1ERES RENCONTRES INTERNATIONALES

1ERES RENCONTRES INTERNATIONALES

organisées par le CHU de TOULOUSE

Intérêts et limites de la sûreté de fonctionnement

Pierre LAVÉDRINE

Ingénieur ENSMA - ENSAé

Airbus Toulouse

TOULOUSE 15-16 Juin 2009

Qu’est-ce que la sûreté de fonctionnement ?

- Une PERFORMANCE d’un système ?

  représentant ses caractéristiques de Fiabilité, Disponibilité, Maintenabilité, Sécurité (R.A.M.S en anglais).

- Une DISCIPLINE TECHNIQUE - voire SCIENTIFIQUE ?

  associant des savoirs, des outils, des règles…

- Une COMPOSANTE DU MANAGEMENT DE PROJET ?

Qu’est-ce que la sûreté de fonctionnement ?

- PERFORMANCE, DISCIPLINE, FONCTION ? Un peu TOUT et RIEN de cela :
  - Les PERFORMANCES d’un système (industriel, organisationnel, hospitalier,…) ne peuvent être définies qu’en fonction de :
    - sa ou ses MISSIONS (pour quoi est-il fait ?)
    - les IMPACTS ET RISQUES qu’il est susceptible de générer (pour l’homme / intervenant du système ou extérieur, pour l’activité / l’entreprise, pour l’Environnement, pour la Société…)
  - La Sûreté de Fonctionnement regroupe des méthodes, des outils,.. Mais une réelle DISCIPLINE (voire SCIENCE…) s’est-elle vraiment formalisée ?
  - Même lorsque la Sûreté de Fonctionnement intervient dès de la conception, sa fonction de vérification (ou justification) reste la plus visible.

Construire la sûreté de fonctionnement

- Exemple du transport aérien civil :
  - MISSION : transporter des passagers payants de manière sûre et rentable, d'où :
    - **des OBJECTIFS D'OPÉRABILITÉ / DISPONIBILITÉ qui conditionnent la crédibilité du transport aérien et du constructeur,**
    - **des OBJECTIFS DE MAINTENABILITÉ, qui sont un élément de compétitivité,**
    - **des OBJECTIFS DE SÉCURITÉ, qui sont réglementés par les Autorités de Sécurité Aérienne (FAA, EASA).**
  - Le respect de ces objectifs va nécessiter :
    - Une conception (architecture) qui intégre les objectifs et leurs antagonismes éventuels (par exemple : opérabilité vs sécurité)
    - Des allocations d'objectifs par sous-systèmes ou fonctions,
    - Des objectifs de FIABILITÉ par équipements.

Exemple d'objectifs de sécurité avion

- Niveau décisionnel : *Autorités de Certification (FAA / EASA)*
  - *Objectifs par CONDITION DE PANNE (pour 1 heure de vol) :*

Probabilité (par heure de vol)	10^{-3}		10^{-5}	10^{-7}	10^{-9}
	« Fréquent »	**« Probable »** (peut arriver plusieurs fois dans la vie d'un avion)	**« Peu probable »** (peut arriver plusieurs fois dans la vie de la flotte)	**« Très peu probable »** (n'arrivera sans doute jamais dans la vie de la flotte)	**« Extrêmement improbable »** (ne doit pas se produire)
Classe d'effets	**Mineure**		**Majeure**	**Dangereuse**	**Catastrophique**

  - *<u>Structures</u> :* contraintes spécifiées, conception « fail safe »
  - *<u>Logiciels</u> :* méthodes de développement et de validation
  - *<u>Risques particuliers</u> (feu, collisions oiseaux, éclatement turbines, foudre,…) :* critères de qualification
- Les démonstrations doivent être approuvées par les Autorités pour obtenir le Certificat de Navigabilité de Type

Métiers de la sûreté de fonctionnement

- Un rôle d'EXPERTISE auprès de la Direction de Projet, du Responsable des Opérations :
  - Support à la définition des objectifs, à leur allocation, réalisation et gestion des Analyses globales, vérification des analyses détaillées, intégration des résultats, rôle d'alerte, traitement du retour d'expérience.
  - *Compétences* : sûreté de fonctionnement (approches), analyse systémique, compréhension et expérience du domaine.

- Un rôle d'ANALYSE (Bureau d'études) :
  - Réalisation d'analyses, exploitation des analyses fournies par des industriels ou sous-traitants, analyse des modifications. *Compétences* : sûreté de fonctionnement (méthodes et outils), technologies utilisées dans le domaine.

Limites et difficultés (vraies ou fausses) ?

- La question de l'exhaustivité des analyses : ***« On ne peut pas tout imaginer… »***
- Le problème des probabilités : ***« Nous manquons de données… »***
- Les exigences de rentabilité / d'urgence : ***« Il faut faire des choix… »***
- Les cultures de métiers : ***« Je suis spécialiste, je n'ai besoin de personne… »***
- La faible valorisation de l'activité : ***« en matière de sécurité, tout le monde a une idée - c'est juste du bon sens - etc.»***
- L'évolution des technologies : ***« Les systèmes actuels sont devenus très fiables… »***
- La relation avec les fournisseurs : ***« Ils savent ce qu'ils font… »***
- Le doute sur la crédibilité des résultats : ***« Oui mais il y a toujours des accidents… »***

L’exhaustivité des analyses

- Techniquement : la sûreté de fonctionnement ou l’analyse de risque ne sont SURTOUT PAS un travail d’imagination, elles s’appuient sur des méthodologies et des démarches rationnelles
- Déontologiquement : un professionnel ne peut en aucun cas s’abriter derrière l’impossibilité d’être exhaustif.

  Par contre, il se doit :

  - De définir explicitement le cadre de ses travaux, et en particulier les familles de risques qui en sont exclues : c’est le cas en général des agressions volontaires (sauf si les menaces à prendre en compte sont clairement spécifiées).
  - De mettre en place une méthodologie-cadre assurant la couverture des familles de risques retenues, et les fonctions analysées. Par exemple, une Analyse Préliminaire des Risques.

- La véritable limitation à l’exhaustivité est celle de la connaissance humaine des phénomènes en jeu.

Les exigences de rentabilité / d'urgence

- Il s'agit très rarement d'attitudes irresponsables des managers, mais la généralisation des indicateurs de performance tend à induire une « green culture » :
  - Non-information des responsables sur des problèmes, dont on pense qu'on va les régler sans « alerter la planète »,
  - Communication de résultats partiels pour respecter des délais difficiles à tenir, etc.

- Seule l'intégration de la sûreté de fonctionnement dans les organisations, et un fort soutien de la part du management peut éviter cet écueil.
- Les travaux prévisionnels de sûreté de fonctionnement peuvent être d'une grande utilité dans des situations accidentelles.

Le problème des probabilités

- Le réel danger n'est généralement pas le manque de données, mais plutôt :
  - l'utilisation illégitime de chiffres, et en particulier de statistiques (sources indéterminées, définitions peu claires, extrapolations abusives,…),
  - les modélisations de défaillances erronées ou incomplètes masquant des « modes communs ».

- Des informations souvent pertinentes sur la fiabilité des composants peuvent être obtenues par un retour d'expérience interne. Par exemple : « combien de pompes ont été remplacées en 5 ans ? ».
- Les objectifs de sûreté de fonctionnement (et les analyses) ne sont pas nécessairement probabilistes.

Les cultures de « métiers »

- Elles se rencontrent dans des secteurs de très forte compétence / expertise, qui ressentent peu le besoin d'échanges avec d'autres « métiers »
- Elles rendent très difficile toute activité transverse, qui apparaît comme une instance de contrôle, une remise en cause de la compétence, etc.

- Ceci souligne l'intérêt du rôle d'EXPERTISE de la sûreté de fonctionnement, au niveau des responsables de projet (ou d'exploitation) qui seuls ont le pouvoir d'intervenir comme architectes - intégrateurs. Mais aussi la nécessité de démontrer des capacités de spécialistes (crédibilité technique).

La faible valorisation de l'activité

- Les méthodes de sûreté de fonctionnement, les techniques de fiabilité sont peu connues et peu enseignées,
- Les notions de « risque », « sécurité » concernent tout le monde (et toutes les professions), et par conséquent paraissent familières, voire simples, et sujettes à débats plutôt qu'à études,
- Une image souvent négative a été donnée par des consultants en Risk-management à l'anglo-saxonne (pas d'analyses, exploitation d'interviewes et recommandations « à dire d'expert »),
- La demande du « risque zéro » s'accommode mal des réponses données par la sûreté de fonctionnement…

- Le métier reste à formaliser…

L’évolution des technologies

- Commercialisation de technologies pas toujours matures (faible retour d’expérience),
- Intégration électronique (hard-soft) rendant difficiles les redondances fonctionnelles, documentations souvent fragmentaires,
- Logiciels « temps réel » non démontrables à 100%,
- Nouveaux marchés des composants électroniques dominés par les applications « grand public » (jeu vidéos, téléphones portables),
- Composants « sensibles » (ex : batteries Li-Ion, Li-Po),
- Changement de solvants (aspects environnementaux ou sanitaires bénéfiques, mais occasionnant des modifications des processus).

- Ceci requiert de la part des analystes en sûreté de fonctionnement des compétences d’ingénieur généraliste, et les moyens d’assurer une veille technologique.

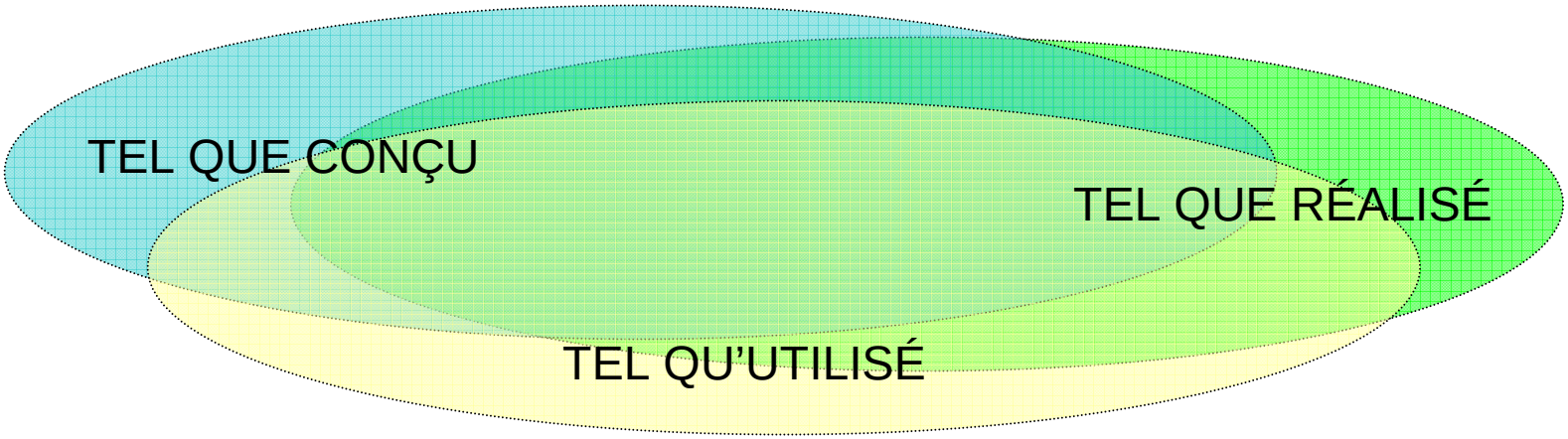
Donneurs d’ordres et fournisseurs

- Recours massif à la sous-traitance, sans que la capacité de management technique de cette sous-traitance soit toujours en place,
- Par effet de cascade, perte de visibilité sur les fournisseurs ou sous-traitants de niveau supérieur à 2,
- Aspects juridiques incitant à la non ingérence, notion de « risk sharing partners »,
- Evolution des organisations Qualité (certifier les organisations et les process plutôt que de contrôler les fournitures),

- La répartition (allocation) des objectifs de manière cohérente, et l’intégration des analyses deviennent des enjeux importants.

Limites des modèles, méthodes, analystes

- Danger des « modes communs » (fonction ou composant),
- Difficulté d'analyse de processus séquentiels,
- Difficulté d'identification des conditions insidieuses (« sneak »),
- Syndrôme de « l'armoire aux AMDEC » (qui les a relues ?),
- Recours aux analyses automatisées : les pièges…
- Ecarts entre l'analyse, et la « vraie vie…



Limites des modèles, méthodes, analystes

- Adapter les méthodes à chaque problématique, par exemple :

	QUALITATIVES	PROBABILISTES
NON CAUSALES *(méthodes représentatives)*	- Analyse fonctionnelle (M) - Analyse des conditions insidieuses - Analyse de zone (M)	- Diagrammes de fiabilité - Graphes de Markov (S) - Réseaux de Petri (S) - Méthodes statistiques
INDUCTIVES *(bottom-up)*	- A.P.R. - AMDEC et dérivées - Graphes causes-conséquences (S)	- Graphes causes-conséquences (S) - Analyses temporelles (S) - Analyse des pannes fonctionnelles
DEDUCTIVES *(top-down)*	- Arbres des causes (M) - Analyse des ressources (M)	- Arbres des causes (M)

Le doute vis-à-vis des résultats

- Il est extrêmement difficile d'évaluer le retour sur investissement de la sûreté de fonctionnement, du fait de la nature même des bénéfices qu'elle peut apporter…
- Des systèmes qui ont fait l'objet d'analyses de risques approfondies (spatial, nucléaire, chimie, armement…) ont malgré cela connu des accidents…

- Convaincre par l'exemple : dans la pratique, la mise en évidence par les techniques d'analyse de risque de points faibles, mais aussi de gains en termes de performances globales (par exemple disponibilité / coût) montre très rapidement son intérêt.

Intérêts de la sûreté de fonctionnement

- EXPRIMER par des OBJECTIFS les attentes en matière de « performance Sûreté de Fonctionnement », qui complètent les objectifs opérationnels, et définissent le « RISQUE ACCEPTABLE »,
- ANALYSER les risques dès la conception générale, et non a posteriori,
- TRACER les décisions prises,
- DOCUMENTER les « modèles de risques » afin de permettre le suivi des évolutions, les modifications, le retour d'expérience (« faits techniques »), le pilotage de situations d'urgence.

Mais toujours :

- Apporter des ÉLÉMENTS OBJECTIFS ET JUSTIFIÉS à la prise de décision en matière de gestion des risques.

En matière de sûreté de fonctionnement, comme dans bien d'autres activités professionnelles,

Seule la démonstration permanente d'un professionnalisme, d'un niveau de compréhension et d'exigence, et d'un pragmatisme reconnus par les spécialistes du domaine analysé permet :

- De gérer les difficultés culturelles propres à ce métier, peu connu et transverse aux « cultures de spécialité »,
- De maîtriser les difficultés techniques,
- De fournir aux véritables responsables des risques, les éléments leur permettant d'assumer cette responsabilité avec confiance et réalisme.

Merci de votre attention