1ÈRES RENCONTRES INTERNATIONALES

1ÈRES RENCONTRES INTERNATIONALES

organisées par le CHU de TOULOUSE

La maîtrise des risques, la sûreté de fonctionnement et la notion de risque acceptable illustrées à travers la conduite d'un projet industriel de conception et de construction d'avion

Pierre LAVÉDRINE

Ingénieur ENSMA - ENSAé

Airbus Toulouse

TOULOUSE 15-16 Juin 2009

Préambule : quels risques ?

- Dans la plupart des activités humaines, la notion de « risque » peut couvrir des problématiques extrêmement variées : accidents corporels, défaillances ou aléas techniques, pertes financières, échecs de projets, etc.

- Les éléments de réflexion de cette présentation s'intéressent aux risques majeurs à caractère sociétal (mise en cause de l'intégrité, voire de la vie humaine, dans un contexte collectif). Autrement dit, aux scénarios susceptibles d'occasionner des « accidents majeurs ».

- Il s'agit d'une analyse personnelle, reposant sur les activités de l'auteur dans différents secteurs à risques majeurs (armement, aviation, transports), et destinée à contribuer à l'échange d'idées et d'expériences voulu par les organisateurs des présentes Rencontres Internationales.

Notion de « risque acceptable »

- **Historique :**
  - Outils : statistiques de fiabilité des composants électroniques (années 60), analyse des causes (Fault Tree, Bell Laboratories),
  - Analyses de « sécurité des systèmes » : Rapport WASH 1400, dit rapport Rasmussen (centrales nucléaires USA, fin des années 60),
  - Objectifs probabilistes de sécurité (systèmes d'armes, nucléaire, aéronautique, années 70) : « le risque zéro n'existe pas ». En corollaire, tout risque peut et doit être identifié, analysé, évalué.

- **Un concept remis en question :**
  - Perte de confiance envers les « hautes technologies »,
  - Evolution socio-culturelle vers un refus d'exposition collective à des danger / à des risques « nouveaux », et la négation du « fait accidentel » (responsabilité sans faute ?) -> remise en cause du « risque acceptable ».

Objectifs de sûreté de fonctionnement

- **La sûreté de fonctionnement requiert la définition d'objectifs,**
  - …pour disposer un référentiel, pouvoir comparer, éviter la subjectivité et l'acceptation de fait des résultats obtenus, autoriser des hypothèses pénalisantes sur des problématiques complexes, etc…
- **Implicitement, définition d'objectifs = acceptabilité du risque,**
  - ..qui doit être définie au niveau de responsabilité adapté : Management de l'entreprise / du projet (objectifs de performance « internes »), Autorité externe (sécurité des tiers ou de l'environnement), etc…
  - …qui n'est pas nécessairement qualitative (= probabiliste), mais peut s'exprimer sous la forme de règles (critères de conception, tolérance aux fautes,..)
- **Le niveau décisionnel d'approbation des études de sûreté de fonctionnement doit correspondre au niveau décisionnel de définition du risque acceptable.**

Aéronautique : sécurité en conception

- La sécurité et la navigabilité (Airworthiness) des aéronefs civils sont sous le contrôle des Autorités internationales de Certification (FAA / EASA).

- Ces Autorités sont en charge de la définition des objectifs / règles de sécurité et de l'approbation de la démonstration de leur respect :
  - ***Systèmes*** ***: objectifs probabilistes (cf ci-après)***
  - ***Structures*** ***: principe du « fail safe » + essais de qualification***
  - ***Risques particuliers*** ***(incendie, ruptures de turbine, foudre, oiseaux,…) : épreuves de qualification***
  - ***Logiciels*** ***: principes de conception et de validation***
- Elles délivrent le droit de concevoir / produire / maintenir des aéronefs sous la forme d'Agréments (DOA / POA / MOA), les Certificats de Navigabilité des aéronefs, et les licences des pilotes.
- Elles émettent des Directives de Navigabilité (exploitation du suivi des incidents / accidents).

Objectifs de sécurité - Conception avion

- Retour d'expérience (accidentologie) :
  - ***la probabilité d'accident pour toutes causes dans la flotte commerciale est comprise entre 10^{-7} et 10^{-6} par heure de vol.***

- Exemple d'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**

Organisation sécurité - Conception Avion

Directeur de Programme Axxx

Vice President Engineering

Autorités de certification

Dpt Navigabilité

Ingénieur en Chef Axxxx

Centres de compétences

Concepteurs

Chaque concepteur doit être « habilité »par une double <u>Autorité Technique</u> :

- Compétence

- Connaissance avion

La cascade d'<u>Autorité Technique</u> n'est pas dépendante du management de l'Entreprise.

Cette organisation est agréée par les Autorités de Certification

Aéronautique : risques en production (1/2)

- **Trois familles de « risques » pris en compte :**
  - Risques professionnels,

    (référence : Code du Travail)
  - Risques / aspects environnementaux,

    (références : Code de l'Environnement / Arrêtés Préfectoraux + engagement ISO 14001)
  - Risques industriels / arrêt de production.

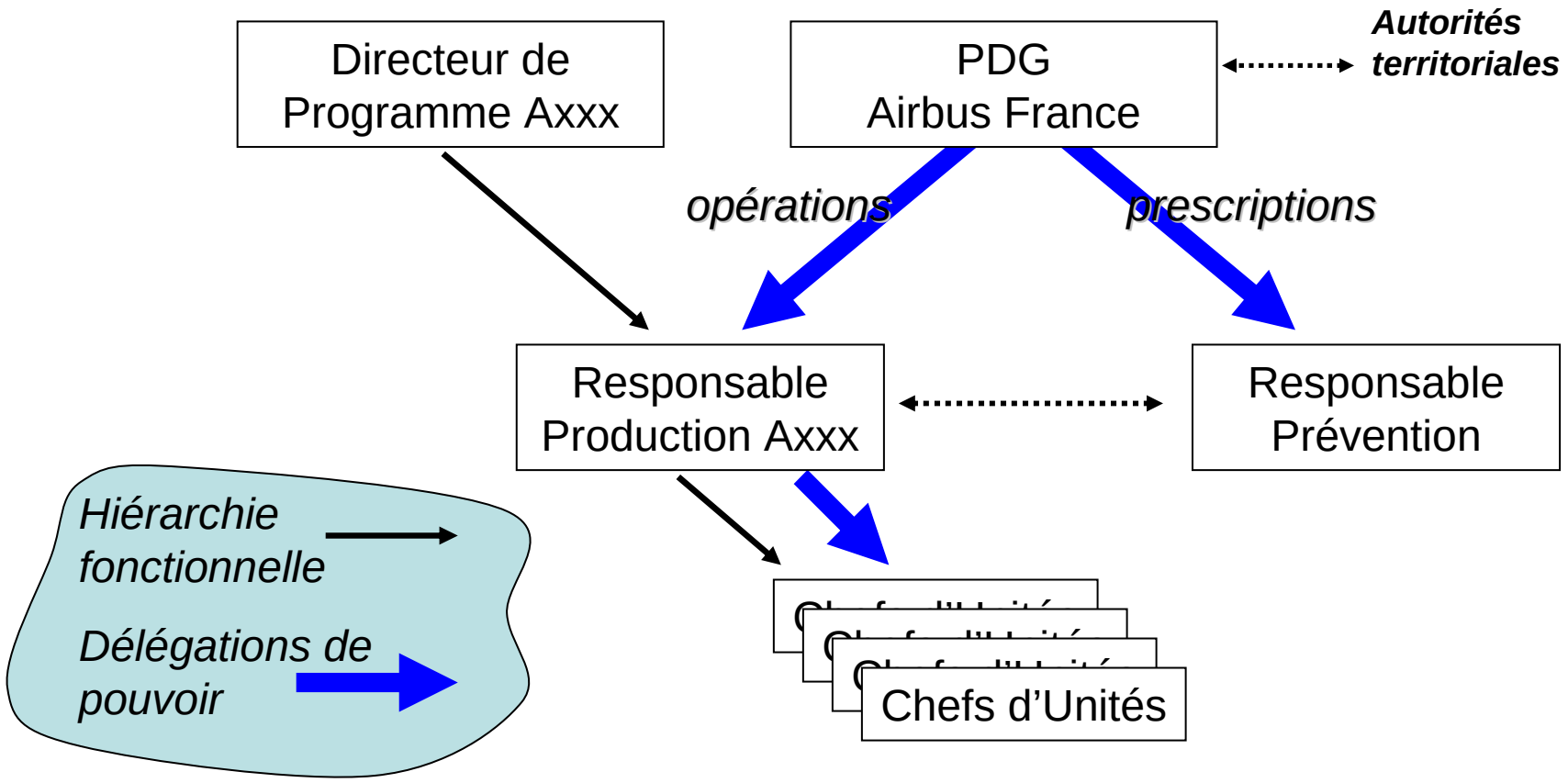
    (références : exigences internes EADS / Airbus et relations avec les assureurs)

Aéronautique : risques en production (2/2)

- **Pas d'objectifs quantifiés, mais :**
  - Matrices (qualitatives) d'acceptabilité des risques,
  - Principes de conception pour les risques potentiellement graves des nouvelles installations. (« fail safe », « fault tolerant », etc.). Ces principes sont traduits dans les spécifications techniques, et toute dérogation fait l'objet d'une revue. Ils concernent par exemple :
    - ***Assemblages mécaniques***
    - ***Chaînes fonctionnelles***
    - ***Automates, commande-contrôle***
    - ***Démarrage / mise en sécurité / phases transitoires***
    - ***Source et distribution d'énergie***
    - ***Stockage (combustibles, produits dangereux)***
    - ***etc.***
  - Catégorisation des risques des trois familles, aidant à l'exhaustivité
  - Reporting vers les décideurs des risques majeurs en termes de gravité (et non de criticité).

Organisation « risques » - Production

- ***Notion de délégation de pouvoirs (juridique) :***



Quelques constats d'expérience (1/2)

- La formalisation d'objectifs de sécurité et/ou de sûreté de fonctionnement (et donc implicitement la définition d'un risque acceptable) nous semblent un préalable à cette activité.

- En effet, l'absence de cette formalisation conduit à :
  - **La subjectivité (traitement des peurs, ou des risques ?),**
  - **Le manque de référence pour la conception (« on fait au mieux »),**
  - **L'absence de critères d'acceptation des analyses / des résultats,**
  - **Des priorités / des décisions soumises au conjoncturel : finance, image de marque, sensibilité du management, accidents à fort impact médiatique,..**

- La définition du RISQUE ACCEPTABLE se doit de :
  - **Prendre en compte l'évaluation, mais aussi les diverses dimensions d'appréhension des conséquences redoutées : individuelles, sociétales, environnementales,…**
  - **S'appuyer sur des critères formels ou des éléments de comparaison statistiques justifiés,**
  - **Etre recevable (sinon agréée) par l'ensemble des « parties intéressées ».**

Quelques constats d'expérience (2/2)

- Les outils de sûreté de fonctionnement ne sont qu'un support à des analyses d'abord systémiques (Analyse Fonctionnelle, Analyse Préliminaire des Risques,..) puis détaillées (AMDEC, etc.). Ces analyses doivent être approuvées par une autorité compétente (interne ou externe) : la SdF ne doit pas être de facto déléguée aux analystes…

- Le « Métier » de la sûreté de fonctionnement doit intervenir à deux niveaux : Support au décisionnaire, et Bureau d'analyse.

- Les évolutions technologiques (électronique / informatique) posent des problèmes nouveaux de maîtrise des systèmes : composants à large intégration, moniteurs temps réel,… D'où le besoin des compétences techniques d'ingénieurs généralistes.

Pour tenter de conclure… (1/2)

- Au delà d'une option à caractère philosophique, la notion de « risque acceptable », implicite ou explicite, est à notre sens le préalable indispensable à une approche objective de la sécurité. Elle pose toutefois la question de la responsabilité de définition de l'acceptabilité.

- La formalisation du « risque acceptable » en objectifs (sécurité, sûreté de fonctionnement) nécessite une réflexion approfondie sur le système à prendre en compte, ses missions et impacts potentiels, les situations à considérer, les éléments techniques et sociétaux pouvant être pris en référence,…

- Les objectifs de sécurité / sûreté de fonctionnement peuvent être probabilistes, mais aussi qualitatifs (fail safe, fault tolerance, ségrégation, principes d'architecture, options technologiques …).

Pour tenter de conclure… (2/2)

- L'exemple de l'aviation civile montre un bénéfice à l'existence d'une autorité internationale, compétente et incontestable pour une famille d'activités / de risques majeurs. Une telle entité apparaît comme la mieux placée pour définir des objectifs, mais aussi pour juger de leur respect. Ceci requiert une autorité morale, mais également technique.

- La complexité d'architecture des systèmes (technologiques, organisationnels) rend très difficile le découpage a priori du travail d'analyse (top-down -> bottom-up). Une vision globale est nécessaire, elle nécessite une culture de l'analyse systémique, et un solide retour d'expérience dans le domaine analysé.

- Les analyses prévisionnelles de sûreté de fonctionnement ne sont qu'une étape. Le suivi des évolutions et l'exploitation du retour d'expérience sont indispensables aux progrès dans la maîtrise de nos systèmes complexes.

Merci de votre attention