Appel d'offres DGAC N° 96/01

Lot N° 7:

Développement d'une méthodologie d'analyse des incidents opérationnels

RAPPORT FINAL

Auteurs:
J. Paries & A. Merritt, Dédale
M. Schmidlin, Airbus Industrie

Responsables:
J. Paries, Dédale
J. J. Speyer, Airbus Industrie

SOMMAIRE

1. Introduction

L'aviation commerciale est un secteur où le niveau de sécurité est très élevé. Le taux d'accidents par rapport au nombre de vols est de l'ordre de 10^{-6}. À un tel degré de sécurité, il devient difficile d'apporter des améliorations au système et pourtant elles sont indispensables, en particulier en raison du développement croissant de ce secteur. Les solutions uniquement basées sur la réaction (design-fly-crash-fix) ne sont plus de mise. Il est désormais nécessaire de mettre en œuvre des solutions non intuitives et proactives afin d'améliorer encore la sécurité. L'enjeu est alors de détecter les défaillances intégrées au système avant qu'elles ne causent des dommages. Les systèmes de compte-rendu et d'analyse des incidents opérationnels - *Operational Incident Reporting and Analysis Systems* (OIRAS) sont de plus en plus considérés comme des instruments clés, et leur importance s'est confirmée au fil des ans. Le Comité Icarus de la *Flight Safety Foundation* a déclaré : "un programme interne de compte-rendu d'incidents correctement géré peut faciliter la détection de nombreuses défaillances. Grâce à la collecte d'informations, à la confrontation puis à l'analyse des comptes-rendus d'incidents, les responsables de la sécurité peuvent mieux comprendre les problèmes spécifiques rencontrés lors des opérations des compagnies aériennes. Cette connaissance leur permet de trouver des solutions de base au lieu d'apporter des corrections au coup par coup qui occultent les véritables problèmes." (*Icarus Committee*, 1998).

A priori, il semble logique de se servir des rapports d'incidents pour la prévention des accidents. En effet, les incidents sont souvent des embryons d'accidents et la répétition d'incidents similaires traduit généralement un risque d'accident. L'analyse des incidents pourrait donc théoriquement permettre de déceler des signes précurseurs d'accidents. Les analyses d'incidents ont fait naître des espérances et des convictions, qui ont été renforcées par l'utilisation de puissantes bases de données informatiques. La magie des grands nombres associée aux immenses capacités de stockage informatique donne d'autant plus l'illusion que la détection des défaillances dans le système de l'aviation peut être spontanée. On pense qu' "il suffit d'alimenter la base de données et l'ordinateur identifiera les problèmes".

Malheureusement, bien que de nombreuses bases de données soient alimentées de toute part dans le monde de l'aviation, les ordinateurs restent silencieux –ils ne peuvent localiser les problèmes à eux seuls. Reconnaissant la nécessité d'une meilleure compréhension des informations que les incidents peuvent fournir et de la façon de les traiter, la Direction Générale de l'Aviation Civile (DGAC) a lancé un appel d'offre pour une étude de recherche visant à développer une méthodologie pour les systèmes de compte-rendu et d'analyse d'incidents (OIRAS). Le présent document présente les conclusions de cette recherche. Il ne tente pas de décrire en détail un nouveau système de compte-rendu d'incidents, mais présente et justifie une approche différente grâce à *une série de concepts* à mettre en œuvre en matière de compte-rendu et d'analyse d'incidents.

Dans ce rapport, nous traiterons différents aspects des comptes-rendus et analyses d'incidents. Tous ces aspects seront directement ou indirectement liés à la même question: comment tirer des enseignements du ou des événements ? Une métaphore nous permettra de mieux comprendre le problème. L'utilisation des incidents pour prévoir puis prévenir les accidents est comparable à la chasse à l'or. Les événements ne sont pas tous pertinents. Il faut tamiser le sable puis le rincer et filtrer des tonnes de boue avant de trouver un peu de poussière d'or. Il est rare de trouver une pépite. Dans ce cas, le problème n'est pas tant la taille du tamis que la capacité à distinguer une vraie paillette d'or d'une fausse ou du gravier. La plupart des efforts déployés pour améliorer les comptes-rendus d'incidents ont permis d'augmenter la taille des tamis et le nombre de chercheurs d'or mais se sont peu intéressés à la capacité de différenciation. Sous prétexte qu'on ne sait pas vraiment ce que l'on cherche jusqu'à ce qu'on le trouve, il

existe actuellement une mentalité de ruée vers l'or – les systèmes de compte-rendu d'incidents sont devenus des "fourre-tout" non structurés.

L'efficacité de l'OIRAS repose sur des orientations et une structure claire. Actuellement, les chercheurs d'or travaillent tous sur le même terrain et avec les mêmes outils, avec une approche opportuniste. Il n'est donc pas étonnant qu'ils aient tendance à chercher (et ignorer) tous la même chose. Mais, un chercheur d'or a parfois de la chance. Des chercheurs expérimentés en matière d'accidents ou d'incidents ont la capacité impressionnante de se souvenir de l'événement similaire, de reconnaître des caractéristiques significatives ou de deviner la prochaine application de la loi de Murphy. Il existe sans nul doute un don particulier pour ce type de découvertes propres à la mémoire humaine. Mais il s'agit d'une qualité de l'intelligence humaine et non d'un résultat issu d'une base de données (comme certains l'avaient imaginé). Un des défis de tout OIRAS est de conserver ou d'adapter cette prédisposition lorsque la masse de données dépasse la capacité mémoire de l'homme.

Nous ne prétendons pas avoir découvert des outils magiques pour le traitement des bases de données. La question n'est pas de savoir comment introduire l'intelligence humaine dans une base de données, ou comment créer une base de données intelligente. Nous ne tentons pas de révolutionner les capacités de traitement des données. Notre approche consiste à utiliser la base de données de façon différente. L'approche traditionnelle est "outside-in": l'analyse des incidents est habituellement considérée comme une façon d'identifier et de résoudre les problèmes, en se référant aux modèles de risques basés sur une logique de "structuration" (ingénierie et conception de l'avion). Les organisations sont assimilées à des bureaucraties, dirigées par des principes standardisés et donc prévisibles.

De plus, la plupart des OIRAS résultent d'une adaptation des modèles d'enquêtes sur les accidents (*accident investigation* - AI) qui sont de par leur nature des solutions réactives. Ces modèles considèrent qu'un événement doit faire l'objet d'une enquête détaillée afin d'en établir précisément les causes avant de pouvoir en tirer des enseignements en matière de sécurité. Il est plus important de trouver les causes que de tirer des leçons (bien que ces deux aspects se chevauchent). Pour revenir à notre métaphore de chasse à l'or, les "chercheurs d'accidents", ayant écho de la découverte d'or, commencent à creuser la montagne pierre par pierre, convaincus que le travail effectué sur cette montagne leur permettra de trouver de l'or plus rapidement dans *d'autres* montagnes.

Le traitement des incidents et des quasi-incidents opérationnels ressemblent plus à la découverte de paillettes d'or ou de simili or. Ils sont plus fréquents que les accidents et ne peuvent faire l'objet d'une enquête aussi détaillée que les accidents pour des raisons uniquement logistiques. Mais cette adaptation du modèle d'enquête au système OIRAS a encouragé les analystes à se tourner vers le passé plutôt que vers l'avenir, et de ce fait à donner trop d'importance aux détails et aux facteurs causals. Mais avons-nous besoin de connaître précisément la séquence linéaire des facteurs causals de chaque incident pour en tirer des enseignements de sécurité ? La principale différence entre les accidents et les incidents réside dans les facteurs de détection, de protection et de récupération qui permettent qu'un incident ne se transforme pas en accident. Ces facteurs doivent prendre une place plus importante dans les OIRAS afin d'augmenter les connaissances acquises grâce aux modèles d'enquête sur les accidents. Nous devons également veiller à l'efficacité des mesures prises à partir d'un OIRAS, afin d'évaluer si ces comptes-rendus permettent réellement à une organisation de "tirer des enseignements".

En résumé, la plupart des systèmes OIRAS existants sont issus de protocoles d'enquête sur les accidents et ont été relativement efficaces en tant que stratégie réactive de sécurité afin de corriger des défaillances identifiées telles qu'elles sont perçues par les modèles de sécurité actuels. Mais l'intérêt de ces systèmes en tant qu'outils proactifs permettant aux organisations de tirer des enseignements nouveaux et plus approfondis nous paraît discutable. De même, il nous semble peu probable que l'application des systèmes OIRAS puisse améliorer les niveaux de sécurité actuels. Notre approche reconnaît que le système OIRAS peut fournir des informations essentielles pour une organisation en matière de sensibilisation aux risques et de processus de gestion des risques. Nous pensons qu'une base de données

OIRAS est efficace lorsqu'elle permet d'expliquer et de contester les présomptions de sécurité en vigueur dans une organisation. Enfin, le succès de tout système OIRAS devrait être évalué en fonction du succès des mesures proposées.

2. Les limites des systèmes OIRAS

Dans la première partie de ce projet, huit systèmes de comptes-rendus opérationnels ont été examinés :

- BASIS, British Airways Safety Information System
- ICAO ADREP, Accident/Incident Data Reporting System
- ECC-AIRS, pilot study on feasibility of EC reporting system
- MORS, Mandatory Occurrence Reporting System, CAA, UK
- OASIS et SIAM, Bureau of Air Safety Investigation, Australia
- CHIRP, Confidential Human Factors Incident Reporting Program, UK
- ASRS, Aviation Safety Reporting System, US-NASA
- EUCARE

Nous avons constaté que ces systèmes étaient différents sur plusieurs points :

- objectifs du système
- définition de l'expression "événement pertinent"
- degré de sophistication du modèle de sécurité
- confidentialité
- format du compte-rendu
- systèmes de codage et d'analyse
- retour et transfert des informations

Dans le chapitre suivant, nous résumerons les limites et les contraintes que présentent les systèmes opérationnels de compte-rendu et d'analyse d'incident actuels (OIRAS).

2.1 Le rapporteur

Dans le secteur de l'aviation, nous comptons sur les opérateurs directs pour rapporter les événements pertinents. Les acteurs d'un événement sont donc simultanément des observateurs et des rapporteurs de leur propre expérience. Cela implique inévitablement un biais, notamment en matière d'incidents opérationnels où le comportement est un élément clé :

- La perception d'un événement est subjective. Elle est conditionnée, influencée et limitée par les intentions de l'acteur et sa conscience de la situation.
- "Chacun est le héros de sa propre histoire" – comme le montrent les descriptions d'événements et l'attribution des causes.
- La perception des risques, élément sous-jacent de la plupart des rapports, reste extrêmement subjective. Si aucun risque n'est perçu, il n'y a généralement pas de compte-rendu.
- L'opérateur décide du contenu de son compte-rendu. Les révélations volontaires d'une personne constituent une violation du droit de non divulgation d'une autre personne.
- La perception d'un rapporteur est locale, limitée dans le temps et dans l'espace, alors que la plupart des événements impliquent une causalité systématique plus étendue.
- Les événements les plus importants peuvent ne pas faire l'objet d'un rapport en raison d'un refoulement, de l'ignorance des conséquences de sécurité, de la volonté d'éluder le problème ou par crainte de représailles (malgré les garanties existantes en la matière).

Le premier obstacle pour une bonne exploitation est donc le fait que les acteurs/rapporteurs fournissent un sous-ensemble biaisé et incomplet d'événements potentiellement pertinents.

2.2 Le formulaire de compte-rendu

Les formulaires de compte-rendu constituent un deuxième obstacle car ils sont également sujets aux biais.

- Un formulaire de compte-rendu doit être suffisamment succinct et accessible pour inciter les opérateurs à l'utiliser. De ce fait, le nombre de questions est très limité.
- L'utilisation de questions entièrement ouvertes (récit) peut nuire à l'obtention d'informations utiles.
- Les questions peuvent orienter le rapporteur, mais elles peuvent également déformer sa perception des faits, entraînant le rapporteur sur des conclusions biaisées.
- Le modèle de sécurité implicite utilisé pour l'OIRAS détermine le choix des questions du formulaire de compte-rendu.
- L'éventail des événements possibles est tellement large qu'un formulaire standard ne peut recueillir toutes les informations. L'analyste doit donc souvent contacter le rapporteur pour obtenir des informations spécifiques.

En résumé, un formulaire de compte-rendu comportant uniquement des questions ouvertes ne parviendra pas à recueillir des informations de qualité ; un formulaire de compte-rendu avec des questions trop nombreuses ne sera pas complété, et un formulaire de compte-rendu basé sur le modèle de sécurité implicite de l'analyste contraint et donc influence le rapporteur en lui insufflant inconsciemment la vision de l'analyste.

2.3 Bases de données

Les bases de données constituent une troisième source d'influence involontaire dans les OIRAS.

On utilise les bases de données afin de stocker des informations pour différentes raisons :

- car elles seront *nécessaires* plus tard (recherche totale)
- car une *partie des informations sera nécessaire* plus tard (recherche partielle)
- car *une partie* de ces informations *pourrait s'avérer utile* à l'avenir (police d'assurance)
- pour élaborer un historique des événements passés (recréer le passé)
- pour justifier la continuité d'un programme (la quantité implique la qualité)
- parce qu'il est possible de les archiver (capacités informatiques).

Les bases de données OIRAS actuelles ont été créées pour toutes ces raisons. Pourtant, la collecte et la classification à outrance de données relatives aux incidents et quasi-incidents et à leurs causes impliquent une quantité de ressources très importante ('resource heavy') même pour les organisations directement intéressées.

Beaucoup d'organisations ont rencontré des problèmes avec les bases de données OIRAS :

- Les informations stockées en vue d'une recherche ultérieure doivent être classées en différentes catégories.
- Cela ne pose pas de problème par rapport aux paramètres physiques objectifs du vol, mais par rapport à la description plus subjective de l'événement et à l'attribution des causes.
- Comme pour le formulaire de compte-rendu, il est impossible de prévoir toutes les possibilités et donc de créer une liste exhaustive de mots-clés.

- De plus, les mots-clés sont statiques, binaires (présents ou non) et ne peuvent être reliés que de façon linéaire. Il s'agit donc d'une ébauche très simplifiée du monde réel.
- Les informations sont recherchées en fonction de leur mode de saisie. La classification issue du modèle de sécurité de l'analyste détermine donc les paramètres de sortie. Par exemple, si aucun mot-clé ne désigne la "défaillance technique" dans la base de données, cette "défaillance technique" ne sera jamais considérée comme une cause d'incident dans cette base.
- Un modèle de sécurité, explicite ou implicite, qui influence la classification devient une prophétie auto-validée. A partir des données présentes, on ne peut extraire et confirmer (dans la mesure du possible en fonction des contraintes précédemment citées) que des informations déjà connues. Par exemple, la plupart des OIRAS influencent la classification par mot-clé en faveur du CRM. De ce fait, le CRM constitue souvent à la fois la cause du problème et sa solution (plus de formation CRM permettra de corriger les défaillances de CRM perçues).
- Ce raisonnement en boucle ne permet d'apprendre que ce que l'on sait déjà.
- La plupart des informations saisies dans les bases de données ne seront jamais consultées.
- Si la recherche à partir d'un mot-clé aboutit sur un cas, l'analyste doit généralement se référer au compte-rendu initial pour comprendre tous les détails dans le contexte (en raison de l'utilisation de mots-clés inadaptés).
- Lorsque la base de données s'accroît au-delà de la mémoire de l'analyste, elle devient un dépôt et ne représente pas la mémoire de l'analyste – le matériel est "oublié".
- La structure prédéfinie basée sur les mots-clés est une source d'erreur. Les comptes-rendus sont analysés de façon à "s'adapter" aux mots-clés. Les détails qui ne correspondent pas ne sont pas pris en compte. En conséquence, les informations ignorées le restent et la base perd de sa crédibilité.

De nombreux efforts ont été déployés pour la création et la gestion de bases de données, mais peu ont été consentis à l'enregistrement et au suivi des réponses apportées par une organisation en matière de sécurité. Une base de données qui assurerait le suivi et l'évaluation de l'efficacité des réponses de l'organisation en matière d'incidents, et proposerait une meta-analyse avec un aperçu global du système de sécurité aurait deux avantages:

- Elle permettrait au système de se concentrer sur les stratégies de perfectionnement et de distinguer les stratégies efficaces. En effet, l'utilisation répétée d'une même stratégie implique que cette stratégie ne permet pas d'améliorer le système.

- La base de données permettrait également d'expliciter les modèles de sécurité sous-jacents utilisés dans l'organisation. Par exemple, l'utilisation répétée d'une stratégie basée sur "plus de formation" montrerait que l'organisation repose trop sur la formation.

2.4 Analyse des données

Il existe actuellement deux types d'analyse des données. Lorsqu'un nouveau compte-rendu est transmis, il est intégré à une base de données (bien que ce processus engendre une quantité de ressources trop importante, l'industrie a adopté cette norme incontestée qui consiste à intégrer chaque compte-rendu dans une base de données). Les rapporteurs reçoivent une notification confirmant la réception de leur compte-rendu. Puis l'analyste décide des mesures à prendre et les initie. Il agit généralement en fonction de sa perception des risques que l'incident présente pour l'organisation. S'il considère que l'incident est suffisamment grave, il utilisera les ressources pour comprendre l'événement en détail. Il s'agit d'une approche objective. Selon la nature de l'événement, les membres de l'organisation impliqués dans le processus de résolution du problème sont différents. En substance, l'approche objective, basée sur l'étude de cas, correspond à une mini-enquête d'accident.

Le second type d'analyse – analyse de tendance de la base de données – n'a pas tenu toutes ses promesses.

2.4.1 Analyse de tendance

Les paramètres physiques objectifs d'un vol présentent l'avantage d'être facilement collectés et difficiles à contester. Ils peuvent être utilisés efficacement pour suivre des schémas. On peut retrouver ces informations dans la plupart des OIRAS. Par contre, les données objectives relatives aux "déviations" n'apparaissent pas dans les OIRAS mais dans les FOQA ou autres systèmes de collecte de données de vol. (Il faut rappeler qu'un OIRAS ne contient qu'un sous-ensemble biaisé d'événements pertinents).

Les tentatives visant à obtenir une analyse de tendance significative à partir des paramètres plus subjectifs des bases de données OIRAS ont été peu concluantes pour diverses raisons :

- Il est difficile de compresser des données brutes en informations structurées sans perdre des informations essentielles (en particulier si on ne peut déterminer quels éléments sont pertinents qu'à posteriori).
- Les limites de la classification par mots-clés (pour tenir compte entièrement du contexte).
- Les limites des bases de données (les événements pertinents ne sont pas tous rapportés, ou ne sont pas rapportés en détail).
- L'incapacité à prévoir les paramètres qui s'avéreront importants, ce qui implique parfois un révision onéreuse de la base de données.
- Les conclusions des analystes sont différentes à cause de:
    - modèles de sécurité implicites différents
    - d'une formation insuffisante en matière de procédure d'analyse
    - de la nature subjective de l'attribution des causes faite par les rapporteurs et les analystes
    - de l'étendue des causes possibles dans les systèmes complexes

Ces problèmes logistiques sont considérablement accentués lorsque les données de différentes bases sont combinées, comme c'est le cas pour les autorités ou un avionneur. La plupart des compagnies aériennes emploient des analystes qui connaissent le contexte (par exemple, un commandant de 747 analysera les comptes-rendus rédigés pour la flotte de 747). Cette compréhension contextuelle d'un problème n'existe plus lorsque les données sont réunies. De ce fait l'analyse de tendance devient discutable lorsque les données subjectives de différentes sources sont combinées. Plus les données sont objectives, plus l'analyse de tendance est plausible. Malheureusement, les systèmes OIRAS sont subjectifs par nature.

Outre les contraintes d'ordre logistique, le principal obstacle à l'analyse de tendance est le manque de questions intelligentes posées dans les bases de données. Les résultats des bases de données sont généralement des synthèses statistiques de différentes combinaisons de mots-clés. L'analyste doit interpréter ces données et poser des questions plus complexes. Cette étape peut s'avérer difficile si l'analyste n'est pas conscient de son propre modèle de sécurité et des présomptions qu'il implique, ou s'il en est conscient mais n'est pas disposé à tester ces présomptions. Ce problème s'accentue pour les analyses de tendance des facteurs causals car l'attribution des causes découle directement du modèle de sécurité utilisé par l'analyste. ("J'ai retrouvé les causes telles que je les avaient entrées" – la base de données ne fait que refléter la pensée de l'analyste).

Autre facteur justifiant le manque d'analyses de tendance significatives : en raison de la nature inévitablement imparfaite des bases de données OIRAS, les analystes préfèrent développer des hypothèses basées sur une approche objective d'étude de cas puis tester le système de façon précise et proactive (directement, en temps réel) plutôt que de se fier à la base de données (réactive et incomplète). Par exemple: après avoir détecté un problème particulier, le Département de Sécurité décide de mener une enquête auprès des pilotes sur ce problème donné afin de déterminer plus précisément la fréquence réelle de cet événement et les risques correspondants dans le système.

Ainsi, l'analyse de tendance n'a pas été concluante pour les systèmes OIRAS. Cette constatation doit

également soulever la question de l'utilité réelle des bases de données OIRAS.

2.5 Apprenons-nous quelque chose ?

Outre les problèmes logistiques liés à l'archivage et à la recherche de données subjectives dans une base de données, le véritable défi posé par le système OIRAS est de remettre en question notre raisonnement sur la sécurité du système et d'apprendre quelque chose de nouveau.

Les systèmes OIRAS présentent différents défis :

- Il faut pouvoir être véritablement "surpris" par les données, c'est-à-dire percevoir les données de façon à remettre en question nos propres idées sur la sécurité.
- L'intuition - être capable de "distinguer" des événements ou des profils pertinents non reconnus jusqu'à présent
- ‘généraliser’ la compréhension d'un événement isolé pour parvenir à une compréhension des faiblesses ou échecs génériques dans les défenses du système.
- Comprendre les interconnexions complexes du système en étudiant des événements isolés (voir la forêt *et* les arbres)
- Développer des hypothèses à partir des comptes-rendus qui peuvent être testées à partir de la base de données existante ou grâce à un test proactif du système.
- Forger une crédibilité aux enseignements tirés concernant les faiblesses du système en matière de sécurité
- S'apercevoir si une stratégie de sécurité a été sur-optimisée ou n'est plus efficace
- S'apercevoir si la solution d'un problème peut créer un autre problème dans le système (comme nous l'avons vu avec des exemples d'automatisation).

Les systèmes OIRAS ne sont efficaces que dans la mesure où ils permettent de tester (de confirmer ou de réfuter) des hypothèses existantes souvent par l'intermédiaire de modèles de sécurité implicites. Il existe des limites à la qualité et à la gestion des données, en particulier pour les données subjectives. De plus, les ressources nécessaires pour administrer ces systèmes contenant beaucoup de données, et pour dialoguer intelligemment avec eux, sont chères. Beaucoup de données présentes dans les OIRAS ne sont pas utilisées (jamais extraites de la base de données) et les enseignements tirés par l'organisation sont réactifs et/ou diminués. Dans un système de sécurité complexe utilisant différents instruments, le système OIRAS actuel doit considérablement évoluer pour assurer sa pérennité.

3. Un OIRAS amélioré: considérations fonctionnelles et théoriques

3.1 Fonctions d'un OIRAS

3.1.1 Tirer des "enseignements de sécurité"

Un OIRAS peut remplir des fonctions très différentes. La première fonction évidente est certainement de tirer une "leçon de sécurité" explicite d'une ou de plusieurs occurrences. En d'autres termes, l'analyse d'incidents est ici considérée comme une façon d'identifier et de résoudre les problèmes de sécurité.

On peut tirer des enseignements de sécurité à partir de :

- un ou plusieurs incidents similaires car ils peuvent être considérés comme *précurseurs* d'un accident, ce qui signifie qu'ils correspondent clairement à une séquence incomplète d'un scénario accidentel connu.
- un ou plusieurs incidents similaires car ils indiquent la possibilité d'un événement ou d'une situation qui était dissimulée dans l'analyse de sécurité du système ou indiquent clairement qu'une *hypothèse importante sur la sécurité du système est remise en question*. Dans ce cas, comme dans le cas précédent, l'approche la plus efficace et celle de l'analyse "objective" du ou des événements, analogue à l'enquête sur un accident
- un grand nombre d'incidents mineurs, car l'analyse de cet échantillon peut révéler des profils d'insécurité spécifiques d'événements ou de circonstances, permettre de comprendre que certaines fréquences d'événements réelles ne sont pas compatibles avec les hypothèses de sécurité ou détecter des tendances dangereuses. Il s'agit dans ce cas d'une approche épidémiologique: on obtient des indications à partir des grands nombres.
- un grand nombre d'incidents mineurs, car l'analyse de cet échantillon permet de découvrir le rapport entre ces événements et les paramètres relatifs à l'environnement, la procédure ou la situation, suggérant ainsi qu'il peut exister un "lien de causalité" entre ces événements et ces paramètres.

3.1.2 Autres fonctions

L'utilité de l'OIRAS ne se limite pas aux *enseignements de sécurité explicites* qui peuvent être utilisés par les personnes concernées (responsables de la sécurité, autorités, etc.).

Voici une liste non exhaustive des autres fonctions :

- *tenir les opérateurs informés.* Les données statistiques ou les informations anecdotiques ("cela est arrivé à vos collègues") qui sont transmises aux opérateurs en retour peuvent encourager des changements de comportement sans aucune modification structurelle dans le système (formation, modification de procédure ou autre). Dans une compagnie aérienne, le simple fait d'informer les pilotes que selon les résultats du programme FOQA, la plupart d'entre eux faisaient trop pivoter un certain type d'avion a spontanément permis de corriger le problème.
- *faire apparaître plus clairement les dangers.* La sécurité ne peut se fonder uniquement sur une adhésion aveugle aux procédures. Les hommes appliquent en général une procédure de façon plus efficace s'ils estiment que cette procédure les aidera ou les protégera. Il est donc nécessaire que des craintes subsistent dans le système. Mais des systèmes comme l'aviation atteignent un tel degré de sécurité que l'expérience du danger est extrêmement éloignée d'une perspective individuelle. Le risque est en dessous des seuils de perception individuels. Le fait de partager

l'expérience globale du système est la seule façon de maintenir quelques craintes dans le système.

- *montrer les moyens de protection.* Certains incidents correspondent non seulement à des séquences incomplètes de scénarios accidentels imprévus, mais révèlent également des protections imprévues qui par chance, les empêchent de se transformer en accidents. Il est donc important de tester et d'"institutionnaliser" les effets de la chance grâce à des formations spécifiques, une modification des procédures ou simplement en informant les opérateurs.
- *encourager les enquêtes supplémentaires.* Un incident peut indiquer qu'"il faut vérifier quelque chose de plus grave". En d'autres termes, un incident peut soulever des questions sur l'existence, la fréquence et la gravité des situations anormales dans le système, et donc susciter des enquêtes supplémentaires, qui peuvent être réalisées sous la forme d'une consultation de base de données, d'un questionnaire informel ou d'un audit à grande échelle.
- *enseignements pour l'organisation.* Les enquêtes sur les incidents peuvent contribuer à un enrichissement des connaissances de l'organisation à court terme ou à long terme si les employés sont directement impliqués dans le processus, au lieu d'être simplement informés des conclusions. Il est souvent nécessaire de réunir différentes sources de connaissances sur le système pour qu'une analyse d'incident soit efficace. Les employés impliqués peuvent alors développer et compléter leur compréhension des questions liées à l'équipement et à l'exploitation, développer leurs compétences d'analyse et d'imagination, découvrir d'autres questions, se rendre compte de leurs propres limites de compréhension, partager leur expérience et comprendre les interactions complexes entre les activités spécialisées. Ils peuvent développer une compréhension collective des possibilités d'amélioration.

3.2 Bases théoriques de l'OIRAS

3.2.1 Définition d'un incident

L'annexe 13 de la Convention de Chicago de l'OACI définit un incident comme un événement, autre qu'un accident, lié à l'utilisation d'un aéronef, qui compromet, ou pourrait compromettre la sécurité de l'exploitation. Cette convention définit un incident grave comme un incident dont les circonstances indiquent qu'un accident a failli se produire et établit que la différence entre un accident et un incident grave ne réside que dans le dénouement. En effet, l'annexe 13 définit un accident comme un événement lié à l'utilisation d'un aéronef, pendant lequel un dommage (à une personne ou à l'aéronef) plus grave qu'un seuil donné s'est produit ou pendant lequel l'aéronef a disparu.

Le concept d'"incident" a donc deux limites principales :

- La première permet de distinguer les "incidents" des "accidents" : elle est basée sur le niveau de dommage subi pendant l'événement. Il existe un seuil de dommage en dessous duquel une situation sera considérée comme un "incident" et au dessus duquel elle sera considérée comme un "accident".
- La seconde distingue les "incidents" et les "événements normaux" : elle est basée sur la menace à la sécurité "apparue" lors de l'événement. Cette limite est beaucoup plus difficile à déterminer. Elle est liée à notre perception de ce qui rend un système sûr ou non, et également au degré de sécurité qu'on attend du système.

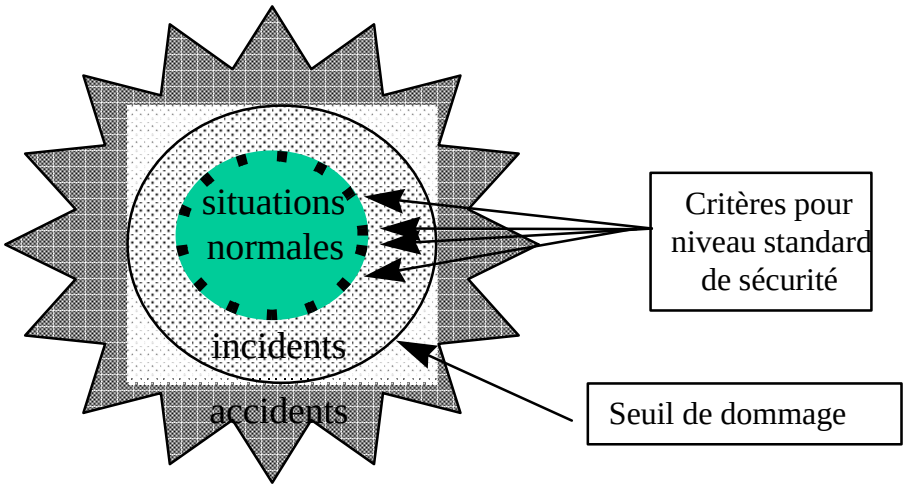
La signification de l'expression "compromettre la sécurité" dans la définition de l'OACI reste floue. La définition est cependant complétée dans l'annexe 13 par une référence à une liste explicite des types d'incidents présentant un intérêt particulier pour la prévention des accidents. Cette liste ne prétend pas être exhaustive. La décision de considérer un événement particulier comme un incident est donc en partie laissée au jugement de l'expert (rapporteur ou analyste). ***Est-il possible d'aider cette prise de décision grâce à une interprétation plus précise de "compromettre la sécurité" ?***

Une première approche est de considérer que la sécurité est compromise lorsque la probabilité qu'un accident se produise a connu une augmentation non acceptable par rapport au niveau "nominal". Cette

approche serait rationnelle. Malheureusement, cette probabilité ne peut être estimée, sauf pour des incidents graves, tels que définis précédemment, c'est-à-dire pour des quasi-accidents. De plus la probabilité "nominale" d'accident est difficile à déterminer étant donné qu'elle varie en fonction de différents paramètres, tels que le profil du vol, la phase de vol, les conditions climatiques, la densité du trafic, l'état de fatigue de l'équipage et autres.

La deuxième approche pourrait consister, comme le montre la figure ci-dessous, à considérer que la sécurité est menacée dans tout événement lorsqu'au moins un des critères "objectifs" acceptés par le système comme indicateur (ou comme condition) d'un niveau standard de sécurité n'est pas respecté. Ces critères comprennent généralement :

- les marges de sécurité : par exemple. X NM ou Y pieds de distance entre deux avions ; X pieds au dessus des obstacles ;
- des limites aux domaines de vol "normaux" (vitesse, altitude, poids et équilibre, facteur de charge, etc.)
- disponibilité des protections critiques (par exemple ; avertisseur de décrochage, GPWS)
- équipement minimum (MEL)



Néanmoins, cette définition d'un incident (tout événement au cours duquel au moins un des critères "objectifs" acceptés par le système n'est pas respecté) serait soit très incomplète soit très limitée. Si nous considérons comme critères de sécurité, la disponibilité des marges ou les protections, elle sera incomplète car beaucoup de pertes de contrôle sont rétablies avant d'atteindre ces critères. Si d'autre part, le concept de critère de sécurité est étendu à tous les types de spécifications du système (procédures), la définition sera alors très réduite car elle visera à égaler la sécurité totale du système et l'absence de toute déviation

On peut distinguer principalement deux stratégies de sécurité – la sécurité par les spécifications et la sécurité par l'adaptation. Une recherche sur ces deux modèles peut permettre de donner une définition plus raisonnable de "compromettre la sécurité".

3.2.2 La sécurité par les spécifications

Une première stratégie pour concevoir la sécurité d'un système est de faire appel à des propriétés fonctionnelles invariables du monde (l'environnement) pour établir des réponses opérationnelles pertinentes. L'idéal est alors de concevoir et de donner des réponses parfaitement adaptées à la demande

imposée par la situation. Ces solutions sont généralement figées dans des organigrammes, spécifiées dans des documents sous la forme de règles et de procédures, stockées dans la mémoire à long terme de l'opérateur sous forme de connaissance des procédures (règles et compétences) et appliquées selon la situation.

Le principal problème est alors de pouvoir rester dans le cadre d'une situation connue, avec des solutions qui ont fait leurs preuves. Dans cette approche, la sécurité est compromise lorsque l'environnement varie (désadaptation), lorsque la technologie échoue ou lorsque la solution standard n'est pas employée (erreur ou violation).

Dans l'état optimal de ce modèle, l'exploitation nominale est l'absence de déviation. Le "processus de production d'une situation dangereuse" est le modèle d'incident traditionnel basé sur ce modèle de sécurité. Ce processus comprend évidemment tout d'abord les déviations non intentionnelles (erreurs) ou intentionnelles (violations) au fonctionnement opérationnel nominal, tel que spécifié dans les procédures, règles et autres.

La première stratégie de sécurité est donc la *prévention des déviations*, principalement par des moyens tels que la correction des conditions propices aux déviations, le développement d'une culture "professionnelle" respectueuse des procédures, ou la menace de sanctions pour les personnes fautives.

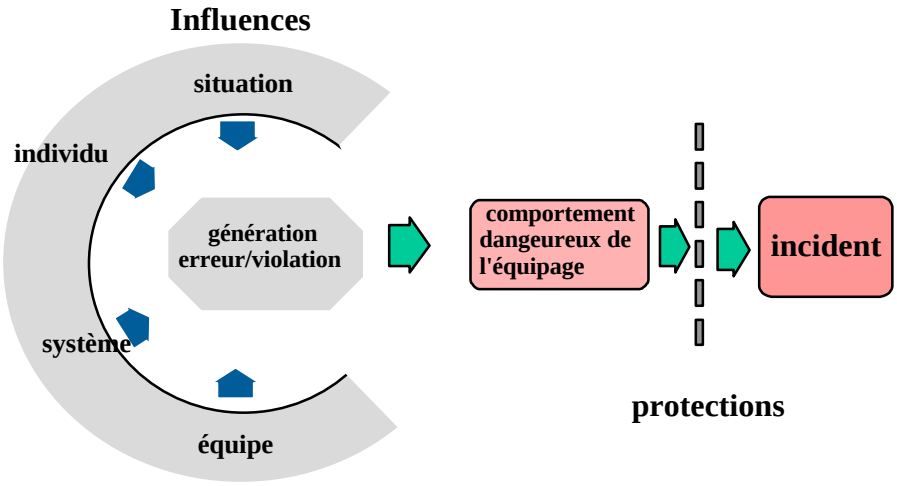
Néanmoins, il est désormais communément accepté qu'un "niveau de sécurité nominal" n'implique pas nécessairement l'absence de déviation par rapport au cours nominal des événements.
Les déviations ne constituent pas une exception car :

- le processus de production est rarement une séquence linéaire d'actions telle que décrite par la procédure. Il existe très fréquemment différents processus concurrentiels, qui entraînent des interruptions mutuelles, et nécessitent l'établissement de priorités ;
- les erreurs humaines sont inévitables ;
- l'équipement technique est rarement conforme aux valeurs nominales : des modifications aboutiront progressivement à des situations particulières pour un aéronef ou un équipement spécifique, la liste du matériel minimum autorisera des vols avec des équipements qui ont dépassé leur durée de vie nominale, des pannes se produiront pendant le vol, etc.
- des déviations volontaires peuvent également se produire, la plupart du temps, elles sont liées à l'établissement de priorités en raison des contraintes citées précédemment ;
- des événements non prévus et des contextes anormaux peuvent également survenir, pour lesquels aucune solution "standard" n'a été prévue à l'avance.

La seconde stratégie de sécurité est la *protection contre les déviations*.
En conséquence les modèles d'incidents qui servent de référence pour les systèmes OIRAS actuels, ont tous plus ou moins la même structure :

- un moteur de *production* d'erreurs (involontaires) ou de violations (volontaires). Le moteur est alimenté par des influences (facteurs contributifs/ déclenchant) au niveau de l'individu, de l'équipe, de la situation ou du système.
- les erreurs et/ou violations associées aux circonstances engendrent alors un comportement "dangereux" (unsafe) de l'opérateur.
- les protections conçues dans le système ou fournies par le comportement positif d'un opérateur humain, ou par la chance, évitent que le comportement potentiellement "dangereux" aboutisse sur un accident.

Ce modèle d'incident est représenté par le diagramme ci-dessous :



On peut affirmer que ces modèles de sécurité fonctionnelle et invariable et les efforts de prévention et de protection qui y sont associés ont contribué à l'établissement des seuils de sécurité actuels dans le domaine de l'aviation. Pourtant, ils ne parviennent pas à améliorer le système au delà du taux actuel (10^{-6}). Une conceptualisation plus réaliste de l'interaction homme-technologie est donc nécessaire. Considérons l'alternative suivante.

3.2.3 La sécurité par l'adaptation

Une seconde stratégie pour concevoir la sécurité d'un système se base sur une approche plus générique et plus souple. Elle est également plus réaliste en ce qui concerne le comportement humain. Elle considère un "système" comme une "écologie" plutôt que comme une machine. Une écologie est un ensemble stable d'inter-réactions entre les éléments du système et leur environnement. Une des questions clés est l'équilibre entre la stabilité et la capacité d'adaptation.

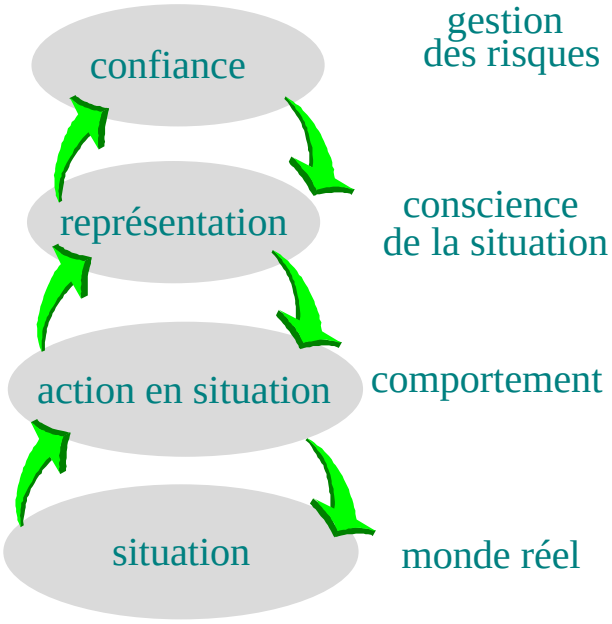
Une des principales différences entre ce modèle et le précédent est que dans ce cas, *les déviations* ne sont pas considérées comme des événements anormaux mais correspondent plutôt à la situation normale. Les hommes agissent dans le monde réel dans lequel ils évoluent (leur environnement) en fonction de leur représentation de ce monde réel. Les représentations ne correspondent jamais à la réalité: elles sont schématiques, déformées, anticipatoires (c'est-à-dire, en partie gérées par eux-mêmes et indépendantes des cycles de retour sensoriel). Les actions sont brutes, imparfaitement contrôlées, sujettes aux erreurs. Le retour sensoriel est un processus de filtrage très limité et orienté.

D'une perspective écologique, les erreurs et les déviations ne sont pas des défaillances, mais l'expression d'une capacité d'adaptation. Elles font partie de la variété nécessaire dans l'éventail des réponses disponibles pour faire face à la complexité de l'interaction avec l'environnement. Les réponses opérationnelles sont constamment imparfaites car elles doivent inclure des solutions latentes et ouvertes pour des situations différentes et imprévues. Elles sont également l'expression de la capacité de l'opérateur à tirer des enseignements de son expérience. De plus, elles fournissent un moyen de découvrir les limites (floues) d'un système, afin de les repérer et de les respecter.

Pour traiter cette incertitude, les opérateurs utilisent leur connaissance des procédures (règles et compétences) basée sur les propriétés fonctionnelles invariables du monde, ainsi que les connaissances déclaratives qui concernent des propriétés plus génériques et abstraites du monde, leur permettant de "comprendre" et d'anticiper lorsqu'il n'existe pas de règle disponible.

On peut assimiler ce processus de contrôle des déviations à l'immunologie - on crée et on développe des défenses en réponse à la reconnaissance d'agents pathogènes (paradigme identitaire), il est donc nécessaire que les agresseurs se développent. Le processus de gestion des déviations comprend un suivi des variations aléatoires ou imprévues, présentes à la fois à l'extérieur dans l'environnement et à l'intérieur dans les réponses opérationnelles (échecs, erreurs et déviations). Les déviations et les événements imprévus/aléatoires sont détectés par des cycles "vertueux". Les actions issues de déviations créent des représentations imprévues générant une évaluation des déviations et des risques, où la nature et l'intensité de la menace potentielle introduite par la déviation sont estimées. Il est important de comprendre que toutes les déviations ne sont pas à corriger. Certaines erreurs ou événements anormaux peuvent être ignorés sans risque. On ne corrigera la représentation et/ou on ne prendra des mesures correctives (atténuation des conséquences des déviations) que si l'évaluation des risques montre que cela est nécessaire.

Le processus de gestion des déviations comprend enfin un contrôle interne de l'efficacité du processus de suivi. Il constitue donc un système d'auto-référencement avec une stabilité de nature dynamique. Un mode stable est un point fixe dans un système d'auto-référencement. Il apparaît lorsque les réactions des opérateurs par rapport aux représentations créent une réalité cohérente avec ces représentations. Ces représentations mentales peuvent être influencées par la confiance, qui affecte à son tour et est affectée par la perception et la gestion des risques. (Je considère que cette situation est simple, familière et présente peu de risques car je suis confiant. Cette confiance se base sur mon expérience).



Il existe des points de bifurcation où les cercles vertueux se transforment soudain en cercles vicieux : les représentations erronées créent des actions erronées qui engendrent une réalité correspondant de moins en moins aux représentations, sans que ce changement ne soit perceptible.

Le premier aspect (souvent la première étape) est la perte de contrôle cognitif. La représentation n'est plus capable de créer des actions de contrôle adaptées en réaction aux *événements* de la situation. Mais le contrôle de la situation n'est pas perdu et la sécurité peut être maintenue si la représentation est encore capable de créer des actions appropriées pour diriger le système vers un *état* stable ou le maintenir dans cet état, en d'autres termes, si toutes ces caractéristiques dynamiques peuvent encore être contrôlées. Par exemple, le schéma mental de navigation peut être erroné, la conscience de la situation latérale peut être perdue, mais la perception de l'altitude de sécurité dans la zone peut être encore acceptable.

Le second aspect est la perte de contrôle de la situation. La représentation est alors tellement inadaptée qu'elle peut uniquement engendrer des actions non appropriées. Il y a une absence de schéma global et la dynamique du système n'est plus contrôlable.

En résumé, la sécurité par le modèle d'adaptation, basée sur le paradigme écologique de systèmes complexes d'auto-référencement, considère que les déviations sont inévitables mais pas inévitablement mauvaises.

3.2.4 Contrôle de la gestion des risques

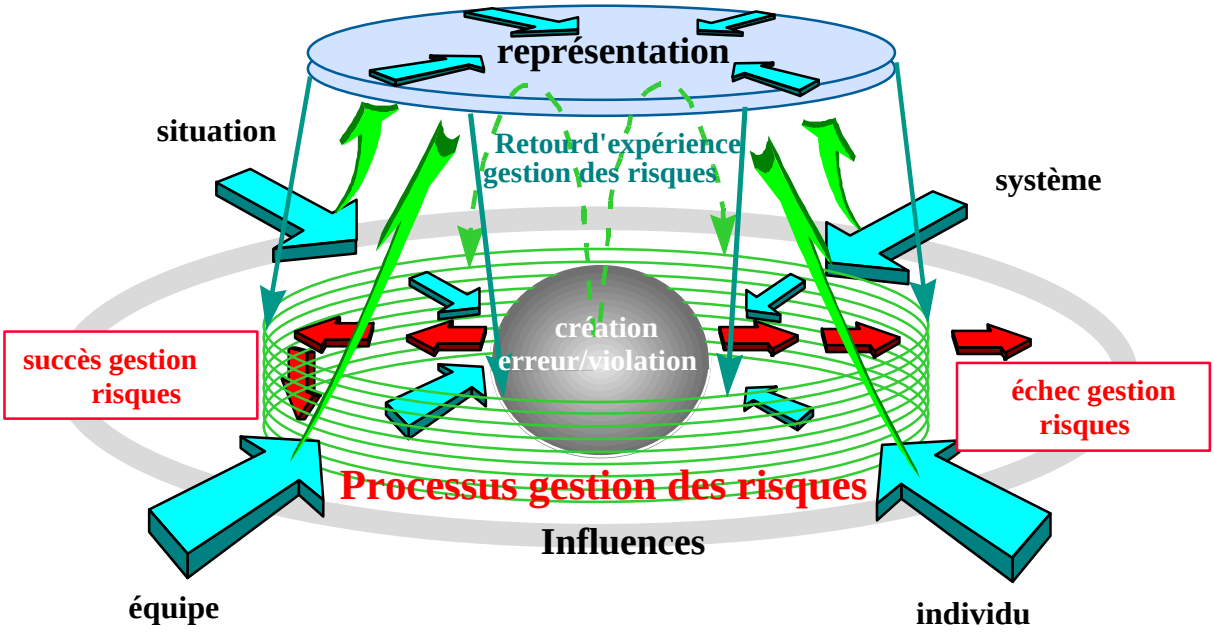
La sécurité de l'exploitation résulte enfin d'un processus permanent d'adaptation du contrôle des risques. Ce processus de gestion des risques repose **à la fois** sur :

- Une prescription normative (une partition musicale) qui décrit les situations potentielles (nominale, anormale, d'urgence), définit et planifie les actions pertinentes, désigne les rôles et la répartition des tâches et définit la coopération homme/ machine et homme/ homme ;

- une application dynamique, en temps réel de la prescription ci-dessus (l'interprétation intelligente de la partition musicale) qui comprend:
    - un processus permanent de gestion des déviations: contrôle, auto-contrôle, détection, établissement de priorités, correction des déviations (pas de toutes); anticipation et/ou reconnaissance des situations anormales (jusqu'à la situation d'urgence) et leur gestion
    - mais également un processus de meta-gestion: gestion des ressources, gestion externe et interne (compromis cognitif) des risques;

Outre les déviations, il faut s'attacher à la prévention de la perte de contrôle du processus de gestion des risques de la situation. De ce point de vue, on peut tirer des enseignements à la fois des échecs (y compris des incidents) et des succès dans la gestion des risques.

Le schéma suivant tente de représenter le rôle du processus de gestion des risques au niveau de l'opérateur direct. Le comportement individuel est sous l'influence de caractéristiques de l'individu (par exemple, manque d'attention), de l'équipe (direction autocratique), de la situation (par exemple, retard du vol) ou du système (formation inadéquate). Le processus de gestion des risques individuel détecte et évalue ces influences (avec des succès variables), et adapte le contrôle du comportement en conséquence. Les déviations – erreurs et violations – ne sont pas directement issues de ces influences, mais du processus individuel de gestion des risques qui dépend de l'évolution des représentations de ces influences. C'est le processus de gestion des risques qui contrôle la probabilité de commettre une erreur ainsi que la probabilité de la détecter. Les erreurs ou violations qui ne sont pas gérées de façon adéquate pénètrent les protections établies par le processus de gestion des risques et deviennent des échecs de gestion des risques. Ces échecs peuvent également être considérés comme des incidents. ***Un incident peut donc être défini comme un échec du processus de gestion des risques.***



3.3 Approches analytiques

En considérant que la gestion des risques fait partie d'un modèle d'incident, trois niveaux d'analyse sont possibles et nécessaires. Le premier est le ***récit*** ou "niveau descriptif". Il replace l'événement dans son contexte (les faits, les circonstances et les paramètres physiques de l'événement). Dans la mesure du possible, il s'agit d'une transposition du compte-rendu à la réalité physique de l'événement avec un degré d'interprétation minimum. Il met en évidence l'importance du contexte (le même événement peut être considéré comme normal dans un contexte et très anormal dans un autre).

Le deuxième niveau est l'***explication*** ou "niveau causal". Dans ce cas, l'analyste s'intéresse aux déviations – le processus de production des erreurs et violations – et également aux défenses qui ont échoué. Toutes les influences et contributions possibles sont étudiées pour permettre d'expliquer la cause de l'événement : individu (personnalité, attitudes, compétences); équipe (synergie, règles, habitudes, roulement d'équipe) ; système (formation, procédures, interface homme/ machine, contraintes de temps, culture, etc.) ; et situation (circonstances, chance, hasard).

Le troisième niveau concerne le ***contrôle des risques***. Dans ce cas, l'analyste peut poser plusieurs questions afin de déterminer la nature de l'échec dans le processus de gestion des risques:

- Quel était le danger (risque) ?
- Quelle stratégie de gestion des risques aurait dû être utilisée ? (principe de sécurité)
- Quelle stratégie de gestion des risques a été utilisée ? Comment a-t-elle fonctionné ?
- Quel enseignement peut-on en tirer ?
- Quelle mesure a été prise ?
- Qui devrait en être informé ? (faut-il modifier les représentations mentales concernant ce risque ?)
- Quelle est la prochaine vérification concernant l'efficacité de la mesure prise ?

Ces trois niveaux d'analyse permettront de comprendre entièrement l'événement. Ils étudieront non seulement l'événement individuel mais donneront également des informations sur les processus de gestion des risques de l'organisation en mettant en évidence des faiblesses à une plus grande échelle. Cette approche intégrée permettra également d'expliquer et de remettre en question différentes hypothèses de sécurité, comme nous le verrons dans le chapitre 4, "Spécifications fonctionnelles".

Veuillez vous reporter au chapitre 5, "le rôle du Département de Sécurité" pour de plus amples informations sur la traçabilité et l'évaluation de la réponse de l'organisation.

3.4 Contrôle de la gestion des risques dans le système

Il est désormais important de clarifier ce que nous avons appelé le "système" dans ce document. Le "système" correspond à l'ensemble du secteur de l'aviation civile, y compris les compagnies aériennes, les avionneurs, les organismes, syndicats, organisations internationales, et autres. A ce niveau, la question porte sur la sécurité globale de l'aviation civile et les problèmes sont d'ordre politique, économique et culturel. Il s'agit d'un macro-système. Seuls les aspects les plus génériques ou universels de la sécurité aérienne peuvent être traités à ce niveau.

Le champ d'application de la réglementation internationale (par exemple JAA) peut correspondre à un niveau inférieur de ce macro-système. Cette réglementation constitue une référence en matière de principes de sécurité du système. Toujours à l'échelle du macro-système, le niveau de l'aviation civile nationale est pertinent car les questions culturelles, économiques et politiques à l'échelle nationale ont un impact sur la réalité des opérations aériennes.

Le niveau de l'organisation (compagnies aériennes, avionneurs) est la première entité opérationnelle, directement liée au monde réel. Le niveau pertinent suivant est celui de l'équipe locale d'opérateurs directs (corporation). Enfin, au niveau individuel, les opérateurs directs (acteurs de premier plan) agissent en interaction et en temps réel avec le monde réel, en assurant la maintenance, le ravitaillement et le pilotage d'avions réels.

Si l'on considère l'OIRAS comme un outil de gestion des risques, il peut être utile tant au niveau global qu'au niveau de l'organisation, et pas seulement au niveau de l'opérateur direct. Les représentations du processus de gestion des risques seront différentes car les influences varient.

Tous les niveaux posent des problèmes spécifiques comme le montre le tableau suivant. On remarque notamment les différents points de vue issus de l'intersection entre le niveau dans le système et les considérations théoriques précédemment évoquées. Les hypothèses sur la sécurité sont présentes à quatre niveaux – ce sont ces hypothèses qu'il faut expliquer, gérer et remettre en question avec le système OIRAS approprié.

Tableau. Points de vue théoriques pertinents dans le système

	Individu	**Equipe**	**Organisation**	**Global**
Questions clés: Modèles génériques	Rassmussen SHELL Sécurité écologique Psychologie Psychologie cognitive	Dynamique de groupe CRM	James Reason Sociologie de l'organisation Fiabilité de l'organisation	Sociologie Sociologie des risques
Questions clés: Sécurité normative	Compétences Procédures Connaissance	Procédures Communication Synergie	Procédures Normes Protections	Culture Réglementation de sécurité
Questions clés:	Connaissance	Stratégies de	Culture (sécurité)	Perception des

Sécurité écologique	Confiance Gestion des risques Contrôle cognitif Contrôle de la situation	gestion des risques	d'entreprise Retour d'expérience pour l'organisation	risques

4. Un OIRAS amélioré: Spécifications fonctionnelles

Dans ce chapitre, nous décrirons les fonctions qu'un OIRAS devrait remplir pour constituer un instrument de contrôle de la gestion des risques. Nous commencerons par les fonctions de niveau supérieur destinées aux analystes ou autres utilisateurs du système puis nous étudierons le niveau inférieur et décrirons comment l'OIRAS devrait être organisé pour assumer les fonctions de niveau supérieur.$$ (voir avec M. MASSON)

4.1 Caractéristiques de base du système proposé

Les caractéristiques suivantes sont destinées à fournir des réponses acceptables aux défis décrits précédemment, à exploiter les ressources potentielles des nouvelles technologies et à constituer la première étape d'une conception plus étendue du processus de compte-rendu de sécurité en tant qu'élément du "processus de retour d'expérience de l'organisation".

- L'OIRAS sera orienté vers la "*gestion des risques"* et non vers la recherche des "causes de l'incident". En d'autres termes, le but du processus de compte-rendu et d'analyse n'est pas l'analyse des causes de l'incident mais l'amélioration de la compréhension du système et de la gestion de ses propres risques. Le traitement des informations suivra donc le raisonnement suivant:
    - A quel type de risque opérationnel cet événement (famille d'événements) est-il lié ?
    - Ce domaine de risque opérationnel est il déjà considéré comme une priorité dans le contrôle des risque ? Si non, pourrait il devenir une priorité ?
    - Quelles stratégies de gestion des risques (principes de sécurité) sont associées à ce domaine de risque ?
    - Lesquelles ont effectivement été utilisées pendant l'événement? Lesquelles ont connu un succès ? Lesquelles ont échoué ?
    - Le taux d'échec est il cohérent avec les hypothèses d'objectif de sécurité ?
    - Cet événement nous apprend il quelque chose de nouveau ?
- L'OIRAS sera conçu pour les compagnies / organisations et non pour les "spécialistes de la sécurité". Le traitement des informations sera *réparti* dans l'organisation :
    - Le rôle du Département de Sécurité auprès des compagnies aériennes, avionneurs, organisations ATM, organismes de l'aviation civile, sera principalement de divulguer les informations, favoriser les questionnaires de sécurité, encourager le retour d'informations. (voir chapitre 5).
    - Le Département de Sécurité sera responsable de la sécurité du réseau : une partie des analyses seront effectuées par les différents départements spécialisés (Exploitation, Maintenance, Formation). Le Département de la Sécurité peut également demander à des ateliers CRM d'étudier une question de sécurité spécifique et de lui communiquer les conclusions.
    - Le processus d'analyse intégrera les avionneurs le cas échéant pour éclaircir des questions techniques ou opérationnelles, la philosophie de conception, etc.
- L'OIRAS ne se limitera pas aux incidents : il comprendra tous les "événements pertinents en matière de sécurité" qui ont connu un processus de récupération réussi.
- Les résultats de l'OIRAS ne se limiteront pas à une analyse des causes et à des recommandations concernant des modifications à apporter au système. Ils comprendront également :

    - Des "anecdotes" pour améliorer les représentations des acteurs du système concernant les risques et les stratégies de gestion des risques
    - Des outils d'enrichissement des connaissances d'un individu ('self-debriefing') pour que l'équipage soit immédiatement informé de la reconstitution du vol; etc.
    - Des relations avec le système de formation: pour que le système de formation (ateliers CRM, simulateurs) dispose de scénarios, d'études de cas, etc.
- Mots-clés évolutifs
    - Compte tenu du caractère évolutif d'un OIRAS en tant qu'outil d'enrichissement de l'organisation, on admet que certains groupes de mots-clés seront des "listes évolutives" qui augmenteront en fonction des données reçues des opérateurs et en fonction des modifications apportées par les analystes grâce aux enseignements tirés. Concrètement, les listes de principes de sécurité, modes de défaillance, modes de récupération et des mesures correctives augmenteront à chaque nouveau compte-rendu.
- L'OIRAS sera structuré comme un outil d'analyse à plusieurs couches et un réseau reliant différents niveaux d'organisation: équipage, compagnies aériennes, avionneurs, autorités de l'aviation civile.
- La conception du système informatique de l'OIRAS permettra une collecte, un archivage et un traitement multimédia des informations. En effet, les nouvelles technologies de l'information permettront rapidement de rapporter des événements grâce à différents supports: son, vidéo, données numériques. Les prochains cockpits disposeront certainement de systèmes simplifiés de transfert des données permettant un téléchargement de CVR, DFDR ou Video.

4.2 Résultats fonctionnels du système

Le système doit pouvoir:

- Permettre à des personnes autorisées d'accéder à la base de données grâce à un mot de passe puis de compléter ou modifier les données.
- Archiver et retrouver des informations relatives à des événements isolés sous un format multimédia
- Eviter la saisie répétée d'un même événement
- Distinguer les données factuelles (objectives) et les informations interprétées (subjectives)
- Distinguer les données descriptives et l'interprétation des causes issue de l'analyse objective d'événements isolés.
- Distinguer les différentes sources d'information: le rapporteur, le ou les analystes, les départements exploitation des compagnies aériennes, l'avionneur, etc.
- Permettre de mettre en relation des événements isolés et des stratégies de gestion des risques
- Permettre de mettre en relation des événements isolés et des modes de défaillance
- Permettre de mettre en relation des événements isolés et des stratégies de récupération
- Permettre de mettre en relation des événements isolés et des actions de suivi
- Retrouver un ensemble d'événements ayant des caractéristiques communes
- Mettre en évidence des facteurs contributifs pour un ensemble d'événements donné.
- Mettre en évidence des schémas potentiels de comportements de gestion (prévention, détection, récupération) des déviations (erreur, violations, échecs, événements imprévus) pour un ensemble d'événements donné
- Sélectionner les informations relatives à des événements isolés afin de les communiquer à des tierces parties sous un format approprié pour les destinataires potentiels : DGAC, avionneurs, autres compagnies aériennes.
- Afficher automatiquement des "signaux" d'alerte concernant des conditions "anormales" programmées (taux de fréquence de l'événement, combinaison spécifique de facteurs, etc.)
- Archiver les résultats attendus des actions de suivi, et les moyens pour évaluer les effets concrets de ces actions.

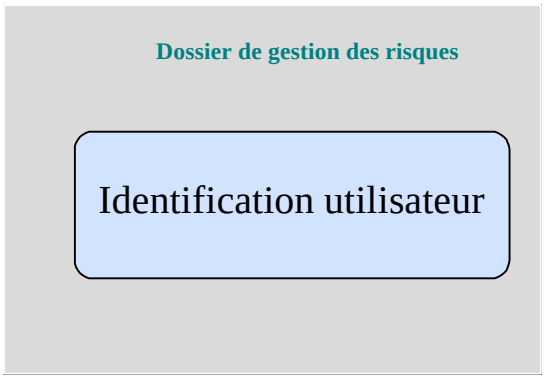
4.3 Format de la Base de Données

4.3.1 Objectifs

Ce chapitre vise à décrire l'organisation fonctionnelle de la base de données. Comme indiqué ci-dessus, la principale différence entre cette base de données et les OIRAS actuels, réside dans le fait qu'elle est orientée vers la gestion des risques plutôt que vers l'analyse des incidents. L'accent est mis non pas sur la description des incidents et leurs causes, mais sur la gestion des risques. L'approche traditionnelle est donc inversée. Au lieu de rechercher des stratégies de gestion des risques dans les rapports d'incident, il s'agit, dans l'approche proposée, d'examiner les rapports d'incident selon des stratégies de gestion des risques préétablies : un incident est analysé en rapport avec les stratégies de gestion des risques qui existent au niveau de l'organisation.

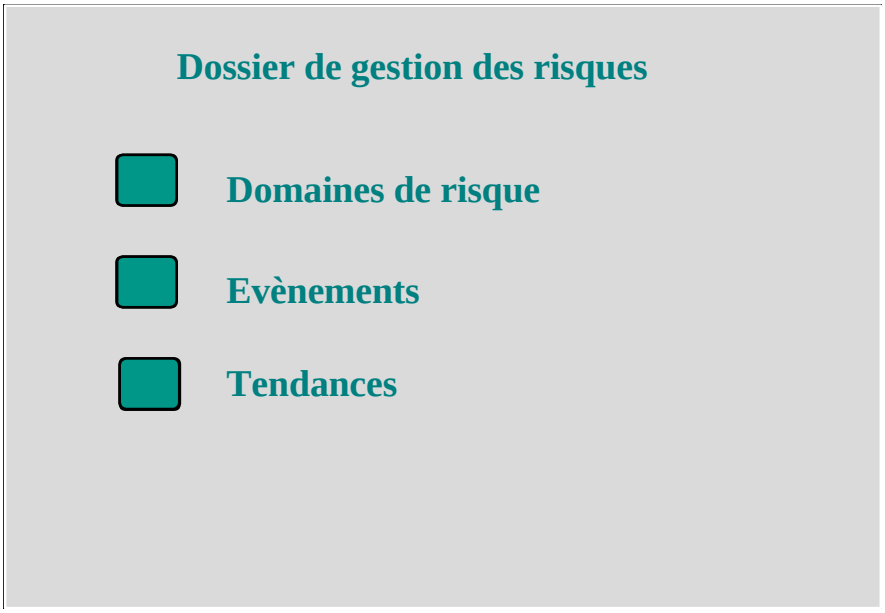
4.3.2 Structure globale

Au centre de cet OIRAS amélioré figure le Dossier de Gestion des Risques (RMF- *Risk Management Folder*). A condition d'entrer le mot de passe requis, quiconque dans l'organisation peut accéder à ce fichier informatique, rechercher des données et les modifier.



L'ouverture de ce dossier donne accès à un menu de trois rubriques :

- la rubrique Domaines de Risque sera décrite ci-après.
- la rubrique Evénements permet d'accéder à la liste des événements archivés qui peuvent être triés par leurs descripteurs (date, aéroport, type d'appareil, ...) et par des renvois aux champs de la rubrique Domaines de Risque. Il faut cliquer sur un événement pour accéder à une Page de Description de l'Evénement.
- la rubrique Analyse de Tendance permet d'accéder à un outil classique d'analyse de tendance.



4.3.3 La page des Domaines de Risque

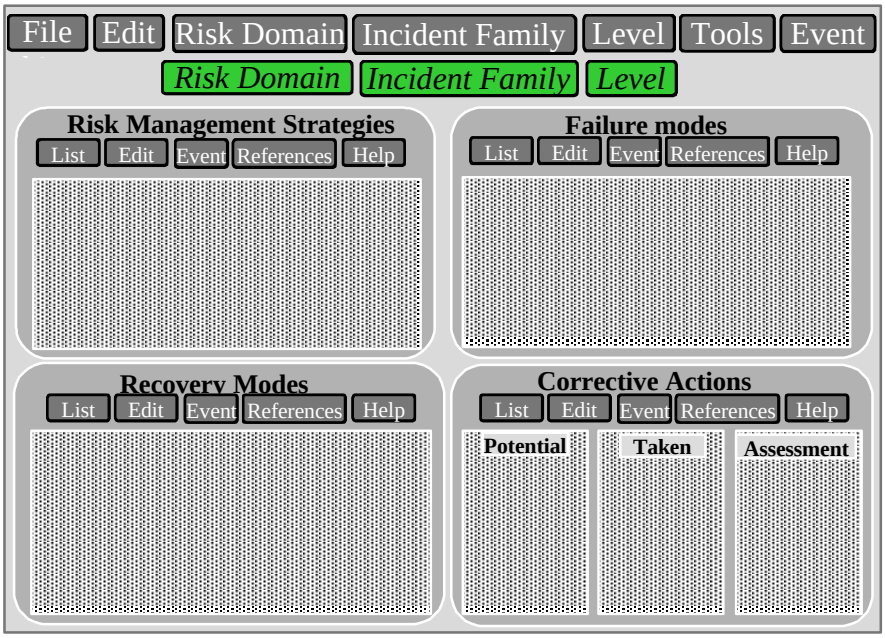
Les domaines de risque peuvent être considérés comme des accidents types potentiels que l'organisation a identifiés et qu'elle s'efforce de prévenir. Voir la liste suivante à titre d'exemple :

Exemple de liste d'accidents types

1 CFIT/ montée initiale /remise des gaz/ approche finale	7 Collision au sol sur la piste en service
2 CFIT/ montée/ croisière/approche initiale	8 Très fortes turbulences
3 Perte de contrôle (décollage/montée initiale/approche finale)	9 Incendie non maîtrisé en vol
4 Perte de contrôle (montée/croisière/approche initiale)	10 Défaillance technique non maîtrisée en vol
5 Sortie de piste à une vitesse élevée (atterrissage /décollage)	11 Atterrissage forcé
6 Collision en vol	12 Evacuation d'urgence ratée

Les familles d'incidents peuvent être considérées comme les principaux précurseurs potentiels des accidents types. A partir de la liste des accidents types, l'organisation établit une liste des familles d'incidents, contenant chacune tous les événements imaginés susceptibles de se terminer par cet accident type, s'ils ne sont pas prévenus. Par exemple, une famille d'incident intitulée "Collision au sol sur la piste en service" pourrait regrouper les sorties de piste, les atterrissages sur une piste autre que celle désignée, et les accidents dus à l'utilisation simultanée de pistes qui se croisent. Chaque domaine de risque peut générer une ou plusieurs familles d'incident, ou n'en générer aucune.

L'ouverture de la page Domaines de Risque permet d'accéder à un écran tel que représenté ci-dessous :



File:	Fichier
Edit:	Edition
Risk domain:	Domaine de risque
Incident family:	Famille d'incidents
Level :	Niveau
Tools:	Outils
Event:	Evénement

Risk Management Strategies:
Stratégies de gestion des risques

Failure modes:
Modes de défaillance

Recovery modes:
Modes de récupération

Corrective actions :
Mesures correctives

Potential :	potentielles
Taken:	prises
Assessment:	évaluation

Sub-menus	Sous –menus :
List:	Liste
Edit:	Edition
References:	Références
Help :	Aide

Certains menus ont des catégories prédéfinies et d'autres sont conçus de façon à être modifiés, au moyen du menu Edition, en fonction des comptes-rendus à entrer. Les principaux menus sont :

- Fichier : permet de manipuler le fichier (ouvrir, fermer, enregistrer, formater)
- Edition : permet de mettre à jour le contenu des menus : Liste des Domaines de Risque, Liste des Familles d'Incidents, Liste des Niveaux de l'Organisation
- Domaines de risque : permet de visualiser la liste des domaines de risque et d'en choisir un.
- Famille d'incidents : permet de visualiser la liste des familles d'incidents et d'en choisir une.
- Niveau (de l'organisation) : permet de choisir le niveau de l'organisation auquel l'analyse sera effectuée : opérateurs directs (acteurs de premier plan), équipe d'opérateurs directs (corporation), compagnie ou constructeur, autorités
- Outils : donne accès aux outils de traitement de données
- Evènement : donne accès aux données des événements individuels.

La page comprend aussi les quatre fenêtres interactives suivantes :

- Stratégies de gestion des risques : comprend une liste des principes de sécurité. Il s'agit d'identifier les "principes de sécurité" pertinents par le biais de la question suivante : comment le système était censé être protégé contre ce risque ? (avant que l'incident survenu ne révèle qu'il n'était peut-être pas réellement protégé)
- Modes de défaillance : comprend une liste des défaillances des principes de sécurité. Il s'agit d'identifier les "agents pathogènes" et d'analyser la vulnérabilité du système. Quel principe de sécurité est apparemment remis en question ? Procéder à un essai de substitution [Que se passera-t-il si on change le type d'appareil, l'équipage, la compagnie, l'aéroport,...] pour évaluer la portée réelle de la défaillance.
- Modes de récupération : comprend une liste des protections et des défenses connues contre l'issue dangereuse des modes de défaillance.
- Mesures correctives : comprend une liste des mesures correctives possibles ; une liste des mesures correctives réellement mises en œuvre et des stratégies d'évaluation des actions de suivi.

Ces quatre fenêtres ont chacune un sous-menu :

- Liste : visualise la liste des stratégies de gestion des risques, des modes de défaillance, ... dans la fenêtre correspondante
- Edition : permet de modifier la liste
- Evènement : donne accès aux données respectives de chaque événement
- Références : donne accès aux référence pertinentes :
    - principes de sécurité : réglementation, philosophie, politique adoptée, procédures ou littérature en matière de recherche
    - modes de défaillance : littérature en matière de recherche
    - modes de récupération : littérature en matière de recherche
    - mesures correctives : décideur ; justifications de la décision
- Aide

4.3.4 Alimentation de la base de données

Lorsqu'un nouveau compte-rendu d'événement arrive, il faut lui attribuer un numéro d'identification. Ensuite, la première étape consiste à le rattacher à un domaine de risque existant, puis à une famille d'incident dans le sous-menu correspondant. Si l'événement ne peut être classé dans aucun des domaines existants, l'analyste peut juger nécessaire de créer un nouveau domaine de risque. Ce nouvel OIRAS se distingue par cette possibilité de rajouter, si nécessaire, de nouvelles catégories à celles existantes. A la lecture du compte-rendu, l'analyste[1] peut aussi décider de le classer dans un classeur, s'il estime qu'il ne présente pas d'intérêt particulier (incident mineur, sans conséquence, dont il n'y a aucune leçon à tirer). Le rapporteur en sera avisé (il est important d'encourager le retour d'informations des exploitants) et le rapport sera gardé pour être éventuellement réexaminé ultérieurement. Il s'agit là de la première décision "réfléchie" à prendre : l'évaluation du risque potentiel que présente l'événement rapporté pour l'organisation, et son identification par assimilation à un domaine de risque.

Une fois que le compte-rendu a été classé dans un certain domaine de risque et que le menu a été ouvert, on est en présence de quatre fenêtres interactives :

- Stratégie de gestion de risques : identifier les "principes de sécurité" appropriés,
- Mode de défaillance : détecter les "agents pathogènes" et analyser la vulnérabilité du système,
- Mode de récupération : reconnaître les protections et les défenses contre le danger,
- Mesures correctives : identifier les actions correctives possibles et déjà mises en œuvre ainsi que leur suivi.

4.3.5 Stratégies de gestion des risques

La fenêtre Stratégie de Gestion des Risques contient une liste des protections mentionnées. L'élaboration de cette liste pour chaque famille d'incident est une façon d'expliciter le modèle de sécurité de l'analyste (ou de l'organisation). Il s'agit d'envisager toutes les façons d'éviter que survienne un incident donné, ainsi que toutes les caractéristiques du système qui le protègent d'une telle occurrence. Par exemple, dans le cas des sorties de piste (considérées comme une famille d'incident classée dans le domaine de risque "collisions au sol"), les éléments suivants peuvent être envisagés comme stratégies de gestion des risques ou principes de sécurité :

- Roulage sur les pistes : les équipages sont censés savoir où elles se trouvent ;
- Balisage visuel des pistes : les équipages peuvent voir les limites des pistes ;

[1] Dans ce chapitre, pour des raisons de commodité, nous faisons référence à "'l'analyste" comme s'il s'agissait d'une seule personne. Au chapitre 5, Un Département de sécurité Amélioré, nous décrivons les contributions des autres personnes impliquées dans l'analyse des incidents.

- Procédure ATC (contrôle de la circulation aérienne) : les équipages doivent attendre l'autorisation des contrôleurs aériens pour aller sur une piste en service.
- Phraséologie
- Contrôle visuel par l'équipage : les équipages vérifient que la visibilité est claire pour l'approche finale.

Cette liste sera créée par itérations : une première version provisoire peut être rédigée puis améliorée et complétée suite à l'analyse des événements consignés, ou à l'évolution de la philosophie de la sécurité et des règlements applicables. Il s'agit donc d'une liste évolutive, qui exploite les informations en retour pour mieux restituer le modèle de sécurité. De plus, chaque fois qu'un principe de sécurité est jugé approprié par rapport à l'événement rapporté, il est possible en cliquant dessus dans la liste, de créer un lien avec cet événement, par l'intermédiaire de son numéro d'identification. Chaque rubrique de cette liste fait office de résumé : à son ouverture, une liste d'événements en rapport est activée. En cliquant deux fois sur un événement donné, on fait apparaître une feuille de codage de l'événement où les détails de l'incident peuvent être enregistrés quand les résultats de l'analyse sont connus.

4.3.6 Modes de défaillance

Dans la fenêtre Modes de Défaillance, figure une liste des défaillances connues et possibles. Elle est bien évidemment mise à jour à mesure que de nouveaux événements sont rapportés. Elle permet aussi de remettre en question le système de pensée de l'analyste. (Je ne pensais pas que X pouvait tomber en panne... mais cela s'est produit). Pour reprendre l'exemple des sorties de piste, les défaillances possibles pourraient inclure les points suivants :

- Problème d'orientation sur la piste
- Défaillance au niveau de la communication
- Autorisation ATC erronée
- Limites des pistes non perçues
- Atterrissage de l'appareil sur une piste non appropriée

Là aussi, chaque fois qu'un mode de défaillance semble pertinent dans le cas de l'événement rapporté, l'analyste clique sur la défaillance correspondante pour créer un lien avec l'événement, par le biais de son numéro d'identification, ou bien ajoute une autre rubrique à la liste. De même, chaque rubrique de la liste fait office de résumé. A son ouverture, une liste d'événements en rapport est activée. On peut accéder aux détails de l'incident en ouvrant la feuille de données techniques sur l'événement. Il convient de noter que les mêmes défaillances peuvent figurer dans plusieurs domaines de risque, et que cette technique du résumé permet à l'analyste de mettre en évidence les événements à partir des défaillances du système et non l'événement à proprement parler. Dans un sens, ce système permet à l'analyste de prendre plus de recul par rapport aux données respectives de chaque événement et à mieux percevoir les schémas de défaillance les plus importants.

4.3.7 Modes de récupération

La fenêtre Mode de Récupération sera aussi une liste ouverte, à compléter au fur et à mesure que de nouvelles techniques de récupération seront rapportées. Cette liste peut aussi alimenter la fenêtre Stratégies de Gestion de Risque. Il peut y avoir des protections dans les systèmes, non compris dans la liste originale, qui sont clairement identifiés à l'occasion du processus de récupération. Des informations fournies par les opérateurs directs peuvent ainsi faire prendre conscience à l'organisation non seulement de ses points faibles en matière de défense mais également de certains atouts cachés. Ces trois fenêtres servent à donner une image réelle des défenses et des faiblesses de l'organisation. Comme une liste en renseigne une autre, le potentiel d'enrichissement de l'organisation est croissant.

Un autre menu fonctionne de concert avec ces trois fenêtres. Il identifie le niveau de l'organisation auquel interviennent la stratégie de gestion des risques, la défaillance et la récupération. Ces différents niveaux étant :

- Les opérateurs directs (acteurs de premier plan)
- L'équipe locale des opérateurs directs (corporation)
- La compagnie/le constructeur
- La CAA

Il est possible que la stratégie de gestion des risques envisagée au niveau de la compagnie aérienne (conception de l'appareil), ait échoué, et que le processus de récupération ait été initié au niveau des opérateurs directs. Ce menu reconnaît les différents niveaux de fonctionnement dans le système et peut en conséquence mettre en évidence les points faibles (ou les points forts).

Une fois que l'analyste a tranché sur ce qui s'est passé (ou en d'autres termes, qu'il a déterminé les principes de sécurité remis en question par la défaillance et les actions de récupération qui ont suivi), il doit déterminer les mesures correctives appropriées qui s'imposent.

4.3.8 Mesures correctives

La fenêtre Mesures Correctives est un élément essentiel de cet OIRAS, car elle permet de suivre les réponses apportées par l'organisation et de les évaluer. Elle comprend un sous-menu des mesures correctives possibles proposées par les opérateurs directs, les analystes spécialisés en sécurité, et d'autres services. La traçabilité des auteurs de chaque proposition est assurée par le menu "références". La liste des mesures correctives possibles sera complétée au fil de l'expérience cumulée par l'organisation et, à nouveau, cela permettra d'expliciter les modèles de sécurité de ceux qui ont apporté des "solutions". Différents acteurs dans le système pourront également voir plus clairement quelles sont les limites aux solutions qu'ils proposent (par ex, en suggérant toujours plus de formation ou plus de procédures). Sur la base de cette liste de mesures possibles, les mesures effectivement prises seront consignées dans la base de données, ainsi que le nom de la personne qui les a décidées et le groupe ou les groupes sur lesquels elles doivent avoir des répercussions.

Les mesures correctives prises auront un impact sur la liste des stratégies de gestion des risques et devraient être ajoutées à la liste, même à titre provisoire. Les questions qui doivent être posées :

- La mesure corrective (provisoire) a-t-elle un impact sur d'autres stratégies de gestion des risques ?
- Est-ce qu'elle invalide les stratégies antérieures ?
- Dans l'affirmative, est-ce qu'elle invalide une hypothèse ou un principe de sécurité ?
- Dans l'affirmative..... ?

Enfin, la traçabilité des mesures prises doit être assurée dans le but d'évaluer leur efficacité. Une stratégie d'évaluation doit être conçue, *en même temps que la mesure est mise en œuvre*, pour déterminer les critères de succès et les paramètres de l'évaluation. Cette étape est omise dans les OIRAS actuellement utilisés, ce qui signifie que ces systèmes n'ont aucun moyen d'évaluer leur propre efficacité. L'omission d'un tel mécanisme d'évaluation dans un outil de sécurité dont la mise en œuvre est très onéreuse, est une aberration du point de vue scientifique et économique. Un tel mécanisme permet à l'organisation de boucler la boucle du retour d'expérience, de contrôler réellement ses processus d'adaptation et ses stratégies d'apprentissage et de fixer une orientation claire pour l'avenir.

La stratégie d'évaluation doit permettre de reconnaître les signes de succès ou d'échec des mesures correctives. Mais il faut savoir dialoguer intelligemment avec la base de données. Il est possible d'exprimer une hypothèse en entrant des mots-clés, des combinaisons, et des fréquences significatives. Une série de formules logiques "si.., alors" peut être créée et appliquée à la base de données de façon

répétitive et automatique. Ces hypothèses programmées agiraient comme des "drapeaux rouges". Des délais devraient également être instaurés : Quand la stratégie sera-t-elle introduite ? Quand est-elle censée avoir des répercussions sur le système ? Quand certaines familles d'incident seront-elles affectées ?

En résumé, les menus, les fenêtres et les sous-menus du Dossier de Gestion des Risques sont conçus de façon à pouvoir s'alimenter les uns les autres avec des informations mises à jour. Conformément au paradigme écologique de systèmes complexes d'auto-référencement adaptatifs mentionné ci-dessus, cet OIRAS comprend plusieurs boucles qui assurent le retour d'informations d'un élément à un autre. A mesure que le système gagne en expérience et évolue, des modèles de sécurité préalablement implicites, peuvent être mieux explicités, remis en question et adaptés au besoin. L'organisation peut aussi tirer des enseignements plus efficacement en suivant et en évaluant ses mesures correctives.

4.4 Principe de fonctionnement de la base de données

Il convient de noter que les paramètres objectifs des événements (appareil, route, altitude, etc.) ne sont pas enregistrés dans le Dossier de Gestion de Risques. Ils peuvent être enregistrés dans un fichier d'incident qui est activé en identifiant le mode de défaillance pertinent et en cliquant dessus.

Il est recommandé d'utiliser une structure de mots-clés généralement acceptée telle que le système ADREP 2000 car elle permet de transférer un maximum d'informations entre les parties intéressées. En outre, cette structure a été conçue sous la forme d'un réseau avec des ramifications, de sorte que différents niveaux de détails peuvent être enregistrés et revus au besoin. Bien que l'ADREP 2000 et les autres taxonomies proposent des catégories de facteurs causals, le codage des événements en fonction des causes n'est par recommandé pour les raisons de biais mentionnées auparavant. Les informations pertinentes concernant les causes auront dû être extraites lors de l'analyse des modes et des niveaux de défaillance.

Les données objectives relatives aux événements sont archivées et peuvent être récupérées si nécessaire. Une fois qu'on leur a attribué un numéro d'identification, les rapports d'événement peuvent être physiquement classés dans un meuble de classement sûr. Bien que ce système puisse paraître peu évolué, il est efficace pour deux raisons :

- D'abord, cela revient moins cher de classer physiquement le rapport que de saisir les récits complets des rapporteurs. Les informations subjectives restent disponibles sur un autre format que le format électronique et de plus les informations les plus importantes auront dû être extraites dans l'analyse de gestion des risques.
- Deuxièmement, ce système admet qu'une ou plusieurs caractéristiques réellement importantes d'un événement ne peuvent se révéler comme telles qu'avec du recul, et ne peuvent pas être saisies avec des mots-clés pré-établis. S'il dispose d'un classeur avec des rapports numérotés, l'analyste (ou le service compétent) pourra suivre une hypothèse en s'appuyant au besoin sur des documents de première source. Il semble néanmoins, selon les indications de différents départements de sécurité, que ce type de recherches soit plutôt rare.

A en juger le volume du présent document consacré à la description du Dossier de Gestion des Risques et celui consacré au rapport de l'incident à proprement parler, il doit apparaître nettement que nous essayons de déplacer le centre d'intérêt des systèmes de compte-rendu d'incidents. Pour reprendre la métaphore du début, les rapports d'incident peuvent contenir ou non des paillettes d'or. Au lieu de garder tous les matériaux stériles, comme le font la plupart des OIRAS, nous recommandons donc vivement d'utiliser un filtre intelligent pour ne conserver que les matériaux précieux.

4.5 Le formulaire de compte-rendu

Le formulaire de compte-rendu a été conçu en tenant compte d'un certain nombre de contraintes et d'objectifs :

- Les pilotes ne sont pas des rédacteurs, il faut donc que le formulaire reste aussi bref que possible (seulement deux pages).
- Les pilotes ne sont pas spécialisés dans l'analyse des questions de sécurité ; nous avons donc rédigé les questions le plus simplement possible, dans le langage courant.
- Nous avons voulu éviter les questions tendancieuses que nous avons relevées dans d'autres formulaires. Nous avons donc choisi des questions non directives (Que s'est-il passé? Pourquoi? Comment le problème a-t-il été réglé ? Qu'aurait-il fallu faire ?) pour permettre au rapporteur de se référer à son propre modèle de sécurité implicite.
- En même temps, nous leur proposons quand même quelques messages de guidage pour les inciter à élargir le cadre de leur réflexion au niveau système, à penser aux "défaillances du système" (sont-ils passés près ou non, d'un accident), et à réfléchir à leur stratégie de gestion des erreurs.
- La principale différence entre un incident et un accident réside dans le processus de retour à la normale après incident, et nous y avons donc consacré l'une de nos questions (détection et récupération).
- Enfin, fidèles à l'aspiration de l'organisation de tirer des enseignements, nous avons prévu une question qui vise à intégrer le rapporteur dans ce processus d'exploitation du retour d'expérience (à qui faudrait-il donner des conseils et que faudrait-il faire ?). Cette question invite le rapporteur à réfléchir aux leçons de sécurité découlant du compte-rendu et à la façon dont l'organisation (et le système de l'aviation civile) pourrait les exploiter.
- Les consignes pour remplir le formulaire de compte-rendu, sont formulées dans le même esprit :
    - "Rendez compte de l'événement si vous pensez que des mesures peuvent être prises pour éviter d'autres occurrences identiques ou apparentées, ou si vous pensez que d'autres professionnels de l'aviation pourront tirer des leçons de votre expérience ou bien si vous avez réalisé que le système et ses protections n'ont pas été aussi résistants que vous le pensiez".

Ces consignes définissent à elles seules le sens et l'objet du système de compte-rendu d'incident : à savoir, contribuer à éviter la répétition de tels incidents, faire partager son expérience dans l'espoir d'éduquer les autres, et/ou attirer l'attention du système sur ses seuils réels de sécurité. En posant les bonnes questions (des questions ouvertes, non directives), on peut inciter le rapporteur à réfléchir aux problèmes dans le cadre plus large du système, ainsi qu'aux processus internes, à l'intérieur et à l'extérieur du poste de pilotage (ou de son espace de travail). Cette approche ne signifie pas que les rapporteurs sont ignorants. Au contraire, elle admet que les rapporteurs sont les seuls "témoins experts" présents au moment de l'incident. Un témoin éduqué et habitué à la réflexion rendra compte de l'incident avec plus de détails et sans être sur la défensive, en d'autre termes, il fera un bien meilleur compte-rendu de l'incident.

Voir l'exemple du formulaire de compte-rendu à l'Annexe A.

4.6 Les rapporteurs : des pilotes seulement ?

De nombreux systèmes de compte-rendu d'incidents ont l'inconvénient d'être principalement axés sur les actions de l'équipage. Les pilotes sont en mesure d'observer une grande partie du système et ils sont donc les mieux placés pour faire des commentaires sur la santé du système. Mais un système de compte-rendu d'incidents axé uniquement sur les pilotes renforce aussi l'idée que tout incident revient à une erreur de pilotage, même quand d'autres influences "extérieures" sont considérées. Si le système de compte-rendu était étendu à d'autres services, cela favoriserait une plus large diffusion des

informations, ainsi que la création d'une culture de la sécurité à l'échelle de la compagnie. Cela faciliterait aussi les actions de suivi au sein de la compagnie si tous les services souscrivaient à un système ouvert d'échange d'informations et s'ils pouvaient échanger les rapports à prendre en compte. Les possibilités d'amélioration seraient accrues au niveau du système global plutôt qu'en se concentrant uniquement sur les pilotes (où le potentiel d'amélioration est peut-être le plus réduit). Avec un tel dispositif de compte-rendu mis en œuvre à l'échelle du système, les pilotes seraient affranchis de leur rôle habituel de "premiers fautifs". Enfin, les pilotes étant généralement perçus par les autres employés comme une catégorie privilégiée, il serait injuste de donner aux pilotes l'occasion de faire des commentaires sur les autres employés sans offrir cette même possibilité à ces employés (agents d'embarquement, PNC, personnel au sol, personnel de maintenance). Le même formulaire de compte-rendu, bien conçu, pourrait être utilisé dans tous les services.

5. Un Département de Sécurité Amélioré

5.1 Objectifs

Le Département de Sécurité devrait avoir pour but de promouvoir et faciliter les possibilités de tirer des enseignements dans le domaine de la gestion des risques et de la sécurité au sein de l'organisation (et du système global).

Plusieurs voies sont possibles pour réaliser ces objectifs :

- Coordonner et optimiser différentes sources de contrôle de la sécurité (FOQA, OIRAS, audits opérationnels et enquêtes).
- Evaluer les coûts et la valeur des informations obtenues à partir des différentes sources.
- Encourager le retour d'expérience et collecter les comptes-rendus des opérateurs.
- Diffuser les informations sur la sécurité aux autres parties concernées (internes et externes à la compagnie).
- Tenir à jour des bases de données et les rendre accessibles aux autres parties concernées.
- Aider les experts qui étudient le contexte local à analyser les causes et les risques.
- Centraliser toutes les informations relatives à la sécurité.
- Elaborer des hypothèses basées sur l'analyse des paramètres objectifs et des tendances des rapports
- Aider d'autres services à vérifier les hypothèses
- Aider d'autres services à mettre au point des mesures correctives ou d'adaptation
- Publier et/ou communiquer aux opérateurs des bulletins de "leçons de sécurité"
- Coordonner les mesures correctives pour limiter la redondance
- Assurer le suivi et l'évaluation des réponses apportées par l'organisation
- Contrôler le processus d'apprentissage de l'organisation.

Les employés du Département de Sécurité peuvent s'avérer très efficaces comme *consultants internes en matière de sécurité* auprès des services d'exploitation. Ils savent (ou devraient savoir) mener une réflexion complexe sur les questions de sécurité, mais ils ne connaissent pas bien les activités quotidiennes d'exploitation. Les employés des services d'exploitation ont les compétences inverses : ils ne sont pas très familiarisés avec les analyses de sécurité mais sont très au fait de toutes les activités d'exploitation de routine. Le personnel d'exploitation sera tout à fait apte à "lire" un compte-rendu et à percevoir les nuances et les contradictions qu'il contient.

Le Département de Sécurité peut apporter une aide précieuse :

- en guidant le personnel d'exploitation dans l'approche analytique,
- en suggérant différentes façons d'interpréter les données (par ex., du point de vue écologique, du système ou de la gestion d'erreurs),
- en contribuant à la formulation d'hypothèses
- en élaborant les moyens de vérifier les hypothèses,
- en suggérant différentes stratégies d'intervention, et
- en assurant la traçabilité de ces stratégies dans le système.

5.2 Flux de données

Il est recommandé d'analyser au cas pas cas tous les nouveaux comptes-rendus, ce qui peut être effectué de plusieurs façons : un individu peut être chargé de toutes les analyses (c'est peut-être là le défaut des petites compagnies) ; ou bien, un individu peut être responsable de la lecture préliminaire du compte-rendu et de sa diffusion aux parties concernées pour l'aspect opérationnel ; ou bien encore, une équipe opérationnelle composée d'individus de différents services peut se réunir périodiquement pour examiner les comptes-rendus. Ce modèle-là est particulièrement utile pour des cas complexes impliquant plusieurs services.

La méthode la plus économique et la plus efficace réside peut-être dans une combinaison des trois méthodes précitées : un individu est chargé de lire les comptes-rendus, à leur arrivée, et de décider de leur traitement ultérieur en fonction de leur nature ; si le cas est relativement simple, (par ex. la responsabilité d'une seule flotte ou d'un seul service est impliquée), il peut transmettre le compte-rendu à la partie compétente, en lui demandant un retour d'information sur les mesures prises. Si le cas est plus complexe, il peut le soumettre à une réunion inter-services des parties compétentes. La personne qui filtre les comptes-rendus à leur arrivée, devrait également être chargée de suivre les mesures prises et d'enregistrer les résultats dans la catégorie "mesures correctives" de la base de données.

L'analyse des comptes-rendus au cas par cas donne lieu à quatre traitements différents : le premier réactif et simple, le deuxième un peu plus proactif mais encore relativement simple et le troisième et quatrième proactifs à un niveau système plus global.

1. Une ligne de conduite simple, quelques mesures correctives pour remédier à une légère défaillance dans les défenses du système et partager les informations avec les parties concernées ;
2. Une leçon de sécurité, relativement simple, en ce sens que l'action requise semble assez évidente. Il peut s'agir de faire des recherches plus approfondies sur une caractéristique donnée du système risquant de poser un problème et de partager l'information avec les parties concernées.
3. Un doute relatif à la sécurité, qui donne lieu à l'élaboration d'une hypothèse à vérifier, et qui peut être clarifié à l'aide d'une "éprouvette proactive" du système. Comparée à l'approche précédente de "recherche de mots-clés" dans la base de données sur les incidents (où l'on se fie à des rapports incomplets, biaisés), cette approche-ci a l'avantage d'être basée sur une demande de renseignements systématique. Par exemple, en cas de doute concernant une route ou un aéroport ou un type d'appareil donné, la question posée peut être incluse dans les documents de vol à l'intention des pilotes qui volent sur la ligne ou sur l'appareil donné, ou desservent l'aéroport en question.
4. Un principe de sécurité remis en question. Là, la ligne de conduite n'est pas évidente. Les directives pour l'analyse devraient aider l'analyste à identifier un problème qui n'est pas facile à comprendre et qui ne peut pas être "réglé" facilement . Un problème de ce type est traité au niveau système et nécessite une plus grande connaissance et compréhension du système. Ce problème devrait donner lieu à l'établissement d'un indicateur d'anxiété (avec des niveaux variables d'intensité) au sujet du système et à l'élaboration d'hypothèses vérifiables (au mieux) ou à la formulation d'intuitions persistantes (que le système garde en mémoire en vue de les examiner ultérieurement).

5.3 Le suivi de l'apprentissage organisationnel : un nouveau centre d'intérêt

Apparemment, les OIRAS actuels utilisent l'analyse de tendance pour démontrer l'efficacité de leurs interventions. Si des incidents similaires à ceux rapportés ne se reproduisent pas ultérieurement, cela est considéré comme une preuve du succès de l'intervention. Mais, indépendamment des défauts de structure des bases de données actuelles, cette approche est plus sérieusement contestable au niveau système.

Les incidents isolés peuvent être uniquement considérés comme des symptômes révélateurs d'une atteinte à la santé d'un système. Une intervention visant à empêcher la reproduction d'un type d'incident peut réussir à supprimer ces incidents, mais risque simultanément d'occasionner un autre type de problème

(l'automatisation en est l'illustration la plus courante : elle a permis de réduire la probabilité d'erreur dans un domaine donné du vol, mais a généré en contrepartie des problèmes liés à la nonchalance et à l'ignorance des nouveaux systèmes complexes). Par ailleurs, l'absence d'un type d'événement ne garantit pas l'amélioration globale du système. Par conséquent, nous pensons qu'il serait souhaitable de se focaliser un peu moins sur la recherche de la causalité des événements et un peu plus sur les réponses aux événements apportées par l'organisation.

Dans une telle approche, l'analyste devra créer un document évolutif regroupant les réponses données par l'organisation aux rapports des opérateurs. Il enregistrera dans la base de données proposée les mesures correctives (réponses de l'organisation), avec les références des rapports correspondants.

Des réunions périodiques seront organisées pour examiner les mesures prises.

- Ces réunions auront pour but de présenter un résumé des réponses apportées, ce qui permettra de les analyser à un plus haut niveau et de reconnaître les thèmes récurrents.
- Ces résumés mettront en lumière l'ensemble des stratégies qui ont été essayées, et révèleront ainsi les modèles de sécurité implicites sur lesquelles ces mesures correctives se sont appuyées.
- Les thèmes récurrents pourront indiquer l'échec d'une mesure corrective (la mise en œuvre répétée d'une même stratégie pouvant signifier que cette stratégie n'est que partiellement efficace ou totalement inefficace à traiter le problème).
- Des schémas pourront aussi être dégagés, qui ne sont décelables qu'en se distanciant des données, pour y voir plus clair au niveau système (par ex., une solution peut s'avérer efficace localement, alors qu'elle génère un problème ailleurs dans le système).

Il est important de préciser ici que l'équipe chargée d'examiner les mesures prises *ne se concentrera pas sur le résumé des incidents ou événements relatés, mais plutôt sur la réponse apportée par l'organisation aux problèmes de sécurité perçus*. En d'autres termes, l'équipe évaluera avec quelle efficacité l'organisation tire des enseignements. Elle pourra par ex. poser les questions suivantes :

- Sommes-nous en train de répéter nos interventions ?
- Dans l'affirmative, cela signifie-t-il qu'elles sont inefficaces ?
- Peut-être que la solution ne réside pas dans la persistance à répéter la même chose, c'est-à-dire plus de formation, plus de procédures, et qu'il faut envisager une approche totalement différente.
- Peut-être y a t-il plus d'enseignements à tirer des données des réponses apportées ? (il peut y avoir des analyses de plus haut niveau qui débouchent sur des interventions au niveau système, plutôt que sur des réactions isolées.)
- Il y a peut-être davantage de stratégies efficaces, non contre-productives entre elles, que l'on ne peut trouver qu'en prenant du recul par rapport aux données. L'examen des réponses apportées et de leur efficacité peut aider l'équipe à déterminer les mesures à prendre à l'avenir, en émettant des hypothèses sur les échecs et les succès possibles.

5.4 Diffusion des informations

Le Département de Sécurité devra coopérer avec les autres compagnies aériennes et les agences extérieures dans ses efforts pour trouver des améliorations. Le sujet et le délai de la notification aux organismes extérieurs devront refléter le niveau de gravité évalué du dysfonctionnement du processus de contrôle de la gestion des risques. Pour les incidents jugés par l'analyste comme étant "à très haut risque", la partie concernée devra être avisée immédiatement. Pour tous les autres incidents, l'analyste pourra attendre de recevoir un nombre X de comptes-rendus similaires avant d'envoyer la notification à la partie concernée. (les incidents isolés, sauf s'ils sont très graves, attirent peu l'attention. Mais une série d'incidents jugés comme étant "à moyen risque", tous identifiés pour diffusion au constructeur ou aux autorités, attirera plus l'attention) Il sera éventuellement possible de programmer le logiciel pour qu'il reconnaisse la présence dans la liste de deux, trois ou x instances de compte-rendu de la même

catégorie ; cela permettra d'indiquer à l'analyste l'apparition d'un schéma d'incidents classés selon un même niveau de risque, et dont il faut aviser la partie concernée. Le nombre programmé pourra dépendre de la taille de la compagnie et de la fréquence générale des incidents (par ex., 2 instances pour une "haute gravité" ; 10 pour une "gravité moyenne" et 25 pour une "faible gravité") .

Une autre possibilité consiste à émettre des rapports trimestriels à diffuser aux parties concernées. C'est la méthode de base recommandée pour assurer un système périodique d'examen des comptes-rendus et de notification. Seuls les comptes-rendus caractérisés par une gravité ou une occurrence significative devraient être envoyés à une plus grande fréquence, et être aussi complétés par un résumé de compte-rendu systématique trimestriel. Cette approche des résumés trimestriels permettra de poursuivre la réduction des données par leurs classification dans des catégories significatives qui seront transmises d'un analyste à un autre (dans d'autres services ou agences). Les nouveaux mots-clés permettront à l'analyste d'identifier des schémas significatifs, basés sur un niveau de risque, et de notifier la ou les parties concernées. En d'autres termes, la même technologie qui permet à l'analyste de classer les incidents en familles d'incidents, lui permettra également d'effectuer la classification des réponses apportées par l'organisation. Les rapports trimestriels pourront ultérieurement être résumés et réexaminés et donner lieu à des rapports bi-annuels ou annuels. En fait, il s'agit de pouvoir déceler des tendances dans le temps grâce à l'utilisation d'un procédé systématique et qui fait gagner du temps. Des rapports pourront être générés automatiquement, qui fourniront aux parties concernées un résumé des informations ; des renseignements plus détaillés pourront être communiqués sur demande. Cette approche devrait permettre à toutes les agences de travailler efficacement à rechercher des tendances et à élaborer des hypothèses sur la sécurité du système.
Voir ci-dessous un exemple de formulaire de résumé, simple et autorisant un gain de temps, destiné à être utilisé par une compagnie :

Durant le trimestre compris entre le _ et le_, X incidents ont été déclarés auprès de ce bureau, dont Y ont été reconnus comme relevant de votre domaine de compétences.

L'imprimé ci-joint (généré automatiquement en sélectionnant les catégories appropriées dans la base de données) vous transmet les informations suivantes :

- Brève description de l'incident
- Famille d'incident
- Domaine de risque
- Modes de défaillance
- Mesure corrective
- Autres agences auxquelles l'incident a été notifié

Ces informations devraient vous être utiles dans vos analyses de sécurité. Nous pouvons vous fournir un rapport plus détaillé, sur demande. Veuillez nous transmettre toutes les informations en retour susceptibles de nous intéresser.

Ce protocole a été écrit en pensant à un coordonnateur de pilotes de compagnie. Un formulaire semblable pourrait aussi être conçu pour d'autres agences, par ex., pour que le constructeur rende compte aux autorités ; pour que les autorités donnent un retour d'information à la compagnie, etc.
Les rapports des analystes deviennent des données de départ pour d'autres analystes dans un système d'échange à plusieurs couches. Le système fonctionnera plus efficacement quand les informations

pertinentes seront communiquées entre les agences. Là aussi, le principal objectif est de *réduire la quantité des données* à transmettre aux autres parties, tout en générant des produits de données significatifs, interprétables et autorisant une analyse de tendance dans un système qui n'est pas sûr de savoir où ces tendances pourront être trouvées.

6. Exigences en matière de formation

Le succès d'un OIRAS dépend principalement de deux éléments : obtenir des informations de qualité de la part des opérateurs, et en tirer des informations de qualité par le biais de la base de données. Nous proposons un projet de formation pour répondre à ce double besoin.

Les qualités qui rendent une personne crédible et fiable à l'égard de ses pairs (et qui lui permettront d'être choisie ou élue pour remplir les fonctions de coordonnateur de l'OIRAS) sont probablement les mêmes que celles qui lui permettront de réussir à créer un réseau de relations avec la Direction et tous les autres services de la compagnie, et aussi d'interroger les rapporteurs au sujet d'un événement. Mais ces qualités, bien qu'elles soient très positives, ne suffisent pas. Les coordonnateurs devront aussi être des Chefs de Projet, avec des ressources et un budget à gérer (éléments essentiels pour la continuité d'un OIRAS). Ils devront aussi être continuellement formés dans le domaine des théories et tendances actuelles de sécurité afin d'élargir leurs perspectives lorsqu'ils examinent un incident ou élaborent des hypothèses sur la sécurité du système. Enfin, outre la formation en Facteurs Humains, les coordonnateurs du système devraient aussi être formés à l'analyse des données scientifiques (analyse qualitative et quantitative et gestion de base de données), pour apprendre à dialoguer intelligemment avec la base de données.

La formation nécessitera probablement au moins deux stages. Le premier sera consacré aux questions pratiques concernant la mise en œuvre d'un OIRAS dans une compagnie, le second portera sur les détails de l'analyse de la sécurité.
La première étape, consistant à établir la crédibilité du système, est essentielle ; or, l'expérience des dernières années a démontré que de nombreuses compagnies ne se préparent pas correctement à la mise en œuvre d'un OIRAS.
Le travail plus théorique relatif à l'analyse est donc développé dans la deuxième étape, lorsque le système est en place et que le coordonnateur a commencé à recevoir des comptes-rendus. Les deux étapes peuvent être résumées de la façon suivante : "générer des informations de qualité dans un OIRAS" et "extraire des informations de qualité d'un OIRAS".

Les cours pourraient être dispensés par la DGAC au personnel des compagnies aériennes pour promouvoir la normalisation de la transmission des informations aux compagnies, ou sous la forme d'un service général à l'industrie (du transport aérien civil).

6.1 Etape I : Générer des informations de qualité dans l'OIRAS

Voici une proposition portant sur 4 jours de formation pour apprendre aux coordonnateurs à répondre aux besoins de l'Etape I.

6.1.1 Objectifs du stage

A la fin du stage, les participants auront les connaissances, les compétences et les outils nécessaires pour mettre en place et gérer un OIRAS dans leur compagnie. En tant que chefs de projet OIRAS, ils devront aussi être en mesure de :

- convaincre leurs pairs et la direction de l'intérêt d'un OIRAS,
- obtenir le soutien du personnel et obtenir des ressources pour la mise en place d'un OIRAS,
- utiliser le système et son logiciel pour analyser et encoder les comptes-rendus d'incident,

- tenir à jour une base de données active sur les incidents,
- relater et partager les enseignements tirés (retour d'information et répercussion aux parties concernées).

6.1.2 Profil du stage

1. Introduction

- Présentez-vous et demandez à chacun ses motivations et ses attentes concernant la formation.
- Annoncez qu'à la fin du stage, chacun devra présenter sa *checklist* pour la mise en place et la gestion d'un OIRAS au sein de la compagnie, (à entreprendre dès qu'ils réintègreront leur compagnie).
- Montrez-leur quelques formulaires de compte-rendu, et un programme d'OIRAS installé sur des ordinateurs (pour stimuler leur curiosité)
- Expliquez la seule contrainte : apprendre à se servir du programme de l'OIRAS (être réaliste sur le travail du stage)
- Expliquez que le stage s'articulera autour de conférences et d'exercices pratiques destinés à aider les participants à trouver eux-mêmes par des séances créatives (*brainstorm*) toutes les idées possibles pour leur compagnie. Soulignez les aspects pratiques du stage.

2. Vendre le concept

[conférence]

Ce sera une présentation PowerPoint visant à démontrer comment les OIRAS contribuent à l'amélioration de la sécurité. Elle retracera l'évolution des Facteurs Humains dans l'aviation jusqu'à ce jour et illustrera l'idée que des individus et des organismes peuvent apprendre beaucoup à partir des erreurs commises, d'où l'avantage d'utiliser les systèmes de compte-rendu confidentiels comme moyens d'apprentissage et d'enrichissement de l'organisation.

Cette présentation sera le premier "outil" qu'ils pourront rapporter dans leur compagnie respective : elle leur sera donnée sur support papier et sous forme de fichier, avec le commentaire caché accompagnant les diapositives. Chaque stagiaire pourra l'adapter pour son propre usage dans sa compagnie, quand il devra convaincre ses pairs, d'autres services ou la direction de l'intérêt de disposer d'un OIRAS. Informez-les dès le départ de l'objet réel du diaporama pour qu'ils le découvrent en essayant d'avoir les mêmes dispositions d'esprit voire le même scepticisme que certains membres de la compagnie auxquels ils le soumettront.

3. Obstacle à la mise en place

[exercice de groupe]

Immédiatement après la présentation, les stagiaires feront une activité de groupe (ou par compagnie, en fonction du nombre de participants). « Si le projet d'installer un OIRAS est une si bonne idée, pourquoi peut-on avoir des difficultés à le faire accepter ? » Cette question leur fournit l'occasion d'exprimer toutes leurs inquiétudes, leurs réserves et leurs craintes sur leur future mission. Demandez-leur de penser globalement à l'aviation commerciale et plus spécifiquement aux conditions et comportements caractérisant leur compagnie. Demandez-leur de se montrer sceptiques, cyniques, revêches et réalistes, c'est-à-dire, d'imaginer les réactions d'opposition qu'ils risquent de devoir affronter à leur retour de stage. Les stagiaires seront d'autant mieux préparés à faire face à toute forme d'opposition, que les résistances simulées seront variées et radicales.

4. Que dois-je faire pour réussir la mise en place d'un OIRAS dans ma compagnie?

[exercice de groupe]

Incitez les stagiaires à raisonner en tant que Chefs de Projet. Cet exercice peut se faire sous la forme d'une séance créative (*brainstorm*) où ils énumèrent tout ce dont ils ont besoin (en termes de connaissances, compétences, moyens de soutien et ressources) pour surmonter les obstacles précités et mener à bien leur projet. Cet exercice devra aussi bien couvrir les questions théoriques que les petits détails pratiques. Aidez-les à jalonner les différentes étapes du processus et à mettre en lumière les

questions sous-jacentes (confiance et crédibilité pour convaincre leurs pairs qu'ils ne seront pas sanctionnés, convaincre la Direction que personne ne sera sanctionné, pour concevoir un formulaire, organiser sa diffusion et sa collecte, analyser les résultats, en tirer les leçons importantes pour l'organisation et diffuser l'information).

Cet exercice peut être analysé pour montrer que toutes les questions que les participants soulèvent, seront traitées au cours du stage.

5. Rendre compte d'un incident

[exercice individuel]

Demandez à chaque stagiaire de relater un incident qu'il a vécu personnellement ou en tant que témoin (comme copilote) et de faire partager cette expérience aux autres individus du groupe. Il y aura probablement quelqu'un qui demandera « quel genre d'incident voulez-vous que l'on décrive ? » Profitez-en pour orienter la discussion du groupe sur la définition d'un incident et sur la nature des incidents qui doivent être rapportés.

Vous pouvez rappeler l'objectif d'un OIRAS en soulignant qu'il est recommandé de rendre compte des événements susceptibles de permettre à l'organisation d'en tirer des enseignements et d'améliorer la sécurité.

Une fois que les participants ont fini de rédiger leur récit libre, distribuez des formulaires de compte-rendu existants et demandez-leur de reproduire l'exercice, cette fois-ci en remplissant les rubriques du formulaire. Demandez à des volontaires de lire leur récit, ainsi que le compte-rendu détaillé. Puis, lancez le débat et analysez les avantages et les inconvénients des deux styles de compte-rendu (par ex., un formulaire structuré exige plus d'informations). Dites-leur qu'ils devront concevoir leur propre questionnaire plus tard, quand ils seront mieux informés sur le type de données requises. Mentionnez brièvement la différence entre questionnaire confidentiel et questionnaire anonyme, et la nécessité d'utiliser une phraséologie standard.

6. Les besoins en bases de données

[conférence, vidéo et travaux pratiques]

Les stagiaires devront disposer d'un ordinateur portable pour bien comprendre cette séance. Discutez de la nécessité de disposer d'une base de données sur les incidents (entrer et sortir facilement des informations, stocker des données, compiler des rapports, etc...) et d'utiliser une phraséologie standard. Certains seront sans doute déjà familiarisés avec les bases de données et la gestion d'une base et pourront alimenter la discussion. Lorsqu'ils auront bien compris l'utilité des mots-clés normalisés dans une base de données (pour faciliter la saisie et la récupération des données), abordez la structure de la base de données d'un OIRAS.

Pour bien comprendre les catégories de la base de données, les participants devront avoir quelques notions sur les Facteurs Humains, notamment sur les approches système et écologique de la sécurité. Demandez-leur de regarder la vidéo et de noter tous les facteurs d'influence. Visionnez la vidéo sur l'accident de Dryden.

Posez des questions sur la vidéo en soulignant l'ampleur de l'enquête. Discutez de tous les facteurs d'influence, de la chronologie de l'accident et de la démarche pour remonter à l'origine de l'accident.
Introduisez le modèle de Reason et soulignez l'idée des défaillances. Discutez des caractéristiques d'adaptation du système. Indiquez-leur des passages supplémentaires à lire dans leur manuel : soulignez combien il est complexe de comprendre un incident/accident ; expliquez-leur qu'ils ne devront pas organiser une enquête très poussée chaque fois, mais que la notion des " informations pertinentes" va bien au-delà de ce qui s'est passé dans le poste de pilotage.

Rappelez-leur les deux principes essentiels à intégrer : "savoir tirer des leçons d'une erreur" et les approches système et écologique de la sécurité.

8. Base de données 1

[conférence et travaux pratiques]

Commencez par les familles d'incidents et les domaines de risque. Expliquez les termes en lisant la définition donnée dans le manuel avec eux et demandez-leur de citer si possible des exemples. Distribuez deux comptes-rendus d'incident et demandez leur de les classer.

Une fois qu'ils sont d'accord sur les catégories adéquates, aidez-les à saisir le compte-rendu dans le programme. Faites-leur démarrer le programme, saisir le compte-rendu et mettre quelques mots-clés en place. A ce stade, stimulez leur curiosité concernant la base de données et répondez à toutes leurs questions sur le système et sur son fonctionnement de base. Cela les rendra plus confiants à l'égard du système avant de passer aux mots-clés plus difficiles.

9. Mettre en place un OIRAS : créer le système, collecter les comptes-rendus

[exercice de groupe]

Première séance d'une série de trois, cette séance est consacrée à la première étape du Projet : promouvoir le système, établir sa crédibilité et créer un climat de confiance, collecter des comptes-rendus et les saisir dans une base de données. Les participants commenceront à travailler sur leur *checklist* pour la mise en place du système. En fonction du groupe, vous pouvez présenter vous-même les rôles et responsabilités du coordonnateur OIRAS ou faire une séance de *brainstorm* : le formateur pose des questions qui amènent les participants à penser à toutes les réponses et à l'ordre dans lequel elles devront être traitées (Faut-il commencer par obtenir les ressources physiques, établir un réseau de relations avec les autres services, promouvoir le projet dans le journal local, déterminer des rubriques du questionnaire ? Où faut-il mettre les formulaires ? A qui doivent-ils être adressés en retour ? Qui va m'aider ?!) Cette séance, très animée, doit permettre d'aborder des questions d'ordre pratique et inciter les participants à envisager clairement et en détail toutes les démarches. Tous ces points sont à consigner dans la *checklist* pour la mise en place de l'OIRAS.

10. Base de données 2

[conférence et travaux pratiques]

En utilisant le même plan que ci-dessus, expliquez les stratégies de gestion des risques, ainsi que les modes de défaillance et les modes de récupération. Reprenez les deux incidents que vous avez fait classer aux stagiaires auparavant et demandez leur de les classer dans les nouvelles catégories abordées. Faites la mise à jour du programme. Ajoutez deux autres incidents ; demandez aux stagiaires de les classer et de les entrer dans le système. A ce stade, les stagiaires devraient être tout à fait familiarisés avec le programme et capables de se concentrer davantage sur les mesures correctives.

11. Rappels

[Exercices]

Insistez bien sur le fait qu'il est indispensable de disposer des informations pertinentes pour pouvoir comprendre ce qui s'est passé. Attirez leur attention sur les différents points faibles du compte-rendu (biais, omissions, rapporteur sur la défensive...). Soulignez le besoin d'objectivité : pas de suppositions.

Si vous n'avez pas déjà abordé le sujet, démontrez clairement l'intérêt de la confidentialité des comptes-rendus plutôt que l'anonymat. Distribuez des comptes-rendus d'incident qui sont évasifs et/ou qui contiennent un biais ou sont insuffisamment détaillés. Par une séance de *brainstorm*, amenez-les à identifier la nature et la source (pilotes ou autres) des informations dont ils auront besoin. Les stagiaires peuvent éventuellement examiner des comptes-rendus d'incidents déjà analysés et déterminer si d'autres informations sont nécessaires ou non.

Bien qu'ils rendent certains stagiaires mal à l'aise, des jeux de rôles seraient très utiles dans ce contexte. Car il est parfois nécessaire d'être mis en situation pour réaliser combien il est difficile de mener une enquête en restant neutre et objectif. Les participants doivent aussi forger leur intuition et apprendre à reconnaître les comptes-rendus pour lesquels l'investigation gagnerait à être approfondie. Il s'agit principalement d'utiliser à bon escient les ressources consacrées à la recherche d'informations intéressantes.

12. Base de données 3

[conférence et travaux pratiques]

Reprenez le même plan que ci-dessus. Expliquez les catégories des Mesures Correctives et l'importance pour l'organisation du retour d'expérience. Reprenez les quatre cas d'incidents précités et terminez l'analyse. D'autres comptes-rendus d'incident peuvent être remis aux stagiaires, à leur demande, s'ils veulent s'entraîner chez eux.

Une fois qu'ils maîtrisent les catégories et le programme de base, les participants ont acquis le premier niveau de compétences.

13. Mettre en place un OIRAS :

[conférence et discussion]

Le système le plus crédible et la meilleure analyse sont peines perdues s'ils ne sont pas menés à bien de façon systèmatique .

C'est le moment de discuter du retour d'informations aux équipages et de la réinjection des informations recueillies à l'intention de l'organisation et des autres parties intéressées (avionneur, autres compagnies, autorités, contrôle aérien). Discutez des différents types de rapports et de la question de savoir qui devrait voir et/ou agir sur les informations. Parlez-leur de la possibilité de constituer une équipe opérationnelle composée de membres de différents services de la compagnie. En leur qualité de Chefs de Projets, les participants devront démontrer l'intérêt d'un OIRAS. Un succès précoce aidera à faire accepter le projet, notamment si toutes les parties concernées dans la compagnie ont été informées de la mesure prise et si cette mesure permet d'effectuer un changement réel.

Il convient de préciser ici que les stagiaires ne pourront pas devenir de fins analystes en l'espace de quatre jours. Nous pensons qu'ils prendront la mesure de "ce qu'ils ne savent pas" en matière de Facteurs Humains et d'analyse d'incidents grâce à des travaux pratiques sur une base de données. Plutôt que de les submerger de connaissances théoriques, nous estimons qu'il vaut mieux leur donner les bases, souligner les objectifs d'un OIRAS et leur donner la possibilité de faire un apprentissage empirique. Les stagiaires pourront commencer à participer à des conférences sur la sécurité, à s'impliquer dans un réseau avec d'autres analystes. Toutes ces activités seront encouragées. Des rubriques sur les moyens d'entretenir et d'actualiser leurs connaissances, pourront être ajoutées à leur *checklist* pour la mise en place du système.

14. Présentation des *checklists* pour la mise en place du système

[exercice]

Reprenez les exercices visant à "planter le décor : "obstacles à la mise en place" et "que dois-je faire pour réussir la mise en place d'un OIRAS dans ma compagnie ?". Donnez aux stagiaires le temps d'effectuer cela ; faites-leur remarquer que plus ils seront préparés lors de leur retour dans la compagnie, moins ils seront affectés par les déceptions et échecs éventuels du début. Les efforts d'anticipation et de préparation contribueront de façon déterminante à la définition d'une stratégie de mise en œuvre du système réaliste et à permettre un succès précoce.

Ensuite, chaque personne (ou groupe de personnes d'une compagnie) présentera sa *checklist* pour la mise en place du système. Les autres personnes du groupe pourront proposer des suggestions. Une fois que tous auront présenté et partagé leurs stratégies, le groupe disposera d'une *checklist* complète et étendue.

15. Conclusion
Vérifiez qu'ils se sentent prêts à démarrer le projet de mise en place d'un OIRAS. Dites-leur qu'ils peuvent vous contacter pour vous demander de l'aide ou un conseil. Assurez-vous que la liste des coordonnées des contacts est complète, avant de la distribuer. Cette liste de contacts doit inclure le personnel de la DGAC, les autres stagiaires et si possible d'anciens stagiaires. Vous pouvez y joindre aussi une liste avec les références d'ouvrages à lire et des adresses de sites sur le web.

Rappelez-leur que l'analyse d'incidents est une discipline requérant des compétences qui s'améliorent avec la pratique et par la formation.
Rappelez-leur enfin que le but de tout système de compte-rendu d'incidents est de promouvoir l'enrichissement de l'organisation par le retour d'expérience, de limiter les risques et d'améliorer la sécurité.
Souhaitez-leur bon courage.

6.1.3 Justifications de la formation

Plusieurs idées intégrées dans le profil de la formation, sont développées ci-après :

- Il faut encourager les stagiaires à penser à la fonction de Coordonnateur de la Flotte en tant que Chef de Projet : ils devront gérer un budget (ressources : des personnes, du matériel et le rapport argent/temps) ; un échéancier pour la mise en place et la gestion continue du système de compte-rendu ; un objectif ou plusieurs objectifs ; et ils devront être en mesure de démontrer l'efficacité du projet (à travers les statistiques et les mesures prises).
- Il est recommandé d'utiliser des séances créatives (*brainstorm)* dans les cas suivants:
  pour faire accepter le système au sein de la compagnie (leurs pairs, la direction, les services de formation ...etc.) ; il faudra aussi recourir à des présentations officielles, des publications par les compagnies, des notes, des affiches et à des réseaux informels.
- pour aborder la question des obstacles à la mise en place d'un OIRAS (pourquoi un OIRAS ne serait pas approprié dans leur compagnie) par ex.: le manque de confiance, l'insuffisance des ressources, pas assez de soutien de la direction, le système est incompris ou perçu comme inutile, je n'ai pas les compétences, je n'ai pas les moyens nécessaires. Cette démarche doit être faite très vite dans la formation (le matin du 1er jour ?) afin de mettre en évidence les craintes et préoccupations des stagiaires.
- pour décrire ce qu'il faut faire pour que le projet réussisse (ressources physiques et humaines). Cet exercice peut être fait plusieurs fois, au fur et à mesure qu'ils comprennent mieux le sujet. Une liste peut être affichée au mur, que les stagiaires compléteront chaque fois qu'ils penseront à un nouvel élément. Elle peut couvrir des aspects théoriques mais également des petits points pratiques (et il n'en manque pas!!)
- Il est recommandé d'utiliser une grande affiche pour représenter les grandes lignes du stage, avant d'aborder la théorie et les mots-clés. Si les cours sont jalonnés par des repères, les stagiaires ont davantage le sentiment de maîtriser le sujet : les thèmes abordés, ceux qui restent à traiter... Il faut se référer souvent à la grande affiche pour que les stagiaires replacent chaque nouvel élément dans son contexte.

6.2 Etape II: extraire des informations de qualité des OIRAS

Une fois que les coordonnateurs ont quelque expérience pratique avec un OIRAS et que l'exercice sur les comptes-rendus a été réussi, ils sont prêts à passer à la prochaine étape de la formation. Avec les comptes-rendus en mains, ils peuvent être formés à développer leurs compétences analytiques.

6.2.1 Objectifs du stage

A la fin de la formation, les stagiaires auront les connaissances, les compétences et les outils nécessaires pour extraire de la base de données de l'OIRAS un retour d'expérience très enrichissant pour l'organisation. En leur qualité d'analystes OIRAS, ils pourront :

- utiliser le programme de l'OIRAS pour analyser et classer des comptes-rendus,
- tenir à jour une base de données active sur les familles d'incidents et domaines de risques,
- dialoguer intelligemment avec la base de données,
- développer des hypothèses basées sur des événements isolés et répétés,
- aider les parties concernées à vérifier ces hypothèse à l'intérieur et à l'extérieur de l'organisation,
- servir de bureau central et de voie de communications pour les informations sur la sécurité,
- assurer la traçabilité des réponses apportées par l'organisation,
- évaluer l'efficacité de ces réponses.

6.2.2 Profil de la formation

Cette partie de la formation n'a pas été détaillée comme la première partie. Elle consiste principalement à revoir le contenu de la première partie et à approfondir les aspects théoriques ainsi que les problèmes de gestion de la base de données. Des études de cas plus complexes seront proposées et le formateur insistera davantage sur la communication des résultats et sur l'évaluation des renseignements ainsi exploités par l'organisation.

Les sujets suivants seront abordés :

- Théorie en matière de Facteurs Humains : la sécurité par l'invariance et la sécurité par l'adaptation,
- Représentation mentale et contrôle de la gestion des risques,
- OIRAS, des systèmes destinés à exploiter les données en vue d'enrichir les connaissances de l'organisation, et non à enquêter sur des mini-accidents,
- Gestion d'une base de données,
- Elaboration d'une hypothèse,
- Montage d'expériences à l'échelle de l'organisation afin de vérifier des hypothèses (enquêtes, audits),
- Extraction de statistiques résumées,
- Communication des résultats au sein de la compagnie,
- Envoi d'informations en dehors de la compagnie,
- Détermination des ressources à affecter aux enquêtes,
- Compréhension/identifier/tirer les leçons de l'expérience,
- Valeur du "contexte" et expertise interne,
- Comment contrôler et évaluer les réponses apportées par l'organisation,
- A qui s'adresser pour se faire aider (établissement d'un réseau)

7. Annexe A. Formulaire de compte-rendu confidentiel

2.1 Compte-Rendu Confidentiel

Coupon d'identification:

Pouvons-nous vous contacter ? Si oui, veuillez indiquer votre nom et votre numéro de téléphone:

Nom: **Tél:**

1. Date	**2. Heure locale/UTC**	**3. N° de vol**	**4. Enregistrement**
_____ / _____ / _____ Jour Mois Année	Jour / Nuit		

Ces informations sont confidentielles : elles seront retirées du formulaire et vous seront retournées. Il n'y aura plus aucune trace de votre identité

5. Type d'avion	**6. Ligne**	**7. Nombre de passagers**	**8. ETOPS**
	_____ - _____ / _____ De A Dérouté	_____ /_____	Oui / Non
9. Altitude _____ / _____ NV FT	**10. Aéroport le + proche, Aide à la navigation aérienne, ou point**	**11. ASR rempli** Oui / Non	**12. Réf Tech Log** ____ / ____ / _____ Secteur réf. Log . N° Item

13. Météo	**14.** Conditions significat.:modérées/ sévères	**15. Configuration**
IMC VMC _____km	Pluie - Neige - Givre - Brouillard – Turbulences - Grêle – Piste contaminée – Vent cisaillant	Pilot A. / A. Thrust / Train /Volets / Spoilers _____

16. Rapporteur	**17. Temps de vol**	**18. Phase de vol**
☐ Commandant de bord ☐ Co-pilote O Pilote en Fonction O Pilote Non en Fonction ☐ Autre membre de l'équipage	Total _____ heures 90 derniers jours _____ heures Sur ce type d'avion_____	remorquage – stationnement – avion poussé – roulage départ – décollage – montée initiale (< 1500ft) – montée – croisière – descente – attente – approche (< 1500ft) – atterrisage – roulage arrivée

QUE S'EST-IL PASSE ? (décrivez brièvement l'événement, en mentionnant toute information susceptible de nous aider à comprendre totalement l'événement rapporté : par ex.: conditions météo, problèmes techniques, équipage, SOP, aménagement de la piste).

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_ **RISQUE POTENTIEL** associé à cet événement : qu'aurait-il pu se passer si la situation n'était pas revenue à la normale ?

QUE S'EST-IL REELLEMENT PASSE? (décrivez dans quelles circonstances la ou les défaillances ont évolué jusqu'à occasionner un incident, par ex. : problème technique, formation insuffisante de la formation, procédures inadéquates ou mauvaises, réglementation, coordination de l'équipage).

COMMENT LE PROBLEME A-T-IL ETE REGLE ? (décrivez les mesures que vous avez prises entre le moment où vous avez pris conscience du problème et celui où vous avez repris le contrôle intégral du vol. Mentionnez toutes les aides dont vous avez bénéficié.)

VOS RECOMMANDATIONS SUR LA SECURITE : A votre avis, à qui devrait-on rendre compte de cet incident (aux pilotes de cette flotte, au chef pilote, à tous les pilotes de la compagnie, aux instructeurs/formateurs, à la direction de la compagnie, au Département de Sécurité, aux services chargés des standards, aux services de maintenance, à ceux des opérations sol, à l'équipage commercial, aux autres compagnies desservant les mêmes lignes, au contrôle aérien (ATC), aux autorités aéroportuaires, aux autorités de l'aviation) ?