FAILURE MODE WORKLOAD THEORY AND PLANNING

Craig M. Arndt
Armstrong Laboratory
U.S. Air Force

ABSTRACT

Failure conditions have long been a major driver in the design of aircraft systems. There are a number of major changes in the cockpit environment during systems failures and emergency operations. The new environment produced by an emergency or failure conditions can be characterized by a loss of planning and anticipation of coming events. The pilot is forced into a purely reactive mode in a rapidly developing situation. The frequency of failures and emergency conditions may not warrant new systems dedicated to emergency/failure conditions. However, in the area of commercial aviation, avoiding one major incident could save hundreds of lives, and in the military, the number and consequence of failure/emergency conditions will rise dramatically when systems are introduced in a combat environment.

The principle objectives of studying failure mode workload are to: 1. Define and document a study to develop a means to design for failure mode operation workload situations; 2. Examine the history of catastrophic results from induced error during Failure mode operation; 3. Develop and implement designs procedures, and certification standards which will reduce catastrophic error induced by failure mode operation. By studying workload based on failure mode operation we may be able to develop designs and procedures which can help us eliminate some of the most catastrophic operator involved failures.

2 Background

The definition and reduction of failure mode workload requires a background of understanding within a number of areas. These areas include, traditional workload theory, Reliability theory, Pilot error crash history, and Design practices and requirements. By understanding these elements of the study of failure mode workload we can start to understand the importance of developing better designs and procedures to reduce the effect of failure mode workload.

2.1 Traditional Workload

The concept of mental workload is a logical extension of the resource model of the attention. Resource models postulate a limited quantity of resources available
to perform a task, and in order to perform a task, one must use some of or all these resources. The basic notion is related to the difference between the amount of resources available within a person and the amount of resources demanded by the task situation (Sanders and McCormick 1987).

Since the middle to late 1970s, interest in defining and developing measures of mental workload has increased dramatically. A major area of focus of such work has been the assessment of workload experienced by aircraft crew members, particularly pilots.

Traditionally, these measurements are either subjective measurements (asking the pilots what their workload was) or performance measurements (measuring to see if the pilots' performance goes down under high workload). These measurements are made during different parts of a standard mission.

2.2 Reliability Theory
Reliability theory suggests that many systems fail only after being exposed to stress generated by the prior failure of other systems. These cascading failure modes apply equally to human control systems as well as to the failure of engines and wings.

In reliability theory this configuration is called cascaded failures effect and can be described by shared load parallel models. In this configuration, the parallel subsystems equally share the load, and as a subsystem fails the surviving subsystems must sustain an increased load. Thus as successive subsystems fail, the failure rate of the surviving components increases. An example of a shared parallel configuration would be when bolts are used to hold a machine member; if one bolt breaks the remainder must support the load (Kapur and Lamberson 1977). Similarly if one subsystem of a flight control system fails, then some other part of the system (the operator) must support more of the load for the system task.

2.3 Design Practices, Requirements
There are several existing design documents which require investigation failure and safety issues, such as failure mode workload once. Mil-Std-1472D is the standard for human engineering design in military systems states;

4.5 Fail safe design. A Fail Safe Design shall be provided in those areas where failure can cause catastrophe though damage to equipment, injury to personnel or inadvertent operation of critical equipment.

4.8 Safety. Design shall reflect applicable system and personnel safety factors, including minimization of potential human error in the operation and maintenance of systems, particularly under the conditions of alert, battle stress, or other emergency or non-routine conditions.

In addition to the military design standard the Federal Aviation Administration (FAA) has published a human factor plan, which addresses the important issues in the development of systems for commercial aviation. The FAA national human factors plan calls for the study of automation in ATC and cockpit applications and also, the study of crew coordination and pilot error. These design documents clearly demonstrate the importance of identifying methods for reducing classes of potential failure modes.

3 Definition
In order to facilitate the remainder of this paper I will offer a formal definition of Failure Mode Workload here.

Failure Mode Workload is the condition of sudden or unexpected user workload which is caused by the failure of some part of the Aircraft system during operation.

As defined here failure mode workload conditions will have characteristics which will define both the difficulties we can expect during these conditions and the ways we can best deal with these situation. The first characteristic is that procedural changes will take place within the system as operators attend to the tasks of determining the state of the system/aircraft and take corrective actions. These changes can be either unplanned or planned in advance. It is important that these procedural changes be planned and personal trained when ever possible. The next characteristics for failure modes are control and display changes, this is particularly common in highly automated systems and can lead to short term disorientation and loss of situational awareness. The failure will also often add additional tasks to the operator's workload. Even if these tasks are just an increased monitoring load to attend to, the failure of these tasks can make a critical difference in the operator's performance. The last characteristic of failure modes is dynamic task allocation. Under failure mode operating conditions, the next tasks are transient or unknown, creating the problem of needing to decide what to do next under time pressure. These and other characteristic the failure mode conditions tend to create induced operator error.
3.1 Induced Pilot Error

Human error is a major contributor to almost all aircraft crashes. It is important to note however that almost all human error is induced error. By induced error, I mean that the error is not baseline Human Error Probability (HEP) which would be a random event, but an error caused in part by the effects of another condition (inducing factor). The HEP for induced errors is much larger than for the baseline operation of systems. For this reason almost all aircraft incidents are due to an induced error condition. In the case of aircraft operator error, often the inducing factor is a degraded equipment configuration or an other non-normal operating condition. Failure modes increase the human error probabilities because high attention levels which accompany failure mode operation reduce the crew’s ability to attend to monitoring tasks and react to changing situations. Some kinds of failures and emergencies are prone to inducing much higher levels of human error probability. Systems should be designed to be more tolerant of conditions which might induce human error. Remember that it is still much easier for an operator to correct an computer error than for a computer to correct a human error.

3.2 Attention and Crew Coordination

The problems of failure mode operation and workload are often even more complex in the case of multi-crew aircraft where attention and crew coordination are critical. The following are just two examples of what can happen if planning and training for failure mode operation are not fully addressed.

'Preoccupation with a malfunction of the nose landing gear position indicating system distend the crew's attention form the instruments' (Eastern N310EA)

'The captain's preoccupation with an in-flight malfunction and his failure to monitor properly the airplane's flight instruments which resulted in his losing control of the airplane.' (China Airlines N4522V)

Studies and experience tell us that attention, procedure, and crew coordination are significantly altered during failure mode operation. These changes cause shifts in the workload on each crew member and the possibility of critical tasks not being attended to. Changes in equipment design and procedures should reduce these problems.

3.3 Automation

The interrelationship between increasing cockpit automation and problems of failure mode workload and induced pilot error cannot be overstated. As more fully automated systems are becoming common in most aircraft, we are clearly gaining in performance of the system in normal operation. However the potential failure of these systems and the operator interaction with these systems during the failure of other aircraft systems present possibly severe workload problems. There are two things about automated systems that cause their loss to be more dangerous than other systems. The first reason is that automated systems have a tendency to reduce the situational awareness of the operator. When the automated system go down the operator will take time to upgrade his/her situational awareness. The second reason is that because automated systems perform such a large number of tasks the loss of the automated system may present the operator with a very high onset rate of tasks perform, coordinate, and plan.

Due to the quickly changing conditions in a failure mode situation, there have been a number of problems related to an over reliance on automated systems.

'Contributing to the accident was the captain's over-reliance on the autopilot after the loss of thrust on the No. 4 engine.'

This problem is further compounded by reductions in crew size in many new aircraft designs. Altho there is good evidence that during normal operation these new designs require less crew, during emergencies or failure mode operations, the lack of operator may prove catastrophic. I do not propose that automated systems be removed from designs or that crew size designs are unsafe. I do, however, propose that these designs are particularly vulnerable to induced operator error, and that we study the effects of failure mode operation in these designs.

4 Use and Usefulness

Now we come to the very important question of 'so what?'. I have shown that that the issue of failure mode workload is a problem of some concern, but what is the usefulness of addressing this issue.

As aircraft and other human controlled systems become more complex and more automated, the human workload, both physical and mental continues to be reduced. Workload also continues to become more critical some cases. The usefulness of developing procedures and methods for identifying, measuring and
reducing failure mode workload is two-fold. The first advantage is that very little work has been to date in this field and that affords us an opportunity to make considerable progress. The second advantage we gain is that many of the most critical incidents we encounter in the study of man-machine systems fall into the category of failure mode operations and induced operator failure. If we can eliminate the majority of these failure we will go a long way to reducing the sometimes catastrophic effects of systems failures.

5 Recommendations and Study

5.1 Automation Mode Structure

One possible solution to the high failure mode induced workload levels would be to define emergency modes of automation authority which could be manually engaged or disengaged by the pilot. Studies and integration projects have shown that pilots and other operators will accept vastly different levels of automation depending on the condition of operation of the systems. Current aircraft systems maintain several different levels of automation in their control systems. Therefore, it is reasonable and necessary to design new automation systems design for failure mode operating conditions.

5.2 Procedures

Any improvement in failure mode workload will not come just because of changes to equipment. Additional procedures will be needed in order for the operator to maintain attention and workload at acceptable levels and attend to only high priority tasks. One means of improving procedures to deal with sudden failures is the development of more demanding training to deal with these possibilities. The rapidly improving technology of simulators offers the opportunity to train more operators in more situations. In addition procedures need to be developed to deal with transition into failure modes of operation. These transitions are critical to acquiring and maintaining situational awareness of the aircraft and of the failure situation.

5.3 Testing and Certification

As mentioned earlier workload measurement is made over a range of anticipated aircraft mission segments. Because of the catastrophic consequences of failure mode operations, it is important that more of these conditions be tested in workload evaluations based on tasks involved in aircraft in nominal equipment modes.

In many cases certification is based primarily on demonstrating an improvement over a baseline design in nominal equipment operation modes. This is a valid method based on nominal conditions. However, in an attempt to reduce workload over a wide range of nominal conditions automated systems can often create failure modes which are totally unsafe.

It is therefore my recommendation that the certification of aircraft include workload measurement and testing of as many failure modes of operation as possible.

6 Conclusions / Plans

More investigation and study will need to be done before standards can be written on failure mode workload. Current plans for this project include performing additional studies to determine additional parameters of the problem and what existing work can be applied. Also planned are projects to investigate the design implications to over aircraft design and implementation in new and existing aircraft systems. In the development of design and testing for failure mode workload, it will be important to involve the aircraft designers. Simply changing the requirements will not make safer systems. The whole design, testing specification and regulatory community must be involved.

Currently there is considerable interest in this topic within government agencies. The national research council is actively investigating human error as a major issue. The FAA is interested in the possibility of investigating ways to reduce this class of human error in aircraft operation. There are continuing efforts to start a working group with Armstrong Lab, ASD/EN, and the FAA to establish standards and procedures to reduce dangers of failure mode operation.

REFERENCES


732