TRAVAIL COOPÉRATIF ET MAÎTRISE DES RISQUES, DU MYTHE À LA RÉALITÉ

COOPERATIVE WORK AND RISKS CONTROL, FROM MYTH TO REALITY

Arlette Bouzon[1], Julien Faure[2], André Cabarbaye[2&3]

[1]Université Paul Sabatier Toulouse III

115 route de Narbonne, 31000 Toulouse
Tél. 05 61 54 33 32
arlette.bouzon@iut-tlse3.fr

[2]Centre National d'Etudes Spatiales (CNES)

18, avenue Edouard Belin - 31401 Toulouse
Tél. 05 61 28 26 89
julien.faure@cnes.fr
andre.cabarbaye@cnes.fr

[3]CAB INNOVATION

3, rue de la Coquille - 31500 Toulouse
Tél. 05 61 54 68 08
andre.cabarbaye@cabinnovation.fr

Résumé

Bien que devenue aujourd'hui une discipline mature, la Sûreté de Fonctionnement présente des difficultés sur le terrain, tant en raison des évolutions technologiques qu'organisationnelles. L'objectif de cette communication est de montrer les difficultés rencontrées par les fiabilistes pour mettre en œuvre les démarches de la Sûreté de Fonctionnement en conception dans le domaine spatial et souligner l'importance des aspects communicationnels dans la maîtrise de risques.

Summary

Although they are now mature disciplines, Dependability and Safety present difficulties for implementation, both because of technological and organizational changes. The purpose of this communication is to show the difficulties encountered by reliability specialist to implement the steps of Dependability and Safety throughout the design in space field and emphasize the importance of communication in risks control.

1. Introduction

La Sûreté de Fonctionnement est aujourd'hui devenue une discipline relativement mature dont les méthodes et outils font l'objet de multiples normes et standards. Elle fait régulièrement l'objet de colloques et congrès et est aujourd'hui largement enseignée à l'université et dans les écoles d'ingénieurs. Elle intéresse tous les acteurs de la conception à l'exploitation jusqu'au démantèlement des systèmes à risques, tant au sein des grandes entreprises que des PME/PMI. Sa diffusion est renforcée par des textes réglementaires nouveaux, relatifs à la sécurité des personnes, des biens et de l'environnement, et par un jeu de spécifications irrigant tous les niveaux contractuels pour répondre à une très forte demande de qualité de service par les utilisateurs des nouveaux produits.
Mais si cette évolution peut apparaître rassurante pour le consommateur et pour le citoyen, le risque technique en est-il pour autant parfaitement maîtrisé ?
Outre que l'approfondissement des connaissances bénéficie d'abord à la réduction des marges de dimensionnement plutôt qu'à la limitation des risques eux-mêmes et que les nouveaux projets s'avèrent toujours plus complexes en termes d'imbrication des constituants et de la diversité des acteurs mobilisés, l'application des méthodes et outils traditionnels de la Sûreté de Fonctionnement présente des difficultés sur le terrain, tant en raison des évolutions technologiques que d'une activité organisationnelle parfois fort éloignée de celle préconisée par les pionniers de la fiabilité.
L'objectif de cette communication est de montrer les difficultés rencontrées par les fiabilistes pour mettre en œuvre les démarches de la Sûreté de Fonctionnement en conception dans le domaine spatial et souligner l'importance des aspects communicationnels dans la maîtrise de risques.

2. Observation sur le terrain

L'évolution de nos sociétés est caractérisée par l'émergence et la multiplication de systèmes complexes concernant tant les produits que les organisations. Les produits (systèmes spatiaux, avions, TGV, centrale nucléaire, usine chimique, etc.) intègrent de plus en plus de fonctions interdépendantes et hybrident des technologies multiples et variées dont notamment des logiciels informatiques toujours plus volumineux. De par cette intégration croissante, leur sûreté de fonctionnement est difficile à maîtriser, notamment parce qu'une perturbation est susceptible de se propager très rapidement d'un point à un autre par des cheminements divers (électrique, thermique, optique, hertzien, etc.) sous forme analogique ou numérique. Ces systèmes sont, en outre, sensibles à un environnement incertain, qui accroît encore leur complexité et nécessite l'implantation de multiples mécanismes de surveillance et de protection.
Leur conception implique la mobilisation d'une pluralité de savoirs et d'acteurs issus de diverses organisations. Ceux-ci doivent se comprendre et interagir pour maîtriser les risques en analysant les conséquences des éventuels dysfonctionnements qui peuvent survenir durant tout le cycle de vie du produit. Cherchant à anticiper au plus tôt l'aléa, le processus de conception est alors associé à un processus de maîtrise des risques dans lequel la communication est essentielle. Cette dernière permet notamment aux acteurs d'identifier ensemble les risques inhérents au produit en gestation, puis de décider et mener les actions nécessaires pour les éliminer ou du moins les rendre acceptables. Elle intervient également pour valider ce processus de création collective lors de confrontations entre spécialistes durant des revues de conception et auprès des autorités compétentes, si cela s'avère nécessaire.

Mais le travail collaboratif, entre des acteurs contingents motivés par des intérêts de circonstance dans un cadre contractuel évolutif, ne se déroule pas toujours comme indiqué dans les manuels. L'échange et la coopération qui étaient de mise lors de programmes phares, tels que le projet Apollo aux Etats-Unis (premier homme sur la Lune) ou le premier lanceur Ariane en Europe, ont tendance à se déliter quelque peu quand chacun doit protéger son territoire, dans un environnement très concurrentiel, par une multiplication de clauses de confidentialité et que toute information sur d'éventuelles faiblesses peut se retourner contre son auteur. A tous les niveaux contractuels, les documents fournis sont alors remplacés par de simples synthèses et les analyses elles-mêmes sont plus souvent menées sur de vagues synoptiques

que sur des schémas détaillés devenus confidentiels. De même, la collecte d'informations sur des incidents est particulièrement délicate, notamment quand ils relèvent, in fine, d'erreurs humaines.

Ainsi l'AMDEC classique [1] de type « Bottom up », utilisée traditionnellement sur les projets spatiaux, ne fait plus remonter grand-chose des analyses de bas niveau qui descendent de plus en plus rarement jusqu'aux composants élémentaires. Généralisé à l'ensemble d'un système, le maintien des analyses au niveau des composants présenterait de toute manière un coût rédhibitoire dans un contexte bien plus concurrentiel, compte tenu du nombre de composants mis en oeuvre.
De plus, la méthodologie même de l'AMDEC, montre rapidement ses limites sur les systèmes actuels :
- C'est une analyse mono panne qui ne prend pas en compte les défaillances multiples dont l'occurrence est directement liée à la complexité.
- Bien adaptée à l'étude de circuits électroniques à base de composants discrets elle traite difficilement certains modes de pannes telles que les dérives de paramètres ou les pannes des composants très intégrés (ASIC, µP) dont les effets sont rarement déterministes.
- Elle ne couvre pas de manière efficace les erreurs de conception (dont notamment les anomalies aux interfaces) de réalisation (dont notamment les erreurs de logiciel ou les défauts de montage) et d'opérations (erreurs humaines).
- S'appuyant sur une définition détaillée, c'est une analyse tardive qui a peu d'impacts réels sur la conception hormis quelques modifications plus souvent palliatives que correctives.

De même, seules des synthèses d'analyses pire cas, permettant de garantir le bon fonctionnement des produits dans leurs conditions extrêmes d'utilisation, sont aujourd'hui fournies par les industriels, ce qui empêche, à peu près, toute contre expertise sérieuse à un niveau supérieur.

Par ailleurs, l'utilisation généralisée de composants très intégrés tels que les ASIC et FPGA dans la plupart des équipements, pose un véritable problème de validation. En effet, ces composants subissent rarement un cycle de développement aussi rigoureux que celui exigé pour un logiciel de vol. Or leur complexité n'a souvent rien à envier à ces derniers et des comportements exotiques, très éloignés de tout ce qui a pu être imaginé comme mode de défaillance durant les analyses de fiabilité, se manifestent parfois au cours des tests d'intégration d'équipements ou de satellites, voire même en vol.

Outre les démarches d'analyse, les circonstances dans lesquelles sont menées les confrontations techniques ne sont pas toujours optimales et peuvent biaiser la prise de décision. Ainsi, les conditions matérielles de la « revue de projet », qui permet d'achever une phase de conception en autorisant le démarrage de la suivante, sont souvent difficiles. Les délais alloués sont courts, de quelques jours à un mois dans le domaine spatial, d'autant que les membres du groupe de revue ont du mal à se décharger de leurs activités habituelles. La documentation est volumineuse, de un à quinze classeurs sur CD-ROM, à analyser dans l'urgence, par un groupe d'experts constitué d'une dizaine de personnes. En outre, cette documentation n'est pas toujours entièrement disponible au démarrage de la revue.
Les documents eux-mêmes sont imparfaits. Les dossiers examinés sont parfois peu lisibles voire incomplets. Les analyses présentées ne mentionnent pas toujours les hypothèses considérées et les modèles utilisés, ce qui en empêche toute vérification approfondie notamment dans l'urgence. Les conclusions sont parfois absentes et les justifications imprécises. Le nombre de questions soulevées par les membres du groupe de revue est souvent conséquent. La hiérarchisation des problèmes n'est alors pas aisée car chacun a tendance à considérer son point de vue comme prépondérant. Le charisme individuel tout comme la qualité d'animation du président du groupe de revue jouent un rôle déterminant dans l'ordre et le traitement des problèmes; les derniers abordés étant souvent examinés brièvement ou jugés mineurs. Enfin le débat technique est parfois biaisé par des aspects contractuels, les enjeux sous-jacents étant généralement non négligeables. Aussi les réponses aux questions sont-elles souvent formelles et restent parfois superficielles. L'absence de débat technique approfondi peut alors engendrer des lacunes ou se traduire par des recommandations peu étayées ou difficilement applicables.

Enfin, en l'absence d'un processus de certification par une autorité indépendante, comme cela existe normalement pour traiter des problèmes de sécurité, les recommandations relatives à la Sûreté de Fonctionnement sont quelquefois écartées par les chefs de projets en faveur de la performance, de la sauvegarde du planning ou de la maîtrise des coûts.

3. Evolution des approches

Pour tenter de remédier à ces difficultés, les donneurs d'ordres cherchent à développer l'approche «Top down», déjà assez largement employée dans le domaine aéronautique. Dans le cadre d'Analyses Préliminaires de Risques (APR), celle-ci cherche à appréhender l'aléa au plus tôt afin de pouvoir focaliser l'effort de fiabilisation sur les réelles faiblesses de la conception. Cet effort peut notamment porter sur l'imposition aux fournisseurs de règles de conception particulières, en termes de choix de solution ou de méthode de développement, ou à la demande de justifications et analyses ciblées sur des points particuliers.
Ainsi des listes d'événements redoutés apparaissent dans les spécifications techniques auxquelles il faut répondre par des justifications quantitatives et/ou qualitatives précises.
De même des exigences de ségrégation entre éléments et chemins en redondance ou entre fonctions et protections associées cherchent à éviter de laborieuses démonstration a posteriori, souvent peu convaincantes, pour démontrer l'absence de risque de propagation de panne au sein d'un espace restreint, voire d'un même composant.
La crainte de pannes de modes communs peut également conduire à des exigences de diversification de la conception et/ou des approvisionnements de certains constituants critiques, sans avoir une connaissance précise des possibles scénarios de défaillance. Une alimentation de secours par batterie, groupe électrogène, ou source locale d'énergie renouvelable sera, par exemple, préférée à la simple duplication des lignes sur le réseau électrique, même si l'amélioration de fiabilité qu'elle procure est parfois difficile à évaluer.
Les exigences peuvent également concerner des marges de dimensionnement qui doivent être vérifiées à travers des analyses pires cas, qui combinent les conditions extrêmes d'utilisation du produit jusqu'à sa fin de vie prévue, ou des analyses des contraintes, qui permettent de s'assurer que des marges ont été prises sur les caractéristiques intrinsèques des composants électriques (analyse de Derating) ou mécaniques vis-à-vis de leurs conditions d'utilisation.
Outre les modes de fonctionnement nominaux, des modes dégradés répondant plus ou moins imparfaitement aux besoins des utilisateurs, peuvent être également spécifiés, avec pour chacun d'eux des objectifs à atteindre, afin de favoriser une dégradation douce du fonctionnement des systèmes et éviter d'interrompre totalement les services rendus.
En outre l'association de critère quantitatifs et qualitatifs (implantation de barrières de sécurité, concept fail Operational et/ou fail safe, surveillance macroscopique des fonctions critiques, etc.) garantie une certaine robustesse à la conception.
Sur le plan méthodologique, plutôt que balayer uniformément l'ensemble de la conception, les analyses attendues ont tendances à se limiter à quelques parties critiques tout en gagnant en profondeur. Une AMDEC de niveau composant pourra ainsi être demandée pour s'assurer de l'absence de propagation de panne en un point stratégique, tel qu'une interface.

Mais cette évolution progressive qui privilégie la démarche descendante sur la remontée d'information rencontre également des écueils.

La connaissance étant généralement partagée entre le donneur d'ordre et ses fournisseurs, l'APR impose un minimum de coopération entre les intervenants.
Des problèmes contractuels parfois insoupçonnés peuvent alors surgir telle que la simple difficulté à chiffrer a priori le volume des analyses à mener. En effet bien que souvent plus lourde, la charge de travail liée à la réalisation d'une AMDEC est directement proportionnelle au nombre de composants du produit concerné alors que la charge correspondante pour l'APR ne dépend que des risques identifiés au cours de celle-ci.
L'approche déductive impose, par ailleurs, une réelle implication des spécialistes des divers métiers. Le fiabiliste ne peut plus se contenter d'une simple action de vérification de la conception mais participe désormais activement à celle-ci.
Enfin, si ce type d'approche transparaît dans certaines normes, notamment sous le vocable d'AMDEC Fonctionnelle, elle souffre de l'absence de véritables standards reconnus par tous.
La coopération sur un même objectif de réussite de mission requiert, par ailleurs, de multiples actions de sensibilisation et de formation de l'ensemble des acteurs, dont le chef de projet, sans le soutient duquel toute action semble vaine.

4. Conclusion

Dans ces structures souples que sont les projets de conception, dans lesquels l'échange d'information et la prise de décision constituent l'essentiel de l'activité, la confiance tient lieu de mode de coordination entre les acteurs. Elle établit un liant dans les échanges même si ces derniers ne sont pas symétriques dans un univers hiérarchisé. Elément de stabilisation des représentations sociales [2], la confiance évite, en effet à chacun, de vérifier systématiquement la véracité des informations reçues, ou de maîtriser des savoirs diversifiés toujours plus spécialisés. Elle conduit les acteurs à dévoiler en partie leurs savoirs propres pour participer à une co-construction complexe qui traduit l'intérêt collectif, mais aussi les intérêts individuels.
Mais dans un contexte de concurrence effrénée, la relation de travail se joue des frontières de l'entreprise comme de celles des états, et nous assistons progressivement à un « zapping » relationnel aussi bien entre clients et entreprises qu'entre organisations et prestataires, chacun recherchant en permanence le partenaire le plus offrant dans l'immédiat. Cette liberté des échanges suscite aussi des risques pour l'organisation, que celle-ci tente de maîtriser de diverses manières.

Sur des projets complexes tels que les systèmes spatiaux, la démarche de maîtrise des risques cherche à s'adapter au mieux aux réalités du terrain en privilégiant les analyses de risques préliminaires, afin d'identifier, au plus tôt, les faiblesses de conception et mieux cibler l'effort. Par ailleurs, la confiance n'exclut pas le contrôle qui doit s'appliquer tout particulièrement aux analyses de Sûreté de Fonctionnement soumises à revues lors des développements de projet. Si une mauvaise évaluation des risques peut avoir des conséquences particulièrement néfastes, l'information nécessaire à leur maîtrise est souvent partagée entre les experts du fournisseur et ceux du donneur d'ordres. La communication apparaît donc essentielle dans ce processus collectif de maîtrise des risques même si cette dimension semble parfois oubliée par les acteurs eux-mêmes.

Références

[1] – Villemeur A., Sûreté de Fonctionnement des systèmes industriels - Edition Eyrolles, Paris 1987
[2] – Bouzon A., La place de la communication dans les systèmes à risques. L'Harmattan. Paris, 2004.
[3] – Etienne K., Faure J., Laulheret R., Cabarbaye A.. Retour d'Expérience en Sûreté de Fonctionnement dans le Spatial – Lambda mu 2005 - Lille