Human factor and flight safety

by

J.C. WANNER
Ingénieur Général de l'Armement

SUMMARY

The aeronautical safety criteria, built for Concorde during the last decade, can be used for the different systems controlled by human operators as cars, chemical factories, machine tools, ships .. These safety rules are based on the analysis of the different types of incidents which lead to an accident and can be distributed into three classes, Pilotability, Manoeuvrability and Sensitivity to disturbances. The accent is mainly put on the Pilotability which involves the "human factor" and on the special aircraft characteristics which can modify the rules based on this type of criteria.

The design philosophy of systems governing important industrial processes is undergoing a complete revolution.

Recent accidents or serious incidents, such as the great power failure in France by the end of 1978, the stranding of the Amoco-Cadix, the accident of the American nuclear power plant in Harrisburg, the colliding of two Jumbo-Jets in Tenerife, have revealed the leading part played by what is usually called human factor, human error and often improperly human fault (let us recall that the concept of fault refers to a voluntary transgression of the rules whereas error is only an unvolontary transgression implying thus no culpability).

The design of information display and control mecanisms in large systems, although concerning different systems such as oil tankers, nuclear power plants, distillation plants, continuous casting units, etc, must take into account the adaptability of the human operator that seems at first very great but is actually very limited.

The first type of system which has been thoroughly studied is the aircraft control system. Historically, the aircraft was indeed the first system an error of control "in real time" could lead to a disaster.

The problem appeared as a whole in the early 60's, mainly during the design phase of Concorde.

The increasing flight envelope (Concorde flying twice as high and nearly three times faster than a conventional transport aircraft), the coming out of new systems which good working condition is indispensable for safety (the only critical system on conventional transport airplane being the propulsion system) have led safety managers to modify the airworthiness requirements.

The conventional empirical rules elaborated for Douglas DC 3 and cautiously extrapolated to be applicable to Caravelle, Boeing 707 and 747 proved themselves unadapted, uninteresting, and even dangerous for Concorde.

The elaboration of Concorde airworthiness rules thus needed an extensive study of the conditions leading to accident, the philosophy of this study is now known in the field of aeronautics as ISAAC (Investigation on Safety of Aircraft and Crews)or ESAU (Etude de la Sécurité des Aéronefs en Utilisation).
Once this study has been completed and Concorde certification rules elaborated, it became obvious that its philosophy could be applied (but for some slight differences) to all systems controlled by human operators.

We wish to present this philosophy here illustrated with well known examples, leaving to the specialists of each category of system to adapt it to its own particular case.

WHAT IS MEANT BY ACCIDENT ?

A system is in general a set of sub-systems and elements, each one's functioning being characterized by one or several parameters : lubrication oil temperature and pressure, alternator r.p.m., land vehicle wheels deflexion, speed of the vehicle itself, distance from the car to road side, wing angle of attack, etc...

The variation range of each functioning parameter is generally limited. The limits of the authorized domain are very often blurred. Rigorously it is admitted that the accident probability is negligeable at the center of the authorized domain and that it varies quickly in the vicinity of the boundaries to reach about one outside the limits.

Driving a few centimeters beyond the white strip marking the right road side has no dramatic effect, though not recommanded. The accident probability does not vary much around the limit. But on the contrary, if the road side runs along a gully, trespassing the limit becomes rapidly catastrophic !

It remains nevertheless useful to consider the limit of the authorized domain for each operation parameter, keeping in mind the probabilistic aspect of the concept.

It is then possible to represent the system operation by a "functioning point" in a n D. space, each dimension related to one of the operation parameters.

We shall then say that an accident occurs when the vehicle functioning point crosses one of the authorized domain boundaries, as a result of a succession of incidents.

In general, the crossing of a limit is due to a succession of incidents, none of which plays a prominent part. It is therefore useless to look for the "cause" of the accident ; each incident has had a role and if only one had not occured, whichever, the accident would have been avoided.

In the case of near miss, it can be very often observed that the coincidence of only one other incident would have led to a catastrophe, but this incident would still not be the "cause".

THE THREE TYPES OF INCIDENTS

The different incidents whose succession leads to an accident can be divided in three and only three groups :

- Pilotability incidents
- Sensitivity to perturbation incidents
- Manoeuvrability incidents

In the first type of incidents, the operator has at his disposal the controls necessary to maintain the functioning point within the authorized domain, but if the task appears too difficult (required actions too quick or too numerous, unsufficient information concerning the relative position of the limits and the point), the operator lets then the point go close to a limit or even cross it.

The second type of incident, called "due to sensitivity to perturbations" can be described in the following manner. Under the action of external perturbations (gusts, road roughness, swell of sea, overvoltage in power network) or internal perturbations (breakdown, including fire), the functioning point grows close to or crosses a limit, either because it has itself moved (increase of the wing angle of attack induced by a gust, increase of stresses in a structure induced by road roughness or sea swells, loss of altitude or increase of the sideslip angle of a plane induced by an engine breakdown), or because the limit itself nas been altered (decrease of stall attack angle due to flaps breakage, dropping toughness of a structural element due to fire, decrease of skid limits due to a flat tyre, etc...).

It should be emphasized that internal incidents due to sensitivity to perturbations involve only the system transient response to a breakdown. Once the breakdown has occured, it is a new system that must be considered, with its own characteristics and performances and which must be studied just as it is, with respect to incidents of the three types.

Finally, in order to achieve a given programme (modification of the trajectory of a plane, a boat or a road vehicle ; increase of the power output of a power plant to meet the demand), or in order to bring the functioning point back to its nominal value after a divergence due to an incident of the two first types, the operator must start a "manoeuvre" which in general brings the functioning point to move, sometimes even close to the limits; this displacement is called a manoeuvrability incident.

As a result it appears that the functioning point moves close to the limits after a succession of incidents of the three types, so that a final event, still belonging to one of the three types, causes the functioning point to cross a limit.

For instance, during an approach without visibility in turbulent atmosphere, and as a result of a control augmentation system failure, the pilot of an airplane lets a 15 kts airspeed drop occur and flies 50 ft below the normal approach flight path (pilotability). Noticing the altitude discrepancy, he starts a pitching correction (manoeuvrability). Finally a gust coincides with the two previous increases of angle of attack due to airspeed drop and pilot's manoeuvre and results in a stall (sensitivity to perturbations).

SAFETY RULES

After this analysis of the factors inducing an accident, we can establish safety rules allowing a decrease of the incidents occurrence probability of the three types.

We shall hereafter state some general ideas concerning the different rules applicable to each type of incidents. It is nevertheless obvious that they should be carefully studied according to the type of the controlled process. Furthermore it is very difficult to assess a priori the validity of a rule and only experience can give an answer. But results analysis is uneasy because accidents are uncommon and statistic evaluation of small probability variations (the probabilities being small themselves) requires a lot of care.

We shall later go thoroughly into the main rules of pilotability briefly stated below :

- Provide information about the functioning point and its relative location with respect to the limits.
- Do not provide over information, i.e. useless information either redundant or irrelevant.
- Provide all useful information ; though obvious, this rule is often forgotten ; when approaching a road bend the driver generally doesn't know the maximum allowed speed which depends on the turn radius, the banking of the road and the grip of the wheels on the road (depending itself on the surface condition : gravel, rain, ice, etc ...).
- Provide information easy to apprehend (mental processing of information keeps the operator's brain busy so that he might unvoluntarily drop some other information or lack time to carry out some necessary control actions).
- Do not ask for too many control actions, and make them clear, easy to conceive and to achieve.
- Give the operator a feed back functioning option, i.e. let him correct his own actions according to the development of the parameters to be modified. In aeronautical air worthiness requirements, an "open loop operation" corresponds to "actions requiring outstanding pilot skill".

Finally, the role of pilotability rules is essentially to reduce the operator's task ; his work load can be defined as the sum of information he must assimilate, process and reinject into the system. We shall later see that other rules should be added when the task is too light.

The "sensitivity to perturbations" and "manoeuvrability" rules are a lot simpler to establish since they do not involve the human operator and require only a careful study of the system, its operation environment and its mission. An exhaustive study of the problem might not be available with the present state of computers. But its governing laws are well known in physics whereas pilotability rules involve the operator's psychosociologic behaviour and therefore does not depend on a "precise science" as far as now.

WHAT IS HUMAN BEHAVIOUR ?

The human operator can be characterized by three main properties.

1) He works sequentially ; in other words the different operations are taken one after the other : instrument reading, data processing, strategies and tactics elaboration, control actuation, etc... They are not handled concurrently as it is often believed. To counter this statement, it is usually said that human being are able to take notes while liste-

ning to a speech. Actually, speeches are very redundant ; many words and within words, syllables, are useless to strict comprehension ; the brain then shares its time and takes some time off the listening in order to process and transcribe the message. It should also be noticed that once the transcribing order is sent by the brain, the resultant action is partly "reflex" which leaves time for the brain to make other information reading operations. This example suggests two remarks :

a) "Data reading" either visual, oral or using any other human captors (contact, pressure, effort, acceleration, sensed by hands, internal ear, limbs, the whole body, etc...) is voluntary, except if the information is sent as an intense alarm. The data reaches the brain only if the brain lets it in. Besides, it is often verified that alarms, flashes, noise, vibrations, accelerations, chocks, have no signification themselves, but cause the brain to leave its routine tasks and summon all captors to scan all available datas for incident identification. It should therefore be noticed that making information available on an instrument "under the very nose of the operator" is not sufficient to insure its "reading" by the operator (of course the eye is the captor ; the nose plays a secondary part in the process control except as an alarm device in case of abnormal smells).

b) Certain operations are "reflex", i.e. leave the operator's brain vacant for other reading operations, interpretations, elaborations, control actions. The best example of reflex operation is the balance the body keeps when standing or sitting. It results of a training acquired more or less early in existence. Let us mention other facts such as the driver keeping his car at a reasonable distance from the right road side or the pilot's ability to maintain his airplane wings level in VFR flight.
Reflexes do not count in the workload. Nevertheless their identification is preponderant, for fear that changes in control processes may inhibit them.

Indeed the brain is at rest or available for other tasks during these "reflex" periods. The case of automobile, driving is a striking one for it is mostly reflex. Everyone has observed how difficult it is to remember whether or not he has driven by a characteristic point of a given circuit. Driving six or seven hours in a row is made possible thanks to this type of driving (whereas beginners cannot usually drive more than fifty miles without being exhausted).
Thanks to this type of driving also, radio can be listened to. But reflex driving yields to alert control as soon as an incident has been detected. Everyone has sometimes missed an interesting and waited for piece of radio news when shifting to watchful control, requiring total brain alertness for driving and letting aside auditive perception ?

2) The second characteristic of the human operator is his continual search for information and his forecasting ability.

Lack of information is generally distressing for the brain, which tries to collect as much as possible by means of all its available sensors.

This is why solitary confinement is so hard to stand for prisoners. In less dramatic situation, everyone has experienced an uneasy feeling when in an anechoic room for more than a few minutes.
The imperious need for information can also be observed by anyone travelling in the underground where he cannot help reading all surrounding information : headlines of the paper the person next to him is reading ; warnings known by heart already, advertising (advertising managers know well how receptive the underground passenger is). Who can resist the appealing TV images ? (even when there is no sound and the image has no signification !). It is an effort to take your eyes off it !
It is also striking to see that drivers are unable to keep their eyes more than five seconds on a red traffic light blocking their way ; indeed the red light does not give any information at that time ! Therefore the driver is inclined to look for any other surrounding information, useless but attractive. Then, when the light turns to yellow, the driver comes back to the traffic light because he is able to forecast that it will turn green in less than ten seconds. The waiting is then bearable but if ever it takes more than the expected time, the eye slips aside for other information.

This example among many makes clear the notion of forecasting. This extrapolation ability has two consequences :

a) A positive one : the operator can partly devote his attention to watch other parameters when he assumes the one he has just checked is evolving favorably. The never consciently formulated assumption is the following : I took a correcting action to reduce a divergence and I observed it started to decrease, so that I have some time to check, and if required, correct the other parameters. I can also use this "leisure" for some auxiliary task, for instance radio operation on a plane.

b) A second, negative one : boldly extrapolating a stationary situation and deducing wrongly that nothing will ever change in the following hours.

And if no information is given in this situation (stationary situation : constant parameters, no information given by instruments or environment) the operator thinks no incident can possibly occur. Lacking of information, he creates some by thinking about something else : he projects a film in his imagination which cuts him totally from the checking process. This is usually called vigilance loss.

3) The third characteristic is the ability the human operator has to compensate for a more difficult task by increasing his work load.

It is very important to understand that an increase of work difficulty does not imply a decrease of the operator's performance.
In other words the accuracy in the achievement of a task is independent of its difficulty. The operator checks more frequently and increases his work load concurrently with the difficulty.

Of course, there is a limit to this work load. The maximum value depends on what we shall call his physical and mental fitness. Beyond this limit the operator cannot make up for the difficulty increase. A brutal performance degradation takes place and at least one of the parameters is not maintained to its nominal value.

This is easily verified on simulator : for instance the operator is asked to track a target on a cathod ray tube. The target moves more or less at random and rapidly. The transfer function linking controls and "screen aimer" is more or less complicated. The performance can be taken as the sum of the squares of the target-aimer distances, measured at fixed times. After a learning and training period it appears that the task can be made more difficult (target more "turbulent") without having the performance to vary substantially. But beyond a certain level of turbulence, depending upon the operator and his tiredness, the performance drops drastically, the operator experiences a "breakdown".

These remarks have two consequences :

a) Any increase of task difficulty results in a work load increase and therefore renders the breakdown threshhold more liable to be crossed.

This establishes the rule according to which the everyday operator's task should be reduced as much as possible, allowing growing difficulty for only small and probabilistically unfrequent laps of time. This way the product : "probability of having to cope with a level N work load situation" by "probability, in this condition, to overwork the operator" can be reduced reasonably.

Reducing work load does not mean letting the operator lack information which would lead to vigilance loss as we mentioned before.

b) The second consequence is that simple operator's performance measurement is not sufficient to give a fair estimate of the difficulty of a task and correlatively of the corresponding necessary work load.

This is dramatic because it is frequently assumed that if an operator, chosen among the best, rested, perfectly informed, is able to control the system during a test, this system is good for everyone in any condition.

Now, it is practically possible for any well trained operator to accomplish any kind of task. But knowing that a particular operator can cope with a given test operation does not help assessing the necessary work load.

So, devices requiring long operating training can be found on the market but designers did not think of simple means reducing the work load. If ever the operator makes a mistake everyone is furious against him and does not understand the origine of the mistake : it's the operator's "fault" who did not abide by the rules (implying voluntarily).

This phenomenon is fought by the operators themselves. They regard the simplification of their task as tending to discard their precious qualification. This is not always conscious but is still very often encountered.

In order to summarize the human operator's characteristics, we shall say that :

a) He acts sequentially : the work load increases with the number of necessary operations.
b) He cannot stand a lack of information, which refers to the vigilance problem.
c) He compensates a growing task difficulty by increasing his work load, without variations in performances.

HUMAN SENSORS

A complete description of human sensors would be necessary to give a thorough presentation of the human operator. This would exceed the scope of this expose.

Let us just list the different human sensors :
the eye (central vision), the eye (peripheral vision), external ear (sensitivity to sounds), internal ear (triaxial rotary acceleration sensor and reference of apparent vertical axis) ; the skin (touch and contact pressure captor, gives the resultant of external efforts applied to the body which tells again about the apparent vertical), and then efforts sensors not clearly identified (handgrip, efforts in arms and forearms, etc...).

PROCESS MODEL

During his learning and particularly his training the operator progressively modelises the system behaviour. In general this model is only a rough approximation of the complete mathematical model. It simplifies the relations (often differential relations) between controls and the operating point and reduces them to relations between each control and one functioning parameter (and its first or second order differentials) neglecting interactions.

By means of this more simple model and after having manipulated the governing parameters and analysed the outcoming situation the operator is able to forecast the evolution of the system, to determine the controls relevant to this evolution and the necessary amplitude of the actions.

It is of good habit, when designing a new system, to find out which models might be thought of by operators. Different operators are liable to imagine different models (the more so when several complex controls affect several operating parameters).

For one thing, this study brings out the best model : the most simple and efficient one, so that it can be recommended to operators during instruction.
Secondly, the model can be simplified and with it, the work load, by changing the acting means of certain controls or by combining operation parameters directly relative to one control.
Examples : controls acting by double integration should be banished : experience proves that human operators can easily "pilot" a parameter when the control acts directly on the parameter's value (position control) or on its variation rate (rate control) ! On the contrary, control on acceleration is very hard to handle because it necessitates a phase lead in order to nullify the variation rate when the parameter reaches the desired value (all direct effort controls are double integration ones though very simple to think of, except when damping is present).

A LOOK BACK TO PILOTABILITY RULES

This quick look at the human operator 's behaviour allows us to start a list of pilotability rules aimed at reducing the probability of this type of incidents.

1) Provide really useful information, i.e. directly related to the actual position of the functioning point with respect to the limits.

   This might look obvious, but the rule is often transgressed. The accident of the Harrisburg power plant is a striking example. The control panel included a signal lamp indicating that the order that the cooling fluid valves were turned off had been sent by the pressure check system, instead of indicating the outlet valve position on or off. After the secondary circuit failed, the primary circuit was not cooled anymore, temperature and pressure increased. The safety system stopped the reactor, as planned (safety bars descent), opened the outlet valve to absorbe the overpressure and ordered normally its shut off after 12 seconds. The fact that the order had been sent was indicated on the panel but actually the valve remained open which depressurized the primary circuit with water overflow causing extensive damage to the center of the reactor.

   The operator thought the valve was off, according to the signal, and his following reflexion was based on this hypothesis of the valve being turned off, which seemed obvious to him.

   The experience gained from the Harrisburg accident would make a whole report by itself, which is not our present occupation. Let us just recall that an information must have a non ambiguous signification and that it is almost impossible to persuade an operator that his hypothesis is wrong if he got the information wrong in the first place.

2) Do not provide information requiring difficult interpretation. In other words do not let the operator make intricate mental operations when he wants to know the margin with respects to the limits.

Following is an example often encountered : the situation when an operation parameter is displayed digitally whereas its limit is given in an analogical form. Everyone got once into a panic when waiting for a train : the schedule indicating 18.52 and the clock showing ten to seven (analogic) : transposition from one system to the other induces a useless work load and interpretation errors are probable.
Besides, digital display is harmfull for parameter control. Indeed it is extremely difficult to deduce from it the "discrepancy" with respect to the nominal value, its direction as well as rate and direction of its variation (whereas all this is obvious on an analogic presentation).

3) Provide all useful information and carefully discard all useless information .

This again is obvious but often forgotten. Increasing work load by useless parameters reading is bad ; but it is so tempting to add such or such easily measurable parameter to the control panel because it "might" be helpful. It may seem informative to check the parameter's consistency : this usually turns out to be irrealistic for the mental work load is considerably increased by the checking operation and the operator gives it up generally. The Harrisburg operator had 19 other parameters at his disposal allowing him to conclude the valve was not off. He misunderstood some to justify his hypothesis of "turned off" valve and forgot to watch the others (because this check seemed totally incongruous to him since he had confirmation from so many different sources already).

It is useless to present redundant parameters, but on the other hand it is very helpful to use an automatic information consistency checking system, providing the operator with a unique easily interpretable parameter.

4) Provide information allowing anticipation.

This type of information is related to the current state of the system, and the direction and amplitude of its variations. Knowing the preceeding states, the operator can forecast the system evolution by means of his internal system modelisation.

Obviously, anticipation operations add somewhat to the work load : information reading, interpretation of current situation and extrapolation in time. Some people tried to reduce this work load by informing the operator about the control position that would correct the discrepancies with respect to the nominal situation, leaving him uninformed about the situation itself. Undoubtly all work load added by interpretation and control choice is banned but the anticipating possibility disappears concurrently. The operator is then permanently bound to capt orders giving the needed control position for he is no longer able to forecast their evolution. The intelligent interpretation work load is then replaced by a stupid information captation work load, the operator operates as a pure servomechanism.

We want here to make the difference between piloting operations and conducting operations in process "control" operations.

Piloting will be all short term actions aimed at maintaining or changing an operation parameter, for instance : to keep the wing level, in spite of turbulences ; to keep the car at a given distance from the roadside, etc...

Conducting operations are concerned with long term actions allowing the process management. They are founded on evolution forecast and depend on the comparison between forecast and observation.

Piloting operations can easily be made automatic for they depend on very simple decision algorithms. In process control it is always valuable to relieve the operator from piloting operations by making them automatic, leaving to him the noble task of conducting, which requires more careful decision algorithms. Indeed it is usually not easy to consider all the possible situations and therefore to anticipate all necessary answers. For instance it is simple to guide automatically a missile to a military target, but deciding to stop the tracking because the vehicle shows a red cross and then deciding to résume it because the passengers are not casualties but soldiers cannot, by all means, be left to an automatic system ! The operator must not be busy with minor piloting tasks ; on the contrary, he must be free for analysing the situation and choosing strategies.

5) Providing information

We already stressed the idea that the human operator cannot bear a lack of information.

With automatic processes the operator's task is often limited to ascertain that the system remains in his nominal state. All indicated parameters are fixed ; nothing happens. The operator is in charge of a possible action in case of a breakdown. But it is illusory to count on a possible intervention of the operator if the failure scarcely occurs, because of two characteristics of the human operator.

Information shortage makes him "think about something else", i.e. vigilance loss. Besides, the established fact that the system is in a stable state makes him abusively forecast the continuation of this state : he does not believe anymore that a failure is possible. The occurence of the failure might well not be perceived because the operator thinks about something else and does not believe in it !

Providing information about a stable process requires imagination.

Example : during automatic approach landings, all classical indicated flight parameters : velocity, attitude, difference compared with the nominal flight path, etc... are at a standstill and give no information. A colored cathodic screen displaying horizon, runway (perspective computed from the position and attitude of the plane) and ground speed vector would on the contrary provide an attractive information shaped as a moving image (the runway grows bigger with the approach).
If there is no consistency between independent informations about the plane's situation, the runway image distorts itself and immediately informs the pilot who can then decide to go around (the aircraft location is measured by two separate systems, which complement each other and build the runway diagram). If the ground speed vector moves out of the runway threshold, the pilot knows immediately that the automatic landing system is not working properly and can switch to manual control ; he disposes already of the situation analysis (whereas a conventional display requires a preliminary analysis when an alarm goes off, in order to decide to switch to manual and this is time lost).

6) Provide alarms easy to identify

Two types of alarms should be distinguished. Those indicating an abnormal functioning or a system failure and those indicating that one of the operation parameters is approaching a limit.

Those of the first kind are useful since they allow the operator to take a decision or action on his own. The second are meant to reduce the pilotability incidents probability, since they give an increased information about the nearness of a limit.

Experience proves that the heaviest the work load is, the more intense the alarm must be in order to be perceived and interpreted as an alarm. This brings up the classical story, (but characteristic) of a pilot who tells the control tower that an intense buzzing makes radio receiving impossible, at the same time the air traffic controller tries without success to warn him that his landing gear is not down (which had itself set the buzzing alarm on !).

The philosophy of alarm systems design is delicate. The following rules may still be helful :

a) Limit carefully the number of alarms to the minimum necessary. An alarm must easily be identified and interpreted (the alarm panel should not look like a decorated christmas tree).

b) Smartly choose the go off limit of an alarm, indicating the nearness of a limit. An alarm which goes off too soon as the limit is nearly reached is liable to operate too often, loosing its dramatic warning effect. An alarm set to go off too late is also unefficient because the operator has not enough time to react. Each time technology allows, it is interesting to replace an alarm system by an automatic system forbidding the crossing of a limit (this is useful to reduce piloting incidents but inoperant for manoeuvrability incidents).

c) Rather than being displayed as an additional information, an alarm going off can be signified by suppressing a vital piece of information (keeping in mind that the operator must be able to have access again to this vital information as soon as he wants to).
For instance, the warning lamp or buzzer meaning that the landing gear has been forgotten, might not be perceived, coming among a mass of other information. Instead it could be a good idea to hide the airspeed indication, which a pilot cannot miss during an approach phase.

7) Limit the number of actions and facilitate tactics and strategies elaboration.

In order to limit the number of actions, it is possible, as we saw before, to automatize all simple tactical actions where the operator would only act as a servomechanism and leave to him conducting operations which in general do not necessitate many control actuation.

Tactics and strategies elaboration requires a good understanding of the system's state and its evolution. For fairly complex systems, only analogic presentation can be processed rapidly. Digital presentation applies more to accurate analysis, with no time pressure.

Computers have introduced a new form of information in process controls ' that is to say ' tables giving the different states of the system in the past time. This allows a very precise follow up of the system's evolution a posteriori. In no way do they allow an instantaneous analysis of its present evolution or give a global and quick idea of its past evolution.

Conventional peripherals like printers must be installed out of the control zone. They can only be used as informers and must be replaced by cathodic screens giving the evolution with time of the operation parameters to be checked and their corresponding limits (charts, not digital form). The operator must have a control key board at his disposal, enabling him to vary the presentation (scales, grouped parameters, functions of parameters, recall of datas issued in the previous hours, etc...).

This type of information presentation should solve the problem of vigilance loss by lack of information.

8) Study carefully the direction of the action and the mode of control's operation.

This is common sense. It should nevertheless not be forgotten that improving a control, i.e. making the relation between control and controlled parameter more simple, necessitates sometimes expensive technological modifications, whose benefit might not always seem obvious (too expensive, the operator can always train and be careful !). Cranes controls for instance look very much like a forest of identical levers, any one of which has a different action (not very clearly indicated) on the load motion !

Let us finally recall that the choice of a control cannot be made only on the drawing table. Experiments of different solutions on simulators or prototypes are absolutely necessary. The answer can only be found after real experimentation with a well informed operator (be careful with operators who want to show off and prove they are the only ones to master the control system !).

Controls design belongs to a branch or ergonomy called mechanical ergonomy and dealing with shapes, size and position of controls compatible with the dimensions and movement possibilities of the limbs. This fiels is very useful but is only part of ergonomy, as is often forgotten. Mental ergonomy which we already talked about is as important.

SIMULATORS

We noticed that only "real size" experimentation is helpful for studying presentation and control systems. This calls forth the problem of the design of simulators and experimental systems, allowing an assessment of the work load.

For a simulation to be perfect, the operator's task must be identical to the real task, he must dispose of the very same actuation means and the same information about the condition and the evolution of the system.

It appears very quickly that the best simulator is the real system itself. Nevertheless simulation is necessary in order to reduce costs (even a very sophisticated calculator costs less than an Airbus, a nuclear power plant or a tanker), to limit experiments risks (a crash or beach stranding are more comfortable with the simulator), to increase the number of experiments (the computer can bring the plane back to the approach situation in less than a minute and a new trial is possible, whereas the real manoeuvre takes about ten minutes), to allow extreme conditions experiments, identifiable and reproductible (heavy turbulences are rare and since they don't reproduce themselves, it is hard to compare different control systems).

For cost reasons and sometimes (we shall see later) for principle questions the three following criteria cannot be satisfied : identity of the tasks, identity of controls, identity of information. The following points might be helpful to validate necessary approximations.

The first criterion : identity of the task seems the easiest to satisfy : just ask the operator to "act the same" ! Actually, the problem is less simple since very often the operator finds it difficult to forget that he is operating on a simulator and therefore that serious incidents have no consequences at all.

This psychological problem is solved by :

a) Making the environment as realistic as possible : the operator forgets he is simulating if important details are reproduced : a slight vibration, the noise of air-conditioning, engine noise, even smells. Only experienced operators can point out these details. Besides, only these operators are able to recreate the psychologic conditions making them forget the simulation, through memory of real experiences. A senior pilot "feels" accelerations even in a motionless simulator because he contracts his abdominal muscles when capting visual informations and actuating the controls. These reflexes have been acquired during real flights. On the other hand, a neophyte will not feel anything.

It is then indispensable to recruit well trained operators, familiar with the real system, minding that they should be psychologically prepared to accept simulation (some test pilots can never get used to it).

Besides, an operator ignorant of the control of the real system might use small defects of the simulator as extra information, because he does not identify them as defects, whereas a well trained operator will voluntarily ignore them. Some ingeneers in charge of designing simulators, but ignorant of the real conduct of the machine, prove provoking to experienced operators : actually they have to pilot another system than the real one, with different information not existing in reality.

These remarks bring out the fact that it is not feasable to teach flying on a simulator. But in fact a simulator is helpful for the trained pilot who wants to know the characteristics of a new system and wants to practise some particular procedures. In the case of training simulators, the controls and instruments display must be reproduced accurately so as the operator can acquire "automatic reactions" exactly transferable to the real operation.

b) Making control devices as realistic as possible.

Probably the easiest criterion to satisfy. But the problem of distinguishing training simulators and experiment simulators should be raised here. As refered to earlier, a training simulator asks for perfect reproduction of the shape and arrangement of the controls as well as of the laws governing the efforts applied to the controls. Otherwise, automatic reactions learned during simulation are not applicable to the real case.

But for experiment simulators, controls identity can be less stringent. The controls must still look realistic. The pilot will be less disturbed by the replacement of the old stick by a new one (still realistic) than by the absence of noise in the cockpit.

c) Making piloting and conducting informations as similar as possible to the real ones.

Instruments information are easily reproductible. Informations given by the environment are more problematic to reproduce.

A lot of technological solutions are available to represent what the operator can see of the external world : projection on a screen of images taken by a film camera moving around a model, projection of silhouettes, etc...

These devices do not reproduce the volume perception which is sufficient when modelizing relatively distant landscapes : the relative motion of objects is sufficient to give the perception of relief. On the other hand, for all what is in the foreground, absence of relief is very sensible and perturbative for the operator. Improvements should be made in this field.

Inertia forces is an unsolvable problem. Only a reproduction of the real trajectory would transmit the real inertia forces to the operator. Fortunately it seems that human beings are more sensitive to variations of inertia forces than to these forces themselves. With little amplitude motions, these variations can be achieved : the motions of the simulation cockpit are those of the real machine, filtered by a high band filter, the medium attitude is reached back by motions which acceleration is below the perception limit of the operator.

HOW TO MEASURE THE WORK LOAD

It still remains now to interprete the experiments carried out on simulator or on the real vehicle or system.

We already saw that work load variations will not be followed by a variation of the operator's performances.

He compensates an increase in difficulty by an increase of the work load on him and this remains unnoticeable unless compensation becomes impossible. If indeed the necessary work load grows beyond the operator's limit, this one will give up some task and performance will drop. Without going into the details, it can be observed that the operator divides the parameters into three groups : those dealing with short term safety (proper attitude and speed during the approach), those dealing with instantaneous safety (trespassing of a limit leading to an immediate accident : angle of attack for a plane). When the difficulty of the task increases, the operator, unable to compensate by a growing workload beyond his limit, will progressively give up checking the long term safety parameters, then the short term safety parameters. When he is no longer able to check the instantaneous safety parameters catastrophe is imminent.

The system-operator ensemble looses its performance drastically after the operator has given up watching the short term safety parameters and therefore cannot fulfil the objective of his task. When the performances drop dramatically after a small increase in difficulty, the operator has just reached his work load limit. But again before this limit it is not possible to compare different work loads just by observing the operator.

Some authors suggested to give the operator an auxiliary task, easily measurable, and to increase this auxiliary work load until the operator reaches saturation (only one discernible phenomenon) : the main work load is then the lowest when the auxiliary work load inducing saturation is the greatest.

This principle is unfortunely based on the wrong assumption that work load are additive. Actually, carrying out a double task asks for more than the sum of the two work loads necessary for the two tasks taken separately. A management and coordination work load should be added (how and when shifting from one task to the other).

Besides the quantification of the auxiliary task is also very problematic. There is no reason for the work load of a task to be a linear function of the physical parameters corresponding to this task ; even for a task as simple as switching off lamps lit at random.

It should then be accepted that this double task method cannot be successfully applied.

Many attempts have been made to establish a correlation between physiologic parameters and work load. These correlations exist without doubt : diameter of the pupil of the eye, heart pulse fluctuations, etc... vary with work load. But these measures characterize instant work load variations and are no absolute and reproductible indications. They are far too much dependent on other factors and are even more sensitive to these factors than the work load.

The only good tool available presently is the assessment the operator makes of his own work load, by comparison with work loads required for some reference tasks. Experience shows that operators, well aware of simulation problems, are able to give reliable estimates as far as they understand that the point was evaluation of work load and not giving their opinion on the safety of the system.

It should nevertheless be noticed that a fine analysis of the variation of these physiologic parameters and the study of their correlation can provide a load indication : interesting results are expected after completion of French research works.

Let us point out an interesting attempt to build a mathematical model of the human operator in specific conditions. It has been a project carried out by ONERA for eight years. The case is the simulation of a transport plane pilot during an instrument landing approach. The purpose was to verify that the average behaviour of human operators facing almost all possible conditions encountered in flying. This verification has been made in a good number of cases but work has still be done. It is nevertheless a good way of validating, unless ulterior counterproof, certain hypothesis on elementary behaviour, unverifiable directly (operator working sequentially, information reading methods, decision heuristics, etc...)

One these hypotheses validated, it will be possible to use this model, linked to the aircraft behaviour model and deduce from it, by direct measurement, the quantity of input, output and processed information.

This will allow an objective measure of the necessary work load for a given task. This is a long term project ; it is no longer utopic and it will probably even be certainly achieved.

We tried here to expose a summary of our knowledge on the human operator and to deduce from it some common sense rules. A lot of work has still to be done but it is a sure thing that many errors, many "control mistakes" would be avoided if only these rules were not forgotten, and if designers thought from the beginning of adapting the machine to the human being and not the human being to the machine.

But already now it is comforting to observe that design ergonomy has gained recognition in design offices and that ergonoms are now considered positively more like useful partners than ennoying colleagues.