Le retour d'expérience des projets précédents
- Les actions d'amélioration proposées
- Le fonctionnement actuel des projets

Il permet aux acteurs de bâtir, dans un groupe de travail, la nouvelle organisation :

- définition des phases du projet,
- définition de leurs séquence
- définition de leur contenu : activités à réaliser
- positionnement de jalons entre les phases
- établissement de la liste des résultats attendus aux jalons
- mise en place de revues de jalons destinées à décider de passer ou non à la phase suivante
- Audits internes des phases

Un exemple de jalonnement de projet est donné à titre d'illustration à la Fig. 3.

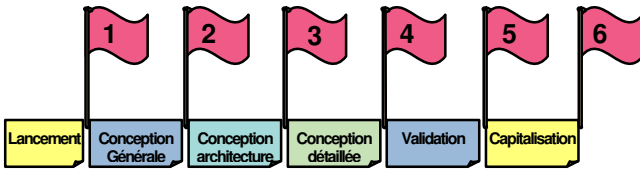


Fig. 3 : Un exemple de jalonnement projet

Chaque phase contient les activités de Conception et de vérification et les activités de Sûreté de Fonctionnement correspondantes, confiées à des acteurs indépendants avec une coordination étroite.

Le contenu de chacune des phases prend en compte les principes du cycle en V représenté à la Fig. 4 : à chaque niveau de la branche descendante dédiée à la conception, correspond un niveau de validation de la branche montante.

La version préliminaire du plan de validation et d'intégration au niveau système est établi dès la phase de conception générale. De même pour le plan de validation des sous-ensembles lors de la phase de conception de l'architecture.

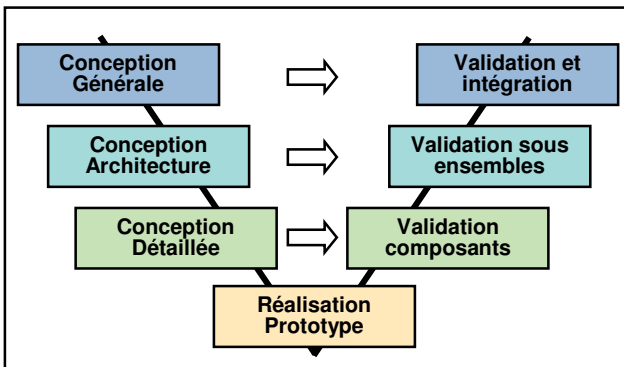


Fig. 4 : Le cycle en V

Cette approche permet de réaliser les validations par rapport aux données d'entrée des phases de conception, donc, pour la phase de conception générale, d'après les exigences du Client, et non pas d'après les résultats de la conception. Elle permet de déceler les dérives dans le processus de conception au moment de la validation.

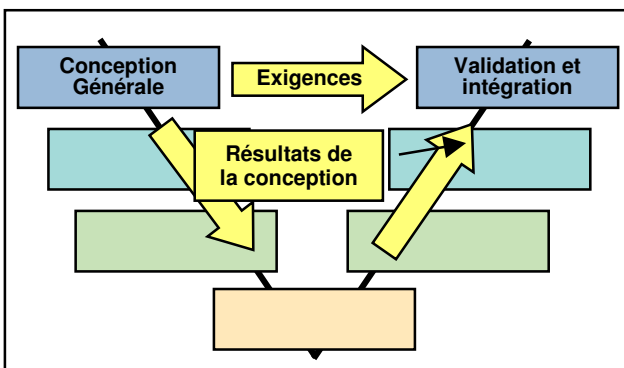


Fig. 5 : La validation est réalisée par rapport aux exigences du Client

Contenu des différentes phases

Phase de lancement

Dans cette phase, les objectifs du projet sont présentés à l'équipe qui a été constituée au préalable.

Le plan de Sûreté de Fonctionnement est établi. Il décrit en détail le **processus Qualité de construction de la Sûreté de Fonctionnement**.

Il est complété, si l'importance du projet le nécessite, par d'autres plans : plan de management, plan Qualité...

Le plan de Sûreté de Fonctionnement détaille les activités, phases, revues, méthodes et outils utilisés.

Il contient les grilles de cotation de la gravité des événements redoutés relatifs au produit et leur probabilité d'occurrence tolérable ainsi que le seuil de leur classement comme événement critique. Il expose enfin la méthode de management des risques du projet.

Au cours de la revue de lancement organisée au début de cette phase, les participants sont invités à établir une première liste des aléas qu'ils estiment pouvoir intervenir dans le **déroulement du projet**, à partir de leur expérience sur les projets antérieurs. Ces aléas constituent les **événements redoutés du projet**, ils sont évalués en gravité et probabilité d'occurrence et font l'objet d'actions de réduction des risques, de la même façon que les événements redoutés relatifs aux produits. Ils sont enregistrés dans la Liste Unique Projet qui est ouverte dans cette phase. Cette liste constitue le "Hazard Log" du projet.

Le paragraphe "Management des risques du projet" à la fin de cette communication présente des outils simples à la disposition du chef de projet pour réduire ces risques.

Phase de conception générale

La phase de conception générale du système comprend l'analyse fonctionnelle des besoins du client et l'établissement, par l'équipe de Conception, de la spécification fonctionnelle.

Dès qu'elle est approuvée, le membre de l'équipe chargé de la Sûreté de Fonctionnement constitue un groupe de travail incluant des représentants des concepteurs pour réaliser l'Analyse Préliminaire des Risques.

Elle met en évidence et évalue les effets des défaillances des fonctions et des interfaces du système.

Les documents créés ou modifiés dans cette phase sont co-gérés par les Concepteurs et le membre de l'équipe chargé de la Sûreté de Fonctionnement : chaque création ou modification est approuvée par les deux parties.

Ainsi, le membre de l'équipe chargé de la Sûreté de Fonctionnement est nécessairement informé des évolutions de la spécification fonctionnelle. De même les concepteurs sont informés du fait que le classement de telle fonction critique a pu évoluer.

Phase de conception de l'architecture

La phase de conception de l'architecture est celle qui permettra de dégager la valeur ajoutée de la démarche proposée, en concevant le système de manière à se prémunir, à priori, de l'atteinte des événements redoutés identifiés précédemment.

L'analyse Sûreté de Fonctionnement de l'architecture est réalisée au moyen d'un arbre de défaillance pour chaque événement redouté critique identifié dans la phase précédente.

A ce stade, le Concepteur des sous ensembles à développer sait :

- **Ce à quoi il doit être conforme**
- **Ce dont il doit se prémunir**
- **Les probabilités de défaillance tolérables**

Comme dans la phase précédente, les documents créés ou modifiés dans cette phase sont co-gérés par les Concepteurs et le membre de l'équipe chargé de la Sûreté de Fonctionnement

Phase de conception détaillée

Au cours de cette phase, les Concepteurs définissent la constitution détaillée des sous ensembles. Les activités Sûreté de Fonctionnement permettent de vérifier la prise en compte efficace des recommandations de conception préconisées et d'évaluer l'atteinte des objectifs alloués précédemment. Compte tenu de l'analyse Sûreté de Fonctionnement de l'architecture réalisée au cours de la phase précédente, aucune itération importante de la conception n'est identifiée à ce stade, si les recommandations de conception ont été exploitées.

Phase de validation système

Au cours de cette phase, les essais de validation système sont réalisés, leurs résultats sont analysés et approuvés par le membre de l'équipe chargé de la Sûreté de Fonctionnement

Phase de capitalisation

Elle comprend une revue formelle du retour d'expérience du projet par les membres de l'équipe et leurs clients internes. Elle a pour but de **réduire les risques** sur les projets futurs et **d'améliorer la performance** de la méthode de management [4]

Management des risques du projet

Tout au long du processus, les risques relatifs à la conduite du projet lui-même sont évalués à l'aide de tables.

La Fig. 6 donne un exemple de cotation de la probabilité à partir du **degré de nouveauté des choix de conception** retenus dans le projet

<u>INNOVATION DES CHOIX DE CONCEPTION</u>	P
Solution "High Tech" Domaine de la R & D	4
Solution complexe Connu par nos concurrents	3
Solution simple Connu mais dans d'autres applications	2
Solution basique Parfaitement connu	1

Fig. 6 : Table de cotation en probabilité

La Fig. 7 donne un exemple de cotation de la gravité.

De même que dans la table précédente, les critères retenus couvrent différents aspects, ici : financier, préjudice pour le client, impact sur le planning, impact sur le projet, réserves du client, crédibilité, de manière à fournir les points de repère à toutes les personnes qui participent à ces évaluations et qui ont des orientations différentes du fait de leurs fonctions.

<u>GRAVITÉ DES ALÉAS DU PROJET</u>	G
Pertes > 300 k€ Préjudice catastrophique pour le Client Décale le planning de manière inacceptable	4
Pertes : 50 k€ Préjudice important pour le Client Décale fortement le planning	3
Pertes : 20 k€ Préjudice faible pour le Client Décale légèrement le planning	2
Pertes : 2 k€ Pas de préjudice pour le Client Ne décale pas le planning	1

Fig. 7 : Table de cotation en gravité

L'identification des risques projet se fait au cours des différentes revues en utilisant une approche de brainstorming simplifiée et au cours des audits internes.

Tous les risques sont inclus dans la Liste Unique Projet. Le chef de projet définit et pilote la mise en place des nécessaires. Après vérification de leur efficacité, le risque résiduel est évalué.

Un indice de risque global du projet est calculé en faisant simplement la somme des points figurant dans la Liste Unique Projet : cotation initiale pour les points restant ouverts et risque résiduel pour les points clôturés.

Son évolution dans le temps, en fonction du passage des différents jalons et sa tendance sont visualisés par un indicateur dont la Fig. 8 donne une illustration. Le taux d'engagement de charge donne une image de l'évolution de l'activité sur le projet.

Cet indicateur complète les suivis de planning et de budget habituels.

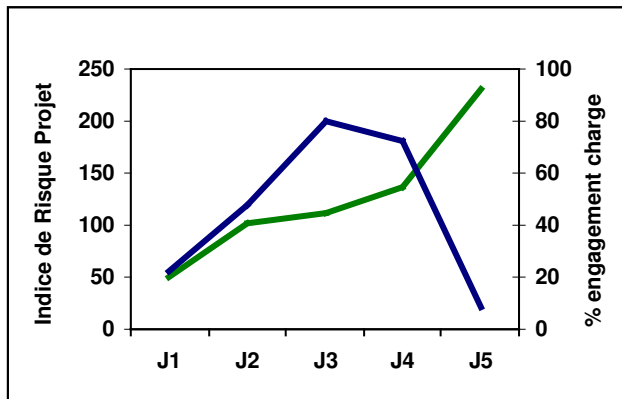


Fig. 8 : Indice de Risque Projet et taux d'engagement de charge

De Jalon 1 au Jalon 3, l'indice de risque augmente du fait de leur identification progressive. Il diminue en phase de conception détaillée et de validation. Le risque résiduel en fin de projet est réduit. La Fig. 8 représente le cas souhaitable correspondant à un management de projet performant.

Conclusion

Cette organisation projet fait appel, d'une part aux méthodes et outils bien connus des Qualityiciens, comme le reengineering et l'approche processus, et d'autre part à toutes les techniques maîtrisées par les experts de la Sécurité de Fonctionnement.

Son application sur plusieurs projets, notamment en PME/PMI, a permis de vérifier l'efficacité des préconisations émises en phase de conception de l'architecture et de réduire de manière significative les reprises d'études. Les outils de management des risques projet ont montré leur efficacité en permettant au chef de projet d'anticiper ses décisions.

Cette approche vise à établir une passerelle entre l'univers des systèmes de management de la Qualité et l'univers de la Sécurité de Fonctionnement pour renforcer le dialogue et la collaboration des spécialistes de ces deux disciplines avec les Concepteurs et ainsi accroître la performance des projets.

Remerciements

Nos remerciements vont à tous ceux qui, collègues ou clients, ont su, par leurs remarques constructives ou suggestions pertinentes, contribuer au perfectionnement de cette approche.

Références

- [1] ISO 9001 : 2000. Systèmes de management de la qualité. Exigences.
- [2] IRIS, International Railway Industry Standard, UNIFE, 2006.
- [3] M. HAMMER et J. CHAMPY, Le Reengineering, Dunod, 1993.
- [4] ISO 10006 : 2003, Systèmes de management de la qualité. Lignes directrices pour le management de la Qualité dans les projets.
- [5] CEI 61508 : 2000 Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité.