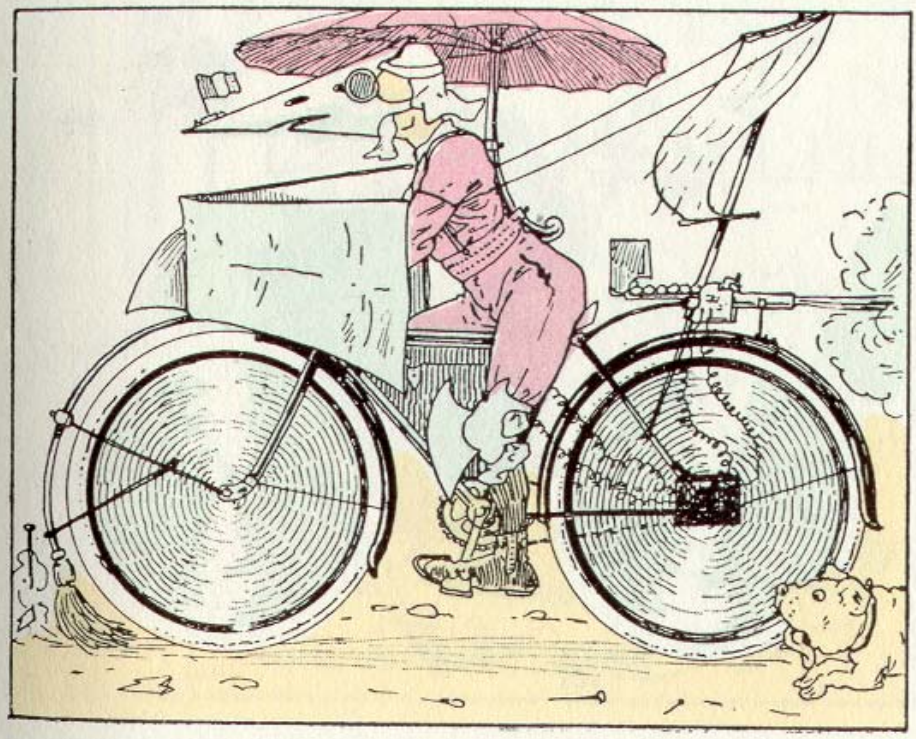
Opérateurs et Sécurité

N.& J.-C. Wanner

CINQDEMI

Tel 05 53 36 46 87
Fax 05 53 36 30 52
Courriel nicole.wanner@wanadoo.fr



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

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

Définition

On entend par OPERATEUR :

TOUT ACTEUR de l'entreprise,

quelles que soient ***sa fonction,***
sa position hiérarchique,

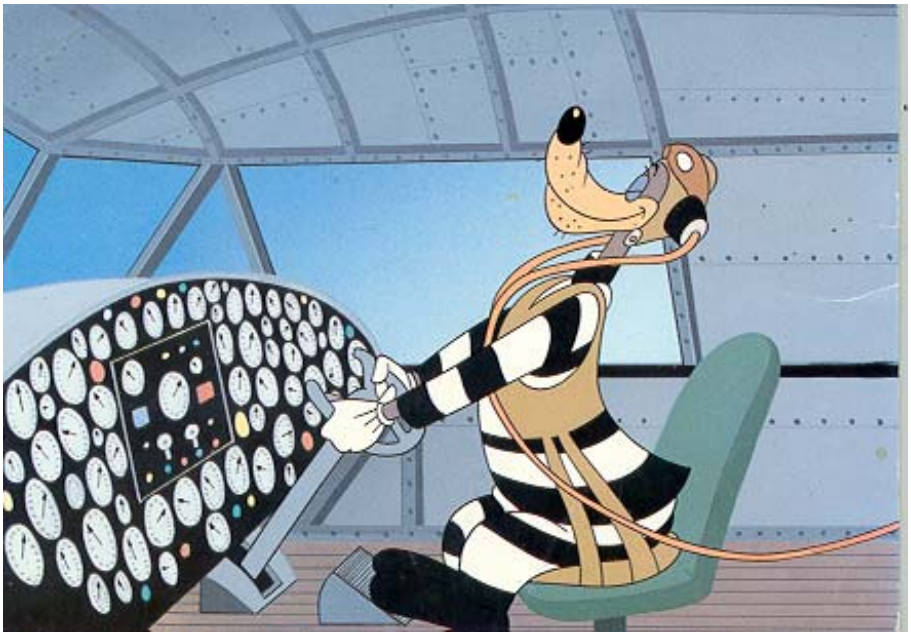
quel que soit ***l'organisme qu'il commande,***

quels que soient ***le département, le service,***
la section, l'équipe, l'atelier
dont il est responsable,

quels que soient ***le système ou la machine***
qu'il pilote, surveille ou entretient.

NOUS SOMMES TOUS DES OPÉRATEURS

Les caractéristiques de l'Opérateur Humain



D'après Tex Avery

L ' Homme est imparfait...
mais ce n'est pas étonnant lorsque l'on songe à l'époque où il fut créé.

Alphonse Allais

1. Fonctionnement en séquence de l'Opérateur. Charge de Travail.

Pour mener à bien une tâche, l'Opérateur doit exécuter une succession d'opérations élémentaires de quatre types :

⇨ **saisir une information, une donnée**

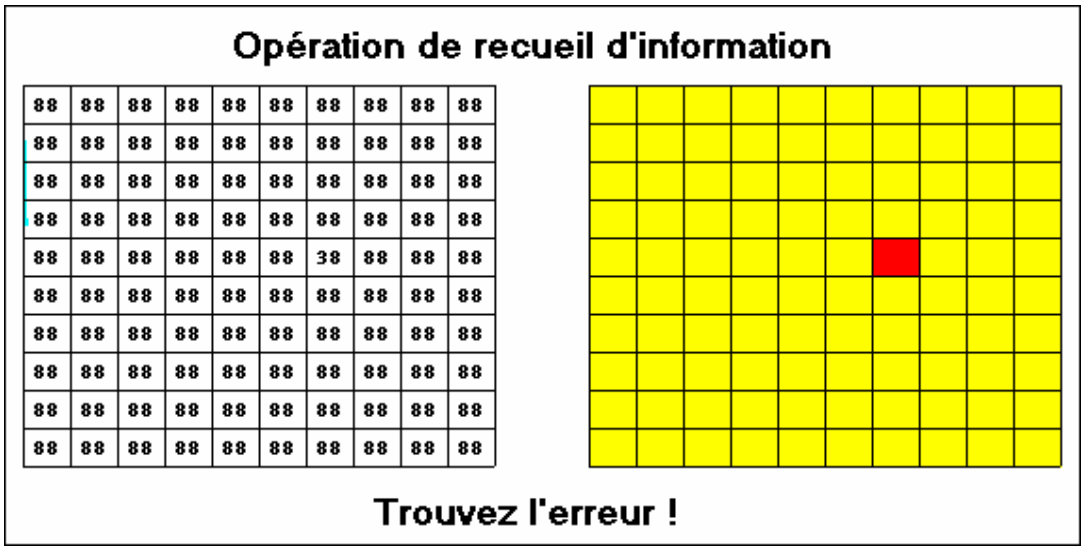
⇨ **traiter les informations dont il dispose et prendre une décision.**

⇨ **transmettre un message**

⇨ **agir sur une commande**

⇨ **saisir une information, une donnée**, par la vue, le toucher, l'ouïe, etc.

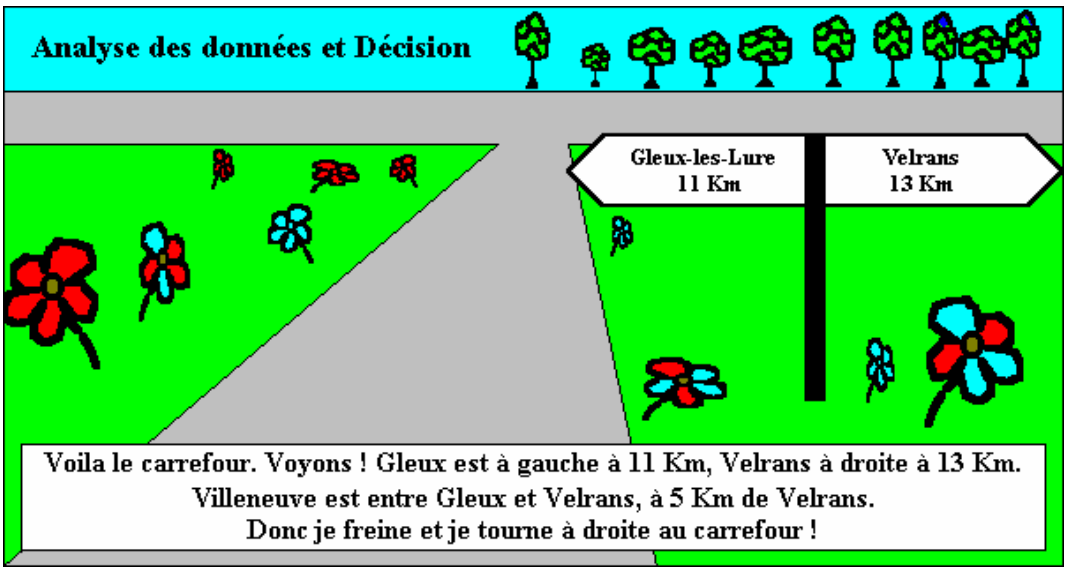
- en observant l'environnement,
- en lisant une valeur sur un instrument,
- en écoutant un message oral,
- en reconnaissant la forme d'une commande,
- en estimant l'effort exercé sur une commande...



⇨ **traiter les informations dont il dispose et prendre une décision.**

L'Opérateur peut ainsi décider :

- d'attendre que la situation évolue d'elle-même,
- de recueillir une autre information pour préciser la situation en mettant en mémoire la position de la source de l'information désirée,
- de transmettre un message en mettant en mémoire le destinataire et le moyen de transmission,
- d'agir sur une commande en mettant en mémoire la position de la commande, son mode d'action (pousser, tirer, tourner,..) et en estimant l'effort ou le déplacement à appliquer,.



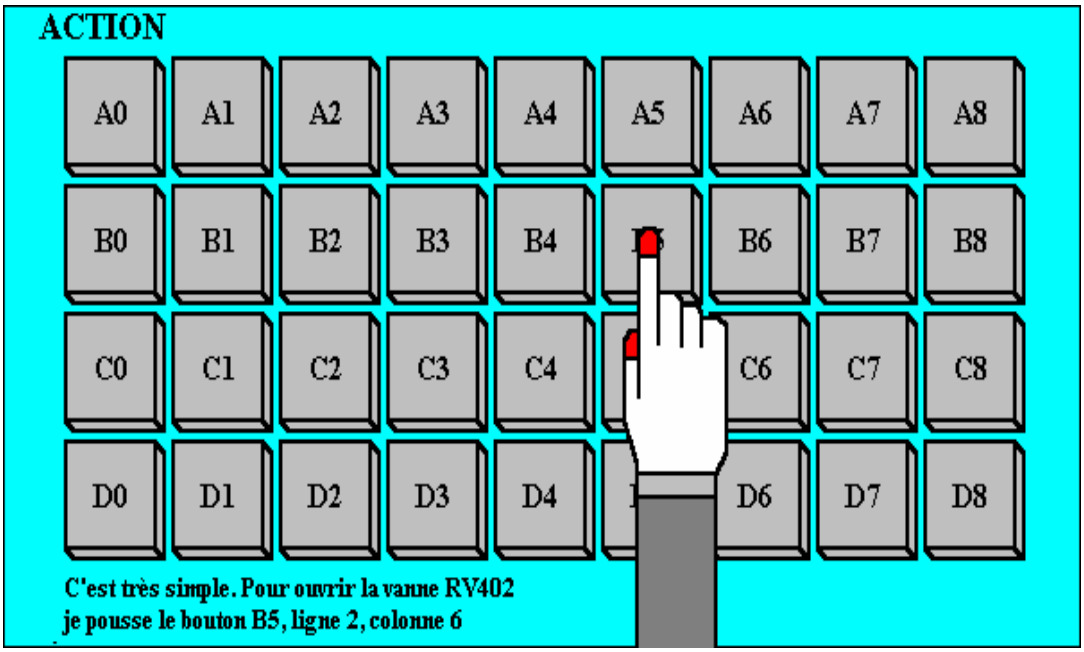
⇨ transmettre un message

- à un autre opérateur,
- à un groupe d'opérateurs,
- à lui-même (pour mémorisation),..

D'après Roger Bollen Ces dingues d'animaux

⇨ agir sur une commande par

- une main,
- un pied,
- un doigt,..



Toutes ces opérations, dites COGNITIVES sont exécutées en séquence.

Fonctionnement dit en Canal Unique

⇨ **UN OPERATEUR PEUT EXECUTER PLUSIEURS TACHES A LA FOIS.**

Mais à chaque instant, il exécute une succession d'opérations élémentaires : elles sont destinées à résoudre UN SEUL problème.

Puis il exécute une autre succession d'opérations élémentaires : elles sont destinées à résoudre UN AUTRE problème...

Par l'entraînement, un opérateur peut mettre en mémoire une succession d'opérations élémentaires nécessaires à l'exécution de tâches simples et répétitives.

L'opérateur peut alors exécuter ces séquences sans avoir à réfléchir.

Les **opérations semi-réflexes**.
Elles sont constituées d'opérations élémentaires du même type :

- **actions**,
par exemple changement de vitesse en voiture, écriture manuelle, écriture au clavier,

- **recueil d'information**,
par exemple lecture globale de mots ou de courtes phrases, lecture de l'heure sur une montre à aiguilles,

- **transmission de message appris par coeur**,

- **décision dans des situations simples, bien connues et répétitives**.

Les **opérations réflexes**.
Elles sont constituées d'opérations élémentaires de types variés :

- **maintien de l'équilibre du corps**,

- **conduite automobile sur route peu chargée**,

- **maintien des assiettes de l'avion en vol à vue en atmosphère calme,..**

Les opérations réflexes et semi-réflexes se superposent aux actions cognitives sans les perturber.
Il est ainsi possible de discuter avec le passager tout en conduisant en réflexes. Il est possible d'observer le trafic routier tout en changeant de vitesse.

Seul l'entraînement permet aux opérateurs d'acquérir ces opérations. Un changement de disposition des commandes et des instruments du poste de travail rend ces opérations caduques.
Exemple de la conduite sur une voiture britannique : il faut réapprendre à changer de vitesse avec la main gauche et à retrouver le rétroviseur !

Conséquences du fonctionnement séquentiel, semi-réflexe et réflexe de l'opérateur.

Chaque opération cognitive élémentaire demande un certain temps d'exécution (de l'ordre de quelques dixièmes de seconde). **Le nombre d'opérations élémentaires exécutables dans un temps donné est donc limité.**

Au-delà d'un certain nombre d'opérations élémentaires à exécuter dans un temps donné, le risque d'erreurs augmente.
Par exemple le non-recueil d'une information critique, décision erronée, oubli de transmission d'un message, oubli d'action, action dans le mauvais sens, action mal dosée, action sur une mauvaise commande, ...

On dit que

la Charge de Travail de l'Opérateur est limitée.

Le risque d'erreur, au cours d'une tâche donnée, dans un temps donné, donc **la Charge de Travail maximale disponible**, dépend :

- de la tâche elle-même,
- de l'entraînement et de la qualification de l'opérateur,
- de son état physique (fatigue, maladie),
- de son état psycho-sociologique (préoccupations heureuses ou malheureuses, mésentente dans l'équipe, présence d'un contrôleur,..)
- etc.

⇨ **La CHARGE DE TRAVAIL disponible d'un Opérateur est limitée.**

⇨ **Toute AUGMENTATION de la Charge de Travail se traduit par une augmentation du risque d'erreurs.**

⇨ **Les opérations REFLEXES et SEMI-REFLEXES sont exécutées sans augmentation de la Charge de Travail.**

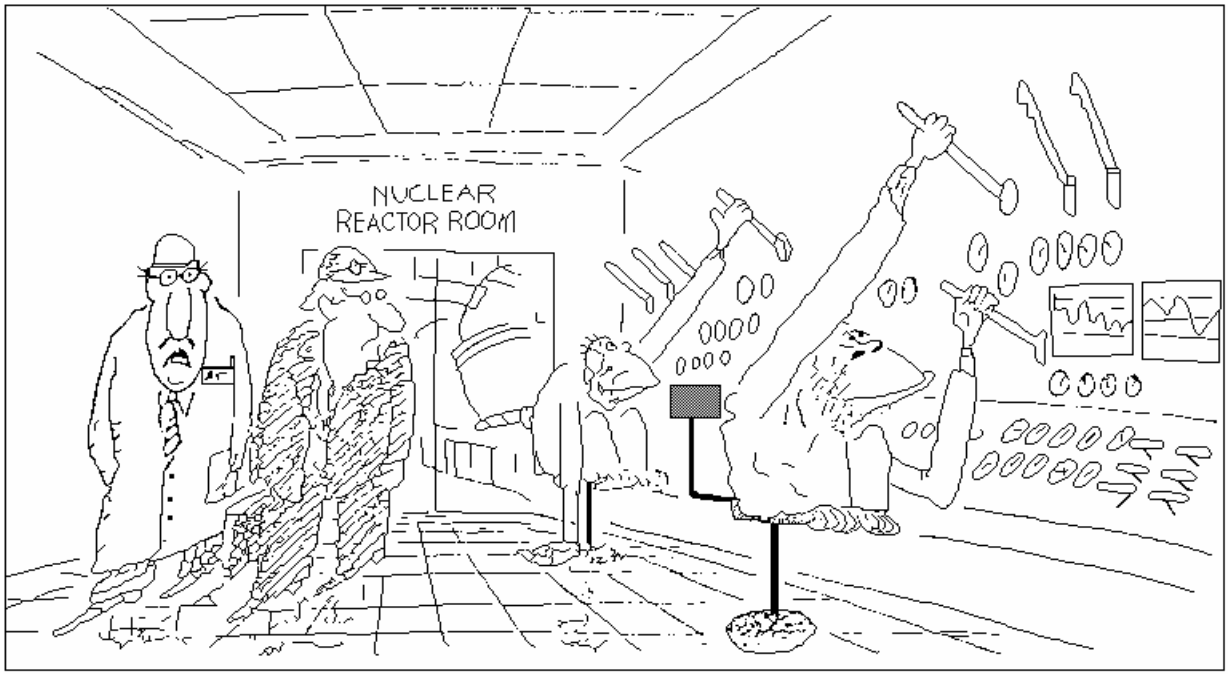
⇨ **Les opérations réflexes et semi-réflexes ont été ACQUISES par l'entraînement.**

Toute MODIFICATION du poste de travail nécessite une reprise de l'entraînement.

.

''Tous ces accidents à cause d'erreurs humaines par charge de travail trop élevée, deviennent drôlement embarrassants..''

''Aussi avons nous décidé de faire quelque chose !''



D'après Stayskal dans le Chicago-Tribune

2. Perte de Vigilance par manque d'informations.

Le cerveau de l'opérateur a besoin d'être stimulé en permanence par un apport d'informations visuelles, auditives, tactiles, gustatives ou olfactives.

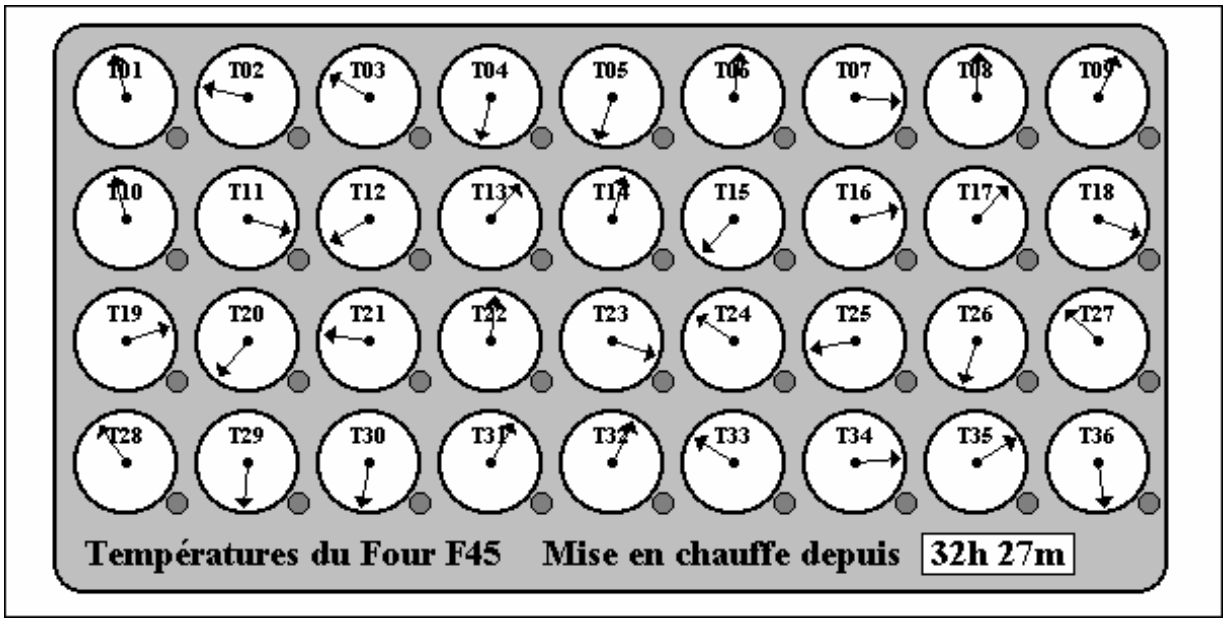
En situation de surveillance d'un processus stable qui ne fournit aucune information (il n'y a information que s'il y a changement d'état), l'opérateur éprouve le besoin d'acquérir toute information disponible même si elle est inutile (dans une voiture du métro dans le tunnel il y a très peu d'informations ; aussi lisons-nous toutes les publicités, les avertissements de sécurité et les titres du journal du voisin !).

Si aucune information n'est vraiment disponible, l'opérateur s'en "fabrique" en pensant à autre chose (le dernier film, le bricolage en cours, ses amours, etc.).
Son attention diminue et il ne surveille plus le processus qu'il doit normalement contrôler.

Cette perte de vigilance due à la non-stimulation du cerveau par absence d'informations, ne doit pas être confondue avec la perte de vigilance due à la fatigue et aux horaires perturbés (fin de la période de quart, travail de nuit, décalages horaires,..).

Il ne faut pas mettre les opérateurs en situation de MANQUE d'informations.

Attention ! Le système VACMA de la SNCF, dit de "l'homme mort", n'est pas destiné à résoudre le problème de vigilance des mécaniciens. Il ne sert qu'à détecter le fait que le mécanicien est incapable de conduire sa machine (évanouissement, mort, etc.). La manipulation de la pédale toutes les quarante secondes devient très rapidement une opération semi-réflexe et n'empêche en aucun cas l'opérateur de penser à autre chose ! (au bout d'une heure d'entraînement, le réflexe est acquis).



Voici ce que peut voir l'opérateur en fin de quart de surveillance du Four F45 qui a atteint son régime permanent depuis 25 heures environ.
Quelle peut être son image mentale ? Vous pourrez la voir page 18.

3. Besoin d'informations permettant la Prévision

Le confort de la surveillance et de la conduite d'un processus est augmenté si l'opérateur peut prévoir l'évolution du système dans le temps. Cela lui permet de gérer sa charge de travail.

S'il prévoit que le système va peu évoluer dans les minutes qui suivent, il peut se consacrer à d'autres tâches que la surveillance du processus.

Si par contre rien ne lui permet d'estimer le risque de voir surgir une variation brutale et inopinée, il est contraint à une surveillance fastidieuse et serrée du processus.

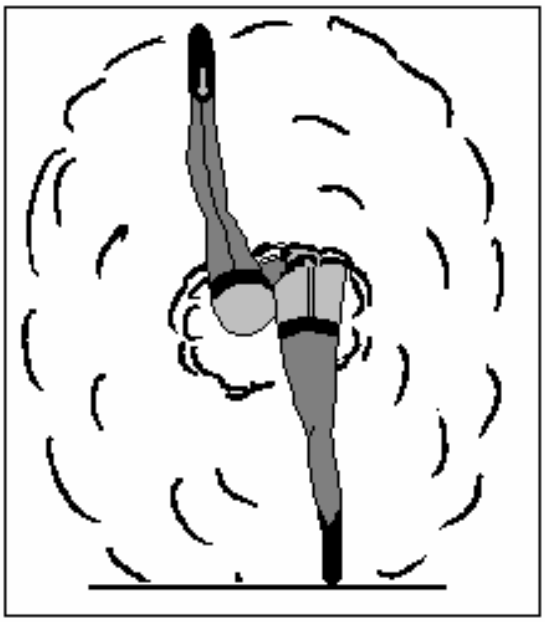
Dans un embouteillage, toutes les voitures à l'arrêt, on voit souvent les automobilistes sortir de leur véhicule pour voir devant. Ils recueillent des informations leur permettant d'analyser la situation et d'en déduire un temps d'attente possible.

Certains programmes utilisés en micro-informatique présentent, dans les phases d'attente, chargement de longs fichiers par exemple, une échelle horizontale qui affiche le temps déjà passé et le temps restant avant la reprise de main par l'opérateur. Cette disposition fait paraître l'attente plus courte et la rend par là même supportable.

Il faut fournir aux opérateurs des informations permettant de prévoir l'évolution du système qu'ils contrôlent.

Cette recommandation prend toute sa valeur pour les processus hautement automatisés.

Les opérateurs doivent savoir à TOUT INSTANT ce que font les automatismes (voir paragraphe **2)** et ce qu'ils vont faire.



Voici **l'image mentale** de l'opérateur surveillant depuis SEPT HEURES les températures du Four F45 (dont le tableau de contrôle est présenté sur la page 16) .

Il a revu French Cancan à la télé la veille !

Pensez-vous qu'il soit dans de bonnes dispositions pour détecter une anomalie et pour réagir rapidement en cas d'incident ?

Ceci illustre le problème de la surveillance des processus qui **n'évoluent pas**.

4. Difficulté d'ESTIMATION des risques de faible probabilité.

Les accidents sont **rares**. Les méthodes de sécurité ont pour objet d'en réduire la probabilité à des valeurs de l'ordre de 10^{-7} par heure*.
Les incidents et pannes ont des probabilités d'apparition comprises entre 10^{-3} et 10^{-6} (ordre de grandeur naturellement).

---

* Une probabilité de 10^{-7} / heure signifie que l'on a une chance sur 10.000.000 par heure d'observer l'événement. Rappelons que 10^{n} = 1 suivi de n zéros. Ainsi 10^{7} = 10.000.000
et que 10^{-n} = 1/ 1 suivi de n zéros. ainsi 10^{-7} = 1 / 10.000.000 = 0,0000001
Si la probabilité d'apparition d'un événement est de 10^{-3}/ Heure, il se produit en moyenne toutes les 10^{3} = 1.000 heures (temps moyen entre deux apparitions successives de l'événement). Bien entendu cela ne signifie pas que si j'observe un événement, le suivant se reproduira dans 1.000 heures. Cela signifie seulement que si j'observe le système suffisamment longtemps, la moyenne des temps séparant deux apparitions successives de l'événement sera de l'ordre de 1.000 heures.

Comment, par observation du fonctionnement réel d'un système, ou au cours d'essais de composants, peut-on estimer la probabilité d'apparition d'un événement ?

La règle, fournie par les statisticiens, est la suivante :

> Si nous avons pu faire fonctionner le système pendant 2,3 10^{n} heures SANS RENCONTRER L'ÉVENEMENT ETUDIE,
> nous pouvons affirmer que la probabilité d'apparition de cet événement est INFERIEURE A 10^{-n} PAR HEURE,
> avec un *niveau de confiance* de 0,9.

Ce *niveau de confiance* de 0,9 signifie que nous n'avons que 9 chances sur 10 pour que cette probabilité de 10^{-n} par heure soit rencontrée effectivement en service réel (il se peut que nous ayons eu de la chance en ne rencontrant pas l'événement au cours de notre observation de 10^{n} heures alors que sa probabilité réelle d'apparition est supérieure à 10^{-n} par heure et il y a une chance sur dix pour que nous ayons été dans ces circonstances trompeuses d'observation).

Si nous voulons augmenter le niveau de confiance de notre estimation il est évident qu'il faut augmenter le temps d'observation sans rencontrer l'événement. Ainsi un niveau de confiance de 0,99 (une chance sur 100 de se tromper dans l'estimation) exige d'observer le système pendant 4,6 10^{n} heures sans rencontrer l'événement étudié.

Donnons quelques ordres de grandeur de la règle 2,3 10^{n} heures* (niveau de confiance de 0,9).

Pour démontrer

- 10^{-3}/heure il faut effectuer 2,3 10^{3} = 2.300 heures d'essais soit 96 jours.

- 10^{-4}/heure il faut effectuer 2,3 10^{4} = 23.000 heures d'essais soit 960 jours, soit 2 ans et 7 mois et demi.

* Ces valeurs de 2,3 (pour le niveau de confiance 0,9) ou de 4,6 (niveau de confiance 0,99) ne sont pas des nombres magiques ! Elles résultent d'un calcul reposant sur l'hypothèse que les intervalles entre apparitions de l'événement sont régis par la loi de POISSON.

- 10^{-5}/heure il faut effectuer 2,3 10^{5} = 230.000 heures d'essais soit 9.600 jours, soit un peu plus de 26 ans

- 10^{-7}/heure (exigence de sécurité du transport aérien) il faut effectuer 2,3 10^{7} = 23.000.000 heures d'essais soit 960.000 jours, soit 2630 ans.

- 10^{-5}/ an (attention la probabilité est ici exprimée par an et non pas par jour), qui est l'exigence de sécurité pour l'industrie nucléaire (un accident majeur tous les 100.000 ans), il faut effectuer 230.000 ans de fonctionnement. Or actuellement l'industrie de production d'énergie nucléaire en France a accumulé environ 700 ans de fonctionnement seulement. On est très, très loin d'avoir démontré, par expérience directe, la sécurité dans le nucléaire (que l'on se rassure, elle est démontrée par d'autres méthodes !).

Conséquences du grand nombre d'heures d'observation nécessaires pour estimer un risque de faible probabilité.

Les opérateurs **sous-estiment systématiquement les risques** en se reposant sur leur expérience personnelle qui est toujours trop réduite.

En particulier les **procédures destinées à se protéger contre des événements rares mais dangereux ne sont pas suivies** car considérées comme inutilement contraignantes.

A titre d'exemple bien connu, citons la phrase combien de fois entendue "Tu peux y aller, je l'ai fait cent fois". En pratique les cent fois se réduisent souvent à une vingtaine, ce qui a pour conséquence que l'expérience personnelle du conseilleur permet de démontrer seulement que la probabilité de catastrophe est de l'ordre d'une chance sur dix, ce qui est anormalement élevé.

Méthodes pour combattre cette caractéristique fâcheuse de l'opérateur humain :

- **expliquer** en détail les raisons qui ont conduit à bâtir les procédures et ne pas se contenter d'en demander l'application sans que le bien fondé en soit compris.

- **montrer**, au simulateur de préférence, les conséquences de la bonne application des procédures lorsque survient l'événement redouté et les conséquences catastrophiques de l'application d'une procédure simplifiée.

- lors de l'entraînement (au simulateur en particulier**) faire survenir l'événement redouté** avec une fréquence supérieure à la fréquence réelle (l'opérateur parvient alors à se convaincre que "ça peut arriver"). Toutefois ne pas faire survenir l'événement redouté systématiquement pour laisser un caractère réaliste à l'entraînement.

5. Les erreurs de représentation.

.

L'opérateur ne perçoit pas directement le fonctionnement des organes de la machine qu'il contrôle.

Le pilote, de nuit ou dans les nuages, ne voit pas directement la position de son avion par rapport au terrain de destination. En vol à vue au milieu de l'Atlantique il lui est tout aussi difficile de se repérer par rapport au sol !

Les opérateurs sont ainsi amenés à se bâtir une représentation mentale de l'état de la machine à partir des informations fournies par les instruments du tableau de contrôle.

Cette représentation mentale peut être une simple "image". Ainsi l'opérateur se représente le niveau de combustible dans les réservoirs à partir de la lecture des jaugeurs et des débitmètres. Le pilote se représente, sur une "carte" mentale, la position relative de son avion par rapport à la piste à partir de la lecture des instruments de navigation.
La représentation mentale peut être plus intellectuelle, valeurs numériques des quantités de combustible disponibles dans chaque réservoir, de la distance à parcourir et du cap à suivre pour atteindre la piste, etc.

Par ailleurs lorsque l'opérateur agit sur une commande, le plus souvent il n'en voit pas directement le résultat sur la machine. Il lui faut alors utiliser un modèle d'action des commandes pour guider ses décisions.

Ainsi l'opérateur sait qu'il doit tourner tel robinet dans le sens à visser pour réduire le débit dans telle canalisation. Le pilote sait sur quel interrupteur agir et comment agir pour mettre en service le pilote automatique. Il sait aussi quelle molette il lui faut tourner et comment la tourner pour changer de cap.

Les opérateurs utilisent de nombreux autres modèles que le modèle d'action des commandes, modèles de position des sources

d'information, modèles d'interprétation des informations fournies par les instruments, etc.

Par exemple pour lire l'heure, il faut transposer la position angulaire des deux aiguilles de la montre en une grandeur exprimée en heures et minutes ; cette transposition est devenue automatique chez la plupart d'entre nous et nous ne réfléchissons plus pour lire l'heure ; mais essayez de lire l'heure en regardant la pendule dans un miroir et vous constaterez que ce n'est pas évident ; il nous faut modifier notre modèle de transposition qui n'est plus le modèle connu.

On constate que bien des erreurs commises par les opérateurs proviennent de l'utilisation d'une REPRESENTATION MENTALE FAUSSE de la situation ou de l'utilisation d'un modèle erroné ou inapproprié.

Ce type d'erreur est connu sous le nom d' ERREUR DE REPRESENTATION.

Dans le cas d'une erreur de représentation, les actions, les décisions de l'opérateur sont logiques pour lui.

Il raisonne juste sur des bases fausses.

Mais ses décisions sont partiellement erronées et leurs conséquences ne sont que potentielles.

Ainsi le pilote se croit au Nord de la piste alors qu'il est au Sud. Il s'imagine que le relief est faible sur sa droite, ce qui est vrai au Nord mais non au Sud. Tant qu'il ne décide pas de virer sur la droite, la situation n'est que potentiellement dangereuse. Avec un peu de chance un complément d'informations lui permettra de reconnaître son erreur avant qu'il ne prenne la décision fâcheuse de virer à droite.

Les conséquences de ce type d'erreur sont différentes de celles des erreurs dues à une charge de travail trop élevée ou à une chute de vigilance.

Dans ces derniers cas une opération élémentaire d'exécution de la tâche est ratée et la conséquence en est rapidement un incident sérieux ou une catastrophe.
Ainsi, surchargé par la lecture de panneaux de destinations trop "copieux", difficiles à lire, le conducteur ne note pas qu'il arrive à un Stop et le passe (on dit en général qu'il "brûle" le Stop ; or ce verbe sous-entend une action volontaire, ce qui n'est pas le cas.). L'incident est immédiat. La conséquence de l'erreur est nulle si le carrefour

est vide ; c'est un incident si la maréchaussée est présente ; c'est une catastrophe si un car de ramassage scolaire est sur la trajectoire.

Donnons quelques exemples typiques d'erreurs de représentation.

⇨ 5.1 Mauvaise compréhension d'un message oral.

Un opérateur annonce à son collègue "Règle la butée basse à seize cents". Ce dernier annonce "Bien compris, je règle la butée basse à sept cents". "Je confirme, butée à seize cents" répète le premier.

Dès cet instant les deux opérateurs ne sont plus dans le même univers mental.

Le premier se croit protégé par une butée correctement positionnée. On voit bien que l'incident n'est que potentiel ; il ne deviendra effectif qu'à terme si la machine dépasse la position non protégée à seize cents.

⇨ 5.2 Mauvaise compréhension d'une représentation symbolique.

Chacun sait que Rouge signifie *Interdiction*, Vert signifie *Autorisation*.
Sur un synoptique, une vanne, signalée par un voyant Rouge, est donc fermée (et le fluide ne circule pas) et signalée par un voyant Vert est ouverte (et le fluide circule).
Par contre Rouge signifie aussi *Danger* et Vert signifie *Sécurité*.
Ainsi un interrupteur électrique signalé en Rouge sur le même synoptique signifie qu'il est fermé (et que le courant passe) et signalé en Vert signifie qu'il est ouvert (et que le courant ne passe pas).

Si l'interprétation Rouge / Vert se fait sous la forme, Fermé / Ouvert il n'y a pas ambiguïté.

Par contre la correspondance Rouge / Vert avec Circule / Ne Circule Pas prête à confusion.

⇨ 5.3 Mauvaise interprétation d'un schéma, d'un panneau d'instruments.

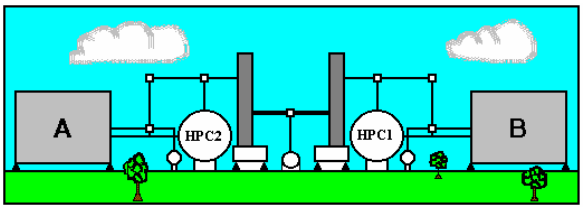
Sur le terrain sont disposés deux compresseurs étiquetés HPC1 et HPC2.

Vus de la salle de contrôle, les compresseurs sont au Sud, HPC1 est à droite de l'opérateur et HPC2 est à gauche.

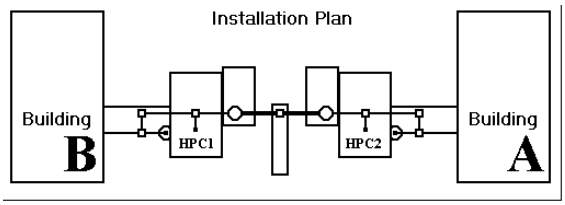
Sur le synoptique les voyants, identifiés par les sigles COMP1 et COMP2, caractérisant la mise en service de ces compresseurs sont placés l'un au-dessus de l'autre (COMP1 au-dessus de COMP2).

Sur le panneau de contrôle, les deux indicateurs de pression (identifiés par les sigles Cg pour le compresseur HPC1 et Cd pour le compresseur HPC2) sont placés côte à côte (Cg est à gauche de Cd ce qui semble logique mais est à l'envers de ce que voit l'opérateur sur le terrain ; le panneau de contrôle a été conçu en se référant au plan orienté vers le Nord ; HPC1 y est à gauche et HPC2 à droite).

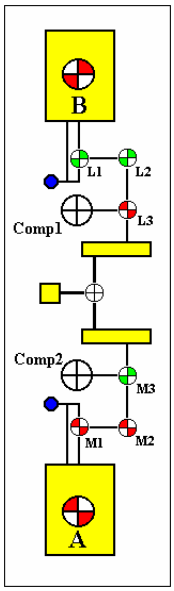
Enfin sur le panneau de commande, le levier de contrôle du régime de HPC1, identifié par le sigle K1, est placé au-dessous du levier de contrôle du régime de HPC2, identifié par le sigle K2.



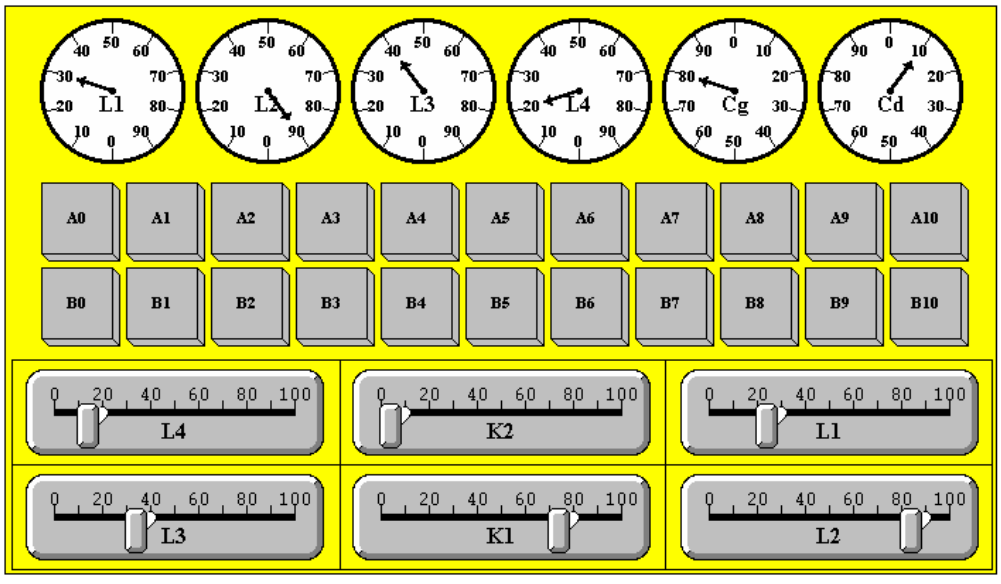
Ce que voit l'opérateur, depuis la salle de commande et placé face à son pupitre.



Plan de l'installation orienté vers le Nord



Synoptique



Panneau de commandes

Le risque de fausse interprétation des informations venant du synoptique, du panneau d'instruments et du plan des installations est grand et le risque d'action sur le mauvais levier de commande n'est pas négligeable.

Nous avons poussé l'exemple jusqu'à l'absurde, mais il n'est pas rare de rencontrer au moins l'une de ces contradictions spatiales entre les instruments, les synoptiques, le plan, les panneaux de commandes et la disposition sur le terrain.

Pour s'en sortir, bien souvent les opérateurs collent des étiquettes personnelles sur les commandes et les instruments ! On voit le danger de telles pratiques.

Cet état de fait provient bien souvent de ce que
la désignation des organes sur le terrain
et la conception du synoptique et du tableau des instruments et des commandes
ont été confiées à des équipes différentes n'ayant pas le point de vue de l'utilisateur.

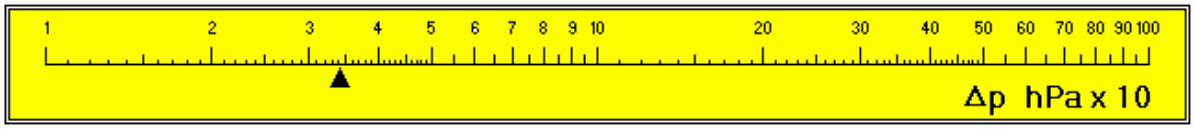
⇨ 5.4 Mauvaise interprétation d'une indication fournie par un instrument.

L'interprétation de l'indication fournie par un instrument classique à aiguille (type galvanomètre), nécessite la connaissance de la valeur d'une graduation, de la position du zéro de la graduation (qui ne figure pas nécessairement sur l'échelle), le sens de variation du paramètre à relever.
Toutes ces grandeurs sont mises en mémoire par l'opérateur au cours de son entraînement (modèles de transposition de l'information).

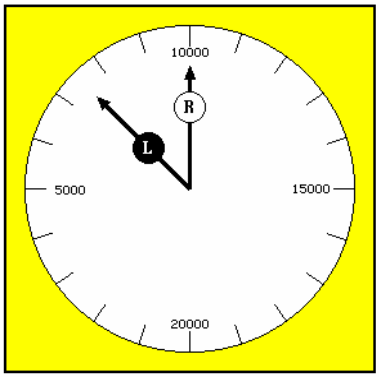
Les possibilités d'erreur de lecture sont alors légions si les instruments ne sont pas gradués avec précaution.

Citons quelques exemples d'erreur de conception des instruments.

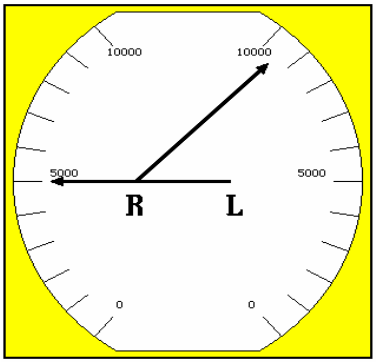
- Quelquefois les échelles sont non linéaires (voir ci dessous) ce qui ne facilite pas les interpolations entre deux graduations.



- Position du zéro de l'échelle. Sur le tableau de bord présenté sur la page 26, on remarquera que les deux tachymètres de droite ont le zéro de l'échelle en haut alors que les quatre autres tachymètres ont leur zéro en bas.



- Présentation de plusieurs paramètres sur un même instrument. Le risque de confusion entre le régime de rotation du moteur gauche (identifié par la lettre L pour Left) et le régime de rotation du moteur droit (identifié par R pour Right) est évidemment élevé car la lecture nécessite une identification préalable des aiguilles.

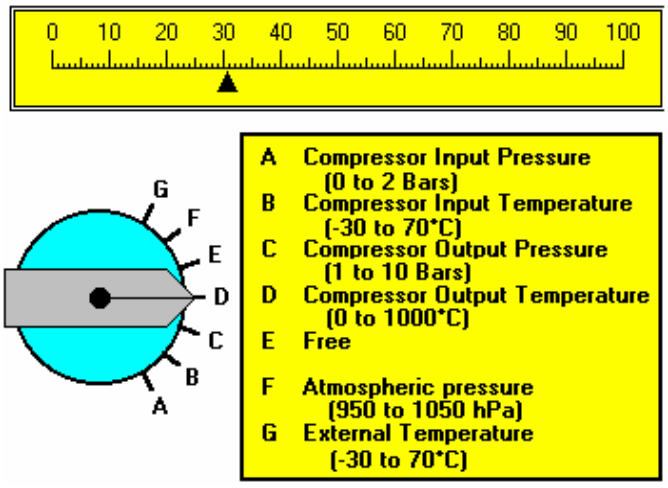


- Difficulté d'identification du paramètre indiqué. Sur le tachymètre double quel est le régime de rotation du moteur droit ?

9500 tours/minute ou 5000 tours/minute ?

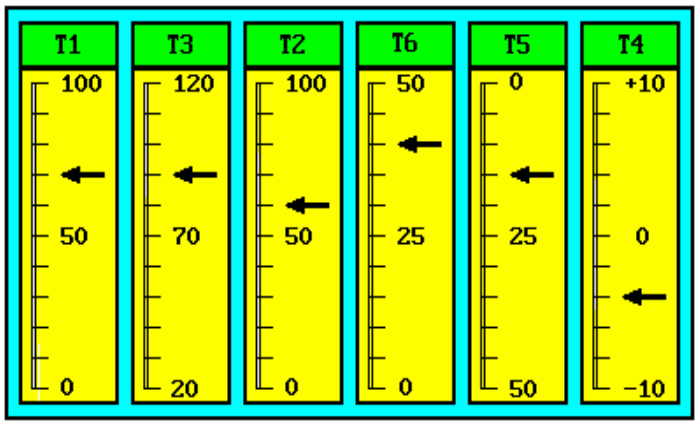
Ces deux derniers exemples ne sont pas des inventions de l'auteur. Tout porte à croire que l'une de ces dispositions est à l'origine d'une catastrophe aérienne.

- La présentation sur un seul instrument de plusieurs paramètres, le choix du paramètre se faisant par un sélecteur à plusieurs positions est également source de confusion, car l'identification du paramètre demande la vérification préalable de position du sélecteur. Dans l'exemple de la figure ci contre le problème se complique du fait que le changement de nature du paramètre relevé (libellé en anglais) s'accompagne d'un problème de changement d'échelle. Enfin on constatera que la liste des paramètres est dans l'ordre inverse des positions du sélecteur, ce qui oblige l'opérateur à lire la lettre affichée devant le sélecteur et à se reporter sur la liste pour identifier le paramètre relevé !

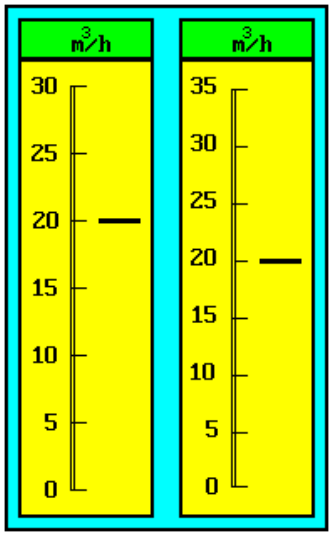


- Citons les échelles d'étendues différentes pour deux instruments voisins donnant deux paramètres de

même nature (deux thermomètres côte à côte avec une échelle de 0° à 100° pour l'un et de 20° à 120° pour l'autre) ou les échelles ayant un sens croissant inhabituel (vers le bas pour les échelles linéaire ou en sens contraire des aiguilles d'une montre pour les échelles circulaires).



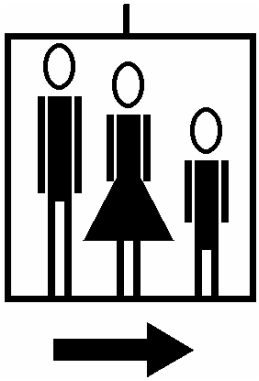
- Dans une installation industrielle, deux débitmètres placés côte à côte sur le panneau de contrôle sont destinés à mesurer les débits entrant et sortant d'un réservoir. L'une des échelles verticales, est graduée de 0 à 35 m^3/heure et l'autre graduée de 0 à 30 m^3/heure. L'opérateur doit faire en sorte que les débits entrant et sortant soient égaux. Il obtient ce résultat avec les index décalés et a l'obligation de lire la valeur sur l'un des instruments pour déterminer le débit à afficher sur l'autre. Il aurait été si simple de mettre la même étendue de mesure sur les deux instruments et de se contenter d'aligner les index ! En réponse à notre étonnement devant le dispositif, il fut répondu que les débits maximaux des deux pompes n'étant pas les mêmes on avait choisi des échelles différentes pour obtenir la meilleure précision possible sur chaque échelle. On avait ainsi privilégié une précision illusoire (les distances entre deux graduations n'étant pas sensiblement différentes pour les deux échelles) au détriment d'une simplification du travail de l'opérateur.



⇨ 5.5 Mauvaise compréhension d'une icône.

- Nous pourrions interpréter cette icône comme signalant la direction à prendre pour rejoindre le point de rassemblement en cas d'ordre d'évacuation du navire. En réalité il s'agit seulement de signaler la direction à suivre pour trouver l'ascenseur, l'explication résidant dans le petit trait vertical au-dessus du rectangle entourant la famille. Ce trait symbolise le câble qui supporte la cabine de l'ascenseur !

- Ne vaudrait-il pas mieux rajouter le mot "ASCENSEUR" (en diverses langues si l'on connaît les principales nationalités des passagers) ? Plutôt que d'avoir un graphisme qu'aucun dictionnaire ne permet d'interpréter, il est préférable d'avoir quelques mots qui ont beaucoup plus de chance d'être compris par la grande majorité des passagers.



Le lecteur nous pardonnera si nous fustigeons cette nouvelle manie consistant à remplacer un langage clair par des symboles incompréhensibles, en disant que nous pénétrons dans l'ère de l' "iconerie" !

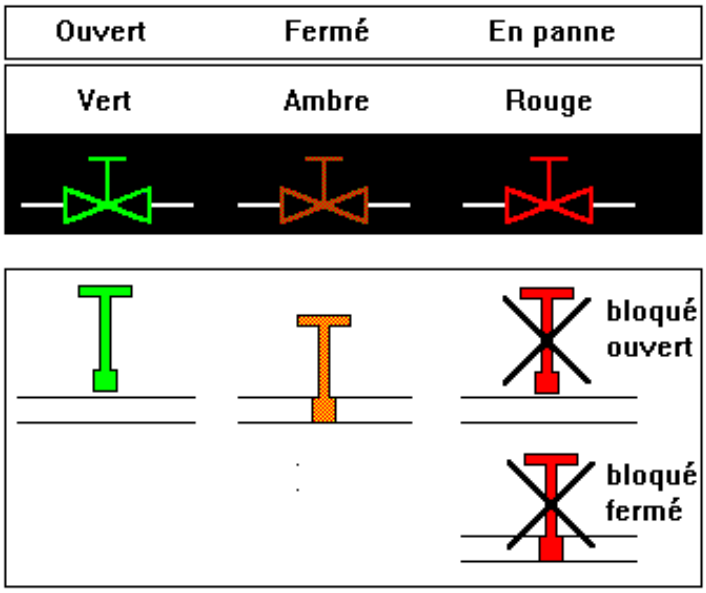
⇨ 5.6 Mauvaise présentation des données sur écrans informatiques.

Les techniques classiques de représentation de l'information avec les afficheurs électromécaniques imposent une représentation symbolique. Il faut représenter un paramètre à l'aide de l'aiguille d'un galvanomètre à déplacement angulaire ou à l'aide de voyants lumineux commandés par relais.

Mais les possibilités offertes maintenant à faible coût par l'informatique viennent bouleverser ces pratiques.

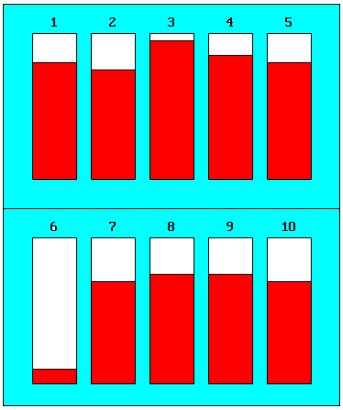
Nous sommes parfaitement capables de fournir des représentations schématiques beaucoup plus faciles à interpréter que les informations symboliques et numériques classiques. Les schémas fixes sur papier peuvent être affichés sur écran. Mais il faut prendre garde à ne pas utiliser les mêmes graphismes que sur le papier. Le choix des symboles destinés au papier a été fait pour rendre le tracé manuel simple et rapide.

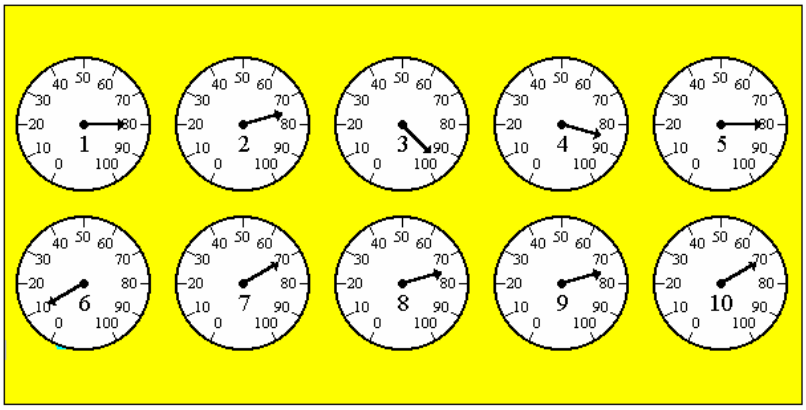
La contrainte n'existe plus pour les schémas sur écran. Une fois un "symbole" conçu, aussi complexe soit-il, il peut être reproduit instantanément et sans effort. D'où la nouvelle règle consistant à ne pas utiliser des symboles arbitraires et simples mais des "schémas" représentant la réalité de façon un peu simplifiée mais surtout claire.



- Ainsi un robinet ne sera plus représenté comme un petit papillon facile à dessiner et sans signification intrinsèque, mais par un dessin représentant sans ambiguïté un robinet. La norme de la mécanique a imposé ces différents graphismes, mais ce n'est pas une raison pour les utiliser pour les représentations sur écrans. Cette norme n'a été bâtie que pour simplifier le travail des dessinateurs et n'a en aucun cas été conçue en tenant compte des possibilités de l'informatique.

En outre la signalisation de l'ouverture ou de la fermeture ne se fera pas par un changement de couleur du symbole, mais par un changement de forme éliminant le problème de l'interprétation. Jusqu'à présent la couleur a été utilisée pour représenter l'état, ouvert ou fermé, marche ou arrêt d'un organe parce que nous ne disposions que de voyants dont l'allumage était commandé par relais. Ainsi un voyant allumé vert signifiait "ouvert" ou "marche", un voyant allumé rouge signifiait "fermé" ou "arrêt". Cette limitation des possibilités d'information a désormais disparu grâce aux présentations sur écrans. Il est dommage de représenter un robinet fermé par un "papillon" rouge et un robinet ouvert par un "papillon" vert. Souvent d'ailleurs le rouge est utilisé pour signaler une panne de l'organe et c'est la couleur ambre qui caractérise la fermeture du robinet. Or il n'est pas toujours évident de distinguer, sur écran, un vert d'un ambre, le vert se traduisant quelquefois par un vert jaunâtre et l'ambre par un jaune verdâtre !





1	80	3	95	5	80	7	70	9	75
2	75	4	85	6	10	8	75	10	70

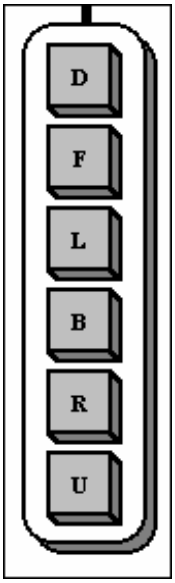
- Pour les mêmes raisons un réservoir sera représenté par un schéma donnant sa position et sa forme approximative et surtout son taux de remplissage ne sera plus fourni par l'aiguille d'un jaugeur classique mais par un niveau de liquide sur le schéma du réservoir lui-même. On évite ainsi les erreurs de localisation de l'information (on ne risque pas de lire le jaugeur d'un autre réservoir) et les erreurs d'interprétation de l'information (il est peu probable de confondre sur le schéma un réservoir plein et un réservoir vide, à partir du moment où l'on y voit le niveau comme si l'on voyait le niveau réel).

On constatera sur cet exemple combien la représentation numérique est peu intuitive et peut conduire à des erreurs d'interprétation graves.

Nous retiendrons donc la règle suivante :

Il faut SCHEMATISER plutôt que SYMBOLISER.

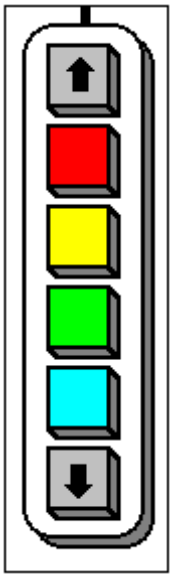
⇨ 5.7 Mauvaise disposition ou mauvaise identification des commandes.



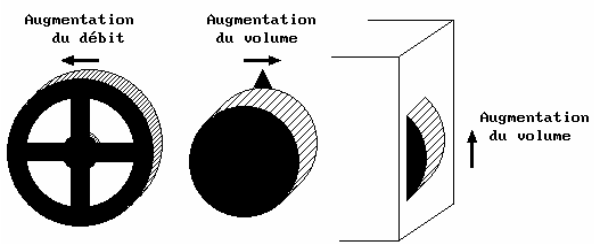
Que penser de cette commande de pont roulant qui tenue à la main peut être orientée n'importe comment par rapport aux déplacements de la charge ?

Les étiquettes sont des initiales de mots anglais (L pour Left gauche, R pour Right droite, B pour Backward arrière, F pour Forward avant). Les touches sont placées dans un ordre arbitraire. En particulier la touche U (pour Up vers le haut) est en bas et la touche D (pour Down vers le bas et non pour Droite !) est en haut.

Il est bien préférable d'identifier les touches par des couleurs et de peindre des mêmes couleurs les parois de l'atelier. Appuyer sur la touche rouge déplace la charge vers le mur rouge quelle que soit l'orientation du boîtier. Il est aussi préférable de schématiser les touches "haut" et "bas" par des flèches ⇧ et ⇩



⇨ 5.8 Sens inhabituel d'action des commandes.



- Le sens normal d'augmentation de débit pour un robinet est le sens à dévisser. Par contre le sens normal d'augmentation de volume pour un potentiomètre de commande d'un amplificateur est le sens à visser. Cette disposition pour les potentiomètres n'est d'ailleurs valable que pour les potentiomètres placés sur la face avant des boîtiers. Si le potentiomètre est placé sur la face latérale droite du boîtier (disposition souvent rencontrée sur les postes de radio portatifs) le potentiomètre doit fonctionner en sens contraire pour que son action reste intuitive (un déplacement du doigt vers le haut augmente alors le volume).

Il est très dangereux d'avoir quelques robinets qui s'ouvrent par rotation dans le sens des aiguilles d'une montre, alors que dans l'installation la plupart des robinets s'ouvrent en sens contraire. Or nous avons pu constater ce défaut sur de nombreuses installations industrielles sans que nous ayons pu obtenir une justification satisfaisante de cette disposition (il semblerait dans bien des cas que ce soit le fournisseur de la robinetterie qui ait fait ce choix de lui-même parce que les seuls robinets dont il disposait au moment de l'appel d'offre et répondant au cahier des charges étaient des robinets exotiques !).

⇨ 5.9 Difficulté d'analyse de la situation.

Souvent les opérateurs se trouvent dans ce type de situation en particulier imposée par des rédactions confuses de procédures.

Essayez de résoudre rapidement le problème suivant :

- Vous vous apprêtez à vous garer. Un panneau annonce "Stationnement interdit côté pair jours impairs". La maison sur le trottoir d'en face porte le numéro 31 ter. Vous savez que le lendemain est le premier mars de l'an 2000. De quel côté vous garez-vous ?
Ne cherchez pas à résoudre ce problème rapidement. Garez-vous ailleurs !

- Autre exemple "Il n'est pas interdit de ne pas fermer le robinet tans que le réservoir n'est pas plein"

⇨ 5.10 Concomitance de deux événements.

- L'opérateur ouvre un interrupteur et une alarme retentit !
Il est très difficile à l'opérateur de ne pas faire de relation de cause à effet entre les deux événements qui peuvent être totalement indépendants.

- Garé à six heures du soir sur les Champs Élysées, l'auteur a été fort troublé de voir l'avenue s'illuminer à l'instant même où il tournait la clé de contact.
Ce type d'erreur est maintenant connu sous le nom d'**erreur Champs Élysées**.

⇨ 5.11 L'effet d'habitude.

- L'opérateur exécute pour la millième fois une procédure de changement de configuration de sa machine. Jusqu'ici les opérations de vérification du nouvel état ont toujours été positives. Ce jour-là l'opérateur exécute scrupuleusement ces vérifications. Or un incident a perturbé les opérations (action ratée sur une commande, panne d'un système,..). L'opérateur est tellement habitué à voir les vérifications positives qu'il interprète abusivement ce qu'il observe et en conclut que le nouvel état est correct.

- Tous les jours un mécanicien d'un train de banlieue passe le kilomètre 24 avec un carré ouvert. Ce jour-là le carré est exceptionnellement fermé et le mécanicien ne le voit pas.

- Tous les jours un automobiliste suit le même trajet pour se rendre à son lieu de travail. Ce jour-là un panneau de sens interdit a été installé provisoirement. L'automobiliste ne le voit pas et pénètre dans le sens interdit.

- Sur un chantier EDF l'opérateur a demandé la mise hors tension de la ligne sur laquelle il doit travailler et cette mis hors tension lui a été confirmée par téléphone. Il branche le VAT (Vérificateur d'Absence de Tension) sur la ligne et l'instrument signale la présence de tension. L'opérateur en conclut que le VAT est défectueux et il s'électrocute.

- Chaque fois que le pilote a mis la palette de train en position sortie, le train est sorti et il a pu observer les trois lampes vertes signalant cette position utile pour l'atterrissage. Ce jour-là une panne du circuit hydraulique interdit la sortie correcte du train. Le pilote vérifie les lampes et interprète les lampes rouges comme des lampes vertes plus visibles que d'habitude. Il en résulte un atterrissage non réglementaire.

Notez que cette anecdote n'est pas le fruit de l'imagination, c'est arrivé à l'auteur de ce papier !

⇨ 5.12 L'effet de la panne connue.

- Sur cet avion de transport on pouvait observer de fausses alarmes de feu en soute. Peu après le décollage, l'alarme feu soute 5 s'allume. Le commandant de bord décide de ne pas en tenir compte. "Encore une fausse alarme". Quelques instants plus tard l'alarme feu soute 6 s'allume "Une double panne d'alarme ! Le service maintenance va m'entendre". La présence de fumées dans la cabine passagers est attribuée à de la condensation de vapeur ! Ce n'est que l'apparition de flammes dans la cabine qui décide le commandant de bord à faire demi-tour pour regagner le terrain (hélas trop tard).

- Au changement de quart l'équipe sortante annonce qu'une panne est survenue et que l'équipe de maintenance est en train de réparer. Peu de temps après la prise de service de l'équipe montante, une alarme retentit. Conclusion "n'en tenons pas compte, c'est dû aux opérations de la maintenance.". Il faut que d'autres alarmes retentissent pour que l'équipe prenne conscience du fait qu'elle est en présence d'une nouvelle panne sans rapport avec la première.

- Après un mois au garage, la batterie est incapable de démarrer le moteur. Démarrage sur batterie de parc. Le conducteur constate que l'alarme batterie est toujours allumée. "Roulons un peu pour recharger !". L'alarme batterie s'éteint aussitôt. Au retour au garage pour charger le coffre, la lampe batterie se rallume. "Diable, la batterie est très faible". Après deux roulages et deux arrêts, les mêmes symptômes persistent. C'est alors que le conducteur note que l'alarme n'est pas l'alarme batterie, mais l'alarme frein à main située juste au-dessous. Obnubilé par le problème batterie il a interprété cette lampe rouge comme signalant le défaut redouté.

Analyse des exemples d' Erreurs de Représentation

Il y a deux types d'Erreurs de Représentation :

⇨ Les erreurs dues à une mauvaise utilisation de l'information, l'information est mal interprétée par l'opérateur parce que mal présentée, confuse, compliquée à analyser, etc.
(exemples 1 à 10).

⇨ Les erreurs dues au fait que l'opérateur, suite à la succession des événements précédents qu'il ne remet pas en cause, se bâtit une image *a priori* de la situation
(exemples 11 et 12).

Dès lors toutes les informations qui pourraient lui signaler que son image mentale est incorrecte, sont ignorées ou interprétées dans le sens confirmant la justesse de l'image.
Il est alors impossible de redresser l'erreur par les moyens classiques d'alarmes et d'avertissements qui sont eux aussi ignorés ou mal interprétés.

L'opérateur persiste dans son erreur.

"Errare humanum est, perseverare diabolicum"
(L'erreur est humaine, persévérer est l'oeuvre du diable).

Ce type d'erreur est connu sous le nom d'erreur diabolique.

En général les Erreurs de Représentation ne sont pas identifiées par les opérateurs parce que ce type de démarche mentale est ignoré.

Dans l'armée de l'air on parle de "viscosité mentale" ce qui est imagé, mais n'explique rien. Il est donc fondamental d'informer les opérateurs sur ce type de phénomène.

Il est également utile de montrer, à l'entraînement, l'apparition de ce genre d'erreurs, car les opérateurs, s'ils admettent qu'ils peuvent commettre des erreurs de représentation dans la vie courante, s'imaginent bien souvent en être à l'abri dans la vie professionnelle en raison de leur compétence.

Il y a deux types d'**Erreurs de Représentation** :

- les erreurs dues à une mauvaise utilisation de l'information,

- les erreurs dues au fait que l'opérateur, suite à la succession des événements précédents qu'il ne remet pas en cause, se bâtit une image *a priori* de la situation.

Les erreurs de représentation

SONT COMMISES PAR TOUT LE MONDE,

même par les plus sérieux, les plus travailleurs, les plus consciencieux, les plus compétents...

Par ailleurs la présentation d'information permettant de suggérer directement la bonne image de la situation est favorable. La vue directe du train d'atterrissage est plus favorable que l'allumage de voyants symboliques (reste le problème technologique pour rendre le train d'atterrissage visible !). La vue directe sur écran, de la position de l'avion sur la carte, évite les erreurs de navigation (il est difficile de se croire au Nord du terrain lorsqu'on voit l'avion au Sud sur la carte avec une représentation du relief).

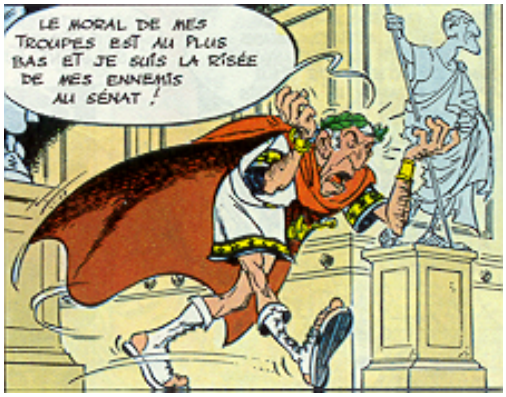
.

Les Erreurs de Représentation
dues à une mauvaise utilisation de l'information
peuvent être combattues

par des modifications technologiques sur les instruments, les commandes, les logiciels.

Les Erreurs de Représentation diaboliques
peuvent être combattues

- par la formation
  (prise de conscience du phénomène),
- par l'entraînement,
- par des systèmes de détrompage automatiques indépendants de l'opérateur
- par des présentations d'informations suggérant directement l'image mentale.



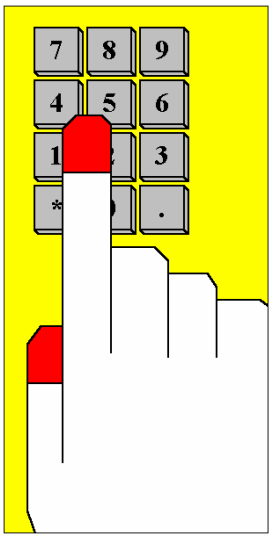
d'après GOSCINNY et UDERZO

Si le lecteur croît assister à une représentation de Julius Caesar de Shakespeare il commet une erreur ... de représentation.

6. Maladresse, Lapsus.

Il arrive à l'opérateur de ne pas exécuter correctement le geste prévu, de ne pas prononcer le mot ou la phrase voulue, etc. Il s'agit de maladresses ou de lapsus.

Les lapsus peuvent être **gestuels** (on accroche une commande avec la manche, on tape sur la touche d'à coté, 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, on entend "bon" au lieu de "non").



Bien souvent la maladresse provient d'une mauvaise ergonomie du poste de travail.

Il est plus difficile de remplir une flûte à champagne qu'un pot de bière !

Les touches de calculettes trop petites facilitent les erreurs de frappe, etc.

Sans commentaire ...

D'après HERGÉ

7. Capacité de raisonnement en Logique Floue.

Par LOGIQUE FLOUE nous entendons toute démarche de décision faisant intervenir une estimation de l'état de la machine ne reposant pas sur des valeurs figées, bien déterminées a priori,
mais sur des tendances, des évolutions chronologiques, une expérience acquise et une vue d'ensemble de la situation.

Par exemple la coupure de l'interrupteur d'une alimentation électrique se traduit, théoriquement, par une mise à zéro de la tension de sortie. Or en pratique le détecteur ne mesure pas une valeur strictement nulle, mais une valeur voisine de zéro. Qu'entend-on alors par voisine de zéro ? Pour qu'un automatisme détecte la mise hors service de l'alimentation, il est nécessaire de fixer un seuil de tension au-dessous duquel celle-ci est considérée comme effectivement nulle.

Des considérations sur la précision de mesure du capteur aident l'ingénieur automaticien à fixer un seuil ; mais ce seuil sera-t-il valable dans toutes les conditions d'emploi et de vieillissement du capteur ? Or il faut fixer une valeur raisonnable évitant les erreurs de détection, assez grande pour couvrir les erreurs de zéro, assez faible pour éviter de confondre coupure normale d'alimentation et mauvais fonctionnement.

Par contre un opérateur humain observant la chute de tension ne s'arrêtera pas à la valeur précise affichée. Il se contentera d'une valeur floue, l'expression "voisine de zéro" lui suffisant pour juger, grâce à son expérience, en observant la chute de tension en fonction du temps. Il lui sera relativement facile de discriminer l'arrêt normal et le mauvais fonctionnement.

Il est évident que si le seuil fixé à un automatisme de détection se révèle non approprié à l'usage, il sera facile de modifier ce seuil et de bâtir une logique plus complexe de discrimination d'état. Mais une telle démarche n'est possible qu'a posteriori si elle apparaît indispensable. Il est impossible de prévoir des logiques complexes pour toutes les détections analogues.

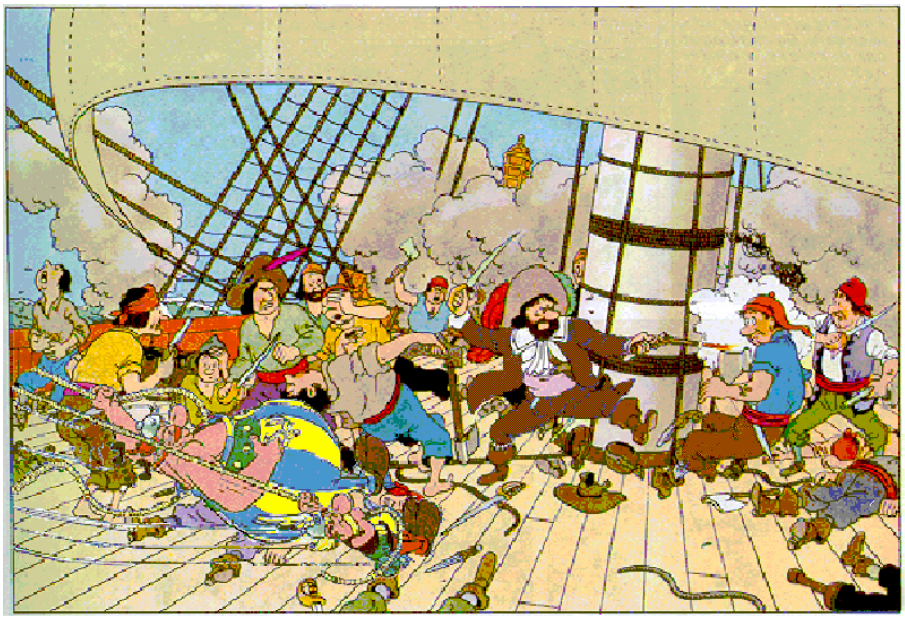
Cette dernière remarque est très générale. L'opérateur humain est très souple d'utilisation en logique floue, mais dès que l'on a bien identifié le problème, grâce à son expérience, on peut le remplacer par un automatisme, la logique ayant dès lors perdu son caractère flou.

8. Capacité de Reconnaissance de Forme

Par RECONNAISSANCE DE FORME, nous entendons toute méthode de saisie globale ou synthétique de l'information analogue à la reconnaissance d'une forme donnée dans une image.

Ce peut être la reconnaissance directe d'une anomalie sur un site (présence d'une fuite de vapeur même légère à un endroit inhabituel par exemple). Le cerveau humain est capable d'identifier très rapidement et avec une grande probabilité de succès une telle situation. Par contre les algorithmes capables d'une même performance avec un système automatique sont loin d'être au point.

D'un seul coup d'œil le lecteur pourra identifier les personnages et découvrir l'anomalie sur le dessin ci dessous. Quel logiciel serait capable d'une telle performance ?



d'après GOSCINNY, UDERZO et HERGÉ

Ce peut être également la **reconnaissance d'une anomalie** sur une présentation synthétique sous forme d'un graphique ou d'une courbe. Par exemple la forme de l'évolution d'un paramètre en fonction du temps, ou d'un autre paramètre, peut être qualitativement différente de la forme nominale, sans que des critères précis et définis a priori permettent de le déceler. Nous sommes là en présence d'une reconnaissance de forme apparentée à la logique floue.

Ce peut être enfin la **reconnaissance d'un bruit**, d'une vibration, voire d'une odeur (fuite de liquide hydraulique par exemple) qui alerte l'opérateur et lui fait deviner une anomalie. Ici encore nous sommes dans le domaine de la logique floue ; comment apprendre à un système automatique à distinguer la fréquence et l'intensité d'un bruit jugé anormal par rapport à la fréquence et l'intensité d'un bruit normal ?

Comment distinguer une odeur anormale au milieu des odeurs normales de vernis, d'huiles, de combustibles, de fumées dans une installation ?

Seul un opérateur humain, entraîné et connaissant bien l'installation, en est capable.

Ainsi la **RECONNAISSANCE DE FORME** repose sur trois caractéristiques de l'opérateur humain :

- L'utilisation de la logique floue,

- La capacité de distinguer des similitudes au milieu des dissemblances de diverses situations,

- La capacité de distinguer des dissemblances au milieu des similitudes de diverses situations.

9. Capacité de Décision sur la base de critères qualitatifs.

Par **Décision reposant sur des critères qualitatifs** nous entendons toute démarche faisant intervenir des considérations qui ne peuvent être chiffrées et donc entrer dans une pondération de critères orientant le choix.

C'est la **différence fondamentale entre l'homme et l'ordinateur.**

Un logiciel d'ordinateur ne peut contenir que des décisions reposant sur des critères du type :

"Si la valeur de X est supérieure à A alors j'exécute l'action 1 sinon j'exécute l'action 2." où X et A sont des *valeurs numériques*.

Le "logiciel" de décision de l'homme peut comporter des raisonnements du type :

"Cette situation est inattendue. Elle ressemble toutefois à une situation un peu différente mais déjà rencontrée. Je vais donc prendre une décision analogue, avec quelques écarts tenant compte des quelques faits nouveaux."

Toute évaluation du risque et des conséquences entraînées par une situation donnée entre dans cette catégorie (Doit-on décider un atterrissage d'urgence par mauvaise météo en cas de crise cardiaque d'un passager ou attendre de meilleures conditions de déroutement ?).

Des considérations d'éthique et de morale entrent en ligne de compte dans ces décisions (le report de l'atterrissage peut avoir des conséquences graves pour le passager malade, mais peut-on pour autant faire prendre des risques aux autres passagers ?).

Il est évident qu'un système automatique ne peut être programmé pour répondre à ce type de questions.

Une fois la décision prise par l'opérateur humain, il peut en confier la réalisation à un automatisme, en fixant par exemple de nouvelles valeurs de consigne.

Ainsi **mettre l'homme dans la boucle** ne signifie pas lui faire "piloter" le système en permanence.

Il est alors fondamental de lui fournir les informations nécessaires et suffisantes lui permettant de connaître en permanence l'état du système, ainsi que les informations lui permettant d'en prévoir l'évolution.

.

L'opérateur humain a trois bonnes caractéristiques :

- Capacité de raisonner en Logique Floue

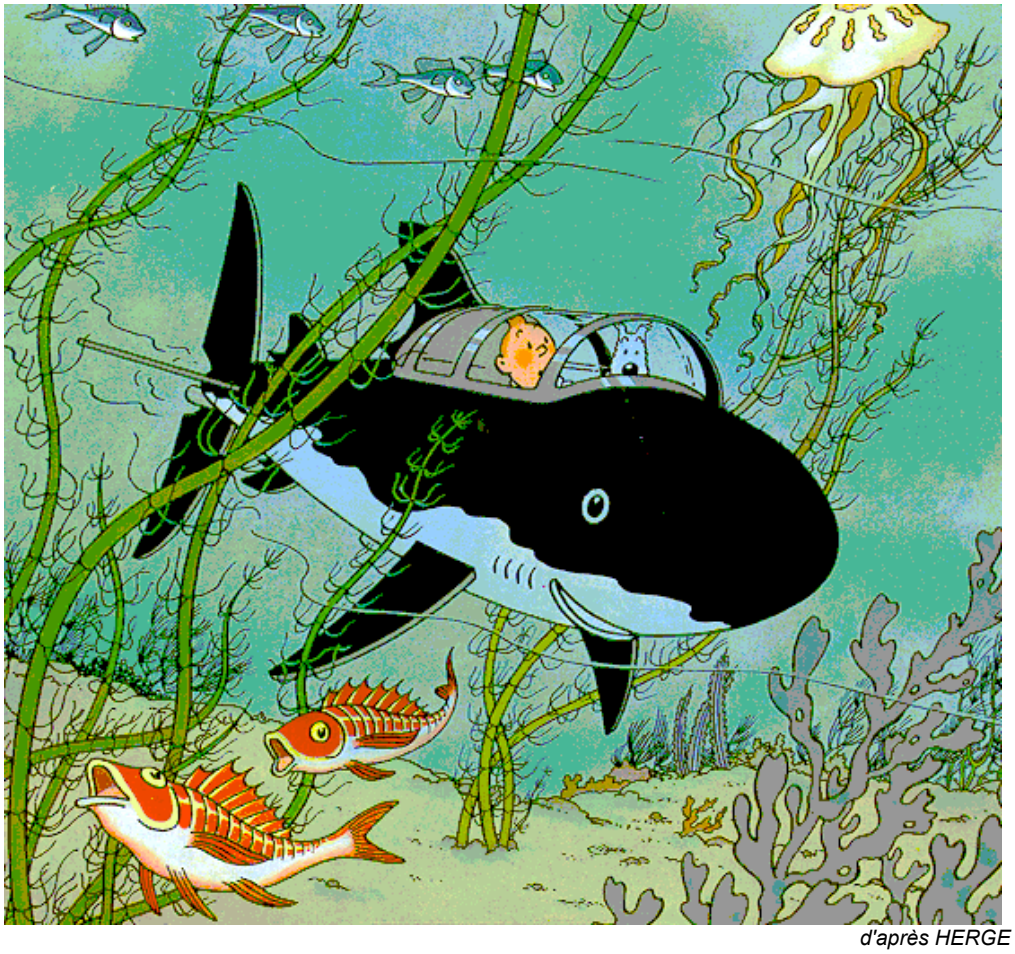
- Capacité de Reconnaissance de Forme

- Capacité de Décision sur la base de critères qualitatifs

SEUL L'HOMME EST CAPABLE DE FAIRE FACE

AUX SITUATIONS NON PREVUES.

Opérateur ou Automatisme ?



d'après HERGE

Le choix **"OPERATEUR HUMAIN OU AUTOMATISME"**
repose sur la philosophie suivante.

Il faut **AUTOMATISER** les tâches dont l'exécution met les opérateurs humains en situation de **risques d'erreurs**

et il faut LAISSER aux opérateurs humains la **RESPONSABILITÉ** des tâches pour lesquelles les automatismes sont **moins performants que les hommes**.

.

⇨ Si la réalisation d'une fonction présente des **dangers physiques** inacceptables pour l'homme, **IL FAUT L'AUTOMATISER.**

⇨ Si la réalisation d'une fonction exige une **habileté exceptionnelle** de l'opérateur, **IL FAUT L'AUTOMATISER.**

Une fonction sera reconnue comme exigeant une **habileté exceptionnelle**

⇨ si, dans le temps imparti, le nombre d'actions de l'opérateur (prises d'information, décision, action sur les commandes) est trop élevé ce qui en rend pratiquement impossible une exécution correcte.
- pilotage d'un système instable ou à temps de réponse très inférieur au temps de réponse de l'opérateur humain (de l'ordre de quelques dixièmes de seconde)
- reconfiguration très rapide du système après panne...

⇨ si la tâche à exécuter exige une précision que ne peut atteindre un opérateur en manuel.
- atterrissage sans visibilité dit zéro, zéro (plafond nul, visibilité horizontale nulle)...

⇨ si la situation et la conception du système imposent une correction initiale sans possibilité de correction ultérieure. La tâche doit être alors exécutée en boucle ouverte.
- tir instinctif...

⇨ Si la réalisation d'une fonction exige un **travail fastidieux et répétitif** (comme le respect d'une valeur de consigne par une action simple, l'attente passive d'un événement rare ou la surveillance d'un paramètre peu évolutif) **IL FAUT L'AUTOMATISER**.

- utilisation du pilote automatique pour les phases de croisière d'un avion ou d'un navire.
- veille devant un écran radar vide pendant des heures dans l'attente d'un écho hypothétique (l'homme ne peut raisonnablement maintenir sa vigilance dans ces conditions).
- interdiction du franchissement intempestif des limites du domaine de fonctionnement autorisé (exemple freinage type ABS sur automobile, limites d'incidence et de vitesse sur avion).

⇨ Si une catastrophe peut résulter d'une **seule erreur d'un seul opérateur**,

⇨ **IL FAUT INTERDIRE L'ACTION ERRONNEE ELLE-MÊME**

- Entrent dans cette catégorie tous les systèmes de détrompage, par exemple les dispositifs mécaniques interdisant des montages erronés, les dispositifs de verrouillage n'autorisant que des enchaînements prédéterminés de diverses commandes.
- Font partie également de ce type de solution, tous les dispositifs automatiques inhibant les actions de commandes conduisant à des dépassements du domaine autorisé comme nous l'avons vu au paragraphe précédent.

⇨ **IL FAUT PREVENIR L'OPERATEUR**

qu'il vient de mettre son système dans une situation qui, à terme, peut devenir dangereuse et lui indiquer de façon simple et claire la procédure à suivre pour revenir dans un état sûr.

Ainsi un système automatique détecte que l'avion est en descente, à basse altitude, basse vitesse, moteurs réduits et train d'atterrissage non sorti. Il prévient le pilote que cette configuration peut être dangereuse à terme si le vol se poursuit ainsi jusqu'à l'atterrissage. Se pose alors le problème de perception de l'alarme dans une situation à forte charge de travail.

⇨ **IL FAUT PREVENIR L'OPERATEUR**

qu'il s'apprête à faire une manœuvre dont les conséquences peuvent être graves et lui demander de confirmer sa volonté d'action par une seconde manœuvre qui ne doit pas être réflexe.

Ce sont de telles dispositions que l'on rencontre sur les micro-ordinateurs personnels lorsque l'on s'apprête à détruire un fichier de données ou à formater un disque ou une disquette non vierges.

⇨ **IL FAUT LIMITER LES CONSEQUENCES DE LA MANŒUVRE ERRONEE EN AGISSANT AUTOMATIQUEMENT**

(dans les cas où la manœuvre ne peut jamais être utile, ce qui n'est pas vrai pour les deux situations précédentes).

- un dispositif coupe la traction sur une locomotive lorsque le mécanicien déclenche une action de freinage.
- un système automatique interdit, sur véhicule routier, le blocage des roues même si, par réflexe, le conducteur écrase le frein.
- si le mécanicien d'un train ne respecte pas la signalisation d'arrêt imposé par un carré fermé, un dispositif automatique (le KVB) freine le train pour lui éviter de pénétrer dans une zone à protéger (en particulier pénétrer sur une voie déjà occupée par un autre train).

En résumé, ces recommandations ont pour objet de ne pas mettre l'opérateur dans des situations où il fait preuve d'une fiabilité physique ou mentale médiocre.

⇨ Chaque fois qu'une **décision repose sur des choix**

- qui *ne peuvent se réduire à des algorithmes peu complexes,*
- qui font intervenir une *logique floue* ou une *évaluation qualitative de la situation,*
- qui nécessitent une saisie de la situation par une méthode du type *reconnaissance de forme,*

IL FAUT METTRE L'HOMME DANS LA BOUCLE EN LE LAISSANT MAÎTRE DE LA DÉCISION,

ce qui ne signifie pas nécessairement maître direct de l'action sur le système.

Par *algorithmes peu complexes* nous entendons des fonctions simples, liant commandes, paramètres à contrôler et consignes, dépendant des états prévus du système. Ces états doivent donc être connus a priori en totalité. L'établissement de ces fonctions repose sur des modèles de comportement du système (réponses aux commandes fonctions des états et des paramètres d'environnement) qu'il importe d'avoir précisément identifiés a priori.

Tout doute sur les modèles de comportement ou l'exhaustivité de la liste des états possibles rend hasardeux l'établissement des algorithmes de contrôle.

Nous venons de dire que **mettre l'homme dans la boucle en le laissant maître de la décision**, ne signifie pas nécessairement maître direct de l'action sur le système.

Nous voulons dire par là que la maîtrise de la décision n'entraîne pas systématiquement la reprise des opérations en "manuel", c'est-à-dire en pilotant directement le système sans l'aide d'automatismes.

L'exemple cité au paragraphe précédent nous permettra d'illustrer ce propos. Un système de surveillance de l'environnement permet de détecter des échos radar d'autres véhicules (navire ou avion) susceptible d'entrer en collision avec notre propre véhicule. Le système automatique a pour seul objet de signaler la présence d'un écho sur un écran généralement vide. Une fois l'écho signalé, la décision revient à l'opérateur. C'est lui et lui seul qui choisira la manœuvre à effectuer pour éviter la collision. Il entre alors dans la boucle. Mais pour effectuer la manœuvre il n'est pas nécessaire qu'il l'exécute manuellement en agissant directement sur la barre ou le manche. Son action peut se réduire à la simple introduction de nouvelles consignes dans le pilote automatique pour modifier la trajectoire. La partie noble du travail de l'opérateur consiste donc à décider de la manœuvre (qui peut se réduire à rien, s'il a reconnu que l'écho est un faux écho !) et à choisir les nouvelles valeurs de consigne.

On voit dans cet exemple que l'automatisme repose sur un algorithme relativement simple de détection d'un signal sortant du bruit de fond. Mais l'on se garde bien de pousser plus loin les fonctions de l'automatisme. On laisse à l'opérateur le soin de juger la situation (reconnaissance de forme sur l'écho, analyse des vitesses et position du véhicule détecté, etc.) et celui de prendre la décision. Confier ces opérations à un automatisme conduirait à définir des algorithmes de décision beaucoup trop complexes pour couvrir toutes les situations possibles (dont les fausses détections !), alors que l'opérateur humain est parfaitement adapté à ce type de tâche. Rien n'empêche toutefois de lui fournir des éléments d'aide à la décision du type vitesse et position relatives du véhicule détecté, calcul de positions futures, etc.

Qui commande, les automatismes ou les hommes ?

Les automatismes se chargent des tâches exigeant une rapidité de réaction dont ne dispose pas l'homme et des tâches répétitives et fastidieuses de surveillance et de contrôles simples. Les hommes se réservent les domaines où une décision non prévue est à prendre sur des bases qualitatives avec une reconnaissance globale de la situation.

L'ensemble automatisme - opérateur humain constitue ainsi un bon exemple de redondance "dissemblable", les défaillances et les faiblesses de l'un n'étant sûrement pas les défaillances et les faiblesses de l'autre.

C'est ainsi que le couple automatisme - opérateur humain peut assurer un niveau de sécurité qui ne pourrait être atteint séparément par l'un ou l'autre seul.

La réponse à la question posée est alors simple,

Chacun, opérateur ou automatisme, ASSURE LA SECURITÉ **dans les domaines où il est le mieux adapté**
et SE REPOSE SUR L'AUTRE **dans les domaines pour lesquels il est peu fiable ou peu performant**.

LA DÉCISION FINALE ne peut revenir **qu'à l'homme** dans les domaines de la logique floue, de l'imprévu, du qualitatif,
mais c'est **à l'automatisme de prendre la décision** (pré-programmée par l'homme, toutefois) dans les domaines du répétitif, du fastidieux et de la réponse très rapide à des événements aléatoires.

d'après GOSCINNY et UDERZO

Il n'y a pas hélas, de potion magique pour rendre les opérateurs humains infaillibles.

Le Retour d'Expérience

d'après HERGÉ

Seule une analyse du comportement des opérateurs en service permet de dégager les circonstances critiques conduisant à l'erreur et trouver des remèdes pour limiter l'apparition de ces circonstances néfastes.

C'est l'objet du **RETOUR D'EXPÉRIENCE**.

Le retour d'expérience comporte les opérations suivantes :

⇨ **Recueil des incidents ou accidents en service**
en identifiant les conditions dans lesquelles ils se sont déroulés. Par conditions nous entendons

- les conditions "internes", par exemple composition, ancienneté, état physiologique (fatigue, maladie), état psychosociologique (soucis personnels, familiaux, professionnels ou événements heureux, naissance, gain à la loterie,..), etc. des membres de l'équipage.

- les conditions "externes", travail de jour, de nuit, éclairage, en turbulence, gros temps, présence d'instructeurs, de personnalités, mouvements sociaux, etc.

⇨ **Analyse de la succession des événements**,
pour tout incident ou accident ayant conduit à une situation potentiellement dangereuse ou catastrophique en précisant, pour chacun de ces événements, les conditions ayant favorisé l'erreur.

⇨ **Recherche du ou des défauts du système ayant créé les conditions**
favorisant l'erreur, une fois un événement identifié,

⇨ Lorsqu'un défaut système identifié participe à un **nombre significatif d'incidents**, **recherche du ou des remèdes possibles** pour l'éliminer ou en réduire les conséquences.

La connaissance des conditions dans lesquelles s'est déroulé un incident est importante car elle permet d'estimer la probabilité de se retrouver dans des conditions analogues et donc de donner un poids aux actions envisageables pour y trouver remède.

Il ne s'agit pas, comme pour une enquête d'accident, de dégager toutes les circonstances à l'origine de l'incident, mais d'identifier les circonstances sur lesquelles nous pouvons agir pour en réduire la probabilité d'apparition.

Il faut agir lorsqu'un nombre significatif d'incidents a été détecté. Ce nombre significatif 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.

LES ÉVÉNEMENTS.

On peut représenter l'état de fonctionnement de la machine à tout instant par un point, dit

POINT D'ÉTAT,

dans un espace à n dimensions,
chaque dimension étant attribuée à l'un des paramètres caractérisant l'état de la machine dans son ensemble, d'un système, d'un sous système ou d'un élément (vitesse, position, régime de la turbine, température du fluide de graissage, etc.).

A chaque position du point d'état on peut faire correspondre une probabilité de catastrophe.

Les règles d'emploi du système imposent à l'opérateur de maintenir le point d'état à une **valeur nominale** ou dans un **domaine** suffisamment éloigné des limites.
En général, le franchissement d'une limite est dû à une succession d'événements qui déplacent le point d'état.
On notera qu'aucun des événements ne joue un rôle prépondérant. Aussi est-il vain de chercher à définir **"la cause" d'un accident**. Chaque événement joue un rôle dans le déplacement du point d'état et il suffit qu'un seul d'entre eux, peu importe lequel, n'ait pas lieu pour que l'accident soit évité.

Un **ACCIDENT** peut se décrire par une succession d'événements dont le dernier conduit au franchissement d'une limite amenant au voisinage de l'unité la probabilité de catastrophe, blessures ou perte de vies humaines, destructions de matériel.

Un **INCIDENT** peut se décrire par une succession d'événements dont le dernier met le système dans une situation dangereuse puisque voisine d'une limite.

Un déplacement du point d'état est provoqué par des événements de trois types et de trois types seulement :

- événements d'Opérabilité,

L'opérateur dispose des commandes nécessaires pour maintenir le point d'état dans le domaine autorisé, mais il laisse le point d'état se rapprocher d'une limite ou même la dépasser.

L'origine de ces événements est à rechercher dans la liste des faiblesses de l'opérateur décrites plus haut.

- événements de Sensibilité aux Perturbations,

Sous l'effet de *Perturbations Internes* (pannes, feu, action intempestive d'un passager,..) ou de *Perturbations Externes* (rafale, impact d'oiseau, givrage,...) le point d'état approche ou dépasse une limite, soit parce qu'il s'est lui-même déplacé, soit parce que la limite a été changée.

- événements de Manoeuvrabilité.

Pour suivre un programme donné, défini par l'objectif de l'opération (suivi d'une trajectoire donnée, fabrication ou manutention d'une pièce, variation de fourniture d'énergie, etc.) ou pour ramener le point d'état à la valeur nominale (ou dans le domaine autorisé) à la suite d'un écart dû à des événements des deux premiers types, l'opérateur doit effectuer une "manœuvre" qui, en général, amène le point d'état à se déplacer et quelquefois à se rapprocher d'une limite. Ce déplacement constitue un événement de Manoeuvrabilité.

L'ANALYSE

L'étude des événements de **Sensibilité aux Perturbations** et des événements de **Manoeuvrabilité** conduit à prendre des marges entre le point d'état et les limites de façon à pouvoir faire face aux perturbations maximales et aux manœuvres maximales raisonnablement probables.

Il est donc important dans l'analyse de retour d'expérience de bien identifier ces événements car, outre l'explication de l'apparition d'événements d'**Opérabilité** dans les manœuvres de corrections, ils peuvent mettre en évidence une insuffisance des marges entre point d'état et limites et conduire à modifier les consignes opérationnelles (par exemple, modification de la vitesse d'atterrissage d'un avion en cas de turbulences).

Ces événements sont résumés dans les grilles

GASP (Grille d'analyse des événements de sensibilité aux perturbations)

et

GAME (Grille d'analyse des événements de manoeuvrabilité)

Ces grilles sont présentées en fin de cet article, à titre d'exemple, dans le cas particulier de l'analyse des incidents et accidents d'avions de transport civils.

L'étude des événements d'**Opérabilité** conduit à des recommandations très différentes de celle des deux autres types d'événements.
Elle a pour objet la prévention des erreurs des opérateurs.

C'est le **domaine des facteurs humains**.

Notons que ce n'est pas **l'erreur** elle-même qui nous intéresse, mais les

circonstances qui ont favorisé son apparition.

Généralement une erreur est commise dans quatre circonstances dont la dernière se dédouble, dites facteurs d'erreur :

⇨ **l'opérateur est débordé par la charge de travail imposée par la tâche**.
Il n'exécute pas l'action appropriée au bon moment, ou bien il ne prend pas la bonne décision parce qu'il n'a pas le temps d'analyser les données dont il dispose, ou bien il ne prélève pas une donnée utile, ou bien il ne transmet pas une donnée importante.

⇨ **le système ne fournit aucun stimulus à l'opérateur parce que tout est stable**.
Dans ces conditions l'attention de l'opérateur est réduite et il rate une action, ne relève pas un changement d'état, oublie de prendre une décision ou de transmettre une information.

⇨ **l'opérateur commet un geste maladroit**,
prononce un mot à la place d'un autre, entend "de travers" un message, lit une valeur erronée sur un indicateur parce qu'il est mal éclairé, etc. Toutes ces erreurs sont regroupées sous le nom de lapsus (gestuel, verbal, auditif, etc.) ou de maladresses.

⇨ **l'opérateur se fait une fausse idée de la situation et il raisonne juste sur des hypothèses fausses**.
Divisé en deux grandes catégories, ce type d'erreur est connu sous le nom d'

ERREUR DE REPRÉSENTATION

⇨ les **erreurs dues à une mauvaise utilisation des données disponibles** (erreur de lecture d'un paramètre, l'interprétation de l'échelle étant délicate par exemple, erreur de transposition ou d'origine d'un message, erreur de localisation ou de sens d'action d'une commande, etc.).

⇨ **les erreurs dues au fait que l'opérateur s'est bâti une image a priori de la situation** et qu'il refuse (de façon totalement inconsciente) toute donnée qui pourrait rétablir une image exacte de la situation réelle. Ce sont les **erreurs diaboliques.**

Ces facteurs d'erreur sont résumés dans la grille dite

GAFE (Grille d'Analyse des Facteurs d'Erreurs).

Tous ces **facteurs d'erreur** ont des causes premières qu'il convient d'identifier pour les combattre.

Ce n'est pas seulement l'erreur finale qu'il convient d'éliminer.

Cette dernière est la conséquence quasi inévitable, sauf coup de chance, de circonstances préalables que seule une analyse fine des événements permet de reconnaître. Il arrive aussi que l'erreur une fois commise n'ait pas de conséquences graves (brûler inconsciemment un feu rouge est souvent sans conséquence ; si la maréchaussée est présente ou si le carrefour est occupé par un camion, les conséquences peuvent être désagréables ou catastrophiques !). Il n'en reste pas moins que cette erreur a été commise et qu'il est important d'analyser les circonstances qui l'ont générée.

En effet, répétons-le, les mêmes causes ayant les mêmes effets, tout porte à croire que ce type d'erreur se reproduira et que l'on n'aura pas toujours la chance qu'elle soit commise dans des conditions telles que les conséquences n'en soient pas sérieuses.

Ainsi nous ne saurions trop insister sur la **nécessité** du retour d'expérience et l'**analyse des incidents en service**,
chacun exposant franchement les erreurs commises, en détaillant soigneusement les circonstances préalables.

Il ne sert à rien de signaler une erreur d'affichage si l'on ne précise pas la succession des opérations, des manœuvres, des décisions, des échanges d'informations qui ont précédé l'erreur.

Il ne s'agit pas de s'indigner devant l'erreur commise et de sanctionner, mais de comprendre l'enchaînement des faits pour éviter que cet enchaînement ne se reproduise trop fréquemment.

Le Retour d'Expérience ce n'est

ni Accuser,

ni Excuser

mais EXPLIQUER.

Cette démarche est fondamentale. On ne peut prévoir tous les cas possibles et qui pourra prendre les mesures nécessaires pour limiter les erreurs si celles-ci sont soigneusement dissimulées ?

Les incidents décrits dans les fiches de RETOUR D'EXPERIENCE doivent être présentés sous forme de chaînes d'événements des 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 Manoeuvrabilité** 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 du Risque d'Erreur**.

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** (Grille des facteurs Amplificateurs du Risque d'Erreur) **dresse la liste des principales conditions générales dans lesquelles se sont déroulés les événements**.

(voir un exemple de GARE en fin du document)

Une fois reconnus les événements d'opérabilité caractérisés par la **GAFE**,

Il nous reste à identifier les causes premières des cinq **Facteurs d'Erreurs** que nous venons de citer et de quelques-uns uns des **Facteurs d'amplificateurs de gravité**.

Ces causes premières se répartissent en cinq groupes de défauts de conception du système.

Le RADOS (Répertoire d'Analyse des Défauts Opérationnels Système) **est destiné à identifier le Défaut du Système ayant contribué à l'apparition de chaque événement d'Opérabilité.**

⇨ les Défauts d'Organisation

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.
Ce type de défaut correspond à la question **"*Qui doit faire ?"***.

⇨ ***les définitions des objectifs, des contraintes, des marges disponibles comportent des erreurs ou des oublis***, ce que nous regroupons sous le terme de Tâches mal définies.
Dans certains cas, 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).
Il arrive aussi bien souvent que les opérateurs s'imposent eux-mêmes des contraintes inutiles, par exemple mettent en priorité la régularité avant la sécurité.
Ce type de défaut correspond à la question
"*Que doit-on faire ?"*.

⇨ ***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.
Cette situation a des origines multiples,

- procédures matériellement défectueuses (erreurs de frappe, photocopie imparfaite, etc.),
- procédures imparfaites parce que mal rédigées, complexes, non expliquées, rédigées en termes juridiques et non opérationnels,
- 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.
- procédures prévoyant des transmissions de données alors que les moyens de transmission ne sont pas disponibles (centre de contrôle fermé la nuit par exemple).

Ce type de défaut correspond à la question
"***Comment faire ?***".

⇨ ***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.
Ce type de défaut correspond à la question
"***Avec qui et quoi peut-on faire ?".***

⇨ les Défauts de Conception de la Machine.

Le matériel n'a pas été conçu en tenant compte des caractéristiques physiques, physiologiques et psychologiques des opérateurs, ou encore la conception repose sur des principes pouvant conduire, dans des cas rares mais possibles, à des situations dangereuses.

Ces défauts peuvent être divisés en trois groupes :
- ⇨ *mauvaise conception de base*.
- ⇨ *mauvaise conception de l'interface sur le plan ergonomie mécanique*.
- ⇨ *mauvaise conception de l'interface sur le plan ergonomie mentale*.

⇨ les Défauts de Conception de la Formation

Ces défauts peuvent être divisés en trois groupes :
- ⇨ *mauvaise conception de la formation de base*
- ⇨ *mauvaise conception de la formation spécifique au système*

Au cours de la recherche d'amélioration de la formation on s'attachera à examiner les méthodes de vérification des connaissances qui bien souvent se contentent de contrôler que les notions ont été apprises par coeur et non pas effectivement comprises.

⇨ les Défauts de conception ou de réalisation de la

Documentation,
Les Informations erronées, non transmises ou matériellement mal transmises aux utilisateurs,

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*

⇨ *Contenu erroné*

⇨ les **Défauts Réglementaires**.

Pour assurer la sécurité, la puissance publique impose, par la loi, un certain nombre de règles que les concepteurs et les utilisateurs se doivent de respecter sous peine de sanctions.

Il arrive qu'une règle, judicieuse à une époque devienne caduque ou même néfaste à une autre époque, compte tenu des évolutions de la technique ou des méthodes d'exploitation. Dans d'autres cas, deux règles, rédigées par des organismes différents et destinées à traiter des événements redoutés différents face à des types d'agression différents, peuvent se révéler contradictoires au moment de leur application.

Remarques:

⇨ Il n'y a pas de correspondance biunivoque entre un Facteur d'Erreur de la GAFE ou un Facteur d'Amplification de Risque d'Erreur et un Défaut Opérationnel Système, tout au plus des corrélations fortes. Ainsi les maladresses ont très souvent pour origine une mauvaise conception du poste sous l'aspect ergonomie mécanique. Les erreurs de représentation par mauvaise utilisation de l'information sont souvent dues à un défaut de conception du poste sous l'aspect ergonomie mentale, mais elles peuvent provenir d'un défaut d'organisation (mauvaise répartition des tâches), etc.

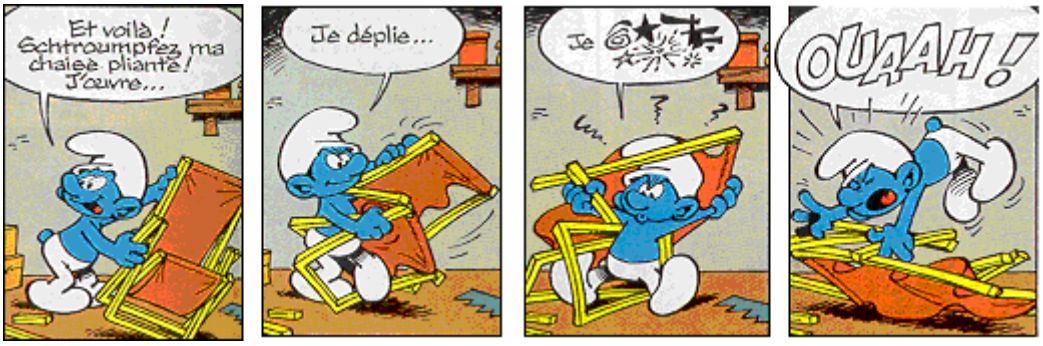
⇨ L'analyse des incidents et accidents est un travail de spécialiste. Il est hors de question de demander au rapporteur de faire lui-même cette analyse et de proposer des remèdes. C'est la confrontation des analyses de plusieurs incidents qui peut mettre en lumière un défaut système, permettre une évaluation des risques qu'il entraîne et guider l'analyste vers une proposition de remède. Il est donc nécessaire de mettre sur pied une organisation de retour d'expérience chargée de collecter les incidents et de les analyser, et de proposer des voies de recherche aux organismes compétents pour trouver des remèdes.

⇨ L'analyste doit faire deux hypothèses fondamentales avant de commencer une analyse, à savoir :

- l'opérateur est discipliné et n'a pas enfreint volontairement les règles de sécurité,

- les faits rapportés ont été fidèlement décrits.

Ce n'est qu'avec des arguments solidement étayés que l'analyste peut conclure, en fin d'étude, que l'opérateur a transgressé une règle de sécurité volontairement et non par suite d'erreurs ou que les faits rapportés sont faux.



d'après PEYO

Voilà un bon exemple d'accident !
Maladresse ?
Mauvaise conception du système ?
Procédure mal adaptée ?

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 (Rapid Analysis Failures Table)(radeau).

"To make a Smurf gasp" signifie "couper le souffle à un Schtroumpf".

Grilles

d'Analyse

GRILLE DES FACTEURS AMPLIFICATEURS DE RISQUE D'ERREUR

GARE

⇨ **Facteurs physiques. (**sigle **Φk** ou **Phik)**

⇨ **Facteurs externes. (**sigle **Φke** ou **Phike)**

⇨ 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
- Éclairage 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, ..)

⇨ État du système à l'instant de l'incident :
- Fonctions non assurées par la machine
- Pannes de :

- Capteurs, chaînes de transmission de données, afficheurs
- Commandes, chaînes de commande, actionneurs
- Chaînes de transmission, émetteurs, récepteurs
- Systèmes, sous systèmes, automatismes

⇨ **Facteurs internes.** **(**sigle **Φki** ou **Phiki)**
- ⇨ Utilisation de médicaments
- ⇨ Absorption d'alcool
- ⇨ Usage de drogues

⇨ **Facteurs physiologiques.** **(**sigle **Φo** ou **Phio)**
- ⇨ Fatigue
- ⇨ Besoins
  - Faim
  - Soif
  - Besoins naturels
- ⇨ États pathologiques
  - Nausées
  - États "grippaux"
  - Douleurs (tête, dents, oreilles, yeux, dos, etc.)
  - Douleurs gastriques, abdominales, musculaires, articulaires, etc.
  - Démangeaisons
  - Incapacitation (évanouissement, décès), etc.

⇨ **Facteurs psychologiques.** **(**sigle **Ψ** ou **Psi)**
- ⇨ 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.)
- ⇨ État psychopathologique (perte de mémoire, "folie", etc.)

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

⇨ Facteurs internes. (sigle Σ**i** ou **Si**)

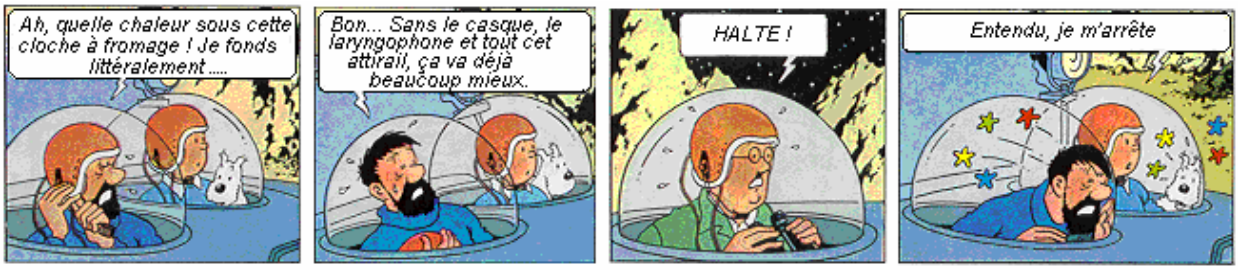
- ⇨ Composition de l'équipe ou de l'équipage
- ⇨ qualification des membres (ancienneté, connaissances)*
- ⇨ sous effectif occasionnel
- ⇨ présence de stagiaires
- ⇨ conflits internes à l'équipe

⇨ Facteurs externes. (sigle Σ**e** ou **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.



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.

*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.
- Équipage constitué de deux commandants de bord de même ancienneté

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

GRILLE D'ANALYSE DES ÉVÉNEMENTS DE MANOEUVRABILITÉ

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

GRILLE D'ANALYSE DES FACTEURS d'ERREURS

GAFE

	OPERATIONS d'exécution de la tâche au cours de laquelle survient l'ERREUR HUMAINE				
FACTEUR D'ERREURS ⇩	**Saisie et traitement de l'information s**		**Décision après traitement de l'information d**	**Transmission de l'information t**		**Action après Décision a**
	information venant de la Machine	information venant d'un Homme		Homme ß Machine	Homme ß Homme	
CHARGE DE TRAVAIL C Charge trop forte (Saturation)	**Cs** Information non captée ou erreur de saisie.		**Cd** Traitement partiel, nul ou erroné entraînant une décision inadéquate ; décision trop rapide (diagnostic réflexe) ou trop lente.	**Ct** Absence de transmission ou transmission partielle ou fausse par saturation.		**Ca** Oubli ou erreur de commande.
ABSENCE de STIMULI A (Perte de Vigilance)	**As** Information non captée ou erreur de saisie.		**Ad** Traitement partiel, nul ou erroné entraînant une décision inadéquate ; décision trop rapide (diagnostic réflexe) ou trop lente.	**At** Absence de transmission ou transmission partielle ou fausse par perte de vigilance.		**Aa** Oubli ou erreur de commande.
MODELES ET REPRESENTATIONS M Modèles erronés Mauvaise utilisation de l'information	**Ms** Erreur de modèle d'information. *Localisation* *Identification* *Transposition*		**Md** Erreur de modèle de fonctionnement. Erreur de modèle de gravité de la situation. *Faux* *Simpliste* *Trop complexe*	**Mt** Erreur de modèle du système de transmission. *Localisation* *Identification* *Sens d'action* *Identification des destinataires*		**Ma** Erreur de modèle de commande. *Localisation* *Identification* *Sens d'action* *Information sur l'état de l'organe commandé*
MODELES ET REPRESENTATIONS P Modèles a Priori (Erreurs diaboliques)	**Ps** Seules sont saisies les informations confirmant le modèle a priori.		**Pd** Refus/oubli de changement de l'image d'état. Refus/oubli de reconnaissance de la gravité.	**Pt** Refus de changement de l'image d'état du système de transmission.		**Pa** Action procédant d'un modèle a priori.
LAPSUS **L** Lapsus gestuels, verbaux, visuels	**Ls** Mauvaise saisie de l'information par lapsus.		**Ld** Confusion dans le traitement de l'information.	**Lt** Transmission défectueuse par lapsus gestuel ou verbal.		**La** Lapsus gestuel, erreur de dosage.
DIVERS X Divers	**Xs**		**Xd**	**Xt**		**Xa**

Origine DCN/STCAN/BCN + TECHNICATOME + N. & J-C. WANNER 1991 Modification 1998

REPERTOIRE D'ANALYSE DES DEFAUTS OPERATIONNELS DU SYSTEME

RADOS

	OPERATION d'exécution de la tâche au cours de laquelle est survenue l'erreur humaine induite par le défaut.			
TYPE DE DEFAUT SYSTEME ⇩	**Saisie et traitement de l'information s**	**Décision après traitement de l'information d**	**Transmission de l'information t**	**Action après Décision a**
ORGANISATION O Qui doit faire ? (responsabilité) **r**	**Ors** Défaut d'information dû à de mauvaises organisations ou répartition des tâches.	**Ord** Décision non prise au bon niveau de l'organisation.	**Ort** Erreur d'interlocuteur.	**Ora** Non respect des règles de partage des tâches. Qualification inappropriée de l'intervenant.
ORGANISATION O Que doit-on faire ? (exécution) **e**	**Oes** Rôle des alarmes mal défini. Alarmes trop proches des limites.	**Oed** Objectifs des tâches mal définis	**Oet** Transmissions mal définies	**Oea** Les marges limitant les actions possibles sont insuffisantes
ORGANISATION O Quels moyens pour faire ? (moyens) **m**	**Oms** Ressources matérielles (moyens de mesure par ex.) non adaptées.	**Omd** Moyens matériels (abaques, schémas, etc.) non adaptés à la prise de décision.	**Omt** Moyens de transmission non adaptés ou inexistants	**Oma** Ressources matérielles et humaines non adaptées.
ORGANISATION O Comment doit-on faire ? (procédures) **p**	**Ops** Saisie non prévue de l'information	**Opd** Méthode de décision non définie ou inadéquate	**Opt** Procédure de transmission absente ou inadéquate	**Opa** Procédure d'action absente ou inadéquate. Procédures "folkloriques"
CONCEPTION de BASE H Conception reposant sur des hypothèses douteuses ou des principes inadaptés **b**	**Hbs** **Hbd** **Hbt** **Hba** Les options de conception n'ont pas pris en compte certaines conditions spécifiques, ce qui peut conduire à des situations dangereuses.			
CONCEPTION des INTERFACES H Mauvaise ergonomie mécanique des interfaces **m**	**Hms** Information fausse, absente, peu lisibles. Procédure matériellement erronée.	**Hmd** Décision inappropriée induite par l'interface.	**Hmt** Système de transmission défectueux; perturbations dues à l'environnement.	**Hma** Défaut d'exécution du système. Commandes inadaptées aux possibilités physiques de l'opérateur
CONCEPTION des INTERFACES H Mauvaise conception des interfaces (ergonomie mentale) **c**	**Hcs** Information difficile à interpréter.	**Hcd** Décision imappropriée induite par une information difficile à synthétiser.	**Hct** Erreur de transmission par difficulté d'identification du canal de transmission ou du destinataire.	**Hca** Confusion entre les commandes due à une mauvaise distribution spatiale. Erreur sur le sens d'action d'une commande.

FORMATION **F** Formation de base insuffisante **b**	**Fbs**	**Fbd**	**Fbt**	**Fba**
	Ignorance des principes de base de fonctionnement mécanique, électricité, électronique, informatique, hydraulique, aérodynamique, résistance des structures, etc. règles de transmission radio, organisation générale de l'entreprise, règles générales de sécurité, discipline, etc.			
FORMATION **F** Formation spécifique insuffisante **s**	**Fss** Modèles de Localisation, Identification, Transposition de l'information mal assimilés	**Fsd** Modèles de fonctionnement faux, simplistes	**Fst** Modèles de Loc. Ident., Sens d'action des commandes de transmission, identification destinataires, mal assimilés	**Fsa** Modèles de Localisation Identification, Sens d'action des commandes mal assimilés
DOCUMENTATION **D** défauts matériels **m**	**Dms**	**Dmd**	**Dmt**	**Dma**
	Documentation absente, détériorée, mal reproduite.			
DOCUMENTATION **D** contenu défectueux Documentation "sauvage" **c**	**Dcs** Informations fausses sur les modèles de Localisation, Identification, Transposition de l'information.	**Dcd** Informations fausses sur les modèles de Fonctionnement	**Dct** Informations fausses sur les modèles de Localisation, Identification, Sens d'action des commandes de transmission, Identification destinataires	**Dca** Informations fausses sur les modèles de Localisation Identification, Sens d'action des commandes, Information sur l'état de l'organe commandé
REGLEMENTATION **R**	**Rs** Signalisation superflue	**Rd** Règles administratives entravant les décisions	**Rt** Règles administratives imposant des lourdeurs	**Ra** Règles bloquant abusivement des commandes
DIVERS **Z**	**Zs**	**Zd**	**Zt**	**Za**

D'après PEYO

Exemple de mauvaise conception de la documentation.

d'après GOSCINNY et UDERZO

Une mauvaise interprétation peut être la source d'une erreur de représentation mais conduit toujours à une représentation critiquée.

FIN