La recherche désespérée du risque nul

Assurer la sécurité, c'est s'engager à limiter raisonnablement le risque, non à l'éliminer.

par Jean-Claude Wanner
Membre de l'Académie nationale de l'air et de l'espace

Incohérences

Lorsque je pénètre dans un avion ou dans le TGV, je souhaite parvenir entier à destination, en d'autres termes je souhaite que le transporteur me donne l'assurance formelle que je ne cours aucun, strictement aucun risque.

De même je souhaite, à chaque instant, être assuré de ne pas être victime d'un quelconque accident dans les heures qui suivent, quelle que soit mon activité, même si cette activité est dite « à risque » !

Ce souhait, parfaitement légitime, est-il réaliste ? Hélas, la réponse est non, irrémédiablement non. La seule réponse que je peux obtenir est : « Nous avons fait tout ce qui est humainement possible pour limiter le risque d'accident et vous souhaitons un agréable voyage ou une plaisante activité » !

Que faire, alors, pour éviter de périr dans un accident d'avion ou de TGV ? Eviter ces moyens de transport ! Et encore je ne peux éviter le risque, faible il est vrai, de recevoir un avion sur la tête ou de me faire happer à un passage à niveau. Même si j'ai pris la décision de ne pas quitter le plancher des vaches, qui me dit que, victime d'un banal accident de la vie de tous les jours, je ne serai pas, inconscient, évacué par hélicoptère ou avion sanitaire, pour périr dans une collision en vol ou dans un atterrissage raté avant d'atteindre l'hôpital le plus proche ?


DR

Que faire pour éviter tout incident, tout accident dans la vie de tous les jours ? Rester chez soi, mais peut-on échapper à tous les incidents domestiques ? Rester dans son lit, mais comment éviter l'effondrement du plafond sous l'effet d'un tremblement de terre, de la chute d'un météore, de la station Mir ou, moins improbable, de la percussion d'un poids lourd ? Tout le monde sait, par ailleurs, que l'examen du nombre de personnes mourant dans leur lit devrait nous faire hésiter à y coucher.

Notre comportement vis-à-vis du risque est totalement incohérent. Nous acceptons sans

sourciller, chaque année, 8 000 morts sur les routes de France, 60 000 morts dus au tabagisme, mais refusons les quelques 3 000 morts par an, dans le monde, des accidents aériens. Les explosions meurtrières dues au gaz, les asphyxies provoquées par des chauffages défectueux sont considérées comme banales. Par contre, tout incident dans une centrale nucléaire est considéré comme une catastrophe mondiale. Nous savons que nous avons vingt cinq chances (ou malchances) sur cent de périr d'un cancer, mais nous sommes prêts à refuser l'administration d'un remède efficace pour nous soulager aujourd'hui si nous augmentons d'un millième le risque d'un cancer dans trente ans ; ce qui ne nous empêche pas de fumer et de consommer de l'alcool !

Choisir

Comment peut-on, non éliminer le risque, mais le limiter raisonnablement ? Minimiser le risque répond à trois impératifs :

✔ un impératif moral interdisant de porter atteinte à l'intégrité des personnes ou du milieu naturel ;

✔ un impératif juridique car un accident peut avoir des conséquences pénales ;

✔ un impératif économique et commercial, car un taux d'accidents trop élevé a un effet évidemment dissuasif sur la clientèle potentielle, provoque une hausse des coûts d'assurance et détériore l'image de marque.

Nous allons voir que, non seulement on ne peut assurer un risque nul, mais que, bien souvent, le responsable, soit de la conception, soit de l'utilisation d'un système, sait estimer le risque résiduel et, en conséquence, accepte ce risque, tout en essayant de le minimiser.

Le responsable, soit de la conception, soit de l'utilisation d'un système, sait estimer le risque résiduel et, en conséquence, accepte ce risque, tout en essayant de le minimiser.

Donnons tout d'abord un exemple de risque évalué et admis par tous les concepteurs d'avions de transport, situation qui peut avoir des conséquences pénales en cas d'accident.

Les gouvernes des avions de transport modernes ne peuvent être actionnées directement par le pilote agissant sur le manche ou le palonnier. Les efforts aérodynamiques sur les gouvernes aux vitesses de croisières sont en effet trop importants pour pouvoir être équilibrés par une liaison mécanique entre commandes et gouvernes. Il est nécessaire d'assister le pilote en plaçant entre la commande et la gouverne un système amplificateur connu sous le nom de servocommande. Les servocommandes sont actuellement constituées par des vérins hydrauliques placés au voisinage des gouvernes. La commande des vérins est soit une commande mécanique (tringles et câbles liant le manche et le palonnier au tiroir de commande du vérin), soit une commande électrique (la position du manche est transmise par câble électrique à un moteur attaquant le tiroir du vérin, le plus souvent par l'intermédiaire d'un ordinateur).

Il est évident que la fiabilité du système de transmission des ordres du pilote aux gouvernes est fondamentale pour la sécurité du vol. Aussi les constructeurs ont-ils le souci permanent d'assurer une fiabilité optimale à ces systèmes. Mais qu'entend t-on par fiabilité optimale ?

On peut améliorer la fiabilité d'un système en lui adjoignant des systèmes redondants, mais combien faut-il en installer et jusqu'où faut-il aller dans cette démarche ? Actuellement les systèmes de commandes hydrauliques sont triplés sur les avions de ligne et rendus physiquement indépendants (autrement dit la panne de l'un des systèmes est sans effet sur le bon fonction-

nement des autres systèmes). Cette disposition conduit à une probabilité de perte totale des commandes de l'ordre de un sur un milliard par heure de vol (10-9/h), la perte d'un seul système ayant une probabilité de l'ordre de un sur mille par heure (10-3/h).

Faut-il aller plus loin et installer quatre systèmes redondants ? Tous les techniciens interrogés répondront non à cette question pour plusieurs raisons :

✔ il n'est pas physiquement possible de disposer plus de trois vérins par gouverne sans avoir à effectuer des changements très délicats de conception ;

✔ installer un système hydraulique supplémentaire augmentera la masse à vide de l'avion et réduira d'autant sa charge marchande (à masse au décollage constante imposée par des considérations de performances minimales assurant la sécurité au décollage) ;

✔ augmenter la complexité de l'installation du système hydraulique augmente les probabilités de non-indépendance des circuits redondants et ne va donc peut-être pas dans le sens de la sécurité (problème bien connu de la défiabilisation par un excès de souci de fiabilisation) ;

✔ les autres systèmes vitaux de l'avion, circuits électriques, circuits d'alimentation en combustibles, structure, etc., ont des fiabilités voisines de celle du système hydraulique. Il serait illusoire d'augmenter la fiabilité du seul système hydraulique sans augmenter la fiabilité des autres systèmes, sinon la fiabilité globale de l'avion n'en serait pas augmentée pour autant.

On peut admettre que le premier argument est réfutable. Les ingénieurs n'ont qu'à faire preuve d'un peu d'imagination ! Il faut toutefois, là encore, penser au fait qu'augmenter la complexité ne va pas toujours dans le sens de la sécurité, comme le rappelle le troisième argument. Au *deuxième argument on peut répondre que le souci de la sécurité passe avant celui de la rentabilité. Ceci est vrai dans la mesure où les « améliorations » de sécurité ne rendent pas le produit fini économiquement inexploitable, ce qui risque d'arriver si l'on augmente la fiabilité de tous les systèmes pour répondre au dernier argument*. Rappelons le *vieil adage, « la sécurité n'a pas de prix, mais elle a un coût »* ! Quelle compagnie achèterait un avion de la taille de l'Airbus A340 pour transporter une vingtaine de passagers seulement !

En définitive, l'ensemble des responsables de la conception des avions des générations actuelles est d'accord pour admettre que le triplement des systèmes hydrauliques, est la solution raisonnable.

Tout le monde admet donc qu'une probabilité de un sur un milliard par heure de vol pour la panne totale d'hydraulique d'un avion est « raisonnable ». Bien entendu, cela signifie que chaque concep-

Keystone

Si la sécurité n'a pas de prix, elle a un coût ! Quelle compagnie achèterait un avion de la taille de l'Airbus A340 pour transporter une vingtaine de passagers seulement ? Ci-dessus, l'assemblage d'Airbus A300 B dans les usines de l'Aéronautique à Toulouse.

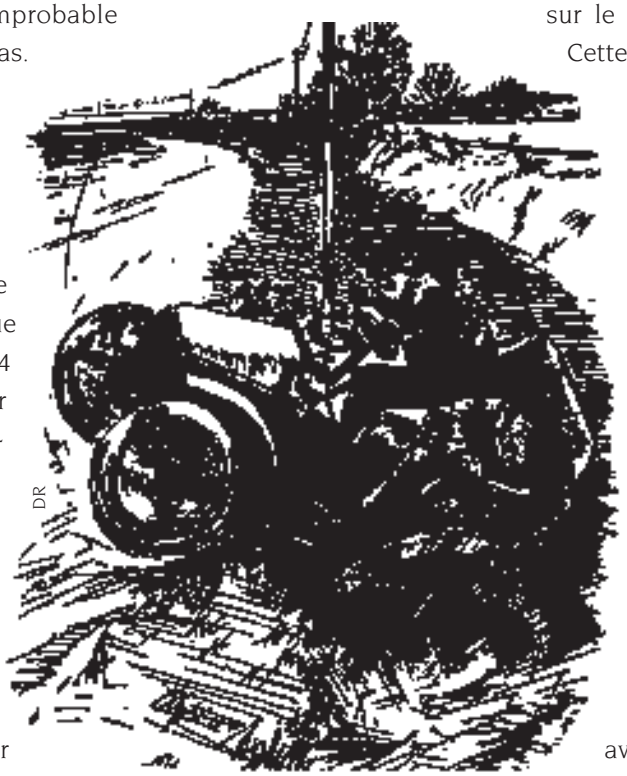
teur s'assure que les systèmes hydrauliques répondent aux règles de l'art et passent avec succès les épreuves sévères de qualification permettant d'affirmer que le niveau de un sur un milliard est raisonnablement assuré.

Attention : danger

Il n'en reste pas moins qu'il reste une chance (ou plutôt une malchance) sur un milliard par heure de vol pour qu'une panne totale des circuits hydrauliques conduise un jour à la catastrophe. Or ce n'est pas parce qu'un phénomène est hautement improbable qu'il ne se produit pas.

Il y a actuellement en service environ 1 000 avions du type Airbus (de l'A300 à l'A340). Si l'on admet que chaque avion effectue en moyenne 14 heures de vol par jour (chiffre certainement sous-estimé), cela représente environ 5 millions d'heures par an et 100 millions d'heures en 20 ans. Ainsi la probabilité d'observer une panne totale d'hydraulique, de probabilité élémentaire de 10-9/heure, sur 20 ans d'utilisation de cette flotte est-elle de l'ordre de dix pour cent !

Que fera alors la justice si un tel événement malheureux se produit ? Cherchera-t-elle un « coupable » ? Bien entendu il lui faudra s'assurer que toutes les règles de sécurité en matière de fabrication, maintenance, conditions d'emploi, formation du personnel ont été respectées, et par le constructeur et par la compagnie utilisatrice. Si une faute a été commise dans l'un de ces domaines, il lui faudra certainement condamner le coupable.


DR

Mais il est parfaitement possible que l'accident ne provienne que de la conjonction malheureuse de la panne « normale et prévue » de chacun des trois circuits. Et si, à l'occasion de cet accident avec pertes de vies humaines, la justice venait à mettre son nez dans les dossiers d'incidents ? Cette fois ce sont les responsables de la sécurité qui se sentent mal à l'aise. Que répondre au juge d'instruction s'étonnant que des incidents analogues se soient déjà produits et que l'on n'ait pas encore réagi ? Plutôt que de risquer une mise en examen et une condamnation ne vaudrait-il pas mieux ignorer les incidents et mettre l'accident sur le compte de la fatalité ?

Cette attitude peut sembler étonnante, mais nous avons connu des responsables d'une grande industrie qui ont refusé de faire des études de sécurité de peur de voir la justice se retourner contre eux dans le cas d'un accident survenant dans des conditions estimées hautement improbables au cours de l'étude et donc écartées à juste titre.

A l'occasion d'un accident aérien, nous avons vu, en effet, des magistrats, d'une nation

étrangère et néanmoins amie, faire le raisonnement faux mais très convaincant suivant : « *Vous me dites que cet événement est hautement improbable, soit, mais il s'est produit. Par conséquent ou bien vous avez commis une faute d'estimation, ou bien vous avez négligé volontairement de traiter ce cas. Vous êtes donc coupable* » !

Il est évident, pour tous les spécialistes des probabilités, que « hautement improbable » ne signifie pas impossible. Pour s'en convaincre il suffit de calculer la probabilité de gagner le gros lot au Loto, c'est-à-dire de prévoir six numéros gagnants sur quarante neuf. Il y a environ une chance sur quatorze millions de gagner, événement par conséquent hautement improbable. Or il y a un gagnant à chaque tirage ou presque, ce qui ne signifie pas que le calcul de la probabilité soit faux, mais que le nombre de joueurs est grand ! En effet, la probabilité pour qu'il y ait un gagnant si vingt millions de grilles ont été joués est de 76 %. Elle monte même à 98,6 % pour trois tirages de vingt millions de grilles (attention, le calcul simpliste consistant à multiplier 60 000 000 par 1/14 000 000 est évidemment faux, la formule de calcul de la probabilité est dans ce cas plus complexe !).

Retour d'expérience

Insistons sur la démarche probabiliste ayant conduit à la décision de tripler les systèmes. On reproche bien souvent à cette démarche de faire des hypothèses peu fondées sur la fiabilité de chacun des systèmes et donc de se leurrer sur la fiabilité globale du système avec ses redondances. L'estimation initiale de la fiabilité de chaque système isolé est faite en se reposant sur des essais d'endurance et sur les résultats observés sur les systèmes analogues. Mais il y a mieux. Le comportement des systèmes est surveillé au cours de l'exploitation réelle. Si l'on observe des taux de défaillance supérieurs à ceux prévus, il est possible d'en trouver les causes et d'y porter remède avant qu'une catastrophe ne se produise, pour ramener la fiabilité au niveau souhaité. Cette démarche est connue sous le nom de **retour d'expérience** et consiste à tirer partie des incidents en service sans attendre la catastrophe pour réagir. Nous allons en reparler.

La tempête de la fin de l'année 1999 nous amène également à réfléchir sur l'aspect économique des mesures de sécurité. Les mises hors service d'un grand nombre de centraux téléphoniques par manque d'alimentation pouvaient être évitées par l'installation, dans chaque centre, d'un groupe électrogène et même, pour plus de sécurité de deux groupes électrogènes. Cette solution, évidente, a été bien des fois avancée dans les médias. Il est évident que la perte des moyens de communication peut avoir des conséquences graves et qu'il faut faire quelque chose. Cette solution ne résout toutefois pas le problème de la destruction des lignes téléphoniques. Qu'à cela ne tienne, installons


DR

des groupes électrogènes dans tous les relais de transmission pour la téléphonie portable ! Par ailleurs, équipons chaque relais d'antennes rétractables pour en éviter la destruction en cas de vents trop élevés. Bien sûr, la rentrée de ces antennes et la mise en route des groupes électrogènes se fera par des automatismes (redondants), alimentés par plusieurs batteries.

C'est alors qu'il faut se poser le problème du coût de cette solution. Pour se prémunir contre un événement exceptionnel comme celui que nous venons de subir, est-on prêt à payer cinq ou dix fois plus cher nos communications ? Nous avons observé un comportement analogue des utilisateurs lors de l'incident de givrage des caténaires de la SNCF en 1997. Pourquoi ne pas équiper les lignes de résistances chauffantes évitant le givrage ? La solution est techniquement possible, mais qui est prêt à payer deux ou trois fois plus cher un titre de transport pour couvrir un incident, sérieux certes, mais exceptionnel ?

Parmi les événements qui risquent de réduire la sécurité, il faut citer tous ceux que l'on ne peut imaginer au moment de la conception et qui ne se révèlent qu'au cours de l'utilisation. Nous n'avons pas assez d'imagination pour « inventer »tous les scénarios dangereux et prendre à temps les précautions permettant de les éviter.

Les trois moteurs du DC 10 sont équipés de bouchons magnétiques qui peuvent capturer, dans le circuit de graissage, des débris métalliques pouvant provenir d'une usure intempestive des roulements. L'examen périodique de ces bouchons permet ainsi de détecter à temps une anomalie et d'y porter remède.

C'est là que le retour d'expérience montre sa nécessité pour détecter les événements imprévisibles au moment de la conception et de la première mise en service.

Que voici une disposition judicieuse, utilisée sur la plupart des moteurs ! Mais elle fut à l'origine d'un incident très grave se soldant par la panne en vol des trois moteurs. Heureusement l'avion, après un vol plané depuis l'altitude de croisière jusqu'à 1 000 m environ, put se poser sans encombre sur un terrain après remise en route ultime de l'un des trois moteurs !

Au cours de la nuit précédant ce vol critique, les trois moteurs furent révisés et, suivant la procédure, les trois bouchons furent démontés pour expertise par le service compétent et remplacés par trois bouchons neufs. Or, le magasin habituel n'ayant pas les bouchons de rechange, les mécaniciens durent s'approvisionner à un magasin auxiliaire qui, contrairement à l'usage, leur fournit les bouchons non équipés des joints assurant l'étanchéité du circuit de graissage. Ce montage défectueux, sans joint, se traduisit par une fuite provoquant la panne des trois moteurs en croisière, une fois les réserves d'huile de graissage épuisées.

A noter qu'à la suite de l'alarme de baisse de pression d'huile sur l'un des moteurs, celui-ci fut immédiatement coupé. Mais l'alarme sur les deux autres moteurs fut interprétée par l'équipage comme une panne d'alarme, jusqu'à ce que les deux moteurs se bloquent faute de graissage. C'est le moteur coupé en premier et non endommagé qui put être remis en route pour assurer l'atterrissage en fonctionnant sur la réserve d'huile épargnée par la première manoeuvre de mise à l'arrêt !

Cet accident, comme tous les accidents, était la conséquence de nombreux événements malencontreux : révision (exceptionnelle) des trois moteurs en même temps, absence de pièces de rechange au magasin (la révision des moteurs n'avait pas eu lieu sur le terrain habituel pour des raisons d'opportunité), fourniture de bouchons sans les joints,

non prise en compte de cette absence par les mécaniciens pressés par le temps (la recherche des bouchons les avait retardés et le temps leur était compté), vérification de l'étanchéité des circuits de graissage par un essai ne permettant pas de détecter ce type de fuite faible, bien que critique, etc. Qui aurait pu envisager un tel scénario ? Bien entendu, une fois l'incident connu, des procédures furent mises en place pour éviter son renouvellement et la sécurité en fut renforcée. En attendant l'apparition d'un autre scénario tout aussi inimaginable *a priori*. Notre expérience des accidents aériens nous a montré que les accidents et les incidents sont de même nature, les accidents n'étant dus qu'à une succession d'incidents bien connus et qui ont « mal tourné ». Le retour d'expérience consiste ainsi à analyser les incidents pour en tirer profit et non à se contenter d'analyser les accidents qui sont peut-être très instructifs mais heureusement peu nombreux, ce qui en rend l'étude peu fructueuse et par ailleurs trop tardive.

Tirer profit des incidents

Dans le cas de l'incident très grave que nous venons de décrire, il faut reconnaître que les utilisateurs du DC10 n'ont pas su tirer partie des précurseurs. En effet, plusieurs incidents avaient montré que des montages de bouchons sans joints s'étaient déjà produits, sans autre conséquence que l'arrêt des moteurs par panne de graissage ; il n'en avait donc pas été tenu compte pour modifier les procédures de stockage des bouchons munis de joints, les procédures de montage comportant une vérification de la présence des joints et les procédures de vérification de l'étanchéité des circuits de graissage. Le scénario de l'accident lui-même était imprévisible, mais la réduction de probabilité de panne de graissage était possible. Assurer la sécurité c'est réduire la probabilité d'apparition d'événements qui, combinés à d'autres événements, peuvent conduire à la catastrophe.

Quittons le domaine aéronautique pour trouver quelques autres exemples de phénomènes dangereux qui ne sont apparus qu'à l'occasion d'accidents.

Ainsi, des fuites minimes de produits chimiques circulant dans les canalisations se répandent lentement sur la laine minérale des calorifuges. L'effet catalytique des fibres et la grande surface du produit ainsi répandu et exposé à l'oxygène de l'air, conduisent à l'apparition de corps oxydés ou peroxydés. Leur combustion spontanée peut se faire alors avec dégagement de chaleur pouvant conduire à des températures de l'ordre de 700 à 800 degrés. Ce phénomène dit « punking » n'a été mis en évidence que récemment. Il a été ignoré pendant longtemps, bien que l'on ait constaté, au cours d'opérations de maintenance, la dégradation de certains calorifuges, sans en comprendre l'origine ni la gravité.
Il a fallu deux ans d'études pour comprendre l'origine de la réaction secondaire qui s'était produite à Seveso et avait conduit à l'émission fâcheuse d'une dioxine dans l'environnement de l'installation. Il était donc bien difficile, pour ne pas dire impossible, de prévoir ce phénomène avec les connaissances du moment. Cet accident est à l'origine de l'analyse de stabilité thermique par micro-calorimétrie.

Ce n'est qu'à la suite de l'explosion d'une seconde tour de distillation de zinc (accident de Métaleurop) que l'on put mettre en évidence l'origine profonde du phénomène, augmentation de la viscosité du zinc liquide due à un mélange avec de l'oxyde de zinc.

Citons, enfin, un accident survenu par excès de précaution. Les opérateurs d'une installation anglaise de production chimique se sont trouvés dans l'incapacité de contrôler un dysfonctionnement grave parce que plusieurs centaines d'alarmes sont apparues en même temps, ce qui interdisait toute analyse logique de la situation !

Quelques principes de conception

Abandonnons les exemples pour aborder la question des principes de sécurité à mettre en oeuvre au moment de la conception.

Lorsque l'on conçoit un nouveau système, c'est avec l'idée, justifiée, de faire mieux que les systèmes en service, « mieux » signifiant des performances supérieures, des coûts de production et d'exploitation inférieurs, une sécurité d'utilisation ou une sûreté de fonctionnement accrues.

La conception nécessite donc le plus souvent une exploration de domaines nouveaux, c'est-à-dire une extrapolation des connaissances. Il est bien évident que toute extrapolation comporte des risques d'erreurs. Bien entendu, le concepteur s'efforce de respecter les exigences de sécurité avec les moyens et méthodes que nous détaillerons plus loin pour montrer que, contrairement à ce que pense généralement le grand public, on ne fait pas n'importe quoi, n'importe comment, dans le seul souci d'améliorer le profit.

Donnons quelques exemples d'extrapolations dans le domaine de la conception des avions.

✔ A performances égales ou voisines, même domaine de vol (vitesses et altitudes), charge marchande du même ordre de grandeur :

• réduction des masses à vide (réduction des coûts de fabrication et d'exploitation) ;

• amélioration de la finesse aérodynamique, ce qui réduit la poussée nécessaire des moteurs et donc la consommation kilométrique de carburant ;

• amélioration du rendement des moteurs conduisant à une réduction de la consommation spécifique (rapport consommation/poussée) ;

• amélioration de la sécurité d'utilisation. Utilisation, par exemple, de systèmes interdisant les dépassements du domaine autorisé pour l'avion ou certains sous-ensembles (interdiction de dépassement de l'incidence de décrochage, par exemple). Mise en place de systèmes redondants dissemblables limitant les pertes de fonctions vitales ;

• amélioration de la sûreté d'emploi. Une augmentation de la sûreté se traduit par une meilleure régularité d'utilisation, les systèmes remplissant leurs fonctions avec une probabilité de défaillance diminuée. Mise en place de systèmes redondants pour limiter les pertes de fonctions interdisant le vol si elles sont détectées avant décollage ;

• augmentation de la durée de vie.

✔ Changement du domaine de vol (vitesse, distance franchissable) ou de la charge marchande.

Les moyens sont analogues à ceux que nous venons de citer, mais les extrapolations sont en général plus audacieuses car il ne s'agit pas de « gratter » seulement quelques pour cents.

Le passage de Mach 1 pour les avions expérimentaux au cours des années 50 a été rendu difficile du fait de la mauvaise connaissance, à l'époque, des phénomènes aérodynamiques autour de cette vitesse critique. Les méthodes de calcul, sans ordinateurs, étaient inutilisables et les résultats expérimentaux inexploitables, parce que les mesures en soufflerie sont perturbées par les multiples réflexions des ondes de choc sur les parois. Seules les

expérimentations en vraie grandeur ont permis d'accroître les connaissances et de résoudre les multiples problèmes de la barrière sonique. Passer du vol transsonique au vol à Mach 2 dans la décennie suivante a nécessité un effort également considérable.

On remarquera, en outre, que les concepteurs de l'époque n'étaient même pas sûrs de l'existence d'une solution pour le programme Concorde. Il s'agissait, en effet, de concevoir un avion de transport d'une centaine de passagers, d'une durée de vie de l'ordre de trente mille heures, volant à Mach 2 pendant deux heures et demi à chaque étape, alors que l'on ne disposait que de l'expérience des avions militaires (durée de vie de l'ordre de cinq mille heures) ne restant en supersonique que quelques dizaines de minutes à chaque vol. Cette remarque prend toute sa valeur lorsque l'on sait que les Américains, à la même époque, ont échoué dans leur tentative de réalisation d'un avion de transport Mach 3 : la technologie alors disponible ne permit pas de trouver une solution et cet abandon ne fut, en aucun cas, motivé par des raisons écologiques comme on a bien voulu nous le faire croire !

L'augmentation de la charge marchande, passer de 450 à 600 passagers par exemple, ce qui est le cas pour les concepteurs de l'Airbus A3XX, pose également des problèmes d'extrapolation délicats. Par exemple, l'augmentation de la taille de l'avion conduit à des modes de vibrations de la structure du fuselage et des ailes qui doivent être amortis avec des moyens différents de ceux utilisés pour des avions plus petits et donc plus « raides ».

Il arrive que l'on ait parfois de bonnes surprises en constatant une amélioration inattendue de la sécurité due à une extrapolation heureuse. On a ainsi pu constater que Concorde ne souffre pas du grave problème de corrosion que l'on rencontre sur tous les avions classiques et qui nécessite une surveillance constante de l'état interne des structures. La corrosion est due au dépôt d'eau provenant de la condensation dans les parties non directement accessibles des structures. Or, le vol en supersonique prolongé, chauffant la structure au voisinage de 100° C, la sèche à chaque vol suivant le processus utilisé dans les lave-vaisselle ! Personne n'avait pensé à cet effet au moment de la conception.

Là encore le retour d'expérience par l'étude des incidents divers observés en service permet de vérifier ou de modifier les hypothèses de départ et, par suite, d'améliorer la sécurité.

Ou le mieux est l'ennemi du bien

Il arrive aussi qu'un souci d'amélioration de la sécurité sur un point conduise une diminution imprévue de la sécurité dans un autre domaine. Un exemple, inventé pour l'occasion, mais analogue à certains rencontrés dans l'industrie, illustrera ce propos.

Une usine de production chimique fabrique, comme produit intermédiaire, de la thiotimoline. Personne ne connaît les effets de la thiotimoline sur les êtres vivants et les végétaux. Les quelques résultats partiels effectués semblent montrer que cette molécule a peu d'effet immédiat, mais un doute subsiste quant à sa nocivité à long terme. Et si elle venait à induire une augmentation de la fréquence des cancers dans les trente ans à venir ?

La sagesse conduit donc à essayer d'éliminer tout rejet de thiotimoline à l'extérieur en cours de fabrication. Les ingénieurs du bureau d'étude ont tôt fait de proposer un balayage des cuves à l'azote, avec récupération de l'azote dans des filtres et neutralisation des traces de thiotimoline. L'opération est coûteuse, mais la sécurité n'a pas de prix !

Deux ans après la mise service, ce dispositif donne toute satisfaction, aucune trace mesu-

rable de thiotimoline n'étant détectée dans l'environnement. Mais il conduit à la catastrophe. Deux compagnons chargés de l'entretien du circuit d'azote sont asphyxiés par anoxie en visitant une cuve d'azote mal ventilée.

On a remplacé le risque inchiffrable d'une fuite de thiotimoline par un risque connu d'asphyxie par l'azote. Chaque année on compte dans l'industrie plusieurs décès par asphyxie de ce type, ce qui peut sembler étonnant puisque l'atmosphère contient quatre cinquièmes d'azote *a priori* non toxique. Or, si un opérateur tombe dans une cuve pleine d'eau, il s'abstient de respirer et peut ainsi résister plusieurs minutes avant l'asphyxie. Un opérateur qui pénètre dans une enceinte remplie d'azote n'en est pas conscient et, en deux à trois inspirations, il se trouve « vidé » de toute sa réserve corporelle d'oxygène (problème de pressions partielles d'oxygène et d'azote au niveau des poumons) et périt dans les dix secondes.

En conclusion

Il existe dans tous les secteurs une panoplie de moyens qui permettent de concevoir un nouveau produit en minimisant les risques d'erreurs, mais sans toutefois les éliminer. Ces méthodes de conception sont complétées par une analyse des risques possibles accompagnée d'une estimation de leur probabilité. Cette analyse permet ainsi d'identifier les situations ou les systèmes critiques et de trouver en connaissance de cause des remèdes améliorant la sécurité.

On peut ainsi, avant la mise en service, assurer un niveau raisonnable de sécurité. Mais on fait souvent remarquer que l'analyse de sécurité repose sur des hypothèses de fiabilité qui peuvent ne pas être suffisamment bien étayées. Ces hypothèses résultent de l'expérience antérieure, d'essais aussi représentatifs que possible, de simulations et de calculs. Mais elles peuvent se révéler erronées.

C'est pourquoi il ne faut pas se contenter de cette analyse préliminaire. Une étude de sécurité n'a de sens que si elle se poursuit pendant toute la vie opérationnelle du système avec un suivi des incidents ; c'est l'un des rôles du **retour d'expérience** de détecter les erreurs d'estimation des probabilités. Si, en service, on constate que la fiabilité d'un système est bien inférieure à la fiabilité estimée, il est possible, par analyse des raisons de cette perte de fiabilité, de trouver des remèdes et ainsi de rétablir la fiabilité, nécessaire, sans attendre qu'une catastrophe ne vienne mettre ce défaut en évidence.

Assurer la sécurité ce n'est pas éviter tous les incidents mais les rendre suffisamment improbables pour qu'ils ne dégénèrent en accident qu'avec une probabilité raisonnablement faible. Ce n'est pas attendre de connaître en détails tous les risques « possibles », « plausibles », « faiblement probables » et leurs conséquences, avant de concevoir ou de mettre en service un nouveau système, ce qui reviendrait à s'abstenir soigneusement et « précautionneusement ». Ce n'est pas s'abstenir de toute nouvelle initiative en attendant d'avoir établi la liste exhaustive de tous les risques « probables », « possibles » et même « plausibles » et vérifié que leurs conséquences sont nulles, ce que sous-entend le principe de précaution sujet des débats de ce colloque.

Assurer la sécurité c'est utiliser des procédures éprouvées de conception, analyser soigneusement les risques et bâtir un système de retour d'expérience afin de réagir avant la catastrophe.