Version provisoire

Images et Modèles Mentaux
Conscience de la Situation
Situational Awareness

Pierre Lecomte
Jean-Claude Wanner
Octobre 2003

Ne pas commettre trop d'erreurs exige une grande expérience. L'expérience ne s'acquiert qu'en commettant beaucoup d'erreurs ou en profitant des erreurs des autres.

Philosophe grec anonyme du IV^{ème} siècle AVJC.

C'est une erreur de croire que toutes les fautes ne sont que des erreurs, mais c'est une faute grave de croire que toutes les erreurs sont des fautes.

Frère Jehan d'Héturbine (1606 - 1669)

The meteor which had struck the oxygen tank of the spaceship "Star Queen" was a giant, being nearly a centimeter across and weighing all of ten grammes. According to the table, the waiting-time for collision with such a monster was of the order of ten to the ninth days - say three million years. The virtual certainty that such an occurrence would not happen again in the course of human history gave the crew very little consolation.

Le météore qui avait détruit le réservoir d'oxygène du vaisseau spatial "Star Queen" était un géant, d'au moins un centimètre de diamètre et pesant au moins dix grammes. En se référant aux tables, le temps moyen entre deux collisions avec un tel monstre, était de l'ordre de dix puissance neuf jours, soit trois millions d'années. La certitude virtuelle qu'un tel événement ne se reproduirait pas au cours de l'histoire de l'humanité ne donnait qu'une faible consolation à l'équipage.

Extrait de la nouvelle de science fiction "Breaking Strain, expedition to Earth"
de Arthur Clarke, membre de la Royal Astronomical Society

Avec les précautions que nous proposons, nous ne rendrons pas les explosions impossibles parce que la chose n'est pas au pouvoir de la science; mais nous les rendrons rares et d'un dommage limité. Nous sommes partis de ce principe que tout moyen mécanique entraîne avec lui ses dangers, et qu'il suffit que ces dangers ne dépassent pas une chance de probabilité très faible pour qu'on doive, nonobstant leur possibilité, continuer d'employer les procédés d'industrie qui les font naître.

Laplace, Prony, Ampère, Girard et Dupin
Rapport à l'Académie des Sciences 14 avril 1823

Si tu laisses la porte fermée à toutes les erreurs, la vérité n'entrera pas.

Rabindranâth Tagore

Il n'y a rien de plus difficile à entreprendre, de plus périlleux à poursuivre et de plus incertain à réussir que d'introduire un nouvel ordre des choses, car l'innovateur a pour adversaires tous ceux qui ont réussi dans les conditions anciennes et ne trouve qu'une aide tiède auprès de ceux qui pourront réussir dans les nouvelles.

Nicolo Machiabelli (1469 - 1527)

Ce n'est pas parce que l'on est un bon opérateur que l'on ne commet pas d'erreurs. Ce n'est pas parce que l'on a commis une erreur que l'on n'est plus un bon opérateur.

Variations sur une pensée d'Elie Wiesel

Ne pas frapper de dérision les actions humaines, ne pas les déplorer, ne pas les maudire, mais les comprendre.

Spinoza

Sommaire

La société CINQDEMI a mené depuis de nombreuses années des recherches visant à mieux comprendre les incidents et les accidents aériens et a développé une méthode permettant une analyse en profondeur des événements en cause. Cette méthode a semblé intéressante au personnel de la NASA et de l'Institut Batelle impliqué dans le recueil et l'analyse des données de la base ASRS

A la demande de la NASA plusieurs expérimentations ont été menées pour appliquer la méthode d'*Analyse* de CINQDEMI à divers échantillons extraits de la base de données ASRS. Ces expérimentations ont été en général couronnées de succès en montrant que la méthode était capable de mettre en relief l'essence et les principaux événements d'un incident et d'indiquer dans quels domaines il serait judicieux d'agir pour améliorer la situation afin d'accroître la sécurité du transport aérien.

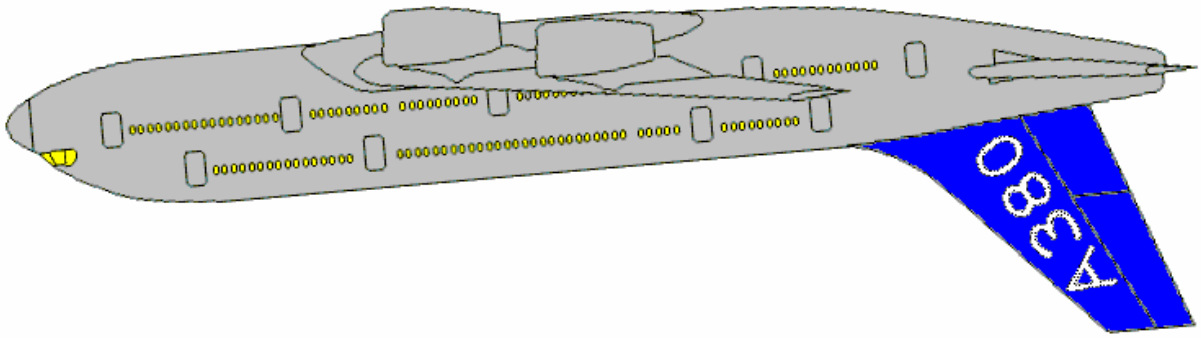
Mais extraire de la base ASRS des sous ensembles rassemblant des incidents présentant des similarités pour essayer d'identifier des précurseurs éventuels à des situations potentiellement dangereuses, resta un problème non réellement résolu.

CINQDEMI développa alors dans ce but, une méthode de *Codification,* dans l'esprit de la méthode d'Analyse. Cette méthode rencontra un certain succès, mais le facteur d'erreur, dit "Erreur de Représentation" apparut très dominant et ne constituant pas un critère suffisant pour échantillonner correctement la base de données. Il apparut nécessaire de le compléter par deux sous critères dits "*scénario*" et "*domaine d'erreur de représentation*".

Le Docteur Irving Statler de la NASA, attira alors notre attention sur le concept de "Situational Awareness" que nous proposons de traduire par "Conscience de la Situation". En creusant cette suggestion il apparut que "Conscience de la Situation" et "Erreur de Représentation" étaient des concept presque équivalents (dans le sens négatif, une Erreur de Représentation se traduisant par une Conscience Erronée de la Situation.). Par ailleurs la notion de "Conscience de la Situation" est mieux connue et mieux comprise par les opérationnels.

Le présent document décrit une étude visant à utiliser cette équivalence pour adapter les précédentes méthodes de CINQDEMI. L'ancienne méthode de *Codification* était une approche montante ("bottom-up"), alors que l'utilisation du concept de Conscience de la Situation, nous a conduit à une approche descendante ("top-down"). Cette méthode est probablement plus facile à utiliser et plus encline à favoriser la définition des sous critères améliorant le processus de codification et par là même conduire à un meilleur échantillonnage de la base de données. La nouvelle méthode d'*Analyse* restera "descendante", mais utilisant les concepts dérivés de l'approche Conscience de la Situation, elle sera sans doute plus facile à appliquer.

Sont rappelés en Annexe les définitions de quelques termes utiles, la présentation des modèles utilisés par les opérateurs et les grilles utiles à la codification et à l'analyse.



Tout baigne, sauf, peut-être un léger dérèglement de l'horizon artificiel !

Les représentations mentales

Les opérateurs (membres de l'équipage, contrôleurs, mécaniciens au sol,..) utilisent des images et des modèles mentaux pour piloter la machine ou le système dont ils ont la charge. Dans ce qui suit, nous appellerons Machine le système contrôlé par l'opérateur (c'est l'avion lui-même pour l'équipage, la cabine passager pour le personnel navigant commercial, le trafic aérien pour le contrôleur,..)

A/ Images mentales.

Elles doivent être divisées en deux sous types.

a/ Image du monde extérieur à la Machine que nous noterons Ext Image.

Position, par rapport à l'avion, des aérodromes, des waypoints, des balises radio, du relief, de la piste.

Position par rapport à l'avion des autres avions.

Position par rapport à l'avion des systèmes nuageux.

Au sol, position, par rapport à l'avion, des pistes, des taxis ways, de l'aire de stationnement, des autres avions…

Interlocuteurs extérieurs disponibles (contrôleurs aériens, équipages des autres avions, personnels au sol de la compagnie, mécaniciens de piste..).

b/ Image du monde intérieur à la Machine que nous noterons Int Image.

Paramètres de vol (incidence, assiettes, altitude, vitesse conventionnelle, cap, route,..).

Configuration géométrique de l'avion (train, volets, becs,..).

Etat des systèmes (moteur, APU, autopoussée, pilote automatique, FMS, système de transfert de combustible, pressurisation,..). Ces états sont "marche", "arrêt", "plein", "vide", partiellement ou totalement "en panne",..)

Paramètres de réglage des systèmes (Nombre de tours ou EPR des moteurs, valeurs sélectées des paramètres du pilote automatique, température sélectée du conditionnement d'air,..).

Interlocuteurs internes disponibles (pilote, copilote, mécanicien, équipage commercial, passagers,..).

Les exemples que nous avons donnés sont valables pour un équipage. Elles peuvent être étendues et généralisées pour les contrôleurs, le personnel de piste, le personnel de maintenance,

A tout moment, l'opérateur bâtit une Image Externe, notée Ext P Image, de l'état actuel du monde extérieur, une Image Interne, notée Int P Image, de l'état actuel du monde intérieur (nous utilisons P pour Présent). Dans ce but il recueille les informations disponibles au travers des différentes interfaces (voir paragraphe 2 ci-dessous).

Au début de chaque sous phase de la mission, l'opérateur bâtit une Image Externe et une Image Interne, notées Ext D Image et Int D Image (D pour Désirée) correspondant à l'objectif de la tâche défini par des valeurs particulières des paramètres de vol (avec des écarts acceptables), valeurs qui doivent être atteintes à l'issue de la sous phase. Là encore nous avons pris l'exemple de l'équipage. Il est possible de généraliser cette notion pour les autres types d'opérateurs.

Les D Images sont bâties à partir des P Images en utilisant des Modèles de Tâche (voir paragraphe 3).

Enfin l'opérateur bâtit un certain nombre d'Images Externes ou Internes, notées Ext F Image et Int F Image (F pour Future) correspondant à la réponse de la Machine et de ses systèmes à différentes actions potentielles sur les commandes (réponse à la question "What if ?", "Que se passera-t-il si ?"). Notons que parmi les actions potentielles l'un d'elles est "ne rien faire".

Les F Images sont bâties à partir des P Images en utilisant des Modèles de Fonctionnement des Systèmes (voir paragraphe 4).

Le nombre des actions potentielles est limité par les connaissances de l'opérateur reposant sur l'expérience acquise en opération, la formation et l'entraînement initial.

B/ Modèles Mentaux.

1/ Modèles d'Interfaces qui peuvent être divisés en deux sous types.

1.a Interface Système

- ⇨ Recueil de données
  - ⇨ Modèle de localisation des sources d'information qui aide l'opérateur à diriger son capteur en général l'œil, parfois l'oreille (pour la capture d'un message) ou une main, un pied, un doigt (pour la capture d'un effort) dans la direction où le paramètre à relever est présenté.
  - ⇨ Modèle d'identification des sources d'information qui aide l'opérateur à reconnaître la source par sa forme, sa couleur, son étiquette.
  - ⇨ Modèle de transposition de l'information qui aide l'opérateur à transformer l'information recueillie en un message utilisable par le cerveau (échelles, sens de variation, position du zéro, signification des symboles, codes de couleur, etc.).
- ⇨ Action sur les commandes
  - ⇨ Modèle de localisation des commandes qui aide l'opérateur à diriger sa main, son pied ou son doigt vers la commande choisie.
  - ⇨ Modèle d'identification des commandes (forme, couleur ou étiquette) qui aide l'opérateur à vérifier qu'il a bien saisi la commande désirée.
  - ⇨ Modèle d'action des commandes qui aide l'opérateur à manipuler la commande (pousser, tirer, lever, tourner à droite, loi d'effort..) afin d'obtenir l'effet désiré sur le système

1.b Interface de communication

- ⇨ Réception de données
  - ⇨ Modèle d'action des commandes de communication qui aide l'opérateur à manipuler les commandes de réception.
  - ⇨ Modèle de localisation et d'identification des émetteurs.
  - ⇨ Modèle de transposition des messages qui aide l'opérateur à comprendre le message et en déduire la tâche à entreprendre en utilisant un Modèle Général de Tâches.

⇨ Transmission de données
  ⇨ Modèle d'action des commandes de communication qui aide l'opérateur à manipuler les commandes de transmission.
  ⇨ Modèle de localisation et d'identification des récepteurs.
  ⇨ Modèle d'élaboration des messages.

L'opérateur est un membre de l'équipage, un contrôleur de trafic aérien, un mécanicien de piste ou un mécanicien de maintenance.

Les Modèles d'Interface sont mis en mémoire lors de l'entraînement initial et peuvent être modifiés ou améliorés par l'expérience.

Les différents Modèles d'Interface sont décrits en détails dans l'Annexe 2 en fin de document.

2/ Modèles de Tâches

La mission de l'opérateur peut être divisée en phases et sous phases. A chaque sous phase correspond une tâche donnée. Généralement une tâche est définie par des valeurs des paramètres de vol (avec des écarts acceptables) que l'opérateur doit atteindre à la fin de la sous phase. Cette liste de paramètres constitue le Modèle de Tâche lié à la sous phase. Ces paramètres sont donnés dans les procédures de vol ou imposés par le contrôle.

Les Modèles de Tâche aident l'opérateur à bâtir les D Images (Images Désirées) correspondant à chaque sous phase.

3/ Modèles de Fonctionnement des Systèmes

Ces modèles décrivent comment fonctionnent les systèmes. Ils sont utilisés pour prévoir la réponse d'un système à une action donnée sur une commande. Ils peuvent être plus ou moins approfondis. Trop approfondis ils sont difficiles à être utilisés rapidement, trop simplistes ou incomplets ils peuvent conduire à une prévision erronée.

L'un de ces modèles est très important. C'est le Modèle de Mécanique du Vol qui est utilisé pour prévoir la trajectoire future résultant de l'action sur une commande (ou d'une action nulle) ou résultant d'une perturbation atmosphérique.

Les pilotes d'avion ont seulement à se mettre en mémoire le modèle de Mécanique du Vol de leur propre avion avec ses performances disponibles.

Les contrôleurs aériens doivent se mettre en mémoire les Modèles de Mécanique du Vol, limités aux performances, de tous les avions qu'ils ont à contrôler. Rappelons que les performances d'un avion de tourisme à hélice sont très différentes de celles d'un avion d'affaire ou d'un transport lourd de passagers.

Parmi les exemples de Modèles de Fonctionnement nous pouvons citer :

Le modèle donnant l'intervalle de temps entre la mise sur "sortie" de la commande de train et la sortie effective du train.
Le modèle aidant le mécanicien navigant à gérer le système de carburant.
Le modèle aidant le mécanicien navigant à gérer le système de pressurisation et de conditionnement d'air.

Le modèle de fonctionnement du pilote automatique donnant le résultat de la mise en service des différents modes.

Le modèle de fonctionnement du pilote automatique donnant les diverses conditions de réversion de modes.

Le modèle de fonctionnement du FMS permettant au pilote de modifier le plan de vol, d'introduire des contraintes, d'entrer une nouvelle piste de destination,…

Les F Images qui sont prévues au travers de ces modèles, sont utilisées pour déterminer les actions à entreprendre afin d'atteindre l'objectif de la sous phase, c'est-à-dire d'atteindre les D Images.

Les Modèles de Fonctionnement des systèmes reposent sur l'application des lois de la Mécanique et de la Physique. Ils ne doivent pas être confondus avec les Images d'Etat des Systèmes qui sont une partie des Int Images et par la même varient avec le temps.

Les Modèles de Fonctionnement des systèmes sont mis en mémoire au cours de la formation initiale et peuvent être modifiés ou améliorés par l'expérience.

4/ Modèles de Risque

Ces Modèles aident l'opérateur à évaluer le risque lié à la situation présente (donnée par les Ext P et Int P Images) et le risque lié à la situation prévue (donnée par les Ext F et Int F Images). L'objectif d'une décision d'action est de remplir la mission et de minimiser le risque.

L'élaboration des Modèles de Risque dans l'esprit de l'opérateur repose sur la formation initiale et sur sa propre expérience. Très souvent l'expérience vécue conduit à minimiser le sentiment de risque parce que les opérateurs pensent avoir rencontré suffisamment d'événements sans incidents les poussant à conclure à l'absence de risque.

"J'ai volé à basse altitude pendant de nombreuses heures sans le moindre problème. Le vol rasant n'est donc pas dangereux !"

"J'ai atterri des dizaines de fois avec une vitesse supérieure de quarante nœuds à la vitesse recommandée. Je me suis très souvent posé sur des pistes inondées sans difficultés. Je me suis déjà posé sur des pistes courtes. Par suite il n'y a aucun problème à me poser sur une piste courte et mouillée avec quarante nœuds de trop au badin"

Ainsi la représentation mentale de la situation est faite d'Images (Externes, Présente, Future ou Désirée, Internes, Présente, Future ou Désirée) et de quatre types de Modèles (Modèles d'Interfaces, Modèles de Fonctionnement des Systèmes, Modèles de Tâche et Modèles de Risque)

.

Une erreur sur la représentation mentale conduit à une

" Conscience Erronée de la Situation"

Nous avons pendant longtemps parlé d'Erreurs de Représentation.

Une erreur de Représentation conduit à une Conscience Erronée de la Situation.

Comme le concept de Conscience de la Situation semble plus compréhensible par les opérationnels, il est sûrement utile de s'y référer plutôt qu'au concept d'Erreur de Représentation.

D'après Lucky Luck et les frères Dalton

Exemple typique d'erreur de représentation ou de conscience erronée de la situation.

Types de Conscience Erronée de la Situation

Il y a cinq types de Conscience Erronée de la Situation

A/ **Une Image Présente, Externe ou Interne, est erronée** ce qui conduit à une mauvaise décision d'action ou à une mauvaise estimation de l'Image Future.

Par exemple, le pilote pense qu'il a déjà dépassé la colline dans l'axe de la piste alors que cette colline est encore devant et il commence sa descente trop tôt.
Le contrôleur pense, à tort, qu'il n'y a pas de trafic sur la piste en service et il donne l'autorisation d'atterrir sur cette piste.

Les origines d'une mauvaise Image Présente sont multiples. La liste donnée ci-dessous est loin d'être exhaustive. Elle ne donne que quelques exemples.

⇨ Utilisation d'un mauvais Modèle d'Interface (Type 1) en lisant un paramètre ou en recevant un message.
Le pilote lit le jaugeur du réservoir 3 au lieu du jaugeur du réservoir 2 (Modèles de Localisation et d'Identification).
Utilisant une mauvaise échelle, le pilote lit niveau de vol 250 au lieu de niveau de vol 150.
Le pilote écoute un message du contrôle à destination d'un autre avion, pense qu'il en est le destinataire et se croit autorisé à atterrir (Modèle d'Interface de Communication).
Le commandant de bord donne un ordre au copilote et pense que le message a été correctement reçu (Modèle d'Interface de Communication).

⇨ Une trop grande Charge de Travail empêche l'opérateur de remarquer la dérive d'un paramètre et l'empêche d'entendre un message.
Etant accaparé par la programmation du FMS, le pilote ne remarque pas que l'avion dépasse le niveau 100 en descente alors que la vitesse est maintenue à 300 kt.
Pilotant l'avion manuellement en turbulence élevée, le pilote n'entend pas un message du contrôle lui demandant un changement rapide de niveau de vol.

⇨ Une chute de Vigilance, due à une Charge de Travail trop faible, empêche l'opérateur de remarquer la dérive d'un paramètre et l'empêche d'entendre un message.

⇨ Un Lapsus visuel conduit à une lecture erronée (en lecture rapide un "8" est pris pour un "3"). Un Lapsus auditif conduit à une mauvaise réception d'un message (le pilot entend "SIX" au lieu de "DIX" ou "NINE" au lieu de "FIVE") . Un Lapsus manuel conduit à taper "Y" au clavier au lieu de "T".

Il nous faut noter qu'un trop forte Charge de Travail, une trop faible Vigilance ou un Lapsus, peuvent conduire à une mauvaise Image, mais peuvent aussi engendrer d'autres types d'erreurs, par exemple une perte de contrôle au cours

d'un décollage avec panne de moteur en atmosphère très turbulente ce qui n'est pas une condition de Conscience Erronée de la Situation. Comme autre exemple un Lapsus conduisant à l'atterrissage à activer le frein de détresse à la place du parachute de freinage (les deux commandes sont côte à côte) conduit à une catastrophe immédiate. Une chute extrême de la Vigilance, par exemple absence des pilotes du cockpit ou pilotes assoupis, peut aussi conduire à la catastrophe (voir page 20).

Ainsi la Conscience Erronée de la Situation n'est pas le seul facteur d'erreur.

B/ **Une Image Future, Externe ou Interne, est erronée** ce qui conduit à une mauvaise décision d'action.

Par exemple, le pilote pense que les performances de l'avion sont suffisantes pour monter rapidement et éviter le sommet de la colline.

Le contrôleur pense que son ordre de décollage va être immédiatement suivi d'effet et qu'en conséquence la piste sera rapidement disponible pour un atterrissage.

Ici encore les origines d'une mauvaise Image Future sont multiples. La liste donnée ci-dessous est loin d'être exhaustive. Elle ne donne que quelques exemples.

⇨ Erreur sur l'Image Présente ce qui évidemment conduit à une erreur sur l'Image Future (pour mémoire, une telle erreur étant à classer dans la catégorie précédente).

⇨ Une Charge de Travail trop élevée amène l'opérateur à rater ou à oublier une action sur une commande.

Le pilote, surchargé, a sélecté une mauvaise altitude sur le pilote automatique, niveau de vol 100 au lieu de 200 et il pense que l'avion va stopper la descente au niveau 200.

Ayant à contrôler un trafic très dense, le contrôleur oublie d'envoyer un message demandant à l'un des avions de changer de niveau et il pense que cet avion va rapidement se trouver à un niveau assurant la sécurité.

⇨ Utilisation d'un mauvais Modèle de Fonctionnement.

Mauvais Modèle de Fonctionnement du FMS.

Le pilote pense que le FMS va exécuter une décélération de 300 à 250 kt une fois atteint le niveau 100 en descente (certains FMS sont programmés pour exécuter cette manœuvre mais ce n'est pas le cas général).

Le pilote a introduit une contrainte dans le FMS mais il ne sait pas qu'une modification de la piste en service, par exemple, efface cette contrainte.

Mauvais Modèle de Mécanique du Vol conduisant à une erreur sur la trajectoire future.

Le pilote pense pouvoir atteindre l'altitude demandée par le contrôle au prochain way point mais la vitesse verticale nécessaire est supérieure à la vitesse verticale disponible.

Le contrôleur pense que l'avion va rejoindre le prochain way point dans cinq minutes, mais il n'a pas pris en compte un fort vent de face.

Mauvais Modèle de Fonctionnement du Pilote Automatique

Le pilote ayant sélecté le mode "Vertical Speed" pense que la vitesse verticale restera maintenue, même à haute altitude.

Mauvais Modèle de Fonctionnement des systèmes avion (système hydraulique, freins, circuit carburant,..)

Le pilote pense que la décélération au sol sera nominale après l'atterrissage alors que l'un des systèmes hydraulique est en panne ce qui réduit les possibilités de freinage.

C/ Utilisation d'un **mauvais Modèle de Tâche** conduisant à une mauvaise Image désirée.

Une mauvaise définition des responsabilités de l'équipage ou une mauvaise définition de la répartition des tâches entre les membres de l'équipage ou entre l'équipage et le contrôleur peuvent conduire à des erreurs sur le choix du Modèle de Tâche et par la même à une erreur sur une Image Désirée.

Par exemple,

- ⇨ L'équipage pense que le contrôle a la responsabilité d'assurer l'anticollision avec le relief alors que le contrôle pense que son rôle se réduit à assurer la sécurité vis-à-vis du trafic.
- ⇨ Le commandant de bord pense que le copilote observe visuellement le trafic alors que celui-ci pense que sa seule tâche est la programmation du FMS.
- ⇨ Le pilote pense que la hauteur de décision est de 100 ft alors qu'elle est de 300 ft sur cette piste spécifique.
- ⇨ Le pilote pense qu'il doit virer à gauche après le décollage alors qu'il doit virer à droite sur cette piste spécifique.
- ⇨ Le calcul des vitesses de décollage a conduit à une erreur sur la vitesse V1. Les origines de cette erreur peuvent être multiples, mauvaise lecture d'un abaque ou d'une table, mauvaise évaluation de la masse au décollage (erreur de lecture des jaugeurs, erreur sur la fourniture du combustible), changement de piste au dernier moment proposant une piste plus courte et l'équipage ne reprenant pas le calcul, etc.
- ⇨ Changement tardif de piste à l'atterrissage nécessitant une manœuvre de changement de cap trop près du sol.
- ⇨ Au cours d'une présentation dans un meeting aérien, vol à basse altitude au voisinage de la vitesse de décrochage.
- ⇨ Au cours d'un vol commercial le commandant de bord se consacre à la formation de son jeune copilote et en oublie d'effectuer ses propres tâches.

D/ Utilisation d'une **Image "a priori"**

L'opérateur ayant exécuté ou croyant avoir exécuté une séquence d'actions décidées au temps T_1, bâtit au temps T_2 une Image Présente identique à l'Image Future qu'il avait prévue au temps T_1 ou qu'il avait bâtie à la suite d'observation d'événements entre les temps T_1 et T_2. Il ne vérifie pas l'exactitude de cette Image ou ne vérifie que les paramètres qui confirment cette prédiction.

Par exemple le pilote a placé sur "Sorti" la palette de train. Il suppose quelques instants plus tard que le train est effectivement sorti et il ne le vérifie pas.

D'après Roger Bollen Ces dingues d'animaux

Le contrôleur a donné quelques vecteurs radar successifs. Ces vecteurs ont été mentalement enregistrés par le pilote qui se bâtit une fausse Image de la position en plan de l'avion. Le pilote ne vérifie pas la position de l'avion ou il vérifie seulement les quelques paramètres qui confirment son hypothèse (le relèvement d'une balise est correct, mais non la distance et le pilote ne prend en compte que le relèvement).

Ce type d'erreur a été qualifié de "diabolique" parce que l'opérateur persiste dans son erreur et n'a aucun doute sur la validité de l'Image Présente. La persistance est toujours présente dans ce type d'erreur mais n'en est pas caractéristique. Par exemple un mauvais recueil de données peut conduire à une Image Présente erronée. Généralement il n'est pas évident pour l'opérateur de mettre en doute la validité de sa lecture et l'erreur persiste là aussi.

Ce qui est réellement caractéristique de l'erreur "diabolique" c'est la construction d'une Future Image "a priori" avec refus ou fausse interprétation des informations qui pourraient aider l'opérateur à mettre en doute la validité de son Image.

Aussi proposons nous d'abandonner le terme "diabolique" et de n'utiliser que le terme "Modèle a priori" pour caractériser ce type de Conscience Erronée de la Situation.

E/ Utilisation d'un mauvais **Modèle de Risque**

L'opérateur a en tête des Images Présentes et Futures exactes, mais il n'évalue pas correctement le risque associé à ces situations.

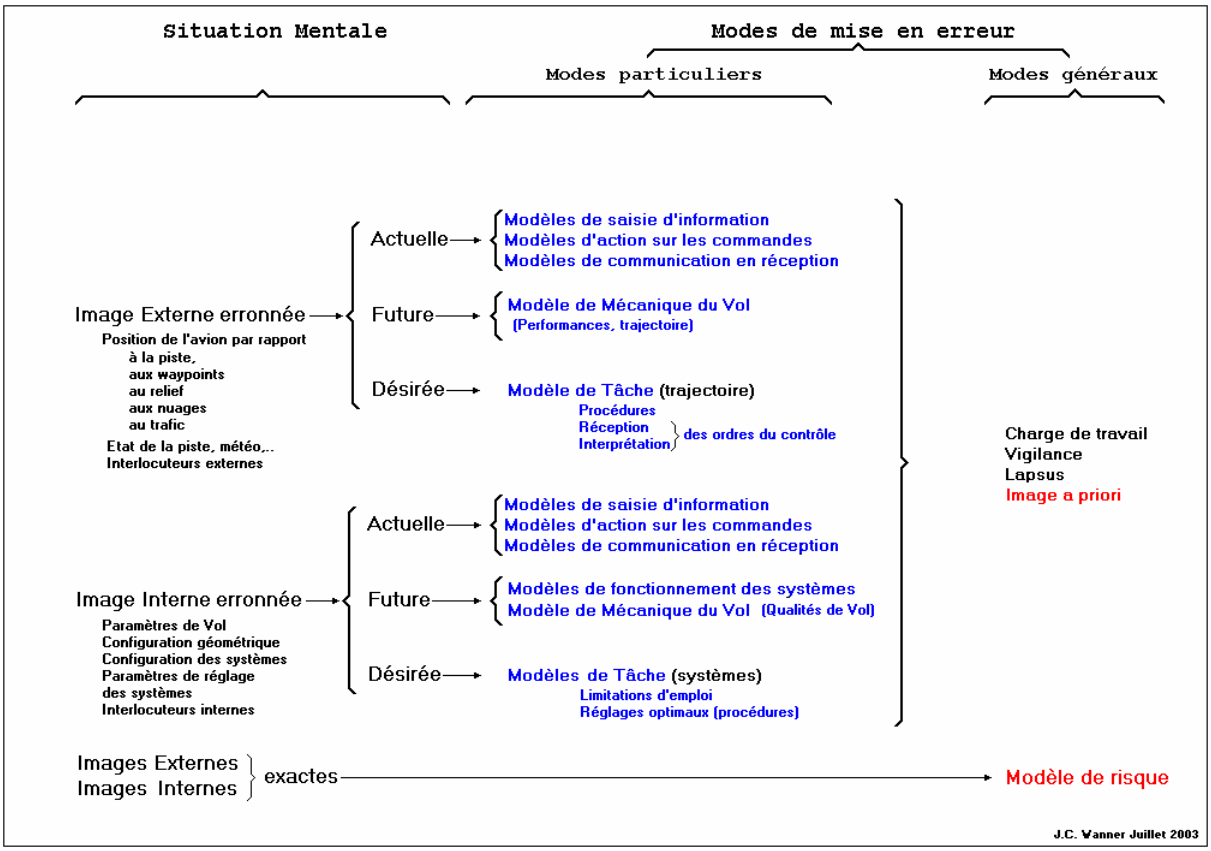
Par exemple, la vitesse d'approche est de cinquante nœuds supérieure à la vitesse recommandée, la piste est courte et mouillée. Le pilote, parfaitement au courant de la situation, décide quand même d'effectuer l'atterrissage pensant qu'il n'aura aucune difficulté à stopper l'avion dans les limites de la piste.

Dans ce cas il est souvent très difficile de faire la différence entre l'utilisation d'un mauvais modèle de risque ("*La distance d'atterrissage est certainement accrue mais je suis suffisamment adroit pour poser l'avion juste au seuil de piste et stopper l'avion avant le bout de piste*") et l'utilisation d'un mauvais modèle de Mécanique du Vol conduisant à une mauvaise estimation de la longueur d'atterrissage.

Autre exemple, la vitesse verticale ne permet de passer le sommet de la colline qu'avec une marge de cent pieds. "*La marge est largement suffisante*". Mais le pilote ignore la présence d'une antenne de télévision au sommet.

Les nuages sur la route sont épais et très noirs avec de nombreux éclairs. Mais le pilote ne change pas de cap ou d'altitude, estimant, de par sa propre expérience, que la turbulence sera acceptable et moins dangereuse que signalée dans les manuels.

La planche suivante résume les situations mentales de l'opérateur et les différents modes d'erreur associés conduisant à une Conscience Erronée de la Situation.



.

.

Méthodes de Codification et d'Analyse

Pour chaque rapport d'incident, nous envisageons deux niveaux d'étude associés à deux différentes méthodes.

Niveau Codification

Il faut noter que le niveau Codification a pour seul objet de fournir des moyens et des critères permettant d'extraire d'une base de données des sous ensembles présentant des similarités afin d'identifier des problèmes opérationnels significatifs et de dégager d'éventuels événements précurseurs. Une fois obtenu un sous ensemble de taille raisonnable par tri automatique, il est alors possible d'entamer des Analyses détaillées.

Dans ce but, le processus de Codification doit être relativement simple à appliquer par du personnel connaissant les systèmes aéronautiques et ne doit exiger qu'un minimum de temps d'exécution.

La méthode de Codification consiste à choisir l'une des rubriques suivantes :

1 - Est-ce que l'un des Facteurs d'Augmentation du Risque (de la liste GARE, voir Annexe 3, page 57) est d'une importance telle qu'il constitue l'explication quasi unique de l'incident ? (par exemple, fatigue ou malaise tels que l'opérateur est dans une situation où il ne peut pratiquement pas agir). Un tel cas doit être explicite.[1]

2 - Est-ce que le principal Facteur d'Erreur est une Charge de Travail extrême ?
Ce cas ne doit être retenu que si la Charge de Travail est si élevée que l'opérateur ne peut exécuter sa tâche tout en ayant une conscience parfaite de la situation. Ce cas doit être explicite ou évident implicite.[2]

3 - Est-ce que le principal Facteur d'Erreur est une Chute de Vigilance extrême ?
Ce cas ne doit être retenu que si l'équipage est totalement hors service, aucun pilote dans le cockpit, équipage en train de dormir ou perturbé par un événement extérieur retenant totalement leur attention. Ce cas doit être explicite ou évident implicite. [2]

4 - Est-ce que le principal Facteur d'Erreur est un Lapsus verbal, oral ou gestuel ayant un effet quasi immédiat et évident ? (langue ayant manifestement fourché, maladresse telle qu'un mouvement malheureux de manchette vient couper un moteur). Ce cas doit être explicite ou évident implicite. [2]

[1] Explicite signifie que le rapporteur a formellement cité le cas.

[2] Evident implicite signifie que le rapporteur n'a pas cité formellement le cas, mais que la lecture du rapport ne laisse aucun doute sur sa réalité.

5 – Si aucune des rubriques 1 à 4 n'a été retenue, nous sommes en présence d'un cas de Conscience Erronée de la Situation.

Ce cas doit être divisé en trois sous rubriques :

5.1 – Image Externe erronée

La Conscience Erronée de la Situation est relative à la situation extérieure (position de l'avion, météo, état de la piste, autres trafics,etc.)

5.2 – Image Interne erronée

La Conscience Erronée de la Situation est relative à la situation interne au système dont l'opérateur est responsable.

5.3 – Les Images Externes et Interne sont correctes mais l'opérateur utilise un mauvais Modèle de Risque.

.

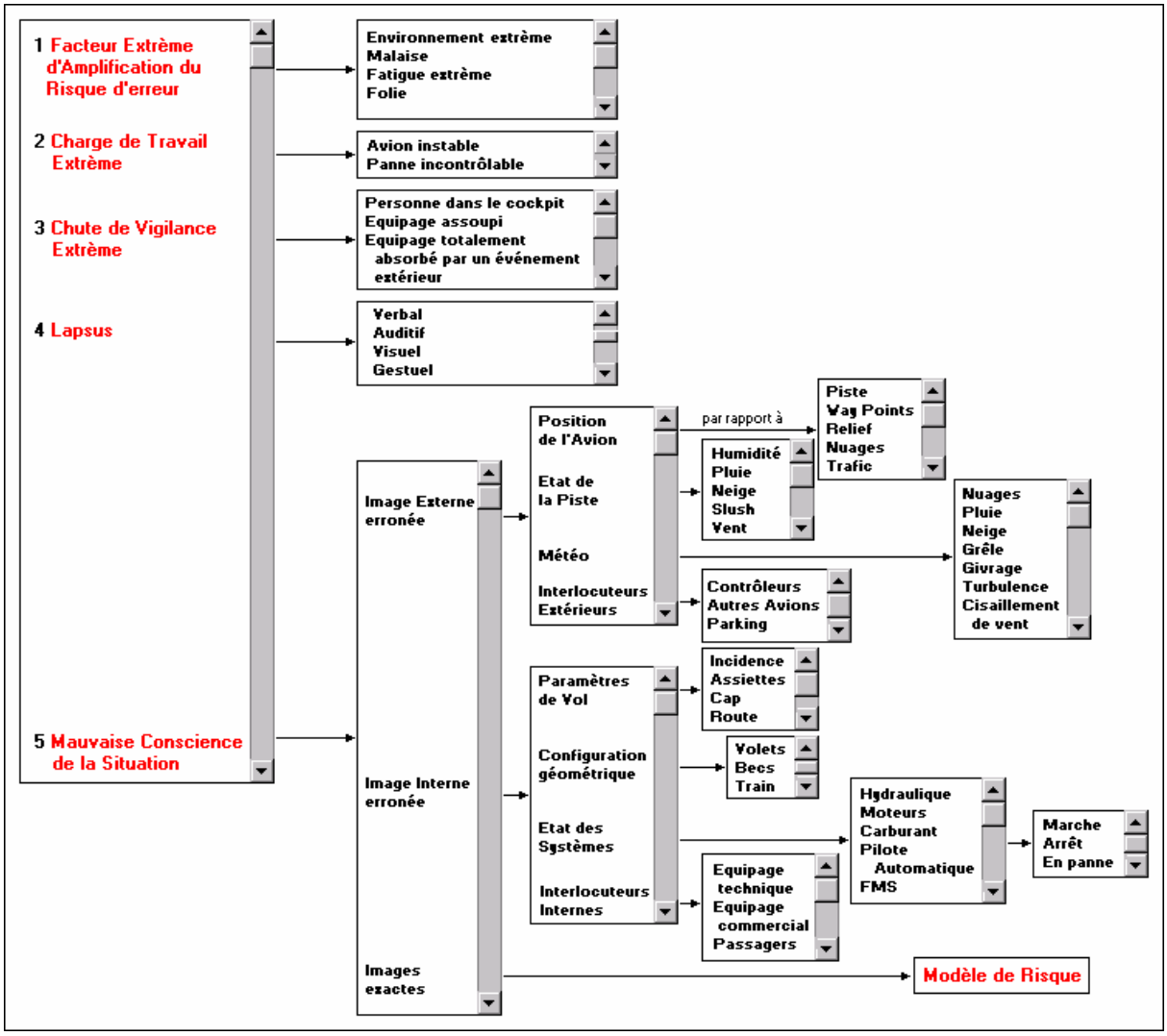
En fonction du degré de détails du rapport, il est généralement possible d'être plus précis et de fournir une sous division des rubriques 5.1 et 5.2. Le plus souvent on pourra définir des listes déroulantes dans lesquelles l'analyste pourra choisir une ou plusieurs rubriques.

En outre l'analyste pourra citer un (ou plusieurs) Facteur d'Augmentation du Risque (s'il ne l'a pas déjà désigné comme cause quasi unique de l'incident).

La planche présentée page suivante schématise le processus de Codification.

L'analyste, au niveau de la Codification, doit essayer de préciser, dans le cas d'une Conscience Erronée de la Situation, quelle Image est erronée, Interne ou Externe. Il est aidé par quelques listes déroulantes proposant les divers types possibles d'Images. Les listes présentées ci-dessous ne sont pas exhaustives. Elles ne constituent que des exemples et doivent être complétées par l'expérience.

Principes de la Codification



Un bon exemple de chute de Vigilance due à une perturbation extérieure

A la suite des derniers crashs, le NTSB a décidé de mettre des enquêteurs sur chaque vol de Boeing 767. Leur seul rôle est de prendre des photos des pilotes toutes les 15 secondes pour s'assurer qu'ils sont bien là où ils sont supposés être.

Voici l'une de ces photos.

Niveau Analyse

A ce niveau l'opération de Codification doit avoir été déjà exécutée, ce que nous supposerons.

L'objectif de l'Analyse est d'obtenir une meilleure compréhension de l'incident en identifiant les Facteurs d'Erreur en cause, s'il en existe d'autres que ceux repérés par la Codification et surtout en mettant en évidence les domaines d'actions possibles pour améliorer la sécurité. Ces domaines sont décrits dans la grille RADOS. La phase d'Analyse est plus détaillée et doit compléter la phase de Codification. Parfois une meilleure compréhension de l'incident peut amener à revoir la Codification. Il faut espérer que cela sera relativement peu fréquent.

Les étapes de l'Analyse sont les suivantes :

A/ Etablir, à partir du narratif, la séquence des événements des trois types possibles,

- Opérabilité
- Sensibilité aux perturbations
- Manœuvrabilité

B/ Caractériser les deux derniers types d'événements à l'aide des grilles GASP et GAME (voir Annexe 3, Page 70).

C/ Caractériser les événements d'Opérabilité à l'aide de la grille GAFE (voir Annexe 3 Page 63)

1 - Lorsqu'une "Conscience Erronée de la Situation" est mise en évidence, essayer de l'identifier, de façon aussi complète que possible en fonction de la qualité du narratif et en tenant compte de toutes les autres informations disponibles. Cela devrait confirmer, compléter ou peut-être rectifier le choix fait durant la phase de Codification. "Compléter" devrait être relativement fréquent, parce que la phase Codification n'extrait que les faits les plus saillants, mais d'autres aspects d'une Conscience Erronée de la Situation peuvent apparaître laissant la possibilité d'une identification plus précise. Il sera ainsi nécessaire d'identifier quelles Images sont erronées et si le Modèle de Risque est mis en cause (en se référant aux cinq types de Conscience Erronée de la Situation décrits de la page 10 à la page 14 et à la planche de la page 15).

2 – Compléter, si nécessaire, la liste des Facteurs d'Augmentation du Risque d'Erreur impliqués.

3 – Utiliser la grille RADOS (Annexe 3 Page 69) pour préciser le défaut Système à l'origine de chaque événement d'Opérabilité et de chaque Facteur d'Augmentation du Risque. Cette dernière tâche de l'Analyse est la plus importante pour identifier le domaine des actions susceptibles d'améliorer la sécurité du système de transport aérien.

d'après HERGÉ

La mauvaise climatisation de la cabine est à l'origine de l'incident mais n'en est pas la cause. Ce n'est qu'un facteur amplificateur de risque.

ANNEXE 1
Quelques définitions

⇨ Paramètres système

⇨ Paramètres d'Etat des Systèmes

Ces paramètres caractérisent comment fonctionne un système donné, par exemple le régime moteur, la fréquence, le voltage d'une alimentation électrique, le niveau d'un réservoir de combustible, la pression dans un système hydraulique, la température de l'huile de graissage, la température d'arrêt et la pression dynamique dans une entré d'air, etc.

⇨ Paramètres de Configuration

Ces paramètres caractérisent la configuration d'un système donné, par exemple, état ouvert d'un interrupteur, état marche d'une pompe, volets en position plein sorti, train rentré, état arrêt du pilote automatique, etc.

⇨ Paramètres de Performance Instantanés

Ces paramètres caractérisent l'état global d'un système, par exemple, la vitesse conventionnelle CAS, la vitesse verticale, la pente, le cap, l'incidence, l'angle de gîte, etc.

⇨ Paramètres de Performance Intégrés

Ces paramètres résultent de l'intégration dans le temps des paramètres de performance instantanés, par exemple la position géographique et l'altitude.

Certains de ces paramètres constituent les objectifs de la mission ou des tâches élémentaires.

Les paramètres des trois premiers types ont des limitations qui sont caractéristiques du système global ou des différents sous systèmes.

Les paramètres du dernier type ont aussi des limitations qui dépendent non seulement du système global (par exemple l'altitude maximale peut être limitée par les performances du système de pressurisation) mais également de conditions extérieures (l'altitude minimale dépend du relief, quelques positions géographique peuvent être interdites, par exemple survol de villes ou d'installations militaires).

⇨ Commandes

⇨ Sélecteurs

Un sélecteur modifie les paramètres de configuration. Par exemple interrupteur Marche Arrêt d'une pompe, poussoir Marche Arrêt du pilote automatique, palette de train, etc.

⇨ Commandes de pilotage

Une commande de pilotage est utilisée pour modifier un paramètre de performance instantané et par suite quelques paramètres de performance intégrés (Manche, Palonnier, Manette des gaz, touches du pilote automatique,etc.)

⇨ Commandes de réglage

Une commande de réglage est utilisée pour modifier un paramètre d'état d'un système. Par exemple, commande de réglage de la température d'air conditionné de la cabine passagers.

Il nous faut noter qu'une commande peut être une commande de pilotage au cours d'une certaine phase de vol et sélecteur dans une autre phase. Par exemple le trim de profondeur et la manette des gaz sont des sélecteurs au

cours du décollage (positions fixées par le Manuel de Vol) et commandes de pilotage au cours de l'approche et de l'atterrissage.

⇨ Paramètres Extérieurs

⇨ Paramètres d'Environnement

Un paramètre d'environnement est caractéristique de l'influence du monde extérieur sur le comportement du système et ses performances. Le temps de variation d'un paramètre d'environnement est généralement long. Par exemple, température et humidité de l'atmosphère, pluie ou givre.

⇨ Perturbations

Une perturbation est une rapide variation d'un paramètre d'environnement. Le terme "rapide" signifie que le temps de variation du paramètre est du même ordre de grandeur que le temps de réponse du système à cette perturbation. Par exemple, rafale, cisaillement de vent.

⇨ Paramètres Système Complémentaires

Les Paramètres d'Etat des Systèmes que nous avons cités sont les "sorties", c'est-à-dire les réponses de ces systèmes aux variations des commandes. En observant les variations de ces paramètres avec le temps, l'opérateur peut suivre l'évolution de l'état du système et ainsi agir sur les commandes afin d'atteindre les objectifs des tâches élémentaires et l'objectif de la mission.

Mais il nous faut ajouter deux autres types de paramètres de sortie.

⇨ Position des Commandes

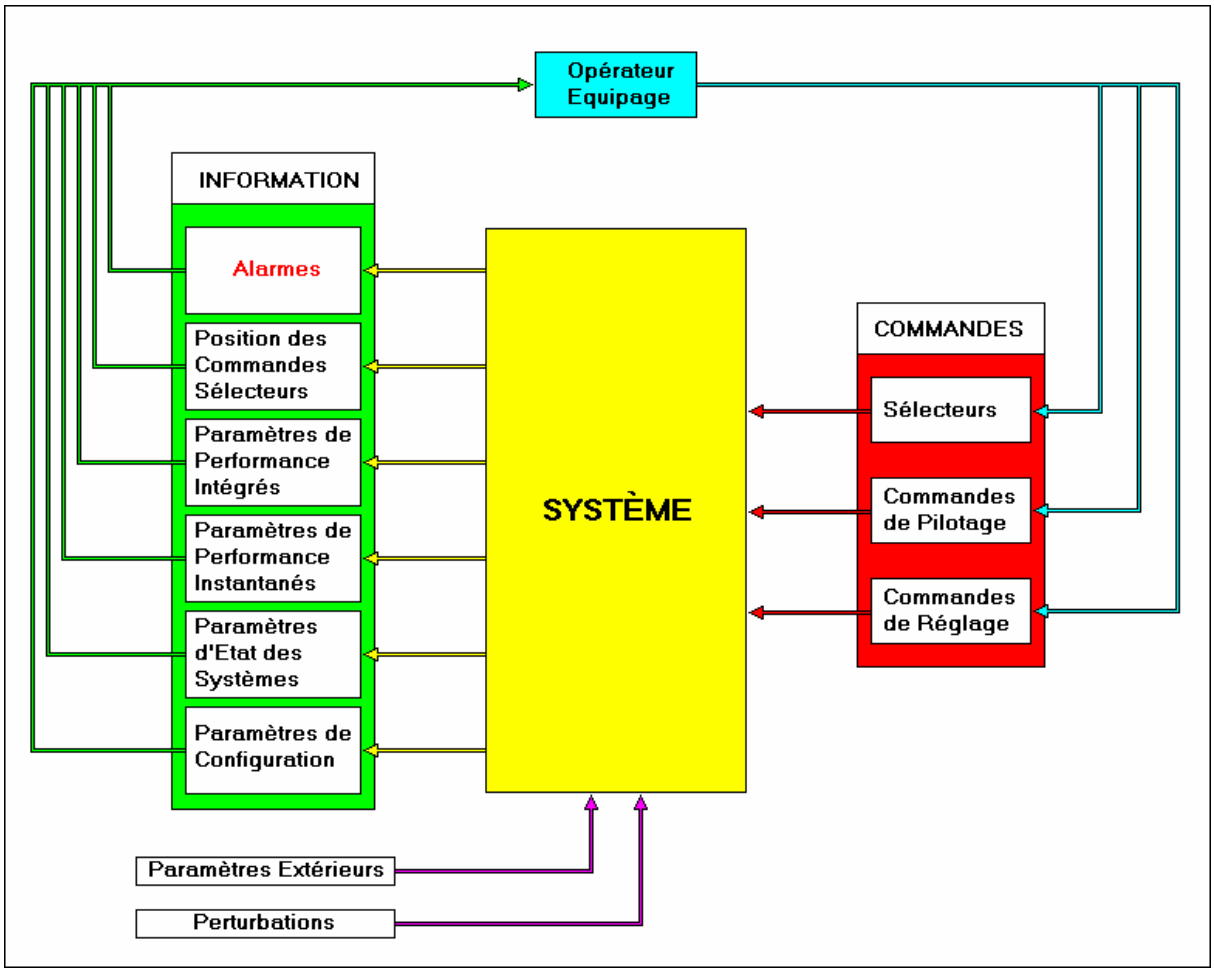
Dans certains cas, la position d'un sélecteur donne l'information nécessaire pour connaître l'état du système commandé. Dans d'autre cas ce n'est que la couleur ou l'allumage d'un voyant qui permet à l'opérateur de connaître l'état actuel du système et non la position du sélecteur lui-même. Par exemple l'opérateur pousse une fois un bouton ce qui met le système en marche. Une seconde pression sur le même bouton met le système sur arrêt. Seul un voyant (allumé, éteint, vert, rouge) peut fournir une information sur l'état du système. Dans d'autres cas encore l'action sur la commande ne donne pas l'état du système. Par exemple l'effet de l'action continue sur l'une des deux touches "ouvrir" ou "fermer" ne peut être connu qu'en lisant un instrument donnant la position de la vanne commandée.

Ainsi nous voyons que le terme Position des Commandes recouvre de nombreux types d'informations, position géométrique, couleur d'un voyant, état éteint ou allumé d'un voyant, instrument affichant la position de l'organe commandé, informations qui aident l'opérateur à connaître l'état des commandes à un instant donné.

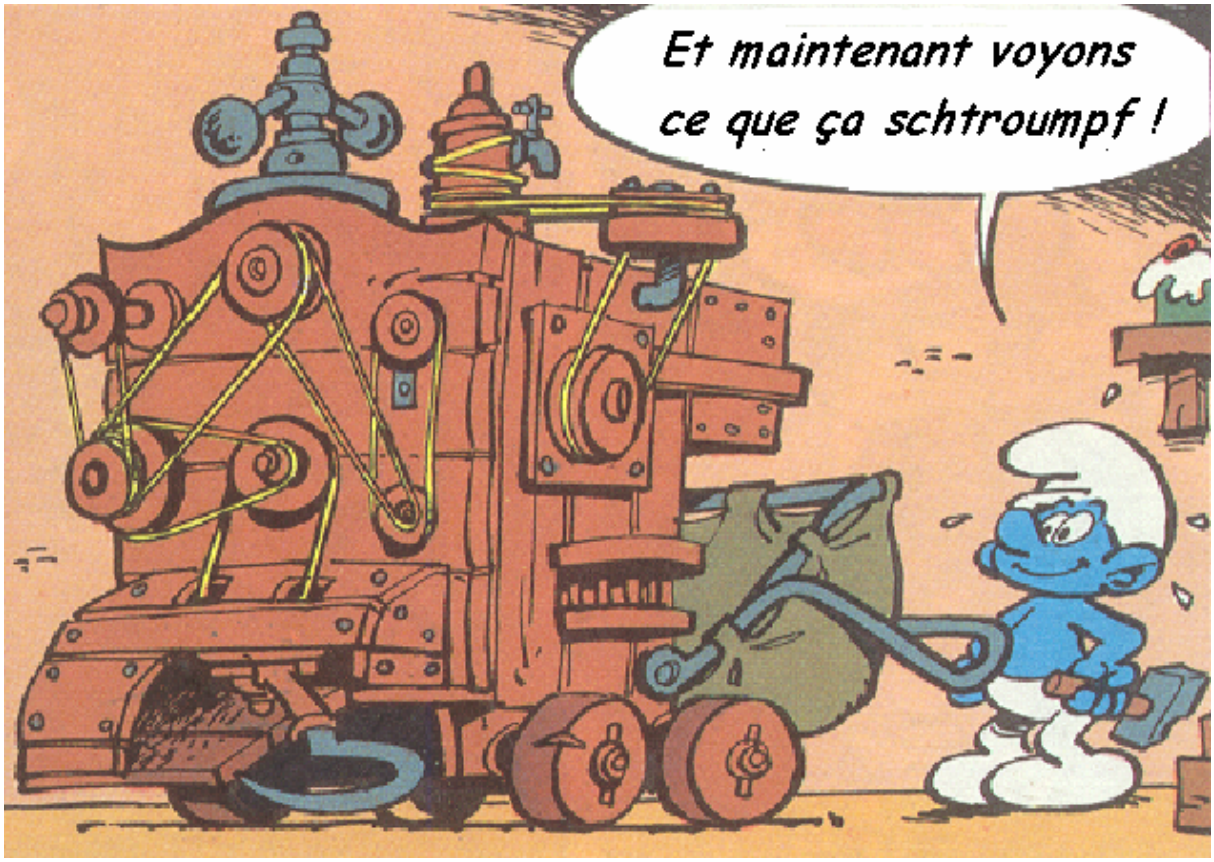
⇨ Alarmes

Ces paramètres sont utilisés pour augmenter la conscience de la situation lorsque celle-ci devient critique.

Ces paramètres sont décrits en détail en Annexe 2 page 45.



Les différents paramètres Système

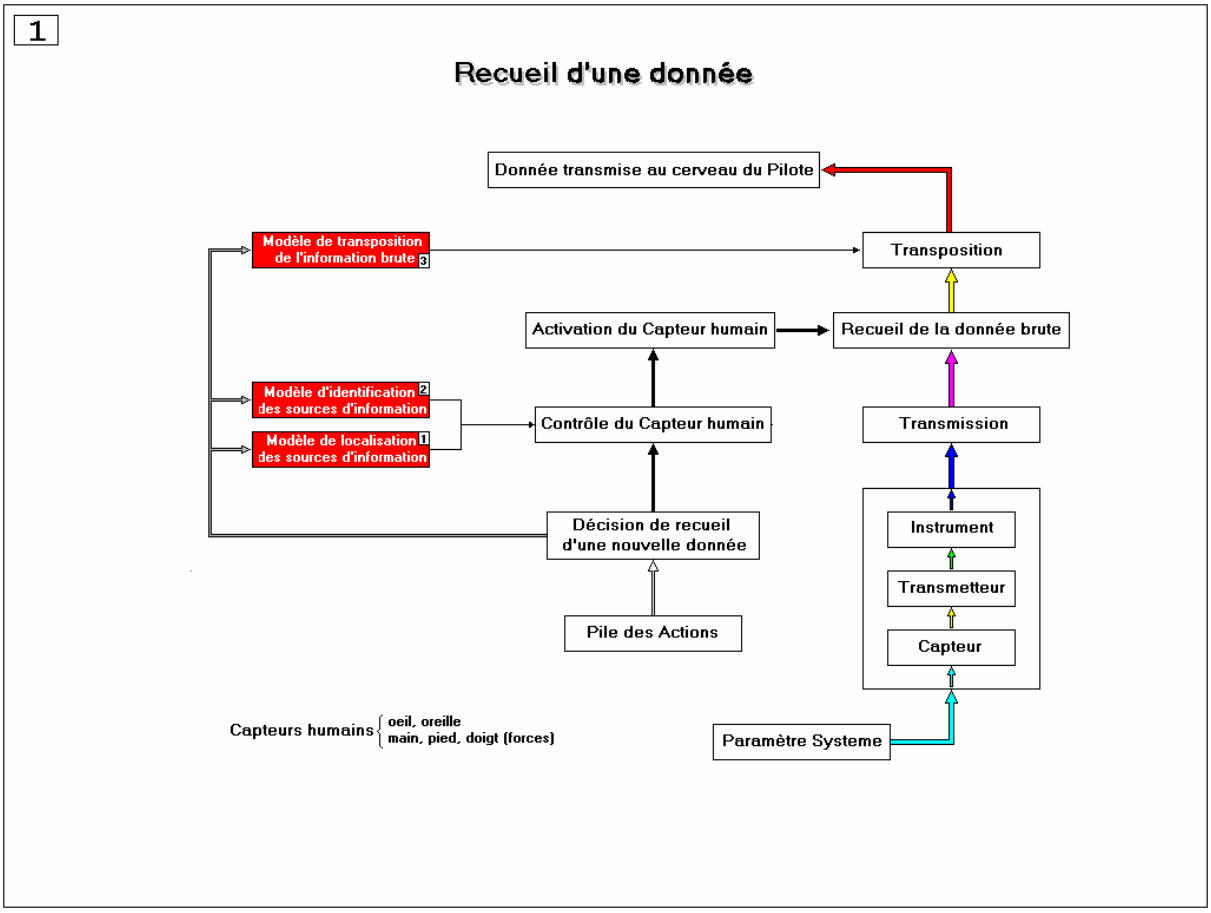


d'après PEYO

Un bon exemple d'interface Schtroumpf - machine

ANNEXE 2

Les Modèles Mentaux



Sur la partie droite du schéma est tracée la séquence de transmission d'une donnée depuis le système jusqu'au capteur humain. On peut y reconnaître la chaîne de mesure classique, capteur physique, transmission interne au capteur, instrument d'affichage du paramètre. Chacune de ces opérations peut être entachée d'erreurs bien connues conduisant à l'affichage d'une valeur erronée.

La transmission de la donnée depuis l'afficheur jusqu'au capteur humain peut être également entachée d'erreurs provenant, par exemple, d'un mauvais éclairage, de la présence de brouillard ou de pluie, d'un panneau d'instrument trop loin de l'opérateur, d'un afficheur trop petit ou trop difficile à voir, de mouvements et de vibrations de la machine conduisant à une lecture inconfortable, à un bruit ambiant trop important, etc.

L'opérateur a mis une action spécifique dans la "Pile des Actions", "*Lire le paramètre X* ". Lors du "dépilage", il appelle deux modèles

- Modèle de localisation des sources d'information (1 sur le schéma) qui l'aide à diriger son capteur, en général les yeux, mais quelquefois les oreilles (pour la saisie d'un message) ou une main, un pied ou un doigt (pour la saisie d'un effort) dans la direction où le paramètre est affiché.

- Modèle d'identification des sources d'information (2 sur le schéma) qui l'aide à reconnaître la source par sa forme, sa couleur, son étiquette, etc.

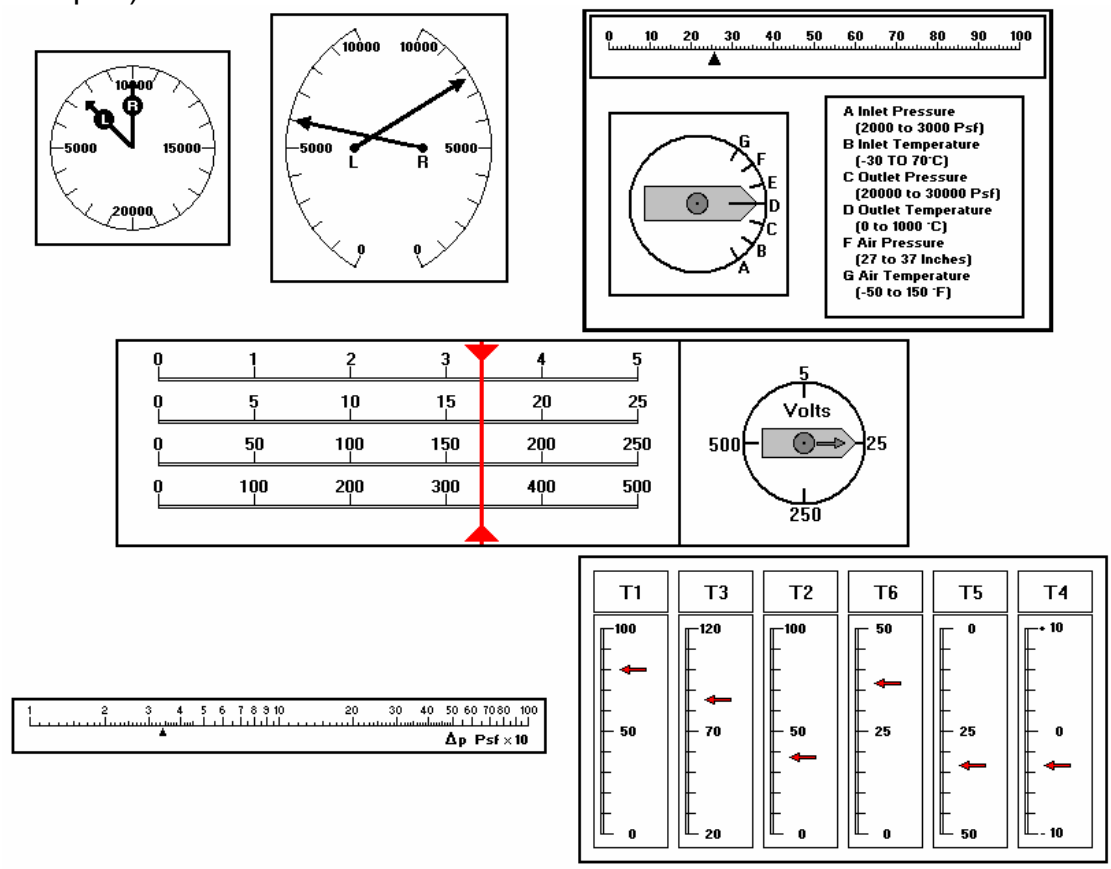
La mise en service de ces deux modèles est représentée sur le schéma par de petites flèches de couleur grise afin de souligner la différence entre ces opérations cognitives et les autres opérations cognitives indiquées par de flèches épaisses diversement colorées.

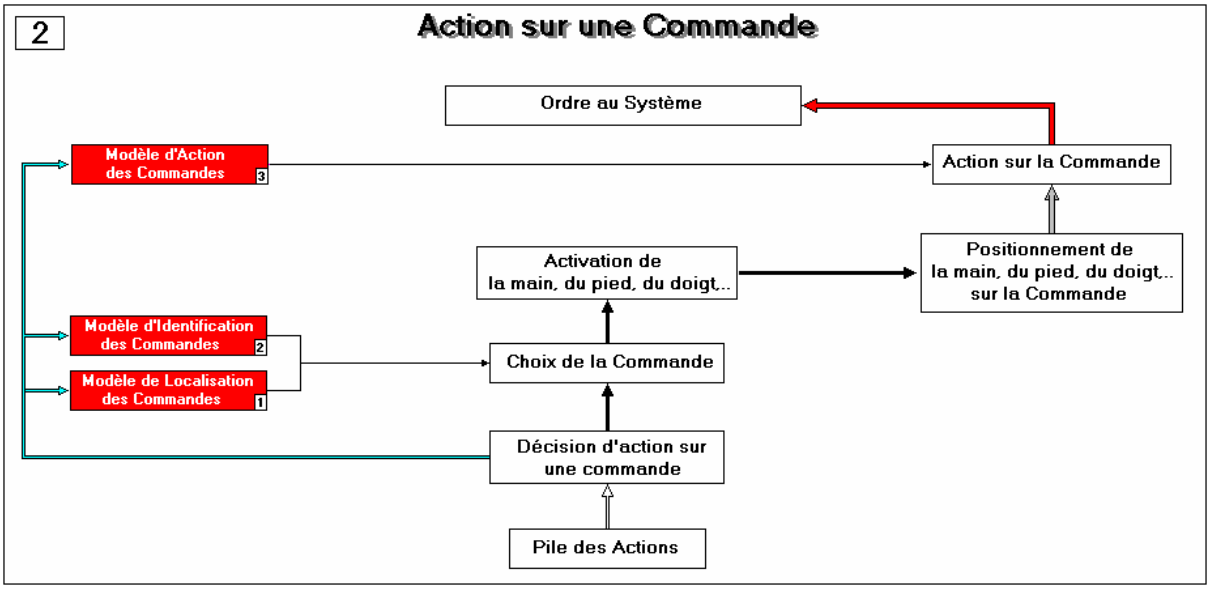
Les erreurs liées à ces deux types d'opérations sont dues à l'utilisation d'un mauvais modèle de localisation, modèle erroné (le simulateur utilisé pour la formation a un panneau d'instruments différent du panneau réel, par exemple), modèle non valide (utilisation d'un seul afficheur pour des paramètres multiples, le choix d'un paramètre dépendant d'un sélecteur). Elles peuvent aussi résulter de l'utilisation d'un mauvais modèle d'identification (étiquettes absentes, effacées, trop complexes) (voir les images en bas de cette page).

Une fois le capteur humain correctement orienté dans la direction de la source, il est mis en service afin de recueillir une donnée brute (position angulaire d'une aiguille, couleur d'un voyant, forme, couleur, position d'un symbole sur un écran, pourcentage affiché en digital,etc.)

Pour transformer cette information en un message utilisable par le cerveau, l'opérateur fait appel à un troisième modèle, le modèle de transposition de l'information (3 sur le schéma). Ici aussi les sources d'erreur sont multiples. Utilisation d'un modèle erroné (erreur sur la position du zéro, sur l'échelle,etc.), utilisation d'un modèle valable pour un autre instrument, confusion entre divers symboles ou sur la signification d'une couleur (un voyant vert signifie qu'un robinet est ouvert, donc que le fluide circule et signifie qu'un interrupteur électrique est fermé, donc que le courant ne circule pas).

Voici quelques exemples d'afficheurs conduisant à l'erreur ! (ces exemples ont été réellement rencontrés dans des systèmes industriels ou des systèmes de transport).





L'opérateur a mis dans la Pile des Actions, l'action particulière "*Agir sur la commande X* ". L'action peut être sur une commande manuelle, sur une commande d'un système automatique, un sélecteur ou une commande de réglage.

Lors du "dépilage", il appelle deux modèles

- Modèle de localisation des commandes (1 sur le schéma) qui l'aide à diriger une main, un pied ou un doigt dans la direction de la commande désirée.

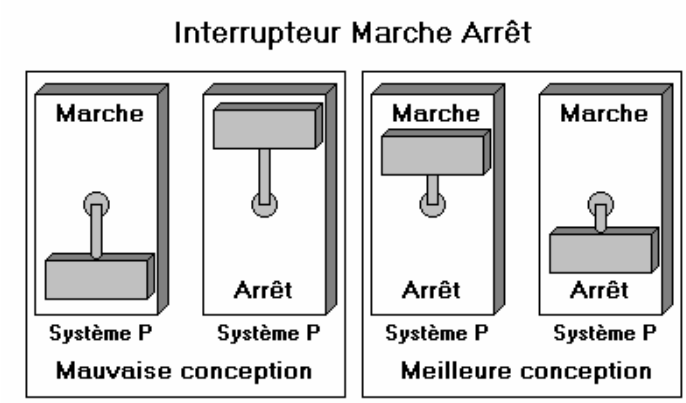
- Modèle d'identification des commandes (2 sur le schéma) qui l'aide à reconnaître la commande choisie par sa forme, sa couleur, son étiquette, etc.

Les erreurs liées à ces deux types d'opérations sont dues à l'utilisation d'un modèle erroné de localisation des commandes (par exemple modèle appris en formation sur un simulateur qui n'a pas la même répartition des commandes que le poste de travail réel), modèle trop complexe (commandes voisines de mêmes formes, panneau de multiples touches similaires, etc.). Elles peuvent être aussi le résulta de l'utilisation d'un mauvais modèle d'identification (étiquettes absentes, effacées ou trop compliquées, etc.).

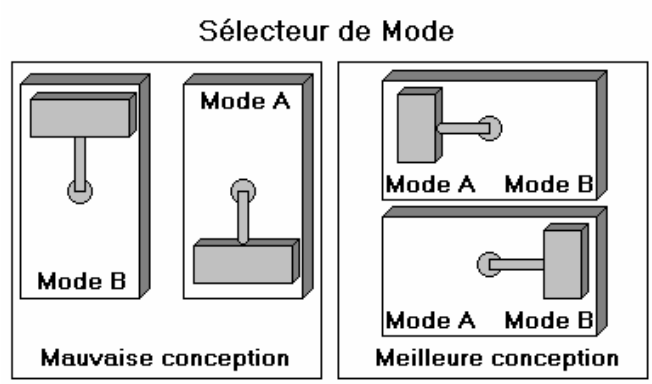
Pour agir sur la commande, l'opérateur fait appel à un troisième modèle, le Modèle d'Action des Commandes (3 sur le schéma) qui aide l'opérateur à manipuler la commande (pousser, tirer, tourner à droite, tourner à gauche, etc.) pour obtenir l'effet désiré sur le système. Ces modèles stockent l'amplitude et la direction des efforts imposés par une tâche donnée.

Ici aussi les erreurs potentielles sont multiples (erreur dans le sens de l'action, par exemple pour ce robinet particulier, la ouverture est obtenue en tournant dans le sens à visser !).

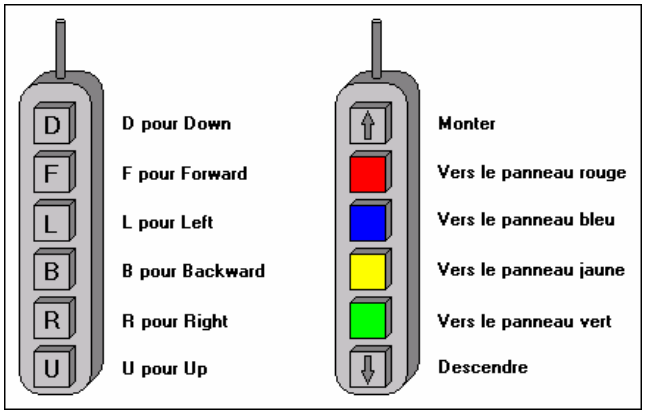
Sur la page suivante sont donnés quelques exemples de mauvaises conceptions favorisant l'erreur (relevé sur un avion bien connu avec un incident sérieux du à une confusion entre deux modes).



Sur la solution de gauche, l'étiquette est masquée par la palette.

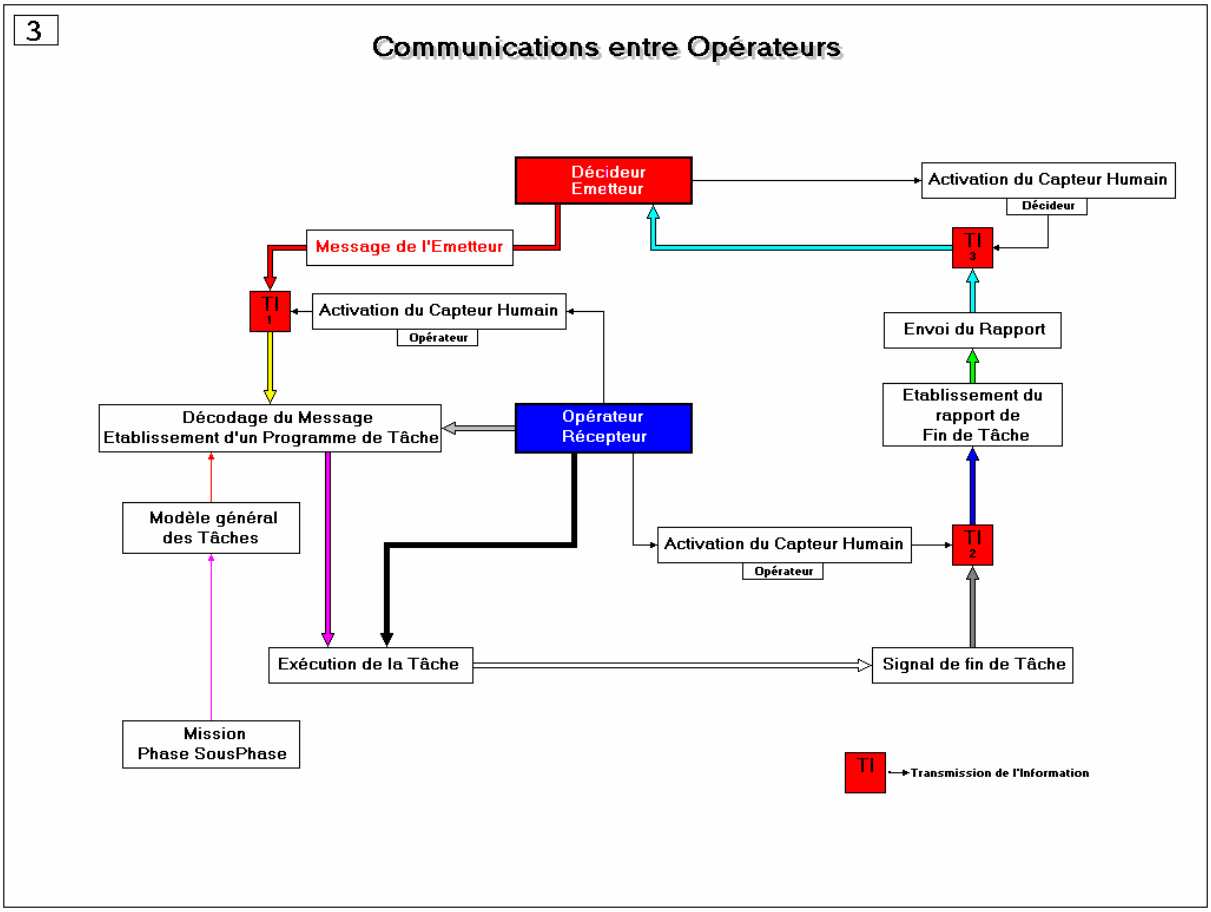


Sur la solution de gauche l'opérateur peut croire que c'est le mode B qui est sélecté.



Sur la gauche une commande typique de pont roulant. Que signifient Forward (en avant) et Backward (en arrière), Left (gauche) et Right (droite) pour un opérateur qui circule autour de la charge qu'il a à manipuler ? Pourquoi la touche Up (monter) est-elle en bas et la touche Down (descendre) en haut du boîtier.

Une meilleure solution est proposée à droite. Les murs de l'atelier sont peints en rouge, bleu, jaune et vert (c'est la solution utilisé dans les halls de montage du pas de tir ELA3 d'Ariane V à Kourou). Cet exemple peut sembler loin des problèmes d'ergonomie des cockpits, mais il se pose pour les ateliers de maintenance.



L'opérateur, nommé ici "Emetteur" ou "Décideur", envoie un message (au travers un système de transmission que nous n'avons pas schématisé pour simplifier le dessin). A ce niveau, plusieurs erreurs peuvent se produire (message erroné, système de transmission hors service, brouillé, receveur du message mal ou non identifié, etc.).

Le receveur du message, nommé ici "Opérateur Récepteur", met en service l'un de ses capteur (œil ou oreille) pour recueillir les données contenues dans le message. Ce recueil de données est représenté par la "boite" TI_1 (**TI** pour transmission de l'information comme décrit sur la planche 1, page 27). Les erreurs liées à ce type d'opération, décrites page 27, peuvent alors survenir. Par ailleurs l'opérateur peut être dans une situation qui lui interdit de mettre son capteur en service (charge de travail élevée, chute de vigilance, conscience erronée de la situation le conduisant à penser qu'aucun message n'a été transmis, etc.).

A cette opération de recueil d'information est liée une seconde opération de décodage du message. A cet effet l'opérateur "appelle" un "Modèle Général de Tâches", lié à la mission, la phase et la sous phase en cours. Au message reçu il attache une tâche spécifique choisie parmi les différentes tâches proposées par le Modèle de Tâches. Ici encore une erreur peut survenir (par exemple, l'opérateur attend un message correspondant à une certaine tâche; il reçoit un message correspondant à un autre tâche et il décode le message reçu comme demandant d'exécuter la tâche attendue et non pas la tâche demandée.).

Lorsque le message est décodé, l'opérateur construit un programme d'exécution de la tâche et prévoit un signal qui lui indiquera que la tâche est accomplie (ou non accomplie).

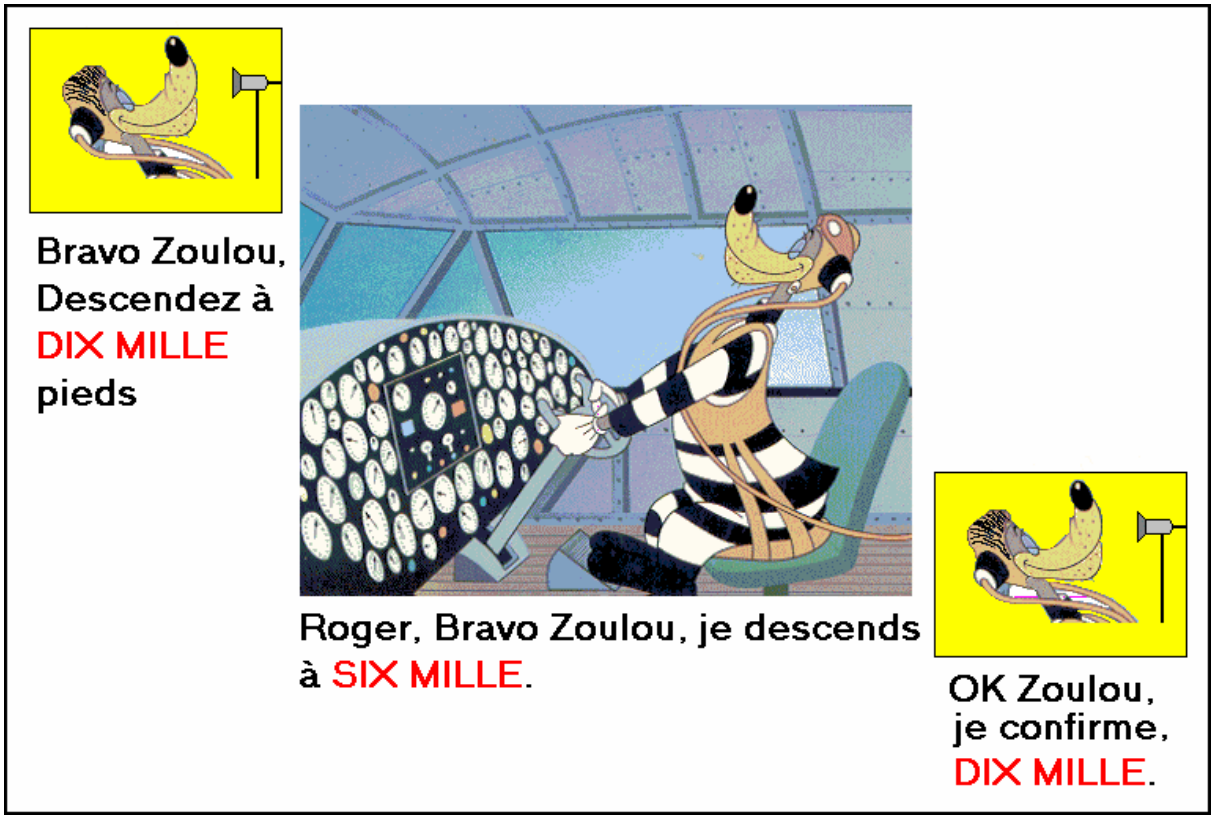
Par exemple, le pilote reçoit le message suivant du contrôleur aérien :

"*Bravo Zulu, from Charles de Gaulle approach, clear for flight level 200*"

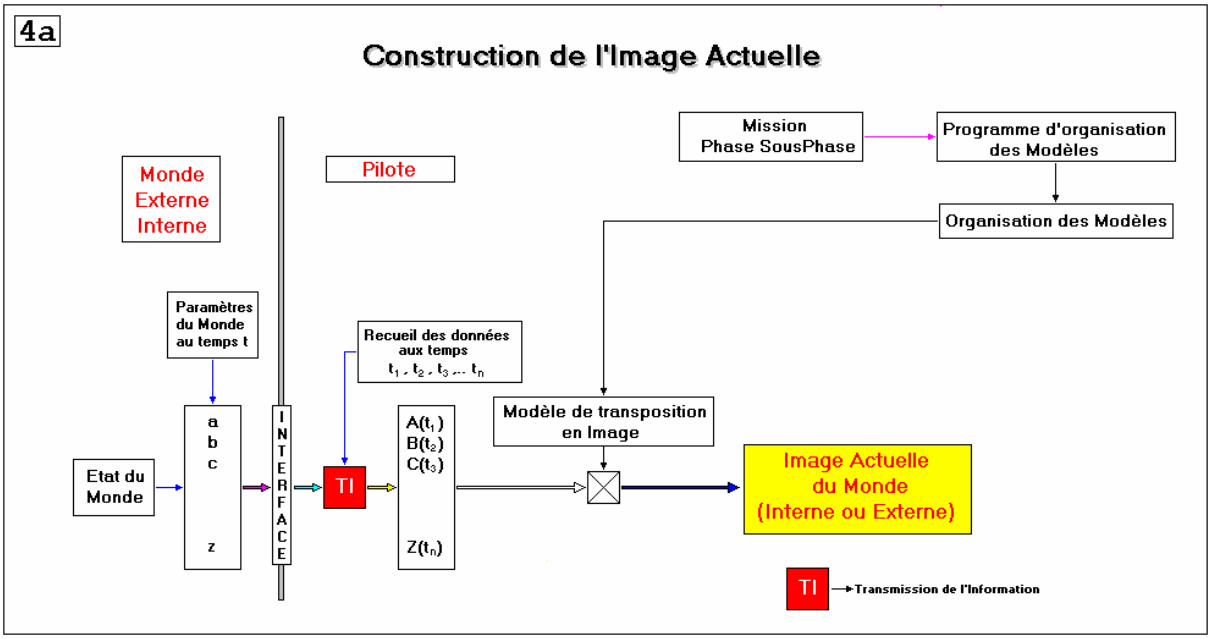
La phase actuelle étant la fin de croisière au niveau de vol 350, le pilote décode le message comme "*l'approche me donne l'autorisation de descendre au niveau 200*". Il en déduit (modèle de tâche) qu'il va mettre l'avion en descente jusqu'à atteindre le niveau 200 (la procédure comprend plusieurs opérations, mise en service du mode descente avec une altitude finale sélectée à 20000 ft, virage pour rejoindre la route de l'aéroport, etc.). Le signal de fin de tâche est évident. La tâche sera exécutée lorsque l'altitude affichée sur l'altimètre au calage Standard sera de 20000 ft.

Lorsque le signal de fin de tâche est perçu (ce qui exige de l'opérateur de mettre en service le capteur nécessaire, voir boite **TI_2**, avec toutes les erreurs potentielles liées à cette opération), l'opérateur bâtit un message de fin de tâche et l'expédie à l'Emetteur.

Maintenant l'émetteur doit mettre en service son capteur (boite **TI_3**) pour recevoir et décoder ce message. A cette opération sont liées les erreurs conduisant à une réception erronée ou à une non réception. Par exemple l'Emetteur a une charge de travail élevée, est en sous vigilance, a une conscience erronée de la situation (un message annonçant que la tâche n'a pas été exécutée est interprété comme un message de bonne exécution). Dans l'exemple donné sur le dessin suivant, l'Emetteur attend "dix mille pieds" et il interprète "six" comme étant le "dix" attendu, ce qui constitue une erreur typique.



d'après Tex Avery



A l'instant t l'Etat des Mondes Externe et Interne est donné par un ensemble de paramètres a, b, c,…, z.

A l'instant t_1 l'opérateur met en service un capteur humain pour recueillir la donnée a (boite **TI**) qui est décodée sous forme d'une valeur A.

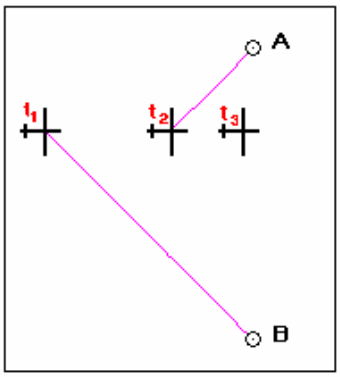
A l'instant t_2 l'opérateur met en service un capteur humain pour recueillir la donnée b (boite **TI**) qui est décodée sous forme d'une valeur B et ainsi de suite.

A l'aide des valeurs $A(t_1)$, $B(t_2)$, $C(t_3)$,…,$Z(t_n)$, l'opérateur bâtit une image mentale de l'état du Monde. Pour ce faire il utilise un "Modèle de Transposition en Image".

Par exemple à l'aide des relèvements et des distances de deux balises, l'opérateur place dans une "carte mentale", la position de l'avion par rapport à l'aéroport.

Quelques erreurs peuvent venir de la différence entre les valeurs $A(t_1)$, $B(t_2)$, $C(t_3)$,…,$Z(t_n)$ et les valeurs $A(t)$, $B(t)$, $C(t)$,…,$Z(t)$, d'un mauvais recueil ou d'une mauvaise transposition d'un ou plusieurs paramètres.

Dans l'exemple ci-dessous, des erreurs peuvent provenir de la différence de positions de l'avion aux deux moments où ont été mesurés les relèvements. Une autre source d'erreur est la mesure erronée de l'un des deux relèvements.



Relèvement de B mesuré au temps t_1
Relèvement de A mesuré au temps t_2

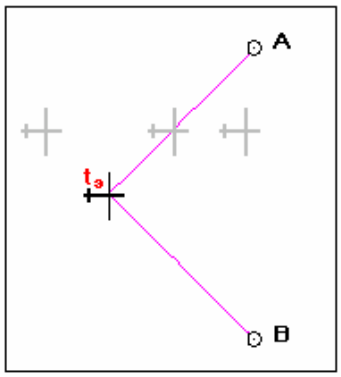
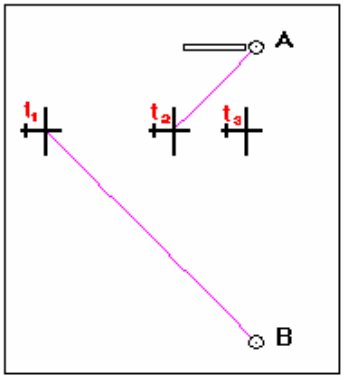


Image mentale à t_3

Due à la confusion entre deux balises en lisant la carte d'approche, le pilote peut aussi croire que l'une des balises est au seuil de la piste, ce qui n'est pas le cas.



Relèvement de B mesuré au temps t_1
Relèvement de A mesuré au temps t_2

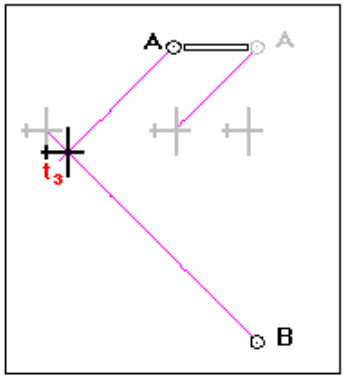
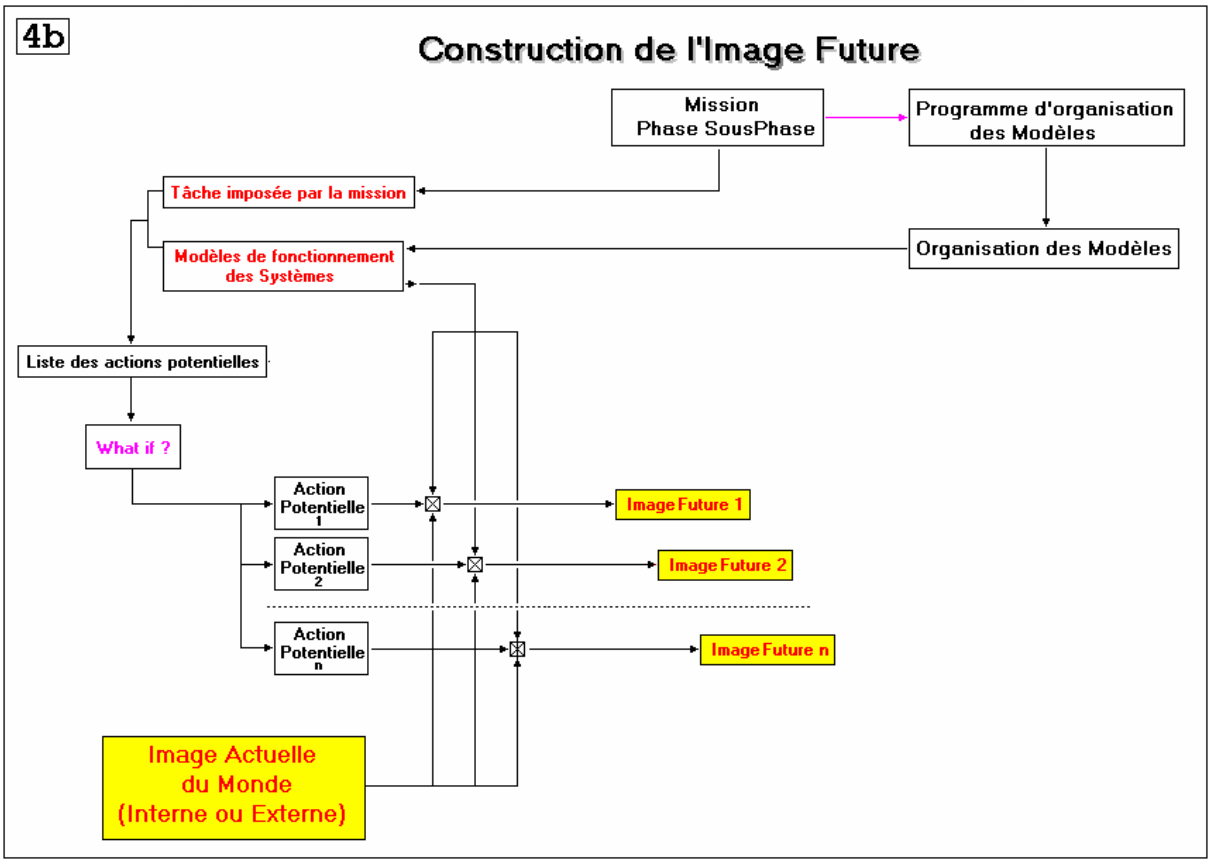
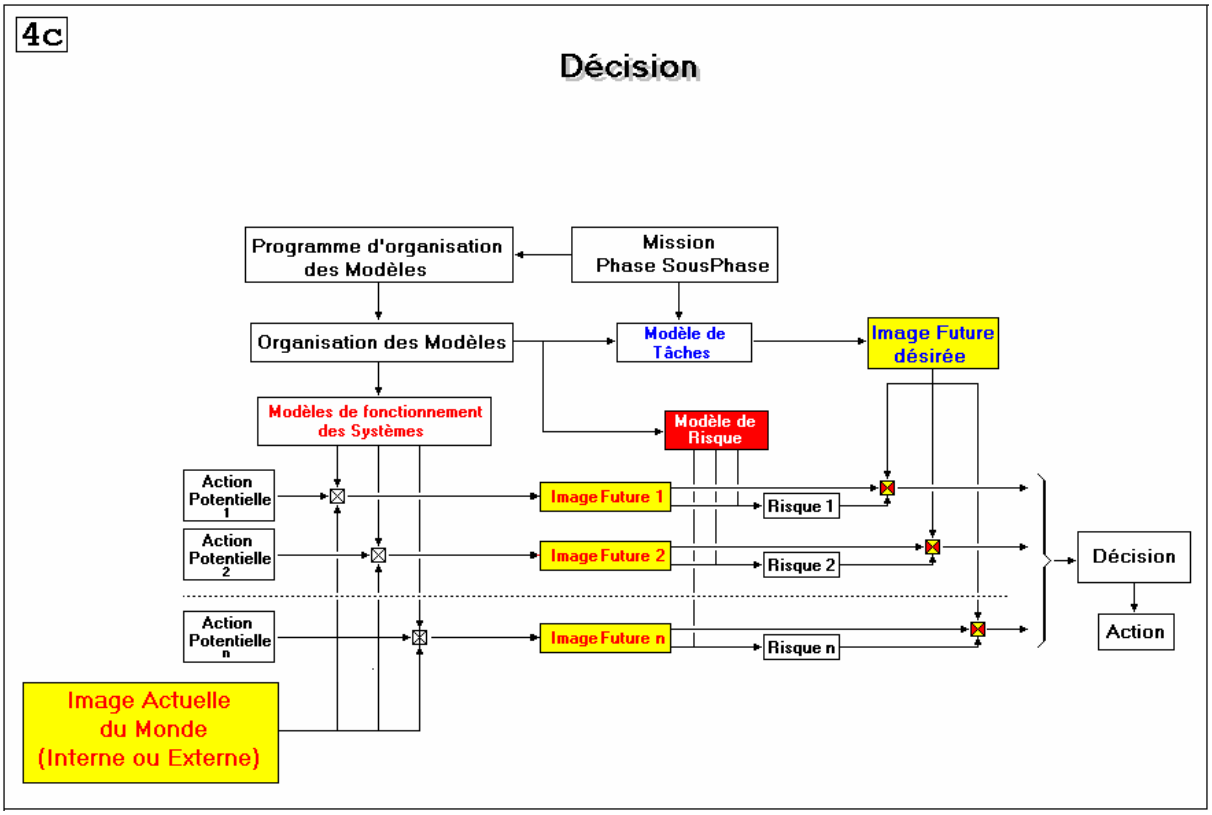


Image mentale à t_3
Erreur sur la position de A



Connaissant la tâche imposée par la mission, le pilote prépare mentalement la liste des actions possibles (cette liste est en général courte parce que limitée par la formation et l'expérience). Pour chaque action éventuelle, il construit une Image future à partir de l'Image actuelle en utilisant un Modèle de Fonctionnement du Système (Modèle de Mécanique du Vol ou Modèle de Fonctionnement du Pilote Automatique pour la prévision de la trajectoire, par exemple).



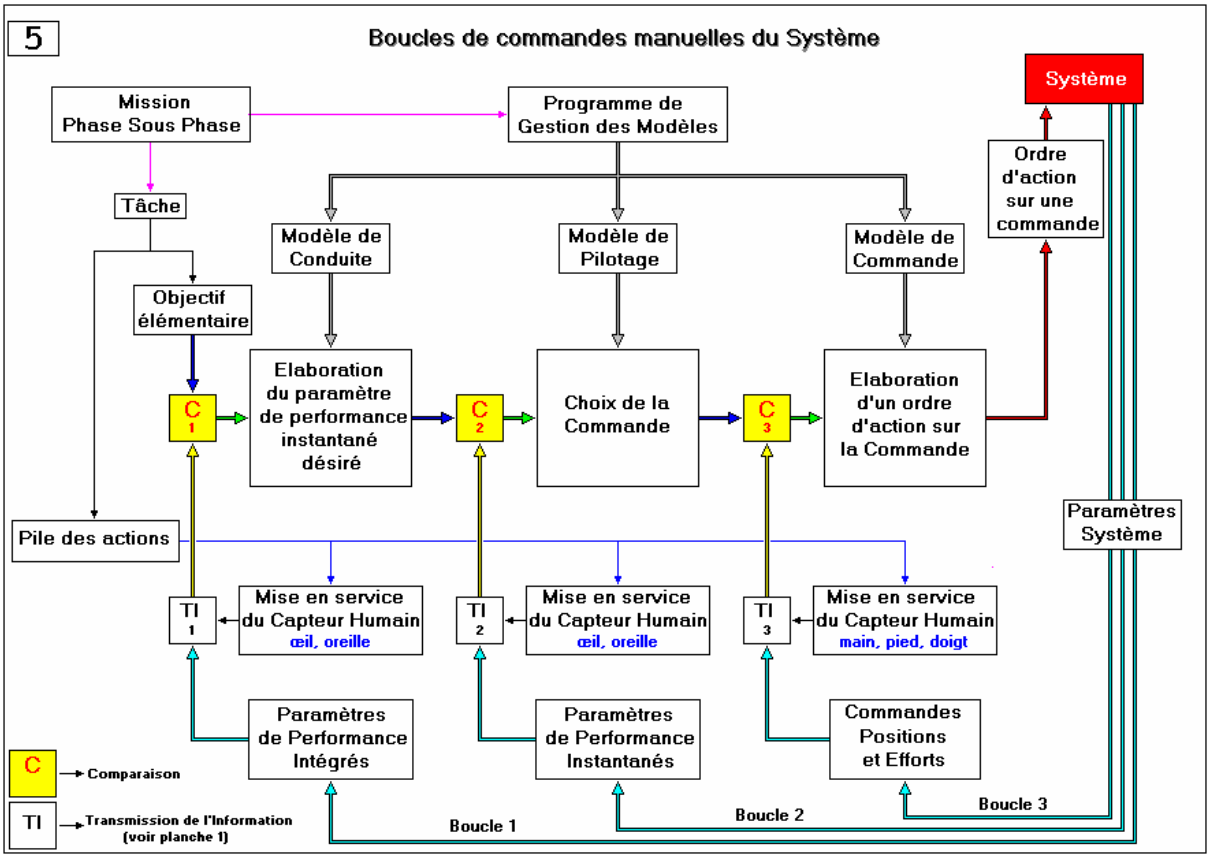
En utilisant le modèle de tâche correspondant à la sous phase actuelle, le pilote bâtit une Image désirée et fait mentalement la comparaison entre chaque Future Image possible et l'Image Désirée.

Le choix de l'action repose sur deux critères :

⇨ Réduire la différence entre l' Image Future et l'Image Désirée.

⇨ Minimiser le risque estimé par le Modèle de Risque

Sur les schémas suivants nous verrons plus en détails quels types de Modèles sont utilisés par l'opérateur pour piloter le système soit manuellement, soit au travers du pilote automatique ainsi que pour gérer la configuration de l'avion et le fonctionnement des différents systèmes.



Pour exécuter une sous phase, l'opérateur doit atteindre un objectif donné et il a en mémoire un Modèle de Tâches. L'objectif de la tâche est généralement défini par un ensemble de valeurs spécifiques de quelques paramètres de performance intégrés. Nous donnons ici plus de détails sur le processus spécifique de décision au cours d'un pilotage manuel.

L'opérateur met en service un capteur humain pour recueillir un paramètre spécifique de performance intégré parmi l'ensemble des paramètres définissant l'objectif de la sous phase (boite **TI_1**).

Par exemple, au cours de la phase d'approche finale, le pilote doit maintenir l'avion sur une trajectoire donnée l'amenant en un point précis en aval du seuil de piste et de maintenir une Vitesse Conventionnelle donnée. Ainsi a-t-il, à un instant donné, à estimer l'écart entre la position réelle de l'avion et sa position théorique et l'écart entre la Vitesse Conventionnelle actuelle lue sur le badin et la Vitesse recommandée. Il doit alors réduire ces écarts.

La boite de comparaison **C_1** entre la valeur objectif et la valeur relevée du paramètre de performance intégré (dans notre cas la position de l'avion le long de la trajectoire) le conduit à élaborer une valeur désirée pour un paramètre de performance instantané. Pour l'aider dans cette opération il fait appel à un "Modèle de Conduite".

Par exemple constatant que l'avion est à droite de la trajectoire théorique, le pilote prépare un angle de gîte de 10 degrés à gauche. C'est le "Modèle de Pilotage", mis en mémoire au cours de la formation et amélioré par l'expérience, qui permet au pilote de préciser sur quel paramètre agir et d'en évaluer l'amplitude nécessaire pour atteindre son objectif. (il n'envisage pas d'agir sur la manette de gaz

pour réduire un écart latéral et ne prépare pas un virage serré pour corriger un écart de cap de quelques degrés !).

Les erreurs à ce niveau peuvent provenir d'une mauvaise évaluation de la situation (par exemple en vol sans visibilité, le pilote pense à tort être à gauche de la trajectoire théorique d'approche) ou bien de l'utilisation d'un Modèle de Pilotage erroné, valable dans le cas général mais mis en défaut dans ce cas particulier (tirer sur le manche met en général l'avion en montée permanente sauf si l'avion est au second régime).

Une fois choisie la valeur désirée pour le paramètre de performance instantané, le pilote met en service un capteur humain pour recueillir la valeur actuelle de ce paramètre (boite **TI_2**).

La comparaison entre la valeur désirée et la valeur réelle (boite **C_2**) est utilisée par l'opérateur, aidé du Modèle de Pilotage, pour déterminer sur quelle commande agir.

Ainsi pour obtenir un angle de gîte de 10 degrés, le pilote décide de pousser latéralement le manche et le Modèle de Pilotage lui permet d'estimer l'amplitude et le sens de l'effort à exercer sur la commande. A ce niveau, il n'y a généralement pas d'erreurs, du moins dans le domaine du pilotage des avions. Mais dans l'industrie on peut voir des erreurs typiques, par exemple une confusion entre les différents leviers, parallèles et identiques, de commande des grues et autres moyens de manutention de charges.

Enfin l'opérateur met en service un capteur humain pour recueillir les informations concernant la position de la commande (ce peut être aussi l'effort sur la commande) (boite **TI_3**) et compare le résultat avec la valeur désirée (boite **C_3**).

En utilisant un "Modèle de Commande", il détermine l'amplitude et le sens de l'action sur la commande et il agit sur la commande jusqu'à atteindre la valeur désirée. Une boucle, " action sur la commande, mesure, comparaison " est parcourue jusqu'à ce que la valeur désirée soit atteinte (boucle 3).

L'utilisation d'un mauvais modèle de commande peut entraîner une erreur sur l'amplitude et le sens de l'action (par exemple l'opérateur tourne un robinet à visser pour le fermer, mais ce robinet spécial s'ouvre sur ce type d'action !).

Une fois obtenue la position désirée (ou l'effort désiré) de la commande, l'opérateur vérifie l'effet résultant sur le paramètre de performance instantané. Si nécessaire il modifie son action sur la commande, jusqu'à atteindre la valeur désirée (boucle 2 avec une boucle 3 interne).

Enfin une fois atteinte la valeur désirée du paramètre de performance instantané, l'opérateur vérifie l'effet résultant sur le paramètre de performance intégré et si nécessaire il modifie la valeur désirée du paramètre de performance instantané (boucle 1 avec une boucle 2 interne, elle-même avec une boucle 3 interne).

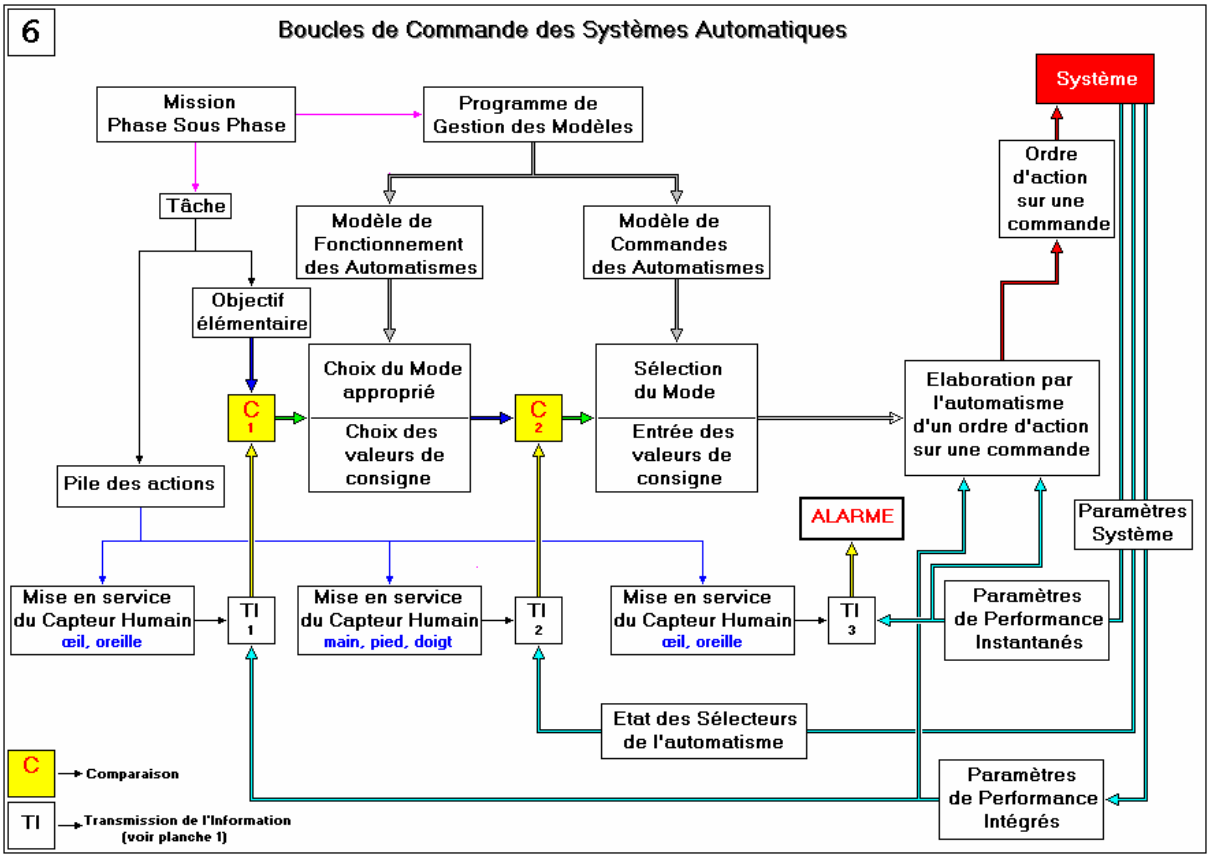
Ainsi la correction de l'écart entre l'objectif de la tâche et la situation actuelle est faite au travers de trois boucles, chaque boucle étant ouverte par la mise en service d'un capteur humain (boites **TI_1**, **TI_2**, **TI_3**) commandée par la pile des actions.

On voit aisément les conséquences de ce comportement de l'opérateur.

- Si les objectifs des sous phases changent trop rapidement ou si l'opérateur doit contrôler de trop nombreux paramètres, il n'a pas suffisamment de temps pour exécuter correctement ses actions et de parcourir les différentes boucles. (Problème de Charge de Travail trop élevée).

- Si le système est instable et si les temps de réponse conduisent à des variations trop rapides des paramètres, l'opérateur n'a pas suffisamment de temps pour exécuter correctement ses actions et de parcourir les différentes boucles. (Problème de Charge de Travail trop élevée).

- Si l'objectif de la sous phase doit être atteint, après analyse de l'écart, par une action à exécuter dans un temps si court qu'il interdit toute boucle de correction, il est difficile pour l'opérateur d'élaborer et d'exécuter directement la bonne séquence d'actions (fonctionnement en "boucle ouverte").

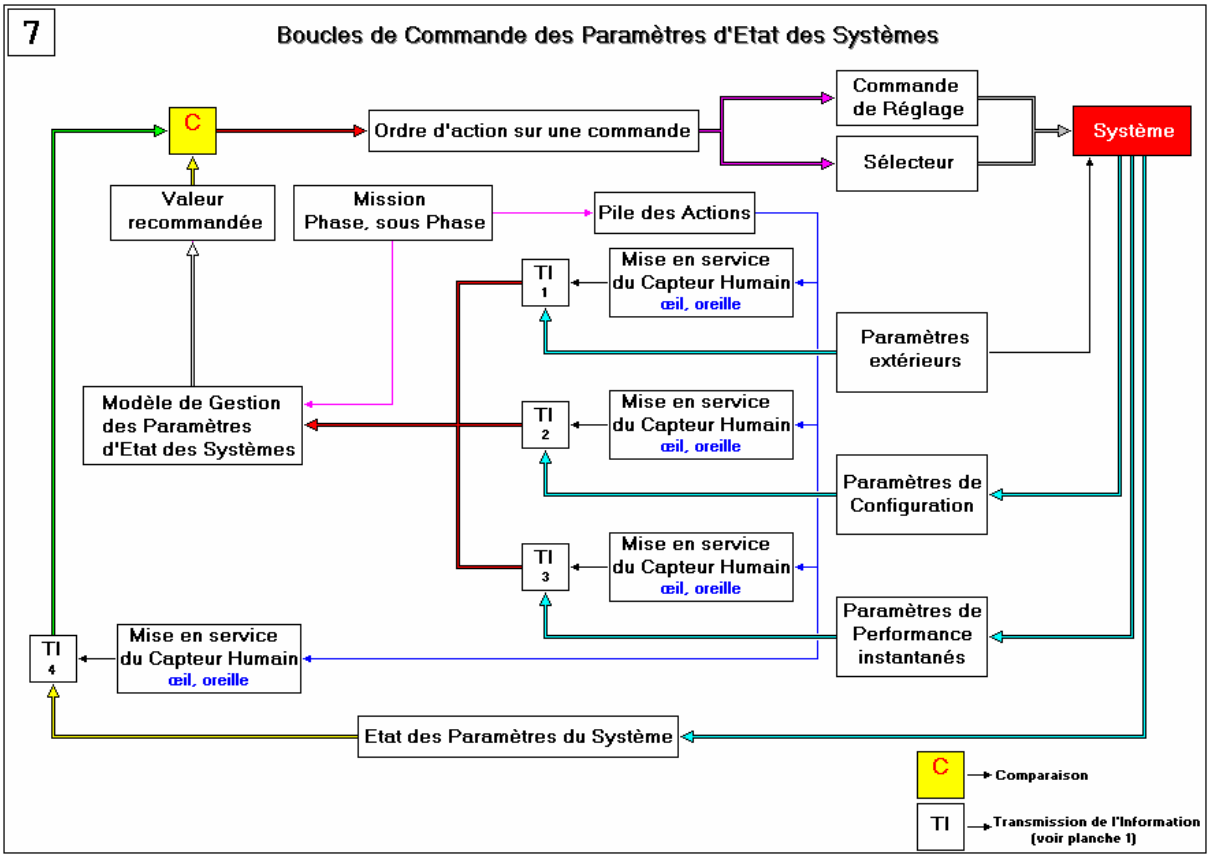


Pour exécuter la sous phase, l'opérateur doit atteindre un objectif déterminé et il a en mémoire un Modèle de Tâche. Nous donnons ici plus de détails sur le processus spécifique de décision au cours d'un pilotage utilisant un automatisme.

L'opérateur met en service un capteur humain pour recueillir un paramètre spécifique de performance intégré parmi l'ensemble des paramètres définissant l'objectif de la sous phase (boite **TI_1**).

En utilisant un "Modèle de Fonctionnement des Automatismes", l'opérateur choisit le Mode à mettre en service et les valeurs de consigne à envoyer au système automatique pour atteindre l'objectif. A cet effet il examine les positions des sélecteurs des divers automatismes (boite **TI_2**) et les comparant avec le mode choisi et les valeurs de consigne envisagées, il exécute les actions nécessaires sur les sélecteurs.

L'automatisme utilise les valeurs mesurées des paramètres de performance intégrés et instantanés pour élaborer les ordres d'action sur les commandes. Contrairement à l'opérateur humain, toutes ces opérations, recueil de données, actions sur les commandes, sont menées en parallèle et non en séquence. En outre toutes ces actions sont plus rapides et plus précises que celles effectuées par l'opérateur humain. Par ailleurs, l'opérateur observe non seulement l'évolution des paramètres intégrés pour vérifier que l'évolution de la situation correspond bien à l'évolution souhaitée, mais également sur les paramètres instantanés (boite **TI_3**) pour détecter, si possible, une éventuelle anomalie de fonctionnement des automatismes en service. Nous avons représenté cette action par la boite "ALARME". Très souvent cette opération est négligée par les opérateurs qui font trop confiance aux automatismes. Enfin des erreurs peuvent provenir de confusions sur l'objectif de la sous phase et un mauvais recueil d'informations, mais ces erreurs ne sont pas typiques de l'utilisation des automatismes.



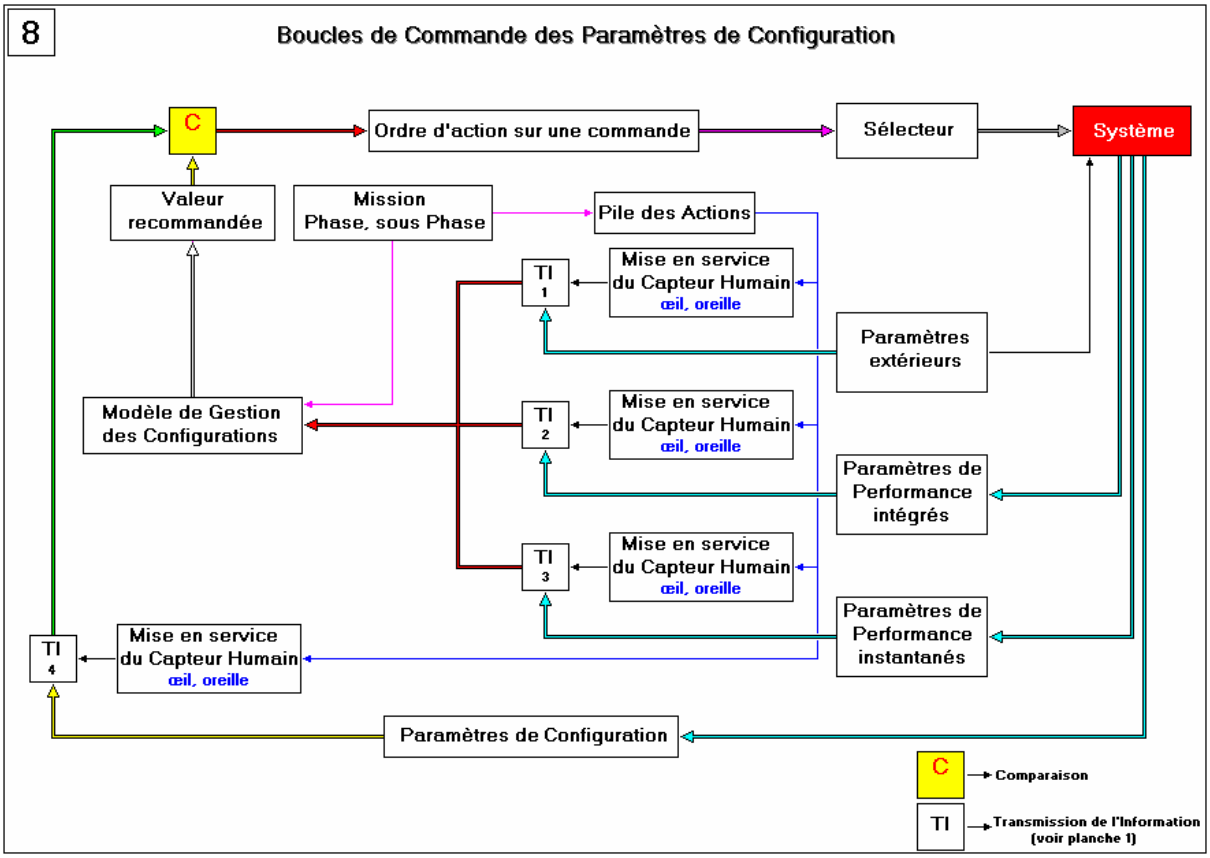
Parmi ses différentes tâches, l'opérateur doit surveiller les paramètres d'état des systèmes et les maintenir dans le domaine des valeurs autorisées.

Dans la pile des actions figurent ces opérations de collecte de ces paramètres, paramètres et valeurs dépendant de la sous phase en cours.

Ainsi l'opérateur relève-t-il les valeurs de paramètres d'état des systèmes (boite **TI_4**) et les compare aux valeurs recommandées par le "Modèle de Gestion des Paramètres d'Etat des Systèmes". Ce modèle contient la liste des paramètres à surveiller, les valeurs recommandées pour chaque paramètre et la liste des commandes de réglage (et leur mode d'action) affectées à chacun d'eux. Cette liste dépend de la configuration des systèmes, des paramètres de performance instantanés actuels et des paramètres extérieurs. Par exemple la température maximale de l'huile de graissage d'un moteur dépend de la configuration du moteur (la température maximale est plus grande si le moteur tourne au régime maximal), de la position des volets du radiateur, de la vitesse avion et de la température extérieure.

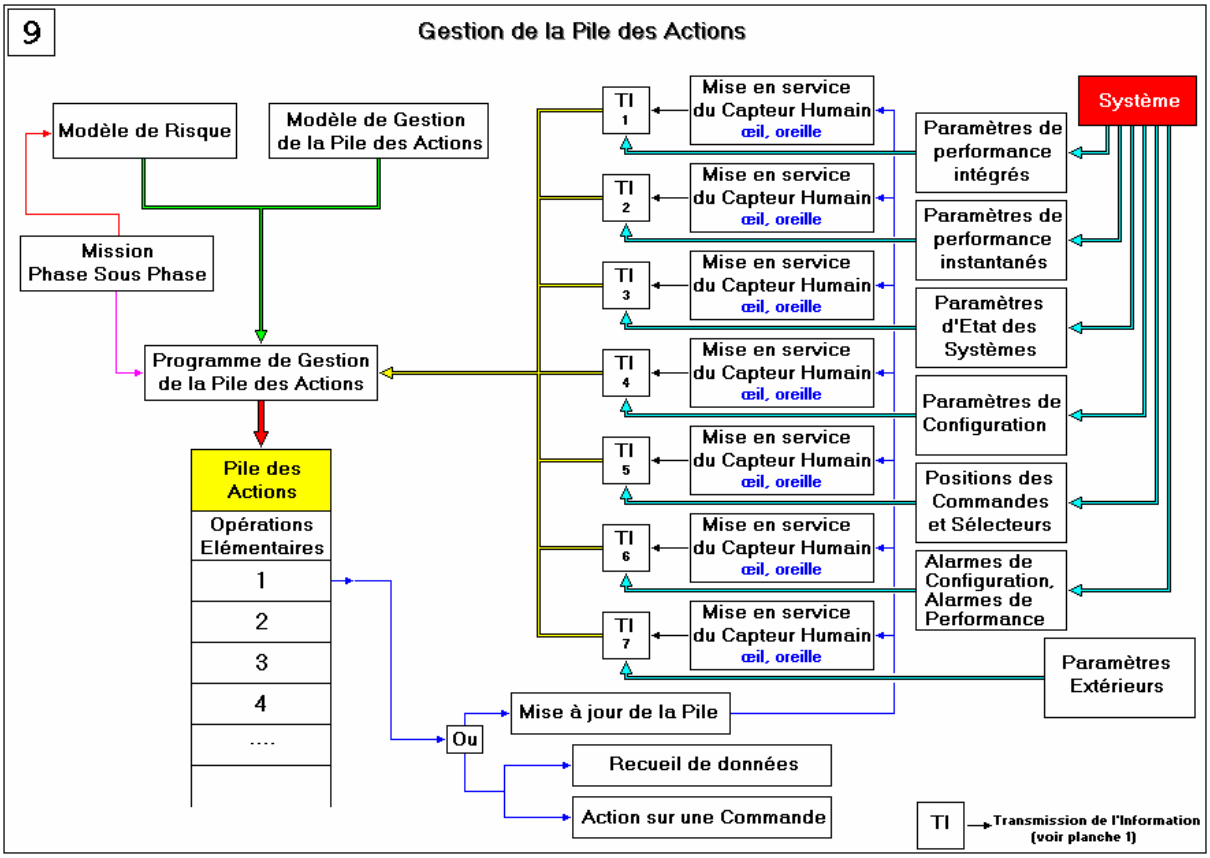
L'opérateur doit alors relever ces différents paramètres instantanés (boite **TI_3**), les paramètres de configuration (boite **TI_2**) et les paramètres extérieurs (boite **TI_1**) pour alimenter le Modèle de Gestion des Paramètres d'Etat du système.

La comparaison entre les valeurs relevées et les valeurs recommandées aide l'opérateur à bâtir un ordre d'action sur une commande de réglage ou sur un sélecteur (quelquefois sur un sélecteur de changement de configuration).



Les boucles de commande des paramètres de configuration sont analogues aux boucles de commande des paramètres d'état des systèmes.

Nous noterons que les Modèles de Gestion de Configuration dépendent des paramètres extérieurs, des paramètres de performance instantanés, comme le Modèle de Gestion des Paramètres d'Etat des Systèmes, ainsi que des paramètres de performance intégrés.



On a vu que la mise en service de chacune des différentes boucles (conduite, pilotage, commande, fonctionnement et configuration) était commandée par un acte volontaire de recueil d'information. Ces actions de recueil d'information ne sont pas les seules effectuées par le pilote. Ce dernier agit également sur les commandes (ou les actionneurs de commande).

Au cours de l'analyse de la situation, l'opérateur ayant observé des écarts entre les valeurs recueillies des différents paramètres et leurs valeurs désirées ou nominales bâtit un plan d'actions, lectures de paramètres et corrections par actions sur les commandes. Ces tactiques, successions d'actions envisagées, sont stockées en mémoire dans la "pile des actions". Le choix des actions à entreprendre, c'est-à-dire le "programme de gestion de la pile", dépend de la mission elle-même et des valeurs recueillies des différents paramètres. Ce programme est établi grâce à un "modèle de gestion de la pile des actions" qui résulte de la formation initiale et de l'expérience acquise et qui a pour objectif d'optimiser la succession des opérations de contrôle.

L'élaboration du programme de gestion de la pile dépend non seulement du modèle de gestion de la pile, mais également du risque tel que l'estime l'opérateur à l'aide de son "modèle d'estimation du risque". Si l'opérateur estime que la situation est stationnaire et qu'aucune perturbation ne va intervenir dans les minutes qui suivent, il est évident qu'il ne mettra que peu d'actions dans sa pile. Si, par contre, il estime que la situation est critique, il mettra beaucoup d'actions dans la pile et la "dépilera" le plus rapidement possible.

Enfin le programme de gestion de la pile dépend de l'observation de la situation, observation déclenchée par le "dépilage" lui-même.

On notera que la sortie de pile (le "dépilage") peut mettre en service un capteur humain pour déclencher l'une des diverses boucles de contrôle (branche inférieure

de la sortie de la case 1 de la pile) ou pour remettre à jour le modèle d'estimation du risque et la gestion de la pile elle-même (branche supérieure). Ce choix est représenté par la "boîte OU" qui ne figure ici que pour représenter commodément ce choix. Il est évident que ce choix n'est pas exécuté au dépilage. C'est l'une ou l'autre de ces deux possibilités qui est mise en mémoire au moment de l'empilage.

Il y a deux modèles typiques de gestion de la pile des actions, l'un pour les situations stationnaires, l'autre pour les situations critiques.

Pour les situations stationnaires, l'opérateur place dans la pile une séquence de relevé de données à basse fréquence, séquence reposant sur la formation de base et l'expérience. Par exemple "*Horizon – Altitude – Horizon – Vitesse conventionnelle – Horizon – Vitesse verticale – Horizon – Cap – Horizon – Altitude – etc*."

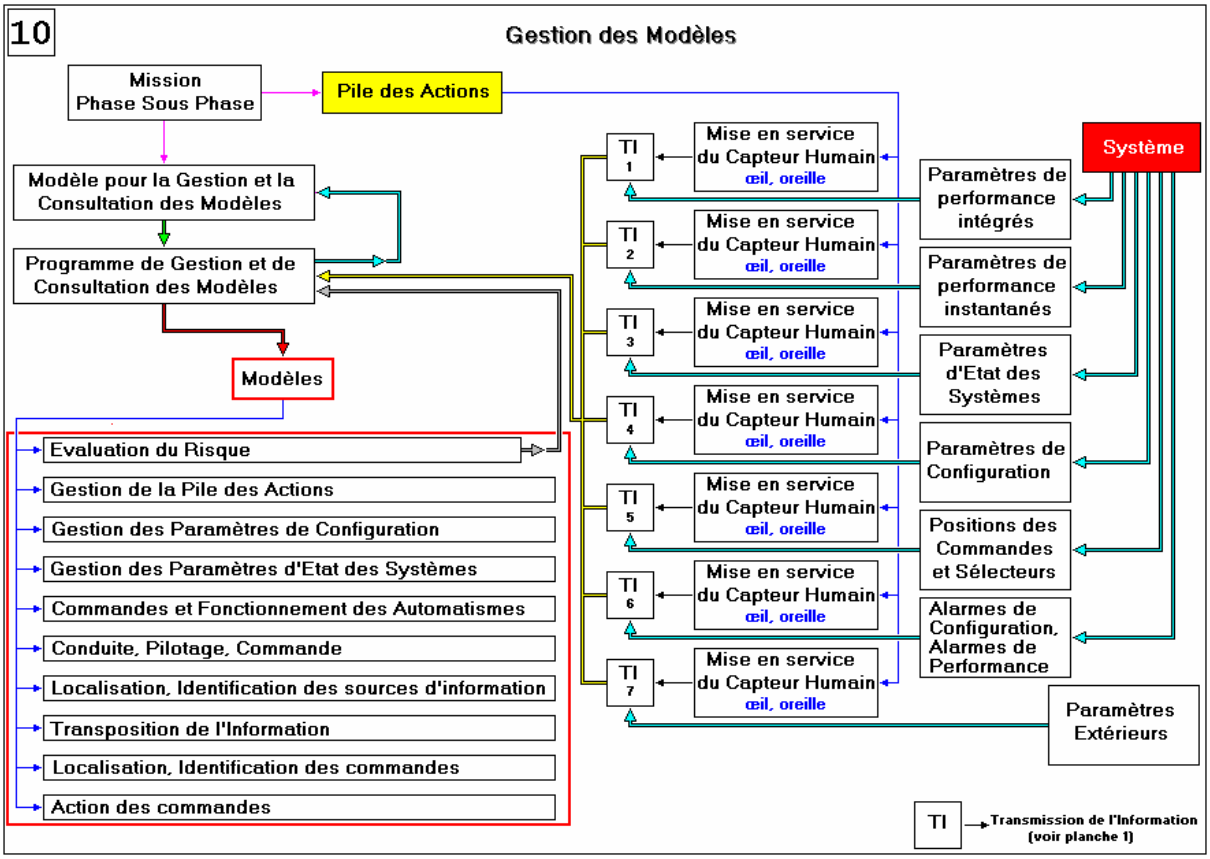
Pour les situations critiques, lorsqu'un écart sérieux est détecté, la séquence est complètement différente. Par exemple en cas d'écart sérieux sur l'angle de gîte du à une rafale la séquence peut être "*Horizon – Angle de gîte – Horizon – Effort latéral au manche – Action sur le manche – Vitesse de roulis – Angle de gîte – Horizon – rapide coup d'œil sur les autres paramètres pour détecter un autre écart – Horizon – etc*." et la fréquence de dépilage est plus élevée que lors d'un état stationnaire. Cette fréquence dépend du risque estimé.

Si l'opérateur place trop d'opérations dans la pile, il risque d'oublier les dernières, surtout si une perturbation survient le poussant à mettre de nouvelles opérations de correction dans la pile.

Un débutant place un grand nombre d'opérations dans la pile parce qu'il a à planifier tous les détails des opérations nécessaires pour atteindre l'objectif de la tâche. Un opérateur chevronné planifie beaucoup moins d'opérations car il est capable de résumer un ensemble d'opérations sous la même étiquette, ce qui ne prend qu'une seule mémoire de la pile.

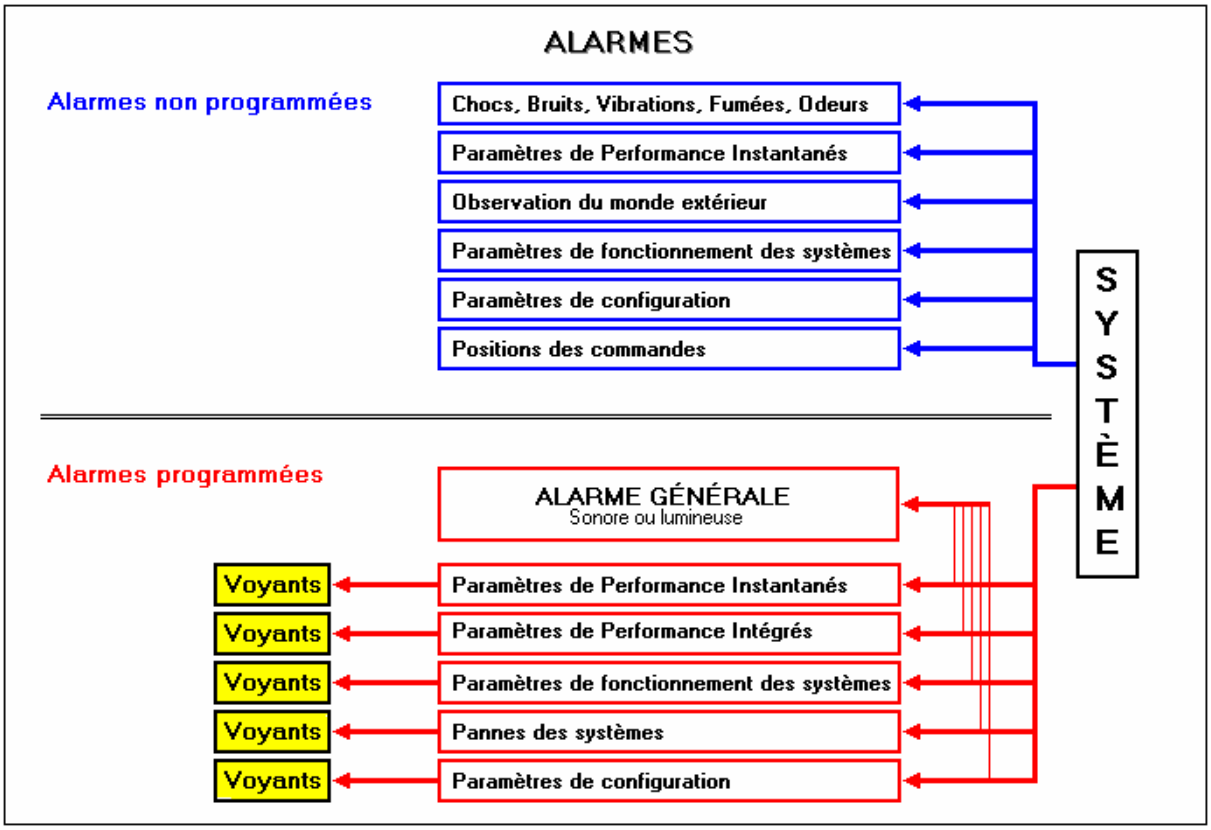
Ainsi un débutant placera dans la pile "*Pousser le manche à gauche – Attendre 30 degrés de gîte - Maintenir l'angle de gîte – Relever le cap - Attendre le cap 180 désiré - Remettre le manche à droite – Attendre l'angle de gîte nul - Mettre le manche au neutre – Relever le cap – etc."*

Un opérateur chevronné placera uniquement dans la pile "*Virer jusqu'au cap 180*", toutes les opérations élémentaires nécessaires étant réalisées "automatiquement". Il peut alors placer dans la pile l'opération "*Appeler le contrôle*" alors que le débutant y placera toute la séquence correspondant à la transmission "*Préparer le message à transmettre – Appuyer sur le bouton d'émission – etc*.". Il risque alors d'oublier la fin de l'opération de changement de cap et de rater le cap objectif.



Le modèle utilisé pour chaque opération est choisi par l'intermédiaire d'un "Modèle de Gestion et de Consultation des Modèles" qui dépend de la mission, de la Phase et de la sous Phase en cours. Le "Programme de Gestion et de Consultation des Modèles" qui en résulte dépend du recueil des paramètres en cours et du modèle de Risque lui-même.

Cette boucle, Choix des modèles, Modèle de Risque, peut être à l'origine d'un cercle vicieux. La situation semble ne pas être dangereuse. Aussi le modèle de Risque n'est pas appelé et l'opérateur ne détecte pas que la situation est devenue dangereuse.



Deux grands types d'informations peuvent parvenir à l'opérateur, s'il est en mesure de les recueillir, pour le prévenir d'une anomalie dans la conduite du système. Ce sont les alarmes programmées et les alarmes non programmées.

⇨ Les **alarmes programmées**.

Les alarmes programmées se répartissent elles-mêmes en quatre groupes de nature très différente. Ces différences de nature exigent de les présenter de façons différentes pour éviter toute ambiguïté sur leur interprétation et sur le type d'action à mener pour rétablir une situation saine.

Malheureusement ce souci est bien souvent oublié sur les panneaux de présentation d'alarmes, ce qui augmente d'autant les risques d'erreurs et de fausses manoeuvres.

⇨ les *alarmes de paramètres intégrés ou de paramètres instantanés anormaux* sont des valeurs particulières de certains paramètres, valeurs au-delà ou en deçà desquelles un risque d'accident apparaît.

Ce type d'alarme n'apporte pas d'information complémentaire à l'observation du paramètre en cause sur les panneaux d'instruments (ou à l'observation du monde extérieur sur les véhicules). Ces alarmes ont pour seul objet d'attirer l'attention de l'opérateur et le forcer à l'observation du paramètre incriminé.

A titre d'exemple, nous citerons sur avion l'alarme basse vitesse (prévention du décrochage) et les alarmes vitesse maximale (prévention d'une déformation de structure) ou nombre de Mach maximal (prévention du décrochage de compressibilité sur les avions subsoniques ou, pour les avions supersoniques, prévention d'une température d'impact trop élevée préjudiciable à la tenue des matériaux transparents et au bon fonctionnement des compresseurs des réacteurs). L'observation de l'anémomètre pour la vitesse et du machmètre pour le nombre de Mach fournit la même information ; ces alarmes ne sont donc utiles que pour attirer plus sûrement l'attention du pilote sur le risque encouru et obtenir ainsi plus rapidement un retour à la normale.

⇨ les *alarmes de paramètres de fonctionnement de système anormaux* sont des valeurs particulières de certains paramètres d'état de systèmes, valeurs au-delà ou en deçà desquelles un risque d'accident apparaît.

Là encore ce type d'alarme n'apporte pas d'information complémentaire à l'observation du paramètre en cause sur les panneaux d'instruments. Ces alarmes ont pour seul objet d'attirer l'attention de l'opérateur et le forcer à l'observation du paramètre incriminé. Dans certains cas toutefois la valeur du paramètre n'est pas fournie par un instrument. Seule l'alarme permet à l'opérateur de constater l'anomalie. Signalons les dangers potentiels de telles pratiques.

A titre d'exemple, nous citerons l'alarme signalant une pression d'huile de graissage trop faible ou l'alarme signalant une température de ventilation trop élevée.

⇨ les *alarmes de pannes* qui signalent la défaillance d'un système, d'un sous-système ou d'un organe.

Un système est reconnu comme défaillant lorsqu'il n'assure plus la fonction pour laquelle il est normalement utilisé.

Nous voyons que ce type d'alarme est très différent des deux précédents. L'observation directe des informations venant du système ne peut fournir l'information de panne. A la rigueur dans certains cas, l'opérateur par la consultation de plusieurs informations et un raisonnement plus ou moins complexe pourrait en déduire qu'un système donné est en panne, mais la démarche peut être longue et le résultat douteux.

⇨ les *alarmes de configuration* qui signalent que la configuration du système n'est pas correcte, compte tenu de la phase de la mission.

En général, ces alarmes sont peu nombreuses car délicates à programmer. Il faut en effet identifier à coup sûr la phase de la mission et comparer la configuration théorique correspondante à la configuration réelle du système.

A titre d'exemple, nous citerons l'alarme signalant, sur avion, que le train d'atterrissage est en position rentrée alors que l'avion est à basse altitude, à vitesse réduite et que les moteurs sont en configuration poussée réduite pour l'atterrissage.

Nous citerons également l'alarme signalant la position rentrée des volets au moment du décollage.

Nous voyons que ce dernier type d'alarme est encore de nature différente par rapport aux trois premiers types.

Les alarmes se présentent généralement sous forme de voyants lumineux diversement colorés, la couleur étant un moyen de les différencier suivant leur type ou suivant la gravité des conséquences de l'anomalie et le degré d'urgence de la correction à apporter.

Elles se présentent quelquefois sous forme sonore, la fréquence du son et la fréquence de répétition du signal permettant une identification de l'anomalie signalée.

Ce type de présentation des alarmes, lumineux ou sonore ne doit pas être confondu avec le *signal d'alarme général*, lui aussi sonore ou lumineux, qui n'a pour objet que d'attirer l'attention de l'opérateur et lui signaler qu'il doit observer le panneau d'alarme pour identifier l'anomalie. Mais cette alarme générale ne transmet que le message "Attention ! Une anomalie vient d'apparaître"; elle ne renseigne pas sur la nature de l'anomalie.

On notera enfin, ce qui est évident, que le système des alarmes programmées nécessite la mise en place d'un système de capteurs particuliers déclenchant la mise en service des alarmes lorsque des seuils sont dépassés, lorsque des fonctions ne sont plus assurées, lorsque des configurations anormales sont rencontrées. C'est la logique de ce système qui constitue le programme des alarmes.

⇨ **Les alarmes non programmées**.

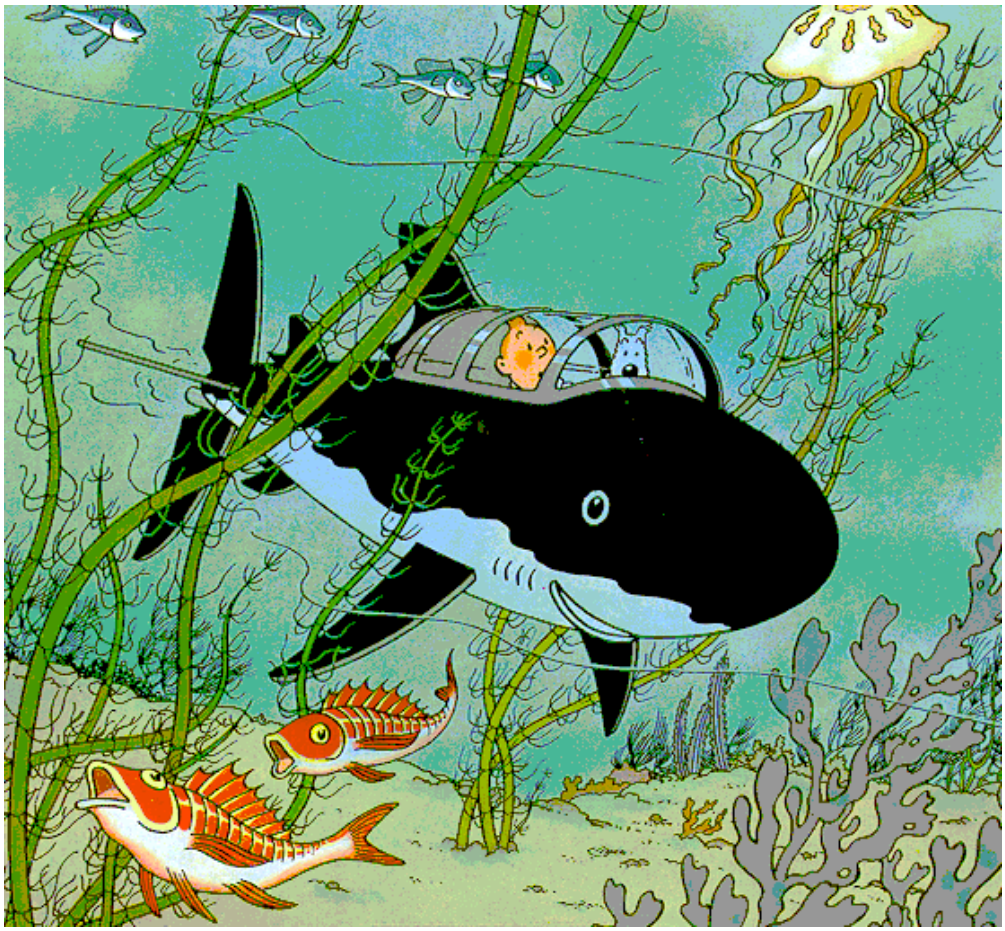
Les alarmes non programmées se répartissent également en quatre groupes :

⇨ Les *alarmes sur les paramètres intégrés et instantanés et les paramètres de fonctionnement des systèmes*. C'est l'observation des instruments qui permet à l'opérateur de détecter que certains de ces paramètres sont au-delà ou en deçà de valeurs limites autorisées. C'est ainsi que sur certains instruments analogiques la plage autorisée est représentée en vert et les plages interdites en rouge pour faciliter l'identification de l'anomalie. Ces alarmes jouent le même rôle que les deux premiers types d'alarmes programmées, mais on compte sur l'opérateur pour assurer la détection des valeurs anormales et établir la logique conduisant à l'alarme.

⇨ Les *alarmes de configuration*. Là encore on compte sur l'opérateur pour noter la différence entre la configuration théorique correspondant à la phase en cours et la configuration réelle. C'est par exemple, le contrôle de la position du train d'atterrissage en phase d'approche finale qui permettra au pilote de décider une remise des gaz si le train est rentré.

⇨ Les *alarmes sur les positions de commande*. Une position anormale de commande peut alerter l'opérateur. Ainsi en vol stationnaire sur hélicoptère, une position très à gauche (ou à droite) du manche prévient le pilote de l'approche de la limite de contrôle par vent de travers.

⇨ Les *chocs, bruits, vibrations, fumées, odeurs*, etc. avertissent l'opérateur de l'éventualité d'une anomalie. Celui-ci concentre alors toute son attention sur le recueil d'information pour détecter l'origine de l'anomalie. Ces alarmes jouent le même rôle que l'alarme générale programmée. Elles n'apportent pas d'information sur l'anomalie elle-même. Elles ne font que signaler l'apparition d'une anomalie.



d'après HERGE

ANNEXE 3

Les Grilles d'Analyse
Guide d'Analyse

Les incidents décrits dans les fiches de RETOUR D'EXPÉRIENCE doivent être présentés sous forme de chaînes d'événements de trois types

- les événements d'Opérabilité mettant en cause les caractéristiques de l'opérateur humain,
- les événements de Sensibilité aux perturbations externes et internes,
- les événements de Manœuvrabilité caractérisant les manœuvres imposées par l'objectif de la tâche ou les manœuvres de corrections d'écarts.

La description des événements eux-mêmes doit être précédée d'une description des conditions générales dans lesquelles se sont déroulés ces événements (conditions physiques telles que température, éclairage, visibilité, etc., conditions physiologiques, psychologiques et sociologiques des opérateurs.).

La connaissance de ces conditions est utile à deux titres.

- D'une part elles peuvent influer sur l'apparition des erreurs. Ainsi des températures extrêmes, une ambiance sonore intense, la fatigue, les soucis personnels, etc. réduisent les capacités des opérateurs et favorisent les erreurs, sans en être pour autant la cause directe. Elles agissent en tant qu'amplificateurs de gravité de la situation. Leur connaissance permet donc d'expliquer l'apparition d'erreurs aux cours d'événements d'opérabilité.
- Leur connaissance permet, d'autre part, d'estimer la probabilité de retrouver des conditions analogues en service et donc permet de juger l'utilité de trouver un remède pour limiter la probabilité d'apparition d'incidents du même type. Si ces conditions se révèlent exceptionnelles, on peut estimer qu'il n'est pas nécessaire de pousser l'analyse de l'incident jusqu'à la recherche de remèdes.

La GARE dresse la liste des principales conditions générales dans lesquelles se sont déroulés les événements, conditions agissant comme Amplificateurs du Risque d'Erreurs.

La GAFE est destinée à permettre d'identifier le Facteur d'Erreur caractérisant chaque événement d'Opérabilité.

Le facteur d'erreur ne caractérise pas à la nature de l'erreur elle-même commise par l'opérateur, mais plutôt les conditions particulières d'exécution de la tâche ayant favorisé l'apparition de l'erreur. Mis dans les mêmes conditions, divers opérateurs commettront des erreurs différentes, par exemple non observation d'une déviation d'un paramètre important, mauvaise décision d'action, action intempestive ou non appropriée, oubli de transmission d'une information, transmission d'une mauvaise information, erreur de destinataire, etc.

Le RADOS est destiné à identifier le ou les Défauts du Système ayant contribué à l'apparition de chaque événement d'Opérabilité, quelquefois à l'apparition des événements des deux autres types et enfin à l'origine des conditions générales favorisant l'erreur.

La GASP est destinée à identifier le type de perturbation d'un événement de Sensibilité aux Perturbations.

La GAME est destinée à identifier le type de manœuvre exécutée au cours d'un événement de Manœuvrabilité.

Ces Grilles et le Répertoire ne peuvent être utilisés sans quelques explications complémentaires qu'il est impossible d'y faire figurer pour des raisons d'encombrement évidentes. Il est donc nécessaire de les compléter par un Guide, objet de cette Annexe.

Ce Guide ne peut être utile qu'au spécialiste de l'analyse des fiches de RETOUR D'EXPÉRIENCE. Son contenu n'a rien de confidentiel, mais il est nécessaire de bien connaître les caractéristiques, bonnes et mauvaises, de l'opérateur humain pour être en mesure de l'utiliser avec profit. Il serait illusoire d'envisager de le confier aux rédacteurs des fiches en espérant les voir effectuer des analyses correctes et utilisables. Il constitue tout au plus un pense-bête permettant au spécialiste de conforter son analyse préalable en consultant les exemples d'erreurs typiques, ou les exemples de défauts du système illustrant chaque case de la Grille ou du Répertoire. Il devra être complété progressivement, par ce même spécialiste, à la lumière du retour d'expérience lui-même.

La Grille GAFE est constituée de quatre colonnes correspondant aux quatre types d'opérations rencontrées dans l'exécution de la tâche et de quatre lignes correspondant aux différents Facteurs d'Erreurs. La quatrième ligne correspondant à une Conscience Erronée de la Situation est elle-même divisée en cinq rubriques identifiant les différents modes de comportement conduisant à ce type d'état mental de l'opérateur.

Le Répertoire RADOS est constitué des mêmes quatre colonnes et de cinq groupes de lignes correspondants aux différents types de Défauts des systèmes. A chaque Facteur d'Erreur identifiée par la GAFE, on peut faire correspondre un ou plusieurs défauts système du Répertoire pouvant favoriser l'apparition de ce Facteur d'Erreur. On prendra garde au fait qu'il n'y a pas de correspondance automatique entre les Facteurs d'Erreur repérées par la GAFE et les types de Défauts du RADOS (bien qu'il y ait généralement une forte corrélation, tel type de Défaut favorisant le plus souvent tel Facteur d'Erreur).

Les grilles GASP et GAME dépendent du type de Machine dont on étudie les incidents. Il est évident qu'un avion de transport est sensible à la turbulence de l'atmosphère, ce qui n'est pas le cas pour une motrice de TGV. Les perturbations internes, c'est-à-dire les pannes, sont spécifiques. Enfin, les manœuvres imposées par la mission ou les manœuvres de correction dépendent du type de machine étudiée. L'annulation du dérapage au moment du toucher des roues au cours d'un atterrissage par vent de travers (manœuvre dite de décrabe) est spécifique à l'avion de transport et n'a pas d'équivalent sur le TGV ou une centrale nucléaire. Aussi ne donnerons-nous, en fin d'annexe, les grilles GASP et GAME utilisées dans l'aéronautique qu'à titre d'exemple.

La grille GARE dépend elle aussi du type de Machine étudiée. Nous donnons toutefois, en fin de ce chapitre, une liste assez complète, bien que sans doute non exhaustive, des facteurs d'Amplification de Risque d'Erreurs les plus courants. Chaque utilisateur pourra éliminer les facteurs non adaptés à son cas particulier.

LES OPÉRATIONS D'EXÉCUTION DE LA TÂCHE

L'étude des opérations exécutées par un opérateur, ou une équipe d'opérateurs, pour accomplir une tâche donnée, montre que ces diverses opérations sont de quatre types. Ainsi toute tâche peut être décrite par une succession d'opérations des types suivants, correspondant au mode de fonctionnement séquentiel dit "en canal unique" de l'opérateur.

- Saisie de l'information,
- Traitement de l'information aboutissant à une décision,
- Transmission de l'information,
- Action

(L'ordre de succession des opérations n'est pas systématiquement l'ordre indiqué ici, la décision pouvant par exemple être de saisir une autre information).

Saisie et traitement de l'information (sigle **s**)

L'opérateur capte une information par l'un de ses sens. Dans un processus industriel, la capture d'information se fait très généralement par les yeux (lecture d'un instrument, observation de l'environnement,...), souvent par l'ouïe (capture d'un message oral, reconnaissance d'un signal sonore, voire d'un bruit,...) ou par le toucher (reconnaissance de la forme, de la position d'une commande, évaluation de l'effort sur une commande,...), plus rarement par l'odorat (reconnaissance d'une odeur anormale,...) ou par le goût (eau plus ou moins salée,...).

La saisie de l'information nécessite:

⇨ la mise en service volontaire du capteur humain (opération cognitive)

⇨ la référence, plus ou moins consciente, à trois types de modèles stockés de façon plus ou moins parfaite dans la mémoire de l'opérateur (voir Annexe 2)

- → le modèle de localisation des sources d'information (pour savoir où capter l'information recherchée),
- → le modèle d'identification des sources d'information (pour pouvoir vérifier, si nécessaire, que la source d'information est bien celle souhaitée),
- → les modèles de transposition de l'information (ces modèles permettent de transformer une information brute, position d'une aiguille, couleur d'un voyant, forme d'un sigle ou d'une icône, en une information utilisable par le cerveau pour une décision ultérieure).

Il peut être utile de préciser si la source d'information est le système lui-même (transmission d'information Machine ⇨ Homme) ou un autre opérateur (transmission Homme ⇨ Homme). Si la source d'information est la machine, l'opération de saisie est déclenchée par une décision de l'opérateur (la décision pouvant être "forcée" par la machine dans le cas d'une alarme). Si la source d'information est un autre opérateur communiquant verbalement, l'opération de saisie est "forcée" par l'émetteur du message et l'information est en général fugitive. Les erreurs sont analogues dans les deux cas mais les défauts système à l'origine peuvent être très différents. Si nécessaire, le sigle **s** pour saisie sera complété du sigle **mh** (transmission d'information Machine ⇨ Homme) ou du sigle **hh** (transmission Homme ⇨ Homme).

Décision (sigle **d**)

Après avoir saisi une ou plusieurs informations, l'opérateur en fait une synthèse pour prendre une décision sur la suite à donner quant à l'exécution de sa tâche. La décision peut être de plusieurs sortes:

⇨ attendre, c'est-à-dire reporter à plus tard, avec un délai estimé, la capture d'autres informations (balayage des diverses informations disponibles ou capture d'un paramètre précis dont on prévoit la variation à terme),

⇨ saisir une autre information précise pour compléter la synthèse,

⇨ déterminer la commande sur laquelle on va agir, avec évaluation du sens et de l'amplitude de l'action sur la commande,

⇨ transmettre une information avec détermination de la nature du message, du mode de transmission et du destinataire.

La prise de décision nécessite la connaissance des modèles de fonctionnement du système à contrôler, c'est-à-dire les relations entre commandes, état de l'environnement et paramètres d'état du système. Certaines décisions peuvent être prises à l'aide de procédures qui facilitent l'interprétation des informations et le choix d'actions qui en résulte, sans passer par les modèles de fonctionnement du système.

Transmission de l'information (sigle **t**)

Les transmissions d'information sont multiples. Elles dépendent de la nature du message à transmettre, du moyen de transmission, du destinataire.

Les **messages** peuvent être

⇨ des messages oraux exprimés en langage naturel,

⇨ des messages exprimés en langage normalisé (message dont la forme et/ou le contenu ont été précisés par une règle générale de transmission),

⇨ des messages exprimés en langage codé (code alphabétique ALPHA pour A, ..., ZOULOU pour Z),

⇨ des messages réduits à la valeur d'un paramètre, valeur numérique, valeur binaire ou discrète, etc.

Les **moyens de transmission** sont également variés,

⇨ transmission orale, par sifflet, etc.

⇨ transmission à l'aide d'un clavier (clavier type ordinateur, pavés spécialisés, touche unique spécialisée, bouton poussoir de commande de la sirène d'alarme générale, etc.)

⇨ transmission par signaux optiques, par gestes, par pavillons, etc..

⇨ transmission par bâton pilote, etc.

⇨ transmission écrite manuelle, etc.

Le **destinataire** peut être

⇨ un autre membre de l'équipe (en vue directe ou non),

⇨ un opérateur ou un groupe d'opérateurs extérieurs,

⇨ l'opérateur lui-même pour une mémorisation de l'information à usage ultérieur.

⇨ un système de stockage de l'information

→ introduction d'une valeur de consigne pour un automatisme
→ entrée d'une donnée dans un historique
→ entrée d'une donnée dans un cahier de signalement
→ entrée dans une fiche de signalement d'avarie
→ compte rendu d'événement (fiche RETOUR D'EXPÉRIENCE), etc.

La **transmission d'information** nécessite pour l'opérateur de disposer de modèles stockés de façon plus ou moins parfaite dans sa mémoire, à savoir des modèles (voir Annexe 2)

⇨ de localisation des moyens de transmission,
⇨ d'identification des moyens de transmission
(pour pouvoir vérifier, si nécessaire, que le moyen de transmission est bien celui souhaité),
⇨ de mode d'action des moyens de transmission,
⇨ d'identification des organismes destinataires.

Il peut être utile de préciser si le destinataire de l'information transmise est le système lui-même (transmission d'information Homme ⇨ Machine) ou un homme (transmission Homme ⇨ Homme). Les erreurs sont analogues dans les deux cas mais les défauts système à l'origine peuvent être très différents.

Si nécessaire le sigle **t** pour transmission sera complété
du sigle **hm** (transmission d'information Homme ⇨ Machine)
ou du sigle **hh** (transmission Homme ⇨ Homme).

Action (sigle **a**)

L'opérateur actionne une commande, en général à l'aide de la main, d'un doigt, quelque fois avec le pied. Pour les opérations de maintenance les commandes peuvent être les divers outils, les commandes des outillages et les commandes des systèmes de contrôle et de mesure.

Toute action nécessite

⇨ la mise en service volontaire de l'actionneur humain (main, doigt ou pied), (opération cognitive),
⇨ la référence, plus ou moins consciente, à quatre types de modèles, stockés de façon plus ou moins parfaite dans la mémoire de l'opérateur, à savoir des modèles (voir Annexe 2)
→ de localisation des commandes (pour savoir où se situe la commande désirée),
→ d'identification des commandes (pour pouvoir vérifier que la commande saisie est bien celle souhaitée); ce modèle peut se réduire à la reconnaissance par la forme, la taille, la couleur.
→ de mode d'action des commandes (pour savoir dans quel sens agir pour obtenir l'effet désiré, tirer, pousser, lever, tourner à gauche, etc.)
→ de localisation du retour d'information sur l'état de l'organe commandé (l'état de l'organe commandé n'est pas toujours fourni par la position de l'actionneur lui-même; ainsi dans le cas d'une commande de vanne par bouton poussoir agissant sur un moteur d'ouverture ou de fermeture, il est nécessaire d'avoir une information sur la position de la vanne *elle-même*).

Certaines opérations de transmission d'information (par manipulation de claviers et de touches) s'apparentent à des actions sur des commandes. On prendra garde à ne pas les confondre. Une action a pour objet une modification de l'état du système, ce qui n'est pas le cas pour une transmission d'information (la distinction est subtile lorsque la transmission d'information est l'envoi d'une valeur de consigne à un automatisme).

Il faut enfin noter qu'une tâche peut être décrite par une succession d'opérations des quatre types décrits; mais, nous l'avons déjà dit, cette succession n'est pas systématiquement dans l'ordre Saisie d'information, Décision, Transmission et Action.

GRILLE DES FACTEURS AMPLIFICATEURS DE RISQUE D'ERREUR

⇨ Facteurs physiques. (sigle **Pk)**

⇨ Facteurs externes. (sigle **Pke)**

⇨ Confort réduit
- sièges
- posture anormale
- local confiné, étroit
- travail dans l'espace

⇨ Tenue de travail gênante
- combinaison de sécurité (sécuracide, spatiale, etc.)
- gants, bottes, casque, lunettes, masque (antipoussière, oxygène), écouteurs, sourdines

⇨ Mouvements de plate-forme
- vibrations
- secousses
- oscillations lentes
- travail en impesanteur
- travail sous facteur de charge

⇨ Ambiance
- Températures extrêmes
- Pression anormale (travail en caisson pressurisé, à faible pression)
- Humidité
- Eclairage violent ou trop faible
- Bruits
- Odeurs

⇨ Horaire d'exécution de l'opération à l'instant de l'incident
- Début de mission, Fin de mission
- Reprise du service, remise en route des installations
  le matin, en début de semaine, après un jour chômé, après une période de congé annuel
- Arrêt du service, arrêt des installations
  le soir, en fin de semaine, avant un jour chômé, avant la période de congé annuel
- Opérations pendant le week end, un jour chômé, pendant la période de congé annuel
- Changement des équipes de quart
- Après un changement des horaires (systèmes de transports)

⇨ Tâches spéciales
- Entraînement sur système réel
- Entraînement sur simulateur
- Essai sur système réel
- Essai sur simulateur
- Mission non commerciale (convoyage, ..)

⇨ Etat du système à l'instant de l'incident
- Fonctions non assurées par la machine
- Capteurs, chaînes de transmission de données, afficheurs en panne
- Commandes, chaînes de commande, actionneurs en panne
- Chaînes de transmission, émetteurs, récepteurs en panne
- Systèmes, sous systèmes, automatismes en panne

⇨ **Facteurs internes.** **(**sigle **Pki)**
⇨ Utilisation de médicaments
⇨ Absorption d'alcool
⇨ Usage de drogues

⇨ **Facteurs physiologiques. (**sigle **Pg)**
⇨ Fatigue
⇨ Besoins
- Faim
- Soif
- Besoins naturels

⇨ Etats pathologiques
- Nausées
- Etats "grippaux"
- Douleurs (tête, dents, oreilles, yeux, dos, etc.)
- Douleurs gastriques, abdominales, musculaires, articulaires, etc.
- Démangeaisons
- Incapacitation (évanouissement, décès)
- etc.

⇨ **Facteurs psychologiques. (**sigle **Pz)**
⇨ Peur
⇨ Angoisse
⇨ Préoccupations personnelles
- heureuses (réussite amoureuse, promotion, gain au jeu, etc.)
- malheureuses (échec amoureux, réprimande, perte au jeu, problèmes de santé, etc.)

⇨ Préoccupations et soucis familiaux (maladie d'un membre de la famille, naissance prochaine, chômage du conjoint, d'un enfant, problèmes financiers, etc.)
⇨ Etat psychopathologique (perte de mémoire, "folie", etc.)

⇨ **Facteurs sociologiques. (**sigle **S)**

⇨ **Facteurs internes. (**sigle **Si)**

⇨ Composition de l'équipe ou de l'équipage
⇨ qualification des membres (ancienneté, connaissances) *
⇨ sous effectif occasionnel
⇨ présence de stagiaires
⇨ conflits internes à l'équipe

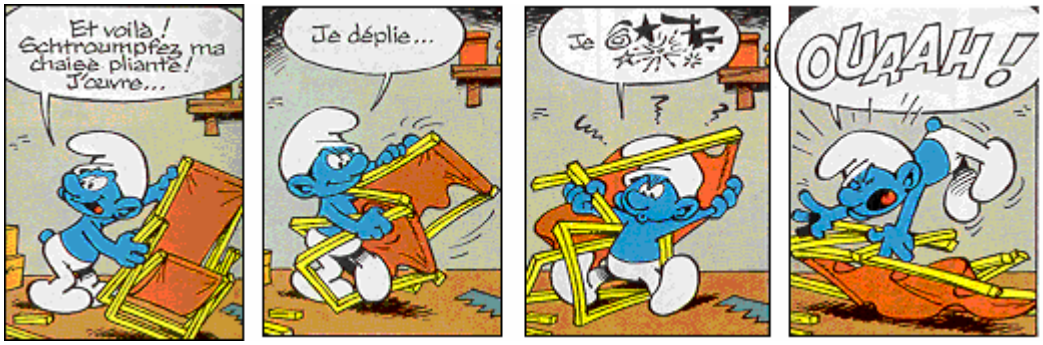
⇨ **Facteurs externes. (**sigle **Se)**

⇨ Climat social (grèves, manifestations)
⇨ Présence d'un visiteur
⇨ Présence d'un instructeur
⇨ Présence d'un examinateur
⇨ Présence d'une personnalité

On notera que parmi ces facteurs, certains sont directement dus à une mauvaise conception ergonomique du poste (confort, tenue de travail, ambiance), à des problèmes d'organisation (horaires, besoins physiologiques ou facteurs sociologiques) ou à des problèmes de conception de base (pannes de la machine). Il faut les signaler à ce stade d'observation car ils constituent des facteurs aggravant pouvant expliquer les erreurs observées, mais il faut également les noter parmi les défauts du système à corriger.

A la suite d'un accident, l'enquête permet généralement de retrouver la plus grande partie de ces facteurs. Par contre, dans bien des cas de simples incidents, il est difficile d'obtenir des renseignements suffisants pour déterminer les facteurs psychologiques et sociologiques internes.

* Voici quelques exemples de composition d'équipage entraînant des risques:
- Un officier brillant, mais jeune et sans grande expérience pratique et un vieux sous officier très pragmatique et peu soucieux des aspects théoriques.
- Un commandant de bord ancien et un tout jeune copilote, avec deux attitudes possibles du commandant,
  - bienveillant, il se préoccupe de la formation de son jeune collègue et en oublie de mener à bien sa propre tâche,
  - malveillant, il ne pense qu'à mettre en évidence les manques de son collègue et à s'en indigner.
- Equipage constitué de deux commandants de bord de même ancienneté.



d'après PEYO

Voici un bon exemple d'utilisation d'un mauvais Modèle de Fonctionnement d'un Système.

LES FACTEURS D'ERREURS (Grille GAFE).

⇨ **Les Facteurs d'Erreur liés aux caractéristiques et limitations anatomiques et physiologiques des opérateurs**

→ **Lapsus** (sigle **L**) ou **maladresses**.
Les lapsus peuvent être gestuels (on accroche une commande avec la manche, on tape sur la touche d'à côté, on écrit une lettre à la place d'une autre ou on inverse les lettres d'une syllabe), verbaux (on prononce un mot à la place d'un autre), visuels (on "voit" un signal qui n'a pas été émis), auditifs (on entend une alarme qui n'a pas retenti).

→ **Charge de travail** (sigle **C**),
La charge de travail est trop élevée, conduisant à un échec de l'opération par saturation des possibilités de l'opérateur.

⇨ **Les Facteurs d'Erreurs liés aux caractéristiques psychologiques des opérateurs**

→ **Absence de stimuli** (sigle **A**),
Le manque de stimuli en provenance du système conduit à une perte de vigilance de l'opérateur.

→ **Conscience erronée de la Situation** (sigle **S**)
Ces erreurs peuvent être divisées en cinq groupes,

→ Une Image Présente, Externe ou Interne, est erronée (Sigle **SPE** ou **SPI**)
La mauvaise image provient en général d'une mauvaise saisie d'une information ou d'un message.
→ Une Image Future, Externe ou Interne, est erronée (Sigle **SFE** ou **SFI**)
La mauvaise image provient en général de l'utilisation d'un modèle de fonctionnement erroné.
→ Une Image Désirée, Externe ou Interne, est erronée (Sigle **SDE** ou **SDI**)
La mauvaise image provient en général de l'utilisation d'un mauvais modèle de tâche.
→ Utilisation d'une Image, Externe ou Interne, "a priori" (Sigle **SAE ou SAI**)
Refus de l'information qui permettrait de rétablir la vérité.
→ Utilisation d'un mauvais Modèle de Risque
Les images présentes, futures et désirées sont exactes mais l'opérateur sous estime le risque lié à la situation. Pour une mauvaise estimation du risque correspondant à la situation externe sigle **SRE**. Pour une mauvaise estimation du risque correspondant à la situation interne sigle **SRI**.

⇨ Enfin une dernière ligne peut être crée portant le sigle **X** pour couvrir les cas qui n'entreraient dans aucune des rubriques précédentes, dans la mesure où nul ne peut prétendre à l'exhaustivité. Bien entendu, un événement ne peut être classé dans cette dernière ligne qu'avec des justifications appropriées et une révision de la grille doit être proposée pour couvrir les cas analogues.

UTILISATION DE LA GRILLE GAFE.

Pour chaque événement d'Opérabilité, il faut se poser deux questions,

- dans quelle catégorie se classe l'opération de déroulement de la tâche au cours de laquelle s'est produit l'événement, autrement dit dans quelle colonne de la grille se situe l'événement décrit ?
- sous quelle rubrique se classe le Facteur d'Erreur d'Opérabilité étudié, autrement dit dans quelle ligne de la grille le plaçons-nous ?

Dans bien des cas il est impossible de choisir une case unique pour caractériser l'événement parce que l'on manque d'informations. Ainsi, seul l'opérateur peut préciser, par exemple, qu'il a saisi la mauvaise commande parce que sa charge de travail était trop élevée (Ca), parce qu'il utilisait un mauvais modèle de localisation des commandes (SPIa) ou par suite d'une simple maladresse (La). Dans le doute, il faut caractériser l'événement par les trois sigles possibles (Ca ou SPIa ou La). Enfin, la reconnaissance d'une maladresse simple n'est à envisager que si l'on peut éliminer les quatre autres cas possibles (C, A, S).

Par ailleurs le choix de la colonne ne fait qu'identifier l'opération au cours de laquelle l'erreur s'est manifestée.

Dans bien des cas le fait qu'une erreur survienne à l'occasion de telle ou telle opération n'est qu'anecdotique. Mis dans les mêmes conditions un autre opérateur ou le même opérateur commettrait une erreur à l'occasion d'une opération d'un autre type.

Ceci est toujours le cas pour le Facteur d'Erreur Absence de Stimuli conduisant à la chute de la vigilance. Dans ce cas, il est inutile en conséquence de préciser la colonne et le sigle caractérisant le Facteur d'erreur se réduira à A sans plus de précision.

C'est souvent vrai pour le Facteur d'Erreur Charge de Travail élevée. Néanmoins il peut être utile de préciser la colonne pour pouvoir vérifier ultérieurement, lors de la comparaison de plusieurs incidents du même type, si l'erreur ne survient pas quasi systématiquement pour le même type d'opération, ce qui peut être un guide utile pour déterminer le type de Défaut Système en cause. Si par exemple on constate que l'erreur survient souvent au cours d'une saisie d'information, il faut vérifier si la procédure ne conduit pas à une surcharge de travail en exigeant de nombreux relevés de paramètres dans un temps trop court.

La précision de l'opération en cours est très utile dans le cas du Lapsus car le type d'opération en cause caractérise le type de lapsus, visuel, verbal, auditif ou gestuel. Par exemple un lapsus gestuel peut être l'indication d'une mauvaise disposition des commandes favorisant une maladresse.

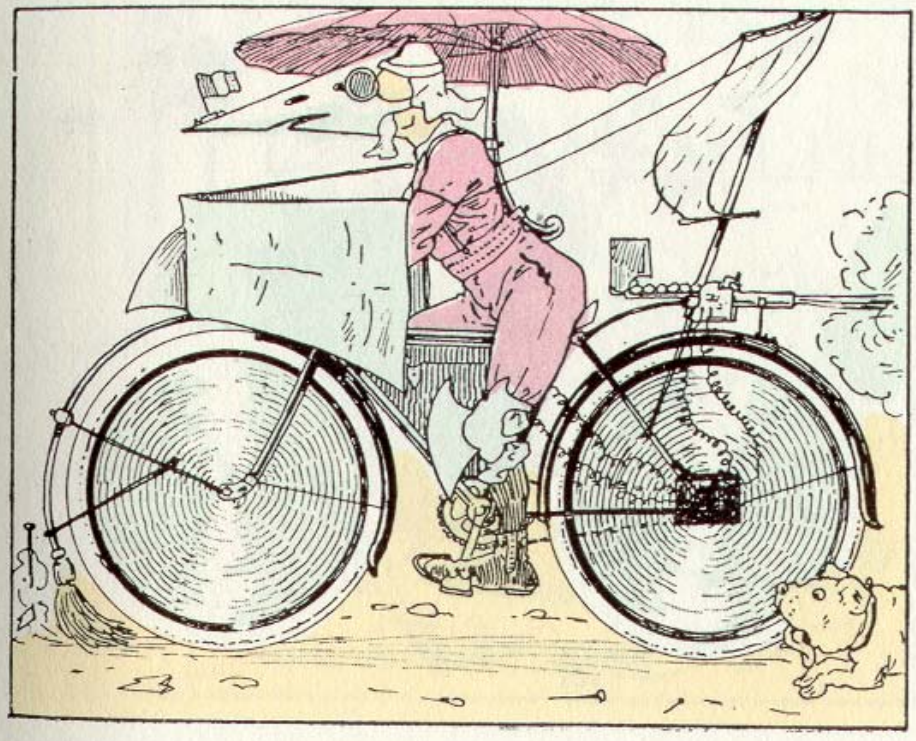
Enfin dans les cas de la Conscience Erronée de la Situation, la précision de la colonne n'est utile que pour la première rubrique, Mauvaise Image Présente, pour préciser au cours de quelle opération, saisie d'information, transmission d'information, action, la fausse image a été forgée. Pour les quatre autres rubriques préciser la colonne ne fait que signaler au cours de quelle opération l'erreur est survenue, ce qui n'est qu'anecdotique et ne caractérise pas le Facteur d'Erreur.

Dans certains cas il est difficile, par manque d'information à la lecture du rapport d'incident, de préciser la colonne de la grille. On remplace alors les sigles s, d, a et t par le sigle *.

GRILLE D'ANALYSE DES FACTEURS D'ERREURS

GAFE

		Opérations d'exécution de la tâche au cours de laquelle survient l'erreur			
FACTEUR D'ERREUR ⇩		Saisie et traitement de l'information s Homme ⇩ Homme (hh) / Machine ⇩ Homme (mh)	Décision après traitement de l'information d	Transmission de l'information t Homme ⇩ Homme (hh) / Homme ⇩ Machine (hm)	Action après décision a
CHARGE DE TRAVAIL C Charge trop élevée Saturation		Cs	Cd	Ct	Ca
ABSENCE DE STIMULI A Perte de vigilance		A			
LAPSUS L		Ls	Ld	Lt	La
CONSCIENCE ERRONÉE de la SITUATION S	Image en cause				
Image Présente Erronée	Externe	SPEs	SPEd	SPEt	SPEa
	Interne	SPIs	SPId	SPIt	SPIa
Image Future Erronée	Externe	SFE			
	Interne	SFI			
Image Désirée Erronée	Externe	SDE			
	Interne	SDI			
Image A Priori	Externe	SAE			
	Interne	SAI			
Modèle de Risque Erroné	Externe	SRE			
	Interne	SRI			



Or ce que Cosinus avait trouvé c'était l'*anémélectroreculpédalicoupeventombrosoparacloucycle*, dans lequel sont utilisées toutes les forces propulsives connues et même inconnues. Il l'a fait exécuter et un beau jour il s'élance, suivi de Sphéroïde.

D'après Christophe

LES TYPES DE DÉFAUTS SYSTEME (Répertoire RADOS)

Les types de Défauts sont regroupés en cinq classes.

⇨ la **mauvaise organisation** du travail de l'équipe, de l'unité, de la direction, de l'entreprise, etc. (sigle **O**).

Ces défauts se divisent eux-mêmes en quatre catégories

⇨ *les opérateurs ne savent pas ce qui est de leur responsabilité*, ce qu'ils doivent faire eux-mêmes, ce qu'ils ne doivent pas faire, ce qu'ils peuvent déléguer, quelles informations ils doivent transmettre. En conséquence, ils omettent une opération croyant qu'elle n'est pas de leur ressort ou exécutent une action normalement impartie à un autre opérateur. Ce type d'erreur est bien souvent à l'origine d'une erreur de représentation pour un autre opérateur.
(Réponse à la question *Qui doit faire ?*, sigle complémentaire **r** pour responsabilité)

⇨ *les définitions des objectifs, des contraintes, des marges disponibles comportent des erreurs, ce que nous regrouperons sous le terme de Tâches mal définies.* En particulier, les situations nominales recommandées sont trop près des limites, ce qui laisse des marges trop faibles pour couvrir les aléas (erreur d'Opérabilité, Perturbations, Manœuvres). Ou encore l'opérateur se définit un objectif de tâche qui ne lui a pas été prescrit ("faire l'heure", "atterrir à tout prix", etc).
(Réponse à la question *Que doit-on faire ?*, sigle complémentaire **e** pour exécution)

⇨ *les opérateurs ne disposent pas de moyens suffisants,* en personnel ou en matériel, pour exécuter leur tâche. Cela conduit en général à des surcharges de travail, quelque fois de courte durée, mais suffisantes pour conduire à l'erreur. Ce cas se rencontre souvent dans les postes de travail à charge moyenne faible ne justifiant pas un nombre d'opérateurs suffisant pour faire face aux pointes.

Tâche prévoyant des transmissions d'informations alors que les moyens de transmission ne sont pas disponibles (centre de contrôle fermé la nuit par exemple).
(Réponse à la question *Quels moyens pour faire ?*, sigle complémentaire **m** pour moyen)

⇨ *les opérateurs ne savent pas comment exécuter leur tâche* ou encore les procédures qu'on leur impose sont mal adaptées aux caractéristiques de l'opérateur humain et aux moyens dont ils disposent en homme et matériel.
(Réponse à la question *Comment faire ?*, sigle complémentaire **p** pour procédure)

Cette situation a des origines multiples,

- procédures matériellement défectueuses (erreurs de frappe, photocopie imparfaite, etc.),

- procédures imparfaites parce que mal rédigées, complexes, non expliquées,
- procédures trop générales laissant l'opérateur devant un choix difficile à faire,
- procédures imposant des charges de travail ponctuelles trop élevées ou imposant des tâches fastidieuses (longs temps d'attente entre opérations, attente d'un événement qui ne se produit que très rarement, surveillance sans événements notoires) néfastes à la vigilance (attention il ne s'agit pas de charger les opérateurs par des opérations artificielles ou inutiles !), etc.

Cela se traduit le plus souvent par des opérations manquées à l'origine d'erreurs de représentation pour l'opérateur lui-même ou pour un autre opérateur qui pense que la tâche de son collègue a été correctement exécutée.

Il est à noter qu'il est quelquefois difficile de distinguer les défauts de type **e** (Que doit-on faire ?) des défauts de type **p** (Comment doit-on faire ?). Est-ce la procédure qui traduit mal la tâche ou est-ce la tâche qui a été mal définie ? Il est toutefois important de faire la distinction car les remèdes sont différents.

⇨ la **mauvaise conception de la machine** (sigle **H**)

La conception de base repose sur des hypothèses ne prenant pas en compte toutes les situations envisageables et conduit dans certains cas, rares mais possibles, à des situations dangereuses.

La conception des interfaces ne tient pas compte des caractéristiques physiques, physiologiques ou psychologiques de l'opérateur moyen.

Les interfaces sont les pupitres d'instruments, les pupitres de commandes, les transparents isolant le poste de commande du monde extérieur, les moyens d'observation de l'environnement, les moyens de communication entre les opérateurs, les textes de consignes et de procédures.

Ces défauts peuvent être divisés en trois groupes,

→ *mauvaise conception de base*
(sigle complémentaire **b** pour base)
Structure ne résistant pas dans des conditions particulières, automatismes conduisant à des situations dangereuses, ..

→ *mauvaise conception de l'interface sur le plan ergonomie mécanique*
(sigle complémentaire **m** pour mécanique)
Eclairage, chauffage, ventilation, sièges, disposition, taille des afficheurs, disposition, taille, forme, débattements des commandes, disposition, forme, taille, couleur, caractères des étiquettes, ..

→ *mauvaise conception de l'interface sur le plan ergonomie mentale*
(sigle complémentaire **c** pour conception)
Echelles, zéros des afficheurs, sens d'action des commandes, synoptiques, schémas sur écran, ..

⇨ la **mauvaise conception de la formation** (sigle **F**)

Ces défauts peuvent être divisés en deux groupes,

→ *mauvaise conception de la formation de base*
(sigle complémentaire **b**)
- méconnaissances dans le domaine de la formation élémentaire, lecture, écriture, calcul mental, arithmétique, langage parlé ou écrit, etc.
- méconnaissances dans le domaine des techniques, mécanique, physique, électricité, électronique, informatique, aérodynamique, hydraulique, résistance des structures, usinage, soudure, langage technique, etc.
- méconnaissances de l'organisation générale de l'entreprise et de ses objectifs, des règles générales de transmission de l'information, des règles de sécurité, méconnaissances en matière de facteur humain, etc.

→ *mauvaise conception de la formation spécifique au système*
(sigle complémentaire **s**)
méconnaissances
- des modèles de fonctionnement du système conduisant à des erreurs de décisions,
- des modèles utilisés pour la captation d'information,
- des modèles utilisés pour l'action sur les commandes,
- de l'organisation en cours (répartition des tâches),
- des procédures,

- manque d'entraînement ou mauvaises méthodes d'entraînement,
- mauvaise mise à jour des connaissances (formation continue).

⇨ les **Défauts de conception ou de réalisation de la Documentation,**
les **Informations erronées, non transmises ou matériellement mal transmises** aux utilisateurs,
(sigle **D**)
La documentation comprend la documentation technique relative aux matériels, les documents de navigation (cartes et documents terrains), les documents administratifs, etc.
Les informations, qui constituent une documentation provisoire, concernent les modifications de matériels, de procédures, d'organisation, les incidents ou accidents identifiés, etc.

→ *Défauts matériels*
(sigle complémentaire **m**)
Documentation inexistante, mal présentée matériellement (photocopie défectueuse, taille ou volume incompatible avec une utilisation dans le poste, etc.).

Information non transmise (erreur de transmission, liste de destinataires incomplète ou erronée), mal présentée matériellement ou mal transmise (Fax défectueux, incomplet, etc.).

→ *Contenu erroné*

(sigle complémentaire **c**)

Les données fournies par la documentation conduisent à des erreurs quant aux modèles utilisés pour la saisie des données, les décisions, la transmission des informations et les actions sur les commandes.

La documentation est rédigée par les concepteurs et non adaptée aux besoins de l'utilisateur qui n'y trouve pas ce qu'il y cherche.

Quelquefois les opérateurs utilisent une documentation "sauvage" (carnet personnel dont le contenu est incontrôlable).

Les informations fournies contiennent des erreurs (codes de référence incomplets ou contenant des fautes de frappes, schémas faux, incomplets ou périmés, etc.).

D'après PEYO

Exemple de mauvaise conception de la documentation.

⇨ **Réglementation inadaptée** (sigle **R**).

L'évolution des techniques, des méthodes d'utilisation des matériels peuvent rendre caduques et même néfastes des règles qui se sont montrées longtemps utiles et efficaces. Ce type d'erreur apparaît surtout lorsque les règlements ont été rédigés en imposant des moyens plutôt que des objectifs de sécurité.

⇨ Enfin, une dernière ligne portant le sigle **Z** peut être crée pour couvrir les cas qui n'entreraient dans aucune des rubriques précédentes, dans la mesure où nul ne peut prétendre à l'exhaustivité. Bien entendu, un défaut ne peut être classé dans cette dernière ligne qu'avec des justifications appropriées et une révision du répertoire doit être proposée pour couvrir les cas analogues.

RÉPERTOIRE D'ANALYSE DES DÉFAUTS OPÉRATIONNELS DU SYSTÈME

RADOS

	Opérations d'exécution de la tâche au cours de laquelle est survenue l'erreur induite par le défaut système			
TYPE DE DÉFAUT SYSTÈME ⇩	Saisie et traitement de l'information **s**	Décision après traitement de l'information **d**	Transmission de l'information **t**	Action après décision **a**
	Homme ⇩ hh Homme / Machine ⇩ mh Homme		Homme ⇩ hh Homme / Homme ⇩ hm Machine	
ORGANISATION **Or** Qui doit faire ? (responsabilité)	Ors	Ord	Ort	Ora
ORGANISATION **Oe** Que doit-on faire ? (exécution)	Oes	Oed	Oet	Oea
ORGANISATION **Om** Quels moyens pour faire ? (moyens)	Oms	Omd	Omt	Oma
ORGANISATION **Op** Comment doit-on faire ? (procédures)	Ops	Opd	Opt	Opa
CONCEPTION de BASE **Hb** Conception reposant sur des hypothèses douteuses ou des principes inadaptés	Hbs	Hbd	Hbt	Hba
CONCEPTION des INTERFACES **Hm** Mauvaise ergonomie mécanique des interfaces	Hms	Hmd	Hmt	Hma
CONCEPTION des INTERFACES **Hc** Mauvaise conception des interfaces (ergonomie mentale)	Hcs	Hcd	Hct	Hca
FORMATION **Fb** Formation de base insuffisante	Fbs	Fbd	Fbt	Fba
FORMATION **Fs** Formation spécifique insuffisante	Fss	Fsd	Fst	Fsa
DOCUMENTATION **Dm** Défauts matériels	Dms	Dmd	Dmt	Dma
DOCUMENTATION **Dc** Contenu défectueux Documentation "sauvage"	Dcs	Dcd	Dct	Dca
RÉGLEMENTATION **R**	Rs	Rd	Rt	Ra

GOOF

RAFT

GASP

GAME

GARE

GAFE a été traduit en anglais par GOOF (Grid Of Operator Failure d'où Goofy, personnage bien connu de Walt Disney) et RADOS traduit par RAFT(radeau) (Rapid Analysis Failures Table)
"To make a Smurf gasp" signifie "couper le souffle à un Schtroumpf".

GRILLE D'ANALYSE DES ÉVÉNEMENTS DE SENSIBILITÉ AUX PERTURBATIONS

GASP

Grille définie pour l'étude des incidents et accidents d'avions de transport civils

Perturbations externes	Sigle
rafale	Sraf
gradient de vent	Sgrv
turbulence	Stur
foudroiement	Sfdr
givrage	Sgiv
grêlons	Sgrl
variation brutale de l'état de la piste (trous, flaque d'eau, etc.)	Spst
oiseaux	Soix

Perturbations internes	Sigle
panne de système (il s'agit de la perturbation provoquée par l'apparition de la panne et non de l'effet de la panne établie)	Span
feu	Sfeu
perte de pressurisation	Sprs
perturbation commise par un passager	Spax

Ces grilles sont caractéristiques du système de transport civil aérien. Elles ne sont valables que dans ce cas.

GRILLE D'ANALYSE DES ÉVÉNEMENTS DE MANŒUVRABILITÉ

GAME

Grille définie pour l'étude des incidents et accidents d'avions de transport civils

Manœuvres correctives	Sigle
correction de vitesse ou de Mach	Mcm
correction d'incidence ou d'assiette longitudinale	Mci
correction de dérapage	Mcd
correction d'assiette latérale	Mca
correction de cap	Mcc
correction d'altitude	Mch

Manœuvres imposées par la mission	Sigle
changement de vitesse ou de Mach	Mmm
changement de pente (en particulier arrondi)	Mmp
changement de cap (mise en virage, virage, sortie de virage)	Mmc
changement d'altitude (mise en montée ou en descente, montée ou descente, mise en palier)	Mmh
changement de configuration (train, volets, etc.)	Mmf

Ces grilles sont caractéristiques du système de transport civil aérien. Elles ne sont valables que dans ce cas.

L'ANALYSE

L'analyse d'un incident doit se faire de la façon suivante.

- Identifier les conditions générales dans lesquelles s'est déroulé l'incident (utilisation de la grille GARE pour préciser les facteurs d'amplification de gravité). Cette première analyse doit permettre d'estimer la probabilité de retrouver des incidents analogues dans les mêmes conditions générales.

- Identifier l'événement final ayant conduit à la catastrophe ou ayant conduit à une situation potentiellement dangereuse. Ainsi, le franchissement intempestif d'un feu rouge en voiture peut se traduire par un accrochage plus ou moins dramatique (pertes de vies humaines, blessures, dégâts matériels), par un incident plus ou moins fâcheux (prison, retrait du permis de conduire, amende, etc.), par une simple peur rétrospective ou par rien du tout si l'on n'a rien vu !. Quelles que soient les conséquences de l'événement final, il est important d'analyser la succession des événements qui en sont à l'origine.

- Identifier et décrire chronologiquement les événements d'Opérabilité, de Manœuvrabilité, de Sensibilité aux Perturbations ayant conduit à l'événement final.

  En pratique, cette recherche se fait en remontant dans le temps la suite des événements en se posant à chaque étape la question "quels sont les événements préalables qui ont conduit le système et le ou les opérateurs à être dans cette situation ?". La chronologie n'est rétablie qu'une fois identifiés tous les événements et doit être vérifiée à nouveau en "descendant" le temps.

- Caractériser chaque événement d'Opérabilité en utilisant la GAFE. Bien noter que plusieurs événements avec erreurs de l'opérateur peuvent être en cause et ne pas s'en tenir à la dernière erreur.
  Noter le Type d'Opération au cours de laquelle l'erreur a été commise et le Facteur d'Erreur, c'est-à-dire les conditions dans lesquelles l'erreur a été commise.

- Une fois la chronologie établie, rechercher pour chaque Facteur d'Erreur ainsi identifié, pour les Facteurs Amplificateurs de Risque et quelquefois pour les événements de Sensibilité aux perturbations et les événements de Manœuvrabilité, le type de Défaut système qui peut être à l'origine de cette situation et le caractériser par une case du Répertoire RADOS.
  Il n'y a pas de correspondance systématique entre une case de la GAFE, une rubrique de la GARE, de la GASP ou de la GAME et une case du RADOS, tout au plus des corrélations fortes. Ainsi une erreur due à une charge de travail trop élevée (Cs ou Ca) est en général la conséquence d'une procédure mal adaptée (Ops ou Opa), mais elle peut aussi avoir pour origine une mauvaise conception de l'interface (Hms ou Hma) ou une erreur d'organisation (Oms ou Oma).
- Il se peut par ailleurs que l'on ne puisse identifier sûrement le Facteur d'Erreur et le type de Défaut. Ainsi l'action intempestive sur une commande

peut être soit un Lapsus (La) résultant d'une mauvaise conception de l'interface (touches de clavier trop petites et trop rapprochées par exemple) (Hma), soit une Conscience Erronée de la Situation Présente (SPIa) (mauvaise connaissance du modèle de positionnement des commandes) due à un défaut de Formation spécifique (Fsa). L'analyse devra proposer ces différentes possibilités.

- Certains facteurs d'amplification de risque d'erreur identifiés par la grille GARE peuvent avoir pour origine des Défauts Système. Il convient d'identifier ces Défauts au même titre que les défauts à l'origine des événements d'Opérabilité. Ainsi l'inconfort dû au port de casques ou de gants mal adaptés relève de Défauts du type Hm (Interface Homme Machine sur le plan mécanique). La présence de visiteurs intempestifs ou de personnalités, la constitution d'équipages "à risque", relèvent de Défauts d'Organisation.
  Bien entendu, les facteurs cités dans la grille GARE n'ont pas tous un Défaut Système pour origine. Ainsi les soucis financiers ou les déboires sentimentaux des opérateurs ne relèvent pas d'un Défaut Système, ce qui ne les empêche pas d'influer sur leur comportement !

- Enfin certains événements relevant de la GASP ou de la GAME peuvent avoir pour origine un Défaut système. Par exemple une procédure mal conçue peut conduire à effectuer une manœuvre d'amplitude anormalement élevée, à subir une rafale trop importante (la procédure n'a pas interdit la sortie en mer par vents force 10), à subir une panne dangereuse (procédure de maintenance défectueuse), etc.

- Une fois identifiés les Défauts Système chercher leurs fréquences d'apparition dans les analyses des autres incidents et si nécessaire envisager des mesures correctives.

  La fréquence d'apparition d'un Défaut, et du Facteur d'Erreur dont il est la cause, n'est qu'un guide pour décider de l'urgence et de la nécessité d'élaboration d'un remède. La fréquence critique peut se réduire à l'unité si les conséquences potentielles de l'incident sont suffisamment graves et surtout lorsque l'on constate que la catastrophe peut être déclenchée à la suite d'une seule erreur humaine, car la probabilité d'erreur humaine est trop grande pour faire reposer la sécurité sur l'hypothèse que l'opérateur est suffisamment formé et entraîné pour éviter l'erreur.

Retour d'Expérience sur le Retour d'Expérience !

Les notions de Facteur d'Erreur et d'Amplificateur de Risque.

L'utilisation des grilles pour l'analyse des incidents, en particulier les incidents de la base de donnée de l'ASRS*, nous a montré que la notion de Facteur d'Erreur n'était pas toujours bien comprise par les analystes. Il y a souvent confusion dans les esprits entre Facteur d'Erreur, Cause et Type d'Erreur.

Un Facteur d'Erreur, rappelons-le une fois de plus, définit les conditions au cours desquelles une erreur est commise, mais ne caractérise ni le type d'erreur commise, ni les causes de cette erreur. Par exemple une Charge de Travail élevée peut amener l'opérateur à ne pas remarquer la dérive d'un paramètre important, d'oublier d'exécuter une action nécessaire de correction, d'exécuter une autre action que celle nécessaire, de mettre trop de temps à l'exécuter, d'oublier de transmettre un message, etc. Mais le même Facteur d'Erreur peut ne conduire à aucune erreur. Mis dans la même situation, avec le même Facteur d'Erreur, par exemple au cours d'un exercice au simulateur reproduisant cette situation, deux opérateurs différents ou le même opérateur au cours de deux exercices différents, commettront des erreurs différentes. Ainsi les types d'erreur ne sont pas caractéristiques d'un Facteur d'Erreur.

Un Facteur d'Erreur définit la situation mentale de l'opérateur au moment où il commet une erreur.

Cette définition explique pourquoi nous avons mis dans la même grille GAFE, la Charge de Travail élevée, l'Absence de Stimuli, la Maladresse et les cinq cas de Conscience Erronée de la Situation.

Montrons, à l'aide d'un modèle de fonctionnement très simpliste du cerveau, ce que nous appelons "situation mentale" de l'opérateur.

Dans le cas du premier Facteur d'Erreur, Charge de Travail élevée, le cerveau de l'opérateur n'a pas assez de neurones disponibles pour exécuter la tâche requise. Dans le second cas, Absence de Stimuli, les neurones sont "déconnectés" de l'évolution de la tâche à surveiller et "connectés" sur une tâche étrangère, souvenir du dernier film, de la dernière partie de campagne, du bricolage en cours,... Pour le Facteur Maladresse, les neurones de l'opérateur ne sont pas correctement connectés, ce qui conduit à une mauvaise exécution de l'opération prévue, recueil d'information, action sur une commande, nature du message oral, etc. Dans ce cas de Maladresse, il est souvent difficile de préciser pourquoi et comment les neurones sont mal connectés, sauf, quelquefois, dans le cas d'une fausse manœuvre quand l'opérateur réagit instinctivement sans noter les obstacles dans son environnement ou dans le cas du message erroné quand l'opérateur utilise le mauvais mot parce qu'il vient juste d'entendre ce dernier. Enfin dans les cas de Conscience Erronée de la Situation, la fausse image conduit à des connexions inadéquates des neurones.

Ne donnons pas à ce modèle du cerveau plus de valeur qu'il n'en a, c'est-à-dire aucune ! Il ne représente qu'une image commode pour illustrer notre propos.

---

* La base ASRS est un recueil, sous la responsabilité de la NASA, d'environ 80 000 rapports volontaires d'incidents survenus dans le domaine du transport aérien. Elle est gérée par la société Batelle.

Au cours d'une analyse d'un accident ou d'un incident, il est très important de ne pas s'en tenir au niveau de la grille GAFE des Facteurs d'Erreur, mais d'essayer d'expliquer la présence de ces Facteurs d'Erreur en examinant la grille RADOS. Les cinq articles de cette grille donnent une origine possible des Facteurs d'Erreur. Nous préférons utiliser le terme "origine" plutôt que "cause", parce que l'identification des causes profondes d'une erreur relève du travail du psychologue et non de celui du technicien. L'identification des origines d'un Facteur d'Erreur, plutôt que de ses causes, est suffisante pour l'objectif poursuivi par le technicien de la sécurité, à savoir définir les modifications à apporter au Système pour améliorer la sécurité.

D'un autre côté, nous pensons que les psychologues doivent maintenir la grille GAFE telle quelle, parce qu'elle aide à préciser la situation mentale de l'opérateur au cours de chacun des événements conduisant à un accident. Mais les psychologues doivent compléter cette grille par une autre grille, parallèle à la grille RADOS, montrant la relation entre les Facteurs d'Erreur et les erreurs elles-mêmes. Ce travail est très important mais il dépasse les compétences des techniciens !

Nous avons également observé, lors de nos études avec la NASA, la tentation, pour les analystes en formation, à mélanger les articles de la GARE avec ceux de la GAFE, c'est-à-dire à confondre les Facteurs d'Erreur avec les Amplificateurs de Risque.

Or il y a une grande différence entre ces deux notions. Un Facteur d'Erreur caractérise une situation mentale temporaire de l'opérateur. Un Amplificateur de Risque est plus permanent et est présent dans un certain nombre d'événements. Un Amplificateur de Risque, par exemple la fatigue ou une préoccupation d'ordre sociologique, accroît le désordre mental lorsque celui-ci est déjà présent. Par exemple, en utilisant notre modèle simpliste du cerveau, la fatigue réduit le nombre de neurones disponibles pour faire face à une charge de travail donnée ou augmente le nombre de mauvaises connexions conduisant à la maladresse. Des préoccupations réduisent les chances de détecter une fausse image de la situation opérationnelle. Mais nous devons noter que la fatigue est sans effet si aucun Facteur d'Erreur n'est présent. Fatigué ou non, un opérateur ne commettra pas d'erreur s'il n'a rien à faire ! Ainsi les Amplificateurs de Risque ne sont-ils jamais seuls à l'origine d'un accident, sauf peut-être dans les cas, peu fréquents, où l'opérateur est totalement hors circuit, mort ou évanoui.

Il est néanmoins important, au cours d'une analyse, d'identifier les Amplificateurs de Risque.

Répétons ce que nous avons déjà dit sur ce sujet. L'ensemble des Amplificateurs de Risque, présents dans un incident ou un accident, donne une idée de la probabilité d'observer le même type de situation dans d'autres cas. A titre d'exemple, une erreur est commise par Charge de Travail trop élevée, avec un équipage très fatigué, une météo exécrable (turbulence, grêle, éclairs,..), un pilote dont l'épouse est sur le point d'accoucher, un copilote en cours de divorce et en présence du président de la compagnie dans le cockpit ! Il n'est sans doute pas nécessaire d'envisager une modification coûteuse du cockpit pour réduire la charge de travail dans une situation analogue.

Par contre les Amplificateurs de Risque ont généralement une origine qui peut être identifiée par un article de la grille RADOS. Les défauts du système ainsi identifiés doivent alors être pris en compte au même titre que les défauts à l'origine des Facteurs d'Erreur.

EXEMPLES ILLUSTRANT L'UTILISATION DE LA GRILLE GAFE

Il s'agit seulement d'illustrer chaque case de la grille GAFE pour mieux faire comprendre ce qu'en couvre le sigle. Les exemples donnés se réfèrent à de nombreux domaines hors aéronautiques pour souligner l'universalité des facteurs d'erreur. Ils ne constituent pas une liste exhaustive, loin s'en faut et doivent être complétés par l'expérience de chacun.

⇨ Charge de travail trop forte

→ Au cours d'une opération de conduite, l'opérateur doit, dans un temps réduit, exécuter trop d'opérations pour accomplir la tâche requise (par exemple reconfiguration rapide après panne). Il n'observe pas une variation significative sur un paramètre important en dehors de son champ d'action immédiat.

Ainsi le conducteur arrivant dans un rond point, doit lire les nombreuses destinations possibles en cherchant mentalement la correspondance entre la destination désirée et les destinations proposées. Il ne note pas que la voiture qu'il suit vient de s'arrêter avant de pénétrer sur le rond point. (**Cs**)

→ Au cours d'une opération de maintenance corrective à effectuer dans un temps limité pour des raisons de délai de retour à la disponibilité opérationnelle, l'opérateur se trompe en relevant une valeur de contrôle à vérifier avant de poursuivre sa tâche. (**Cs**)

→ De nombreux paramètres sont à relever et à synthétiser dans un temps très court. L'opérateur commet alors une erreur de diagnostic en ignorant par exemple un paramètre essentiel ou se contente d'une décision réflexe reposant sur une analyse trop partielle de la situation. (**Cd**)

→ L'opérateur ayant à transmettre un message urgent pendant une période "chargée", ne transmet pas le message, en transmet un erroné, se trompe de destinataire ou de canal de transmission. (**Ct**)

→ Au cours d'une opération de conduite, l'opérateur doit, dans un temps réduit, exécuter trop d'opérations pour accomplir la tâche requise, reconfiguration après avarie par exemple. Il rate ou oublie d'effectuer une action sur une commande ou encore se trompe de commande. (**Ca**)

→ Au cours d'une opération de maintenance corrective à effectuer en temps limité pour des raisons opérationnelles, l'opérateur se trompe de pièce à échanger et laisse la pièce défectueuse en place. (**Ca**)

→ Le conducteur, absorbé par une discussion compliquée sur son téléphone portable, ne voit pas un obstacle sur la route. (**Cs**)

Tous ces exemples montrent que le type d'opération, saisie d'information, décision, transmission ou action, n'a, en général, qu'un caractère anecdotique. Il n'est toutefois pas inutile de le préciser, si possible, afin de vérifier que pour des incidents analogues si c'est très souvent le même type d'opération qui est en cause. Dans ce cas le type d'opération est un guide pour détecter un défaut système contribuant à l'activation du facteur d'erreur. Si par exemple, par charge de travail élevée, les opérateurs commettent quasi systématiquement une erreur de lecture sur un même paramètre, il faut, non seulement rechercher l'origine de la charge de travail elle-même, procédure mal adaptée par exemple, mais également vérifier si l'erreur de lecture ne provient pas d'un

instrument difficile à lire ou à interpréter (défaut d'interface). C'est ce genre d'analyse qui conduit à interdire l'utilisation du téléphone portable au volant.

Une charge de travail élevée suffit quelquefois à expliquer l'incident ou l'accident. Ainsi, une panne de moteur au décollage, peut induire une charge de travail telle que le pilote ne note pas la perte d'altitude ou un changement de cap conduisant à une situation dangereuse ou fatale. Dans d'autres cas la charge de travail élevée peut conduire seulement à une conscience erronée de la situation par mauvaise identification de l'image présente. Il convient dans ce cas de noter, en plus de la charge de travail élevée, cet autre facteur d'erreur, conscience erronée de la situation, dont les conséquences peuvent conduire, à terme et non pas immédiatement, à une situation dangereuse.

⇨ Absence de stimuli, Perte de vigilance

- → L'opérateur placé devant un panneau de contrôle dont les informations sont figées depuis plusieurs heures, ne note pas la dérive d'un paramètre important ou l'apparition d'une signalisation de panne parce que sa vigilance est amoindrie par une situation non évolutive ne lui fournissant aucune information intéressante.
- → Surveillance du scope de contrôle pour la détection des fissures d'essieu, avec une détection très rare d'anomalie.
- → Surveillance du scope radar pour assurer l'anticollision avec les autres navires, avec une détection très rare d'objectifs.
- → Au cours d'une opération de maintenance un opérateur laisse déborder un réservoir car l'opération de remplissage se déroule depuis de longues minutes, sa seule tâche étant d'attendre la fin de cette opération.
- → La situation est stable et l'opérateur en conclut qu'elle va le rester et qu'il n'est pas nécessaire de surveiller le processus. Il peut aussi faire un diagnostic réflexe reposant sur une erreur de reconnaissance de la situation.
- → L'opérateur, ayant à transmettre un message de routine au cours d'une attente avec "rien à signaler", ne transmet pas le message, transmet un message erroné ou se trompe de destinataire. Il peut également se tromper de canal de transmission par erreur de touche.
- → L'opérateur placé devant un panneau de contrôle dont les informations sont figées depuis plusieurs heures n'agit pas sur une commande au moment requis parce que sa vigilance est amoindrie.
- → Le conducteur sur une autoroute quasi rectiligne, sans trafic et de nuit se met à rêvasser et ne note pas un obstacle.

Tous ces exemples montrent que le type d'opération, saisie d'information, décision, transmission ou action, n'a qu'un caractère anecdotique et ne caractérisent en rien le facteur d'erreur. Il est donc inutile de la noter.

Une chute de vigilance peut conduire en outre une conscience erronée de la situation par mauvaise identification de l'image présente. Il convient dans ce cas de noter, en plus de la chute de vigilance, cet autre facteur d'erreur, conscience erronée de la situation, dont les conséquences peuvent conduire, à terme et non pas immédiatement, à une situation dangereuse.

⇨ Lapsus

- → Lecture erronée d'une étiquette, par exemple CR00012 au lieu de CR00021, bien que l'étiquette soit parfaitement éclairée et correctement écrite.(**Ls**)

→ L'opérateur croit entendre un message d'alarme alors que ce n'est qu'un bruit sans signification. (**Ls**)

→ L'opérateur croit entendre le message "DIX" en réponse à une interrogation alors que son interlocuteur a répondu "SIX". (**Lt**)

Il est parfois difficile de faire la différence entre ce type d'erreur, très courante dans la vie de tous les jours, et l'erreur de modèle a priori (**SAE** ou **SAI**) pour laquelle l'opérateur "ne lit ou n'entend que ce qu'il s'attend à lire ou à entendre"

"Le robinet CR0012 doit être ici"; je vois l'étiquette CR0021 et je me dis "c'est bien ce que je pensais, voici le robinet CR0012".

"La situation est délicate! d'ici qu'une alarme retentisse il n'y a pas loin"; j'entends un bruit et me dis "c'est bien ce que je pensais, voilà l'alarme".

"Le collègue doit normalement me répondre DIX"; j'entends un bruit et je me dis" c'est bien ce que je pensais, c'est bien DIX".

→ L'opérateur a bien analysé la situation mais il prend la décision contraire ou toute autre décision par "confusion mentale".(**Ld**)

L'opérateur a identifié que le bogie avant était défectueux et il démonte le bogie arrière tout en pensant qu'il fait attention à démonter "le bon".

Le pilote a parfaitement compris qu'il devait virer à droite mais il prend la décision contraire en confondant droite et gauche.

Il est souvent difficile de distinguer ce type de lapsus du lapsus d'Action (**La**) ou du lapsus de saisie de l'information (**Ls**).

→ Lapsus verbal. Le passager d'une voiture pense qu'il faut commander une manœuvre "à gauche" et il prononce "à droite". Le contremaître commande "à descendre" alors qu'il pense attentivement à bien commander "à monter". (**Lt**)

→ Lapsus gestuel. L'opérateur veut atteindre une commande un peu éloignée et il accroche au passage une autre commande. Sur mouvement inattendu de plate-forme, une commande ou une action "de travers" est enclenchée. Au lieu de passer de la position phares à la position codes, le conducteur manœuvre la commande d'essuie glaces. L'opérateur appuie sur la mauvaise touche ce qui conduit à une erreur de destinataire (qui n'a pas fait un faux numéro de téléphone sans que la Poste soit en cause). (**La**)

C'est souvent ce genre d'erreur qui figure implicitement dans les rapports d'incidents derrière les vocables "maladresses" ou "action malencontreuse". Il est parfois bien difficile à l'analyse de faire la différence entre l'erreur gestuelle et l'erreur de modèle de localisation des commandes.

Il est ici important de noter l'opération élémentaire au cours de laquelle s'est produite l'erreur, car elle est significative du type de lapsus.

⇨ Conscience erronée de la situation

⇨ Image présente erronée

→ L'opérateur oublie de renouveler son image mentale de la situation et raisonne sur une image "vieillie" qui ne reflète plus la réalité, certains paramètres ayant changé. "Il n'y a aucun obstacle autour du véhicule, je l'ai vérifié (en réalité cette vérification date de quelques instants et la situation s'est modifiée); je peux donc effectuer ma manœuvre en toute sécurité !". (**SPEs**)

→ Le courant a été coupé et l'opérateur l'a vérifié il y a plusieurs minutes. Il ne pense pas à le vérifier à nouveau avant une nouvelle intervention, alors que la tension a été rétablie, entre temps, par un autre opérateur. (**SPEs**)

→ L'opérateur confond, lors d'une opération d'échange d'essieu sur une voiture SNCF, le repérage par rapport au boggie et le repérage par rapport à la voiture (mauvais modèle de repérage). (**SPEs**)

→ L'opérateur se trompe d'instrument de contrôle; il lit la température à relever sur le troisième thermomètre et non sur le quatrième. (**SPIs**)

C'est le cas typique d'erreur de modèle de localisation de la source d'information dont les origines possibles sont multiples (voir les exemples RADOS),

- entraînement sur un pupitre simulé non conforme au pupitre opérationnel (l'opérateur est "intellectuellement" au fait de cette différence mais le réflexe acquis à entraînement l'emporte sur la connaissance),(Défaut Système Fss)
- disposition des instruments sur le panneau en contradiction avec la disposition spatiale des points de mesure sur le système réel ou sur le schéma de conduite(Défaut Système Hcs).

Ce type d'erreur peut être aggravé par une erreur du modèle d'identification des sources d'informations si la distinction entre une dizaine d'instruments de mêmes formes ne peut se faire que par lecture d'un étiquetage ésotérique; par exemple étiquettes K22A, K22B, K22C,..... pour des points de mesure repérés sur le schéma T421, T422, T423,....cet état de fait malheureux provenant du fait que les numérotations sur le pupitre et sur le schéma de conception, utilisé pour la conduite, ont été faites par des responsables n'ayant pas les mêmes préoccupations et surtout pas celle de la conduite (Défaut Système Hcs).

→ L'opérateur relève une valeur erronée d'un paramètre parce qu'il n'a pas noté la position d'un commutateur de changement d'échelle. Il interprète la position de l'aiguille avec une mauvaise échelle (erreur de modèle de transposition). (**SPIs**)

→ Un bouton poussoir permet, à chaque appui, de modifier la valeur de l'échelle de mesure et/ou le type de paramètre mesuré. Le résultat de cette action est affiché en bonne et due place, mais l'opérateur ignorant la dernière action sur le poussoir (de sa part ou, plus grave, de la part d'un autre opérateur) oublie de consulter cette information sur l'indicateur auxiliaire et interprète à tort l'information transmise par l'indicateur principal (erreur du modèle de localisation ou erreur de modèle de transposition). (**SPIs**)

→ L'opérateur relève une valeur erronée d'un paramètre parce qu'il se trompe sur la valeur du zéro de l'échelle (c'est le seul instrument du panneau dont la

graduation débute à 20 et non à zéro) (erreur de modèle de transposition). (**SPIs**)

→ Au cours d'une opération de maintenance**,** l'opérateur relève une valeur erronée à l'aide de son multimètre car il a oublié que l'échelle des ohms est croissante vers la gauche (erreur de modèle de transposition). (**SPIs**)

→ Au cours d'une opération de maintenance l'opérateur relève la tension en un mauvais point du circuit (erreur de modèle de localisation de la source d'information). (**SPEs**)

→ L'opérateur utilise un système de transmission inadapté à la situation. Il se trompe de destinataire (il transmet à la hiérarchie au lieu du collègue) ou de nature de message (il croit nécessaire de transmettre telle information alors que le destinataire en attend une autre). Il se trompe de moyen de transmission (message oral au lieu de message écrit). Il estime qu'il suffit de transmettre sur un réseau de diffusion générale, sans préciser son code émetteur ni celui du destinataire, ni s'assurer de l' "Accusé de réception" ("A toi"). (**SPEt**)

Il est parfois difficile de trouver le Défaut Système origine de ce type d'erreur, Défaut d'organisation "qui doit faire ?" (Ort), Défaut d'organisation "comment faire ?" (Opt), Défaut d'organisation "que doit-on faire ?" (Oet) ou Défaut de formation (Fbt ou Fst).

→ L'opérateur ferme une vanne en tournant le volant dans le sens classique alors qu'il est en présence d'une vanne particulière qui se ferme en sens inverse (erreur de modèle de sens d'action), (**SPIa**)

→ L'opérateur ferme CJ 00120 au lieu de CJ00012 par mauvaise identification de la commande (erreur de modèle d'identification des commandes), (**SPIa**)

→ L'opérateur vérifie le résultat de son action sur une vanne par l'intermédiaire d'un poussoir actionnant un moteur de fermeture et se trompe d'indicateur de retour de position. (**SPIa**)

Les deux dernières erreurs sont à rapprocher des erreurs de saisie d'information mais résultats et remèdes sont différents.

→ L'opérateur agit sur le troisième levier au lieu du quatrième, (**SPIa**)

Il est très difficile, sans investigation précise auprès des opérateurs en cause de préciser l'origine de l'erreur. L'opérateur a-t-il saisi le levier trois parce qu'il avait compris, en formation, que c'était sur le levier trois qu'il fallait agir dans ce cas particulier (erreur de modèle de localisation des commandes) ? L'a-t-il saisi à la suite d'une mauvaise décision résultant d'une conscience erronée de la situation due à une mauvaise saisie d'information ? S'agit-il d'un simple lapsus gestuel ? Seul l'opérateur lui-même peut lever le doute, mais non un observateur extérieur.

⇨ Image future erronée

L'opérateur utilise un modèle faux, dû par exemple à une formation inadaptée ou à un modèle simpliste. Il utilise ainsi un modèle général de fonctionnement du système, valable dans 95% des cas, alors que la situation du système exigerait un modèle plus élaboré ou un modèle différent (voir Défaut Système Fsd).

→ Le pilote pense que la trajectoire future lui permettra d'éviter le relief en montée alors que les performances de l'avion sont insuffisantes. (**SFE**)

- → Le pilote pense qu'en tirant sur le manche l'avion va se mettre en montée permanente alors qu'il est au second régime à basse vitesse. (**SFI**)
- → Le pilote pense qu'en mettant les manettes plein gaz, il va obtenir rapidement la poussée maximale alors que celle-ci n'est atteinte qu'avec un délai de plusieurs secondes. (**SFI**). Ce type d'erreur est sans doute l'une des causes de l'accident de l'Airbus A320 d'Habsheim.
- → Le contrôleur aérien vient d'autoriser le décollage et il pense que la piste est immédiatement disponible pour l'atterrissage d'un autre avion. (**SFE**)
- → L'opérateur chargé du profilage des roues au tour en fosse (SNCF) ne change pas les données de référence en passant d'un modèle à un autre. (**SFI**)
- → L'opérateur démonte le troisième disjoncteur et non le quatrième parce qu'il est convaincu que c'est le troisième qui commande le système défaillant dont il a la réparation à charge. Il raisonne sur un modèle de fonctionnement inadapté. (**SFI**)
- → Le pilote a programmé le FMS pour effectuer une mise en palier à 10000 ft avec réduction de vitesse à 250 kt. Mais une modification de la piste en service a effacé cette opération et le pilote ne remet pas en cause la programmation car il en ignore les conditions de modifications.

⇨ Image désirée erronée

- → Le pilote pense que le tour de piste se fait à gauche comme d'habitude alors que c'est le tour de piste à droite qui doit être exécuté sur ce terrain particulier. (**SDE**)
- → Le pilote pense qu'il doit virer à droite après décollage alors que la procédure en vigueur sur ce terrain demande un virage à gauche. (**SDE**)
- → Le pilote pense qu'il est autorisé à décoller immédiatement alors que seule l'autorisation de pénétrer sur la piste et de s'aligner lui a été transmise. (**SDE**)

  Toutes ces erreurs sont difficiles à distinguer des erreurs de saisie d'information lors de l'écoute des messages du contrôle.
- → Le pilote pense que la piste en service est la 22 L alors que c'est la 22 R et il décolle sur la mauvaise piste. Il est souvent difficile de faire la différence entre ce type de facteur d'erreur et l'erreur de saisie d'information conduisant le pilote à prendre, par mauvaise visibilité, la piste gauche pour la piste droite.
- → Le pilote pense que l'altitude minimale de décision est de 300 pieds alors qu'elle est de 500 pieds sur ce terrain. (**SDE**)
- → L'opérateur de maintenance pense qu'il doit effectuer une révision hebdomadaire rapide alors qu'il s'agit d'une grande révision annuelle. (**SDI**)

⇨ Image a priori

- → Au cours d'une opération de conduite ou de maintenance, l'opérateur lit une valeur erronée ou interprète faussement une indication par voyants parce qu'il est convaincu que la valeur relevée ou la signalisation "doit être normale" puisque la situation était jusqu'à présent normale et qu'il a, pense-t-il, effectué correctement les opérations nécessaires.
- → Au cours d'une opération de maintenance, l'opérateur remplace successivement plusieurs exemplaires d'un même système, les jugeant tous défectueux, alors que la panne vient d'ailleurs.
- → Au cours d'une opération de maintenance, l'opérateur met en place un système sortant de révision. Il le juge "bon" a priori et cherche la panne ailleurs si une anomalie est détectée.

→ Au cours d'une opération de maintenance dans un atelier de la RATP, un opérateur ayant terminé sa tâche sur fosse, transmet l'information "train bon", puis, constatant qu'il a oublié d'effectuer une opération, coupe à nouveau le courant, verrouille le disjoncteur avec le cadenas et retourne dans la fosse sans prévenir. Le conducteur chargé de sortir le train, sachant le "train bon" croît que l'opérateur a oublié de remettre le courant et de retirer le cadenas; il rétablit la tension en "court-circuitant" la sécurité imposée par le cadenas.

→ L'opérateur mesure la tension sur un circuit normalement coupé et interprète ce qu'il lit sur le voltmètre comme une erreur de l'instrument et non comme la présence réelle d'une tension. (exemple de mauvaise utilisation du VAT Vérificateur d'Absence de Tension utilisé par EDF).

Dans tous ces cas l'opérateur ne tient compte que des informations confirmant le modèle a priori qu'il s'est forgé (j'ai coupé le disjoncteur et ai vérifié sa coupure; le voltmètre est donc faux et je n'en tiens pas compte; le cadenas est en place, mais je connais l'opérateur, il est étourdi et ce jour là très pressé de rentrer chez lui !).

→ Dans le même esprit, on remarquera que bien souvent, à la lecture d'un compte-rendu de réunion, on constate que les divers participants n'ont entendu que ce qu'ils désiraient entendre.

→ L'opérateur sait qu'une panne est déjà survenue. Un fonctionnement anormal survient, accompagné ou non d'une alarme. L'opérateur attribue ce dysfonctionnement à la panne connue sans faire un diagnostic plus approfondi ("ça y est, ça recommence !).

→ Au moment précis d'une action sur une commande une alarme survient. L'opérateur ne pousse pas le diagnostic plus loin et attribue la cause de l'anomalie à son action.

→ Le pilote a placé la palette de train sur sortie et il pense que quelques instants plus tard le train est effectivement sorti.

→ Le pilote a programmé le FMS pour effectuer une mise en palier à 10000 ft avec réduction de vitesse à 250 kt. Mais une modification de la piste en service a effacé cette opération et le pilote ne remet pas en cause la programmation. Ce cas est différent de celui, analogue, cité plus haut dans le cas de l'Image future erronée. Ici le pilote, bien que connaissant les facéties du FMS, les ignore et se forge une image future a priori. Il est toujours difficile, dans la pratique, de distinguer les deux cas sauf à interroger le pilote.

⇨ Modèle de Risque erroné

→ Le pilote poursuit l'approche au-dessous de la MDA (Minimum Decision Altitude) se croyant suffisamment habile pour réussir l'atterrissage.

→ La vitesse d'approche est très élevée, la piste est courte et mouillée et le pilote tente néanmoins l'atterrissage se sentant capable de stopper l'avion avant la fin de piste.

→ Pour gagner du temps le pilote bâtit une procédure "exotique" passant trop près du relief.

→ Le pilote d'un avion de ligne passe volontairement dans un cumulonimbus très développé en sous estimant le risque de turbulence.

→ Le pilote d'avion léger s'engage dans une vallée étroite sous la couche pensant qu'il sera toujours possible de faire demi-tour.

→ Le pilote d'avion léger passe au-dessus de la couche en comptant sur un trou lui permettant de descendre à vue à destination, alors que l'avion n'est pas équipé pour le vol aux instruments.

→ Le conducteur pense qu'il peut rouler à une vitesse très supérieure à la vitesse autorisée car son expérience lui a montré qu'il n'a encore jamais eu d'incidents dans ces conditions.

→ Le conducteur d'un cyclomoteur brûle les feux rouges en niant le danger de ce type de conduite.

→ Le skieur fait du hors piste alors qu'il a été averti d'un fort risque d'avalanche, estimant que son expérience, ne reposant en réalité que sur quelques séjours dans la station, lui permet de juger ce risque négligeable.

→ Le mécanicien n'effectue pas les vérifications de sécurité avant le départ du train afin de rattraper son retard et ainsi pouvoir "faire l'heure", ce qui ne lui est en aucun cas imposé.

EXEMPLES ILLUSTRANT L'UTILISATION DE LA GRILLE RADOS

Ici encore il s'agit seulement d'illustrer chaque case de la grille RADOS pour mieux faire comprendre ce qu'en couvre le sigle. Les exemples donnés se réfèrent à de nombreux domaines hors aéronautiques pour souligner l'universalité des défauts système. Ils doivent être, eux aussi, complétés par l'expérience de chacun.

⇨ COLONNE (s) Saisie et traitement de l'information

⇨Organisation

→ Organisation (Qui doit faire ?) (**Ors**)

L'opérateur ne relève pas les informations qu'il doit normalement surveiller car il pense que cette tâche incombe à un autre.

- → Au cours d'une opération de maintenance il constate une anomalie (des coffres sont restés ouverts par exemple), mais ne le signale pas pensant que ce n'est pas à lui de la faire (pas dans ses attributions) et que d'autres s'en chargeront normalement.
- → Au cours d'une opération de chargement, l'un des opérateurs, responsable de la surveillance du déplacement des charges, ne s'occupe que d'un secteur géographique restreint pensant que les autres secteurs sont surveillés par d'autres opérateurs.
- → Au cours d'une opération d'accostage du navire un observateur à la passerelle constate la présence d'un obstacle imprévu et ne le signale pas au responsable de la manœuvre pensant que ce n'est pas de son ressort.
- → Au cours d'une approche le copilote pense que ses tâches sont réduites à programmation du FMS et aux échanges radio et il ne surveille pas l'extérieur alors que le commandant de bord pense que la copilote assure l'anticollision visuelle.
- → Après un changement de fréquence entre le contrôle régional et le contrôle d'approche, le commandant de bord pense que ce dernier assure l'anticollision avec le trafic et également avec le relief alors que le contrôle d'approche n'assure que l'anticollision avec le trafic.

→ Organisation (Que doit-on faire ?) (**Oes**)

L'opérateur ne connaissant pas les limites de la tâche à effectuer relève simplement quelques informations partielles et ne saisit pas les informations dont il ignore l'importance. Il n'est pas toujours aisé de faire la différence entre Oes, Ors et Fss.

- → Le pilote se contente de contrôler la navigation et néglige la vérification du bon fonctionnement des automatismes.
- → Le commandant de bord surveille le comportement de son jeune copilote, s'il est bienveillant, afin de l'aider dans sa tâche ou, s'il est malveillant, afin de le critiquer et il oublie les opérations de la tâche dont il est responsable. Ce type d'erreur est sans doute à l'origine de l'accident de l'Airbus A320 de Bangalore.
- → Le mécanicien d'un train ne relève que les informations relatives à son retard et néglige les informations intéressant la sécurité.

→ **Organisation** (Quels moyens pour faire ?) (**Oms**)

→ L'opérateur ne relève pas correctement une information car le moyen de mesure mis à sa disposition est inadapté (précision, échelle trop grande, etc.)

→ L'opérateur ne dispose pas du personnel qualifié pour effectuer une mesure ou lire une information.

→ L'opérateur ne dispose pas du nombre de personnels suffisant pour surveiller le déplacement d'une charge au cours d'une opération de manutention.

→ **Organisation** (Comment doit-on faire) (**Ops**)

→ La procédure mise à la disposition de l'opérateur ne précise pas sur quel instrument relever une information alors que plusieurs afficheurs fournissent la même information mais avec des précisions différentes.

⇨**Conception**

→ **Conception de base** (Hb)

Nous donnons ici des exemples de défauts de conception généraux sans qu'il soit possible de les affecter à l'une plutôt qu'à l'autre des colonnes de la grille.

→ La structure a été conçue en ne tenant pas compte de phénomènes physiques dangereux dans certaines conditions de fonctionnement (phénomènes de fatigue ou de flottement des structures par exemple).

- Exemple du Comet dont la structure avait été conçue sans tenir compte du phénomène de fatigue du fuselage due aux contraintes alternées produites par la pressurisation de la cabine passagers, phénomène mal connu à l'époque.

→ La logique de fonctionnement d'un automatisme ne tient pas compte de certaines circonstances, rares mais possibles, ce qui conduit à des réponses aberrantes de l'automatisme ou à une mise hors service intempestive.

- Exemple de l'accident d'ARIANE V. Un logiciel de surveillance de la dérive latérale au départ de la fusée a commandé la remise à zéro des centrales à inertie provoquant des ordres abusifs de corrections de trajectoires aboutissant à la rupture de la structure. Ce logiciel, parfait pour ARIANE IV a été utilisé tel quel sur ARIANE V, alors que le domaine possible de dérive latérale au décollage était différent.
- Exemple de quelques pilotes automatiques des avions de l'avant dernière génération. Le mode de base du pilote automatique en montée était un mode assurant une vitesse verticale constante. Ce mode était mis en service automatiquement en cas de défaillance du mode en service, sans que l'équipage en soit clairement prévenu. Or à haute altitude, le maintien de la vitesse verticale conduit à une réduction de la vitesse aérodynamique (les moteurs plein gaz ne peuvent assurer la performance de montée). La réduction de vitesse pouvait alors se poursuivre jusqu'au décrochage aérodynamique, c'est-à-dire la perte de contrôle de l'avion (Accident du DC10 d'Aeromexico).

→ La conception de base peut reposer sur des hypothèses fausses de fréquence d'apparition de pannes, ce qui conduit, en service, à des défaillances graves de systèmes avec perte de fonctions utiles à la sécurité.

→ Les seuils d'apparition d'alarme sont trop près des limites et ne laissent pas aux opérateur le temps de réagir pour ramener la machine dans le domaine opérationnel.
→ Pour éviter la sortie intempestive des destructeurs de portance avant l'atterrissage un dispositif automatique n'autorise la manœuvre que si des capteurs détectent l'enfoncement des deux trains principaux. Lors de l'atterrissage par fort vent de travers le pilote ne parvient pas à poser les deux roues au sol et ne peut ainsi profiter de la destruction de portance qui lui permettrait de plaquer l'avion au sol (accident de l'Airbus A320 à Varsovie).

→ **Conception des interfaces** (**Hms**)
→ Un capteur défectueux transmet une valeur erronée à un instrument d'un panneau de surveillance.
→ Une clé dynamométrique mal étalonnée indique une valeur d'effort erronée.
→ Un instrument mal éclairé dont l'aiguille grise se déplace sur fond gris avec des graduations blanches délavées conduit à une erreur de lecture.
→ La signalisation est "masquée" par le soleil.
→ Etiquetage défectueux du système sur lequel doit se dérouler une opération de maintenance (étiquette manquante, masquée partiellement par de la graisse, local mal éclairé).
→ La procédure écrite fournie à l'opérateur comporte une erreur matérielle (ligne manquante en bas de page par suite d'une mauvaise photocopie, pages interverties, erreur de frappe, etc.)

→ **Conception des interfaces** (**Hcs**)
→ Numérotation défectueuse ou ambiguë des organes à identifier.
→ Numérotation anarchique des organes et des instruments.
→ Les synoptiques ne sont pas orientés comme sur le "terrain" alors que l'opérateur peut voir simultanément le synoptique et le terrain.
→ La disposition des instruments sur le panneau est en contradiction avec la disposition spatiale des points de mesure sur le système réel ou sur le schéma de conduite.
→ Un cas particulièrement pervers est celui de la signalisation en relation non biunivoque avec le phénomène à signaler. Par exemple, on ne transmet pas la position réelle d'un organe à l'aide d'un capteur approprié mais un paramètre plus ou moins en relation avec cette position. Par exemple, ordre d'un système automatique de changement de position (en général l'ordre est suivi d'effet sauf s'il y a panne de l'actionneur, alors indécelable par l'opérateur).
- Exemple dans l'industrie nucléaire
Catastrophe nucléaire de Harrisburg (Three Mile Island). Ce n'était pas la position fermée de la vanne de décharge du circuit primaire qui était signalée mais l'ordre de fermeture.
- Exemple RATP
Si le verrou du frein d'immobilisation reste bloqué mécaniquement, la signalisation indique que le frein est desserré, alors que le frein est serré.

- Exemple transport aérien.

Sur le DC10 accidenté à Ermenonville, la signalisation, au tableau de bord, du verrouillage de la porte de soute était liée, non pas à la mise en place du verrou mais à la position de la poignée de fermeture.

⇨ **Formation**

→ **Formation de base** (**Fbs**)

→ La formation de base n'a pas suffisamment insisté sur la nature, l'ordre de grandeur, l'importance des paramètres nécessaires au contrôle du processus.

→ **Formation spécifique** (**Fss**)

→ La formation spécifique n'a pas suffisamment insisté sur la disposition des instruments de mesure (d'où une erreur de localisation de la source d'information), sur les particularités des échelles de mesure (zéro, échelle, sens de variation, etc.. d'où une erreur sur le modèle de transposition de l'information), sur les moyens d'identification des sources d'information, etc.

→ L'entraînement a été effectué sur un système différent du système réel (simulateur par exemple) avec une disposition non conforme des instruments sur le pupitre.

⇨ **Documentation**

→ **Documentation** (**Dms**)

→ La documentation sur les sources d'information est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (plans de grandes dimensions ou manuels multiples), inutilisables en extérieur ou encore contient des erreurs matérielles (fautes de frappe sur des codes d'identification d'instruments par exemple).

→ **Documentation** (**Dcs**)

→ La documentation sur les sources d'information est difficilement compréhensible ou trop dispersée et conduit à des erreurs de saisie de données. Par exemple, il n'est pas clairement précisé que les étendues de mesure des instruments donnant les valeurs de plusieurs paramètres analogues ne sont pas identiques (zéros et échelles différentes).

→ Les schémas fournis sont des schémas de conception et non des schémas d'utilisation, les organes ne sont pas disposés sur le schéma comme sur le "terrain".

→ Une modification des sources d'information n'est pas signalée (Dms) ou signalée avec erreurs (Dcs) aux opérateurs (panne de capteur, changement de type d'instrument avec par exemple changement d'échelle, déplacement des instruments sur le tableau de bord avec par exemple interversion de deux instruments mesurant des paramètres de même nature, changement de fréquence d'une balise, etc.)

⇨ **Réglementation** (Rs)

→ La réglementation impose des signalisations de sécurité qui surchargent inutilement l'opérateur (panneaux multiples d'avertissement de travaux sur la voie).

→ La réglementation impose des types d'instruments d'une technologie dépassée.

⇨ COLONNE (d) Décision après traitement de l'information

⇨Organisation

→ **Organisation** (Qui doit faire ?) (**Ord**)

→ Une décision est prise par un opérateur qui n'a pas les qualifications nécessaires ou le niveau hiérarchique prévu et qui, par suite, n'a pas accès aux informations adéquates permettant cette décision.

Par exemple, un opérateur constate une anomalie, mais ne se sentant pas responsable ne la signale pas à son supérieur pensant que c'est à lui de réagir. Au contraire il décide d'intervenir de sa propre initiative sans signaler au bon niveau de décision l'intervention en cours.

→ Une décision est prise par un responsable de haut niveau qui ne dispose pas des informations appropriées.

→ Un incident survient alors qu'un opérateur de maintenance fait un accompagnement en ligne sur une rame RATP. Il prend sur lui de faire le dépannage sur place, alors que l'objectif des exploitants est de dégager le train le plus rapidement possible.

→ **Organisation** (Que doit-on faire ?) (**Oed**)

→ L'organisation n'a pas prévu les actions à entreprendre dans des situations particulières, rares, mais prévisibles, situations de pannes par exemple.

→ **Organisation** (Quels moyens pour faire ?) (**Omd**)

→ L'opérateur ne dispose pas des moyens matériels nécessaires ou adaptés à sa prise de décision (abaques ou schémas incomplets ou peu précis par exemple). Ce cas est quelque fois difficile à distinguer du cas suivant (Opd), des problèmes d'interface (Hmd et Hcd) ou des problèmes de documentation (Dmd et Dcd)

→ **Organisation** (Comment doit-on faire ?) (**Opd**)

→ Les procédures de décision ne sont pas adaptées ou ne sont pas précisées.

→ Les procédures de décision sont ambiguës ou difficiles à interpréter (en particulier interdiction sur critères négatifs du style "il n'est pas interdit de ne pas ouvrir le robinet si le réservoir n'est pas plein").

→ La procédure prévoit des vérifications avant enclenchement de la suite des opérations (points d'arrêt), mais ne précise pas ce qu'il convient de faire si les vérifications ne sont pas acquises. Par exemple la procédure prévoit, avant intervention sur un circuit, de vérifier qu'il est bien hors tension. Cette recommandation est judicieuse, encore faut-il préciser ce que doit faire l'opérateur s'il constate que le circuit est toujours sous tension, "ouvrir le disjoncteur D312"," en référer à la hiérarchie (comment et dans quels

délais)"," attendre (combien de temps)", etc. Il est clair que laissé à sa propre initiative, l'opérateur peut sortir du domaine de sécurité prévu pour l'intervention, dès lors que les limites, techniques et fonctions du temps, peuvent dépendre d'événements indépendants du seul opérateur.

⇨ **Conception**

→ **Conception de base** (**Hb**)
voir les exemples donnés pour la colonne **s** saisie des informations.

→**Conception des interfaces** (Hmd) et (Hcd)
Ce type d'erreur est généralement rare, une mauvaise décision provenant le plus souvent, dans le cas d'une erreur d'interface, d'une mauvaise information. On peut néanmoins citer les quelques éventualités suivantes.
→ Une erreur matérielle dans la présentation d'un schéma de décision sur écran induit une mauvaise décision de la part de l'opérateur (Hmd).
→ Une erreur de logiciel d'aide à la décision induit une mauvaise décision de la part de l'opérateur (Hmd).
→ Le cahier des charges de rédaction du logiciel d'aide à la décision n'a pas prévu le cas particulier dans lequel se trouve l'opérateur face à son système ce qui amène ce dernier à une erreur de diagnostic donc de décision (Hcd).
→ Un synoptique d'aide à la décision, par une mauvaise présentation (par exemple arbre de décision trop "touffu") ou par des questions mal posées (par exemple avec des doubles négations), peut conduire à une erreur de décision (Hcd).
→ Une formulation ambiguë peut conduire à l'erreur, par exemple "si la condition A n'est pas réalisée, non-interdiction de passer la pompe en grande vitesse" (Hcd).
→ Une information touffue, difficile à synthétiser peut conduire à une erreur de décision (Hcd).

⇨ **Formation**

→ **Formation de base** (**Fbd**)
→ La formation de base a présenté des modèles de principe de fonctionnement du système incompris par les opérateurs (par exemple, l'opérateur croit que la relation pression - température est la loi des gaz parfaits de Mariotte alors que c'est la loi de vapeur saturante qui est en cause).

→ **Formation spécifique** (**Fsd**)
→ La formation spécifique fournit des modèles trop généraux de fonctionnement du système, modèles qui ne sont pas applicables dans quelques cas particuliers. Dans ces cas, là les opérateurs font reposer leurs décisions sur le principe général non applicable.
→ L'entraînement a été effectué sur un système différent du système réel (simulateur par exemple) avec des modes de fonctionnement simplifiés non conformes aux modes de fonctionnement réels.

⇨ **Documentation**

→ **Documentation** (**Dmd**)
- → La documentation sur les modèles de fonctionnement permettant les décisions est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (organigrammes de grandes dimensions ou manuels multiples inutilisables en extérieur) ou encore contient des erreurs matérielles (fautes de frappe sur des codes d'identification d'organes par exemple).
- → Une modification des règles et consignes de conduite, de l'organisation (répartition des tâches par exemple) n'est pas transmise.
- → Une information d'interdiction de survol n'a pas été transmise ce qui conduit l'équipage à une mauvaise décision sur la trajectoire à suivre.

→ **Documentation** (**Dcd**)
- → La documentation sur les modèles de fonctionnement permettant les décisions est difficilement compréhensible, ou trop dispersée, et conduit à des erreurs de décision. Par exemple, les organigrammes de décision comportent des ambiguïtés ou encore ne présentent que le modèle de fonctionnement général du système, et renvoient les cas particuliers à des annexes sans en signaler l'importance sur le plan sécurité.
- → Une modification des règles et consignes de conduite, de l'organisation (répartition des tâches par exemple) est transmise avec erreurs aux opérateurs .

⇨ **Réglementation** (**Rd**)
- → La réglementation impose des accords multiples de la hiérarchie retardant la prise de décision dans des cas d'urgence.

⇨ **COLONNE (t) Transmission de l'information**

⇨**Organisation**

→ **Organisation** (Qui doit faire ?) (**Ort**)
- → L'organisation n'a pas prévu la liste complète des émetteurs et des destinataires des messages dans tous les cas possibles. Par exemple, en situation de maintenance lorsqu'une impossibilité de poursuivre apparaît, qui prévenir et quelle information transmettre ?

→ **Organisation** (Que doit-on faire ?) (**Oet**)
- → L'organisation n'a pas prévu la liste systématique des moyens de transmission des messages et des méthodes d'utilisation des moyens de transmission, en couvrant tous les cas possibles de fonctionnement normal et d'incidents des systèmes de transmission. Par exemple, en cas de panne d'interphone que dois-je faire en fonction de l'urgence et du type de destinataire ?

→ **Organisation** (Quels moyens pour faire ?) (**Omt**)
- → L'opérateur ne dispose pas des personnels nécessaires ou adaptés à la transmission des informations (personnel non qualifié en particulier).

→ L'organisation n'a pas prévu que les moyens de transmission des messages ne sont pas disponibles là où se trouve l'opérateur (absence de téléphone par exemple).

→ **Organisation** (Comment doit-on faire ?) (**Opt**)

→ Quelquefois l'opérateur est obligé de mémoriser un certain nombre de valeurs pendant un temps plus ou moins long (cas de transmission de l'opérateur vers lui-même). Cette opération de mémorisation comporte des risques d'erreurs ou d'oubli. L'organisation a-t-elle prévu des moyens simples de stockage provisoire de l'information (ardoise, papier, planchette, tableau "gras", système d'affichage mécanique ou électronique, etc.).

→ L'organisation n'a pas prévu de procédures simples d'émission des messages d'urgence (numéros d'appel banalisés des services d'urgence à rechercher dans l'annuaire général par exemple).

⇨ **Conception**

→ **Conception de base** (**Hb**)

voir les exemples donnés pour la colonne **s** saisie des informations.

→ **Conception des interfaces** (**Hmt**)

→ Le système de transmission de l'information est dégradé, par exemple par panne ou insuffisance mécanique, électrique ou électronique, par brouillage ou bruitage (ambiance sonore élevée) ou par mauvaise visibilité (éclairage non nominal, brouillard,...).

→ Les claviers de commande des moyens de transmission sont inadaptés à la manipulation (touches trop petites, pas assez espacées, le pupitre est trop éloigné de l'opérateur, etc.)

→ **Conception des interfaces** (**Hct**)

→ Le système de transmission ne permet pas d'identifier facilement le canal de transmission (affichage de fréquence prêtant à confusion) ou d'identifier clairement le destinataire des messages.

→ Les claviers de commande de transmission facilitent les confusions, panneau carrés de cent touches de formes et de couleurs identiques, choix du destinataire (interphone, émission radio) fait par un inverseur indépendant du bouton poussoir d'émission, etc.

⇨ **Formation**

→ **Formation de base** (**Fbt**)

→ La formation de base n'a pas suffisamment insisté sur les règles et les procédures générales de transmission de l'information, nécessité de s'identifier clairement en tant qu'émetteur, nécessité de préciser le destinataire, nécessité d'utilisation de format précis de message (code alphabétique par exemple), etc.

→ La formation de base n'a pas suffisamment insisté sur l'organisation de l'entreprise et les règles de sécurité justifiant les besoins et les moyens de transmission d'information.

→ **Formation spécifique** (**Fst**)

→ La formation spécifique n'a pas suffisamment insisté sur les moyens et méthodes de transmission de l'information et n'a pas justifié les procédures à utiliser.

→ L'entraînement a été effectué sur un système différent du système réel (simulateur par exemple) sans entraînement à la transmission des informations.

⇨ **Documentation**

→ **Documentation** (**Dmt**)

→ La documentation sur les moyens et les procédures de transmission est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (listes multiples de destinataires ou de fréquences inutilisables en extérieur, caractères trop petits difficilement lisibles sous faible éclairage) ou encore contient des erreurs matérielles (oubli de mise à jour, fautes de frappe sur les codes, les noms de destinataires ou les fréquences par exemple).

→ Une modification des règles et consignes de transmission, une modification de l'organisation (changement des destinataires des messages), une modification d'un annuaire, n'est pas transmise aux opérateurs.

→ **Documentation** (**Dct**)

→ La documentation sur les moyens et les procédures de transmission est difficilement compréhensible ou trop dispersée et conduit à des erreurs. Les annuaires ou les listes de fréquences comportent des ambiguïtés ou rendent difficile la recherche d'un code de correspondant.

→ Une modification des règles et consignes de transmission, une modification de l'organisation (changement des destinataires des messages), une modification d'un annuaire, est transmise avec erreurs aux opérateurs.

⇨ **Réglementation** (**Rt**)

→ La réglementation impose l'utilisation de types de messages lourds retardant d'autant la transmission d'information dans les cas d'urgence.

⇨ **COLONNE (a) Action**

⇨**Organisation**

→ **Organisation** (Qui doit faire ?) (**Ora**)

→ L'opérateur n'exécute pas les actions prévues parce qu'il croit que c'est à un autre de les faire. C'est le problème de partage des tâches entre le mécanicien d'entretien et l'électricien (qui doit entretenir les capteurs ?).

→ L'opérateur entreprend des actions normalement dévolues à un autre ce qui peut provoquer des incompréhensions de part et d'autre tant que les opérateurs ne communiquent pas.

→ **Organisation** (Que doit-on faire ?) (**Oea**)

→ L'organisation n'a pas prévu la liste systématique des actions et des procédures à suivre, en couvrant tous les cas possibles de fonctionnement

normal et accidentel des systèmes. Par exemple, a-t-on prévu quelle procédure suivre, ou quitter, en cas d'impossibilité de poursuivre une opération de maintenance ?

→ **Organisation** (Quels moyens pour faire ?) (**Oma**)

→ L'opérateur ne dispose pas des moyens en personnel pour exécuter toutes les actions dans le temps qui lui est imparti pour accomplir la tâche.

→ L'opérateur ne dispose pas des moyens matériels (outillage, engins de chantier, matériel de levage, etc.) adaptés à l'exécution de la tâche.

→ **Organisation** (Comment doit-on faire ?) (**Opa**)

→ C'est dans cette catégorie qu'entrent le non-respect des procédures établies et le recours aux procédures "exotiques" du style "tu vas voir, j'ai ça dans mon calepin". L'analyse nécessite alors de se poser la question "Pourquoi la procédure prévue n'a pas été suivie (impossibilité physique, manque de moyens en homme ou en matériel, mauvaise interprétation, procédure mal adaptée, adaptation de "règles de l'art" non appropriées, etc.) avant d'assimiler l'erreur à une faute contre la discipline.

Ainsi, au cours des manœuvres de refoulement de trains coupés en atelier, la procédure réglementaire n'est pas respectée. Le shuntage de la boucle de sécurité n'est pas mis en place et le manipulateur en loge arrière est utilisé. La manœuvre n'en est pas modifiée, mais le frein de secours est inutilisable.

C'est l'exemple dramatique et réel du pilote qui décide de parcourir la piste avec les réacteurs à fort régime et en freinant énergiquement, afin de chauffer l'atmosphère et ainsi dissiper temporairement le brouillard. Il en est résulté une température anormale des freins qui a conduit à l'explosion des pneumatiques une fois le train rentré après le décollage et la destruction fatale des circuits hydrauliques.

⇨ **Conception**

→ **Conception de base** (**Hb**)

voir les exemples donnés pour la colonne **s** saisie des informations.

→ **Conception des interfaces** (**Hma**)

→ Les commandes ne sont pas adaptées à l'opérateur (touches trop petites, insuffisamment espacées, leviers de taille, forme, débattement rendant la manipulation mal commode ou fatigante, etc.).

→ Les commandes dont la manipulation peut conduire à des changements d'états irréversibles ou dangereux ne sont pas protégées par des caches en interdisant la manipulation intempestive (boutons d'arrêt d'urgence, signal d'évacuation immédiate des locaux, etc.)

→ **Conception des interfaces** (**Hca**)

→ Les commandes sont disposées suivant une logique prêtant à confusion (panneaux carrés de cent touches de formes et de couleurs identiques, repérables uniquement par un code; série de leviers identiques disposés parallèlement , repérables uniquement par un code ou par leurs positions respectives,..) .

→ Les commandes sont disposées suivant une logique sans rapport avec la disposition des organes commandés.
→ Les commandes ont un sens d'action inhabituel (robinet s'ouvrant dans le sens à visser, potentiomètre diminuant le volume d'amplification dans le sens à visser, etc.).
→ Les commandes ont un sens d'action sans relation avec l'effet sur l'organe commandé (un levier tiré vers le haut déplace la charge vers le bas, poussé à droite déplace la charge vers la gauche ou vers l'avant, etc.).
→ Un mauvais fonctionnement du système de commande rend une commande inefficace ou erronée; par exemple un bouton poussoir est appuyé, il s'allume pour signaler uniquement qu'il a été poussé, mais l'ordre n'a pas été transmis au système (effet pervers analogue à celui décrit en Hcs). L'opérateur est ainsi trompé par un faux retour d'information sur l'effet de la commande. Le même effet pervers peut être obtenu par une commande mécanique ou électrique débranchée; le levier ou l'interrupteur a été mis en bonne position mais l'ordre n'a pas été transmis.
→ Une commande du pilote automatique impose soit une vitesse verticale (en pieds/minute), soit une pente (en degrés). Le passage d'un cas à l'autre se fait par appui sur un bouton poussoir, la distinction entre chacun des cas se faisant par la lecture de l'affichage sur une fenêtre unique. Cette disposition est sans doute à l'origine de l'accident de l'Airbus A320 au Mont Saint Odile et a fait l'objet d'une modification.

⇨ Formation

→ Formation de base (**Fba**)

→ La formation de base n'a pas suffisamment insisté, au niveau des principes, sur l'influence, l'effet (sens et efficacité, effets parasites), des commandes sur le processus à contrôler.

A titre d'exemple la présentation de la loi d'Ohm sous la forme $P = R.I^2$ fait croire qu'il faut augmenter la résistance d'une chaufferette (alimentée par le secteur à voltage constant) pour augmenter la puissance de chauffage, alors que la présentation sous la forme $P = V^2/R$ démontre sans ambiguïté qu'il faut effectuer l'opération inverse.

→ Formation spécifique (**Fsa**)

→ La formation spécifique n'a pas suffisamment insisté sur la disposition spatiale des commandes (d'où une erreur de localisation des commandes), sur les particularités des sens d'action des commandes, sur les moyens d'identification des commandes (formes, couleurs, étiquetage, etc.), sur les retours d'information d'état des organes commandés, etc.
→ L'entraînement a été effectué sur un système différent du système réel (simulateur par exemple) avec une disposition, des types de commandes non conformes aux commandes réelles sur le pupitre.

⇨ **Documentation**

→ **Documentation** (**Dma**)

- → La documentation sur les commandes est inexistante, incomplète, mal reproduite, difficilement maniable sur le terrain (plans de grandes dimensions ou manuels multiples) inutilisables en extérieur ou encore contient des erreurs matérielles (fautes de frappe sur des codes d'identification des commandes par exemple).
- → Une modification des commandes (position, forme, identification, sens d'action, etc.) n'est pas signalée aux opérateurs (panne, changement de type de commande avec, par exemple, changement de sens d'action, déplacement des commandes sur le tableau de bord avec, par exemple, interversion de deux commandes agissant de façon analogue sur le système, etc.).

→ **Documentation** (**Dca**)

- → La documentation sur les commandes est difficilement compréhensible ou trop dispersée et conduit à des erreurs d'action. Par exemple, il n'est pas clairement précisé le sens d'action particulier d'une commande, ses effets parasites sur le contrôle du système.
- → Les schémas fournis sont des schémas de conception et non des schémas d'utilisation, les commandes ne sont pas disposées sur le schéma comme sur le poste de travail.
- → Une modification des commandes (position, forme, identification, sens d'action, etc.) est signalée avec des erreurs aux opérateurs (panne, changement de type de commande avec changement de sens d'action, par exemple, déplacement des commandes sur le tableau de bord avec interversion de deux commandes agissant de façon analogue sur le système, par exemple, etc.).

⇨ **Réglementation** (**Ra**)

- → La réglementation impose le verrouillage de certaines commandes interdisant leur utilisation en cas d'urgence.