NASA Contractor Report 4547

Intervention Strategies for the Management of Human Error

Earl L. Wiener

University of Miami at Coral Gables
Department of Management Science
P. O. Box 248237
Coral Gables, FL 33124

Prepared for
Ames Research Center
CONTRACT NCA2-441
August 1993

National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California 94035-1000

CONTENTS

I. THE MANAGEMENT OF HUMAN ERROR 2

- A. Introduction 2
- B. The advent of modern cockpit automation 4
- C. Purpose and limitations of this study 7

II. HUMAN ERROR AND INTERVENTION 10

- A. Lines of defense 10
- B. Intervention strategies - examples 13
- C. Is there an intervention strategy for every problem? 25
- D. Two models of intervention 27

III. INTERVENTION STRATEGIES: TRADITIONAL TECHNOLOGIES 29

- A. Hardware 29
- B. Procedures and supporting documentation 40
- C. Communication 50
- D. Training 55

IV. INTERVENTION STRATEGIES: ADVANCED TECHNOLOGIES 58

- A. Employment of advanced technologies 58
- B. Error management 62
- C. Summary of management techniques 75

V. CONCLUSIONS AND OVERVIEW 76

- A. Human error can be managed 76
- B. Management strategies 77
- C. The role of government 86
- D. Summary 88

VI. REFERENCES 90

VII. NOTES AND ACKNOWLEDGMENTS 101

VIII. APPENDICES 103

- 1. Guidelines for intervention strategies 104
- 2. Wiener-Curry automation guidelines (1980) 107
- 3. Degani-Wiener guidelines for checklists (1990) 109
- 4. Glossary of abbreviations 111

SUMMARY

This report examines the management of human error in the cockpit. The principles probably apply as well to other applications in the aviation realm (e.g. air traffic control, dispatch, weather, etc.) as well as other high-risk systems outside of aviation (e.g. shipping, high technology medical procedures, military operations, nuclear power production).

Management of human error is distinguished from error prevention. It is a more encompassing term, which includes not only the prevention of error, but also means of disallowing an error, once made, from adversely affecting system output. Such techniques include:

- Traditional human factors engineering
- Improvement of feedback and feedforward of information from system to crew
- "Error-evident" displays which make erroneous input more obvious to the crew
- Trapping of errors within a system
- Goal-sharing between humans and machines (also called "intent-driven" systems)
- Paperwork management
- Behaviorally based approaches, including procedures, standardization, checklist design, training, cockpit resource management, etc.

The author stresses "intervention strategies", various means of error management by intervening into the system. A distinction is made between two models of intervention, those directed toward a very specific and well-defined human error (e.g. wrong runway landings), and those directed toward less defined, often vague sources of error (e.g. complacency, fatigue).

Fifteen guidelines for the design and implementation of intervention strategies are included.

I. THE MANAGEMENT OF HUMAN ERROR

> For every evil under the sun,
> There is a remedy, or there is none;
> If there be one, try and find it,
> If there be none, never mind it.
>
> William C. Hazlitt, English Proverbs, 1869

A. INTRODUCTION

Modern transport aircraft, for all of their sophistication of design and manufacturing, are still highly vulnerable to erroneous behavior on the part of crew members. The same is equally true of other types of aircraft, indeed of human-machine systems in general, such as nuclear power plants, shipping, high-technology medicine, and chemical production plants. Some domains have accident rates that are quite appalling when compared to aviation. For example, world-wide one merchant ship a day is lost due to accidental causes. While the focus of this report is on transport aircraft, the principles derived should apply to all human-machine systems, especially those which depend to a large degree on computer-control, often generically described as "automation."

The vulnerability of a variety of human-machine systems to human error has been dramatically demonstrated by accidents such as the crash of Northwest Flight 255 at Detroit in 1987 (National Transportation Safety Board [NTSB], 1988; Lauber, 1989; Wiener, 1989c), the capsize of the sea-going ferry *Herald of Free Enterprise* at Zeebruge in 1987 (Department of Transport [U.K.], 1987), the chemical disaster at Bhopal in 1984 (Meshkati, 1988; Reason, 1990), and the nuclear accident at Chernobyl in 1986 (Meshkati, 1988; Reason, 1990).

There is an ubiquity to such disasters: they are not confined to aviation or any single domain. Perrow (1984) calls these disasters "normal accidents"; Wiener (1987b) speaks of the twin perils of "fallible humans and vulnerable systems." Lautman and Gallimore's widely quoted study (1987) of world-wide hull loss accidents of jet transports revealed that approximately 70 per cent could be attributed to crew error. Additional accidents could be attributed to human errors committed by others (maintenance, weather, dispatch, and air traffic control personnel). Similar figures can be found in studies of general aviation accidents, military aircraft accidents, and non-aviation domains.

The author examines the role of human error in aircraft accidents and incidents, and the methods of managing these occurrences. The term "management" here implies not only error elimination at its source, the human operator, but also means of preventing errors, detecting errors when they occur, and preventing errors from adversely affecting the system once they do occur.

These methods of error elimination or control will be referred to as "interventions." The plan by which interventions are formulated, tested, and implemented is an "intervention strategy." The author will examine both traditional methods (e.g. basic human factors in product design, training, and procedurization) and modern methods which may depend on advanced computer techniques (e.g. fault tolerant designs).

One of the problems that we must confront is the possibility that almost anything that is done which impacts the cockpit or cockpit crew could be considered an intervention strategy. This could be an action as narrow as the most minor hardware change (e.g. painting a stripe on some display or control) or procedural change (reverse the order of two sub-tasks on a checklist). It could also be an action as broad and encompassing as a wide-ranging governmental action (e.g. the "sterile cockpit" rule, to be discussed later), or a major alteration in training curricula (e.g. the introduction of training in cockpit resource management [CRM]). Our problem is determining the boundaries of the term: can any action which is directed toward the management of human error be considered an intervention strategy?

Interventions can involve the most complex, or the simplest of devices. The checklist is an example. It is ironic that with all of the sophisticated and costly devices on board an aircraft, and those supporting the aircraft through the Air Traffic Control (ATC) system, the most important guardian of the safety of the plane and its occupants is a single piece of printed paper, the checklist. Given this fact, it is somewhat disturbing that prior to a recent NASA study (Degani and Wiener, 1990), there had been no systematic research into the human factors of checklists (Wiener, 1987c).

Traditional Approaches

Airlines typically attack error prevention through their training programs, standardization of procedures, quality control (e.g. initial operating experience [IOE], six-month proficiency checks, line checks, etc.), and printed materials such as manuals and checklists. Warning and alerting systems on board the aircraft (e.g. ground proximity warning systems [GPWSs]) and on the ground (e.g. minimum safe altitude warning systems [MSAWs]) also stand as sentinels against human error. Note that most of these systems do not prevent the original error; but they do prevent it from maturing into an accident or incident.

These approaches have generally proven to be successful, as evidenced by the steady improvement in air safety (Lautman and Gallimore, 1987). However it appears that a plateau in accident rates may have been reached in the last decade, at around 0.3 accidents per million flights (Sears, 1989). Although this plateau may be extremely low, any non-zero accident rate is unacceptable to the traveling public, and hence to airlines, manufacturers, and pilots.

Furthermore, airlines, manufacturers, and government agencies are also concerned about the plateau effect, due to the fact that if the accident rate quoted by Sears in hull loss accidents per million flights remains constant, with expanding traffic, the absolute number of accidents will increase to 25-30 annually, or about one every two weeks worldwide (Weener, 1991). Needless to say, the traveling public, and politicians, are sensitive not to rates, which may be quite abstract, but to the publicity surrounding high-visibility accidents when they occur. For this reason, human error prevention and control has been assigned a high priority by the Federal Aviation Administration (FAA) and the manufacturers (Weener, 1990, 1991).

Also there is evidence that air traffic will continue to expand during the remainder of this decade, and the system may be more intolerant of error. In recognition of the potential for traffic increases to generate accidents, there have been proposals to limit traffic growth to ensure safety (Proctor, 1988). At about the turn of the century, improvements in the system should be realized, when the planned modernization of the air traffic control (ATC) system begins to compensate for growth (FAA, 1991). Airline safety experts expressed great concern over the forecast of traffic expansion at a 1988 NASA/FAA/Industry Joint Workshop on Flight-deck Automation (Norman and Orlady, 1989).

B. THE ADVENT OF MODERN AUTOMATION

The High Technology Cockpit

Another factor to be considered is the rapid expansion of automation in the cockpit. Many in the aviation industry have assumed that automation would remove human error, replacing the fallible human with unerring devices. The research of Wiener and Curry, including field studies with airlines bringing highly automated aircraft on line, suggests that this may be overly optimistic, and that automation merely changes the nature of error, and possibly increases the severity of its consequences (Curry, 1985; Wiener, 1985a, 1985c, 1988a; 1989a,b; Wiener and Curry, 1980). The same appears to be true in the other industries mentioned. In brief, computer-controlled flight may invite large blunders while eliminating the small errors seen in manual systems. The ASRS reports below are illustrative of some of the problems of autoflight.

> Narrative: We were cleared to cross 40 nm west of LINDEN VOR to maintain FL270. The captain and I began discuss the best methods to program the CDU to allow the performance management system to descend the aircraft. We had a difference of opinion on how to best accomplish this task (since we are trained to use all possible on-board performance systems). We wanted to use the aircraft's capabilities to its fullest. As a result, a late descent was started using conventional autopilot capabilities (vert spd, max indicated Mach/airspeed, and spd brakes). Near the end of descent, the aircraft was descending at 340 KIAS and 6000 FPM rate of descent. The aircraft crossed the fix approximately 250-500 feet high. Unfortunately we made no call to ATC to advise them of the possibility of not meeting the require alt/fix. This possible altitude excursion resulted because: 1) The captain. and the F/O had differences of opinion on how best to program the descent; A) Both thought their method was the best, the captain's of programming (fooling) the computer to believe anti-ice would be used during descent,which starts the descent earlier. The F/O's of subtracting 5 miles from the nav fix and programming the computer to cross 5 miles prior to LINDEN at FL270. B) A minor personality clash between the captain and the F/O brought about by differences of opinion on general flying duties, techniques of flying and checklist discipline. C) Time wasted by both captain and F/O (especially F/O) in incorrectly programming CDU and FMS for descent, which obviously wasted time at level flight, which should have been used for descent. Observation: as a pilot for a large commercial carrier at its largest base, we seldom fly with the same cockpit crew member. This normally does not create a problem. I do, however, feel that with the new generation glass cockpits being on the property approximately 6 years, which can cause a bit more difficult transition than, say month to month cockpit crew change on a 727 or pre-EFIS DC-9. I have flown commercially for 10 years, and have flown 2-man crew for 8 of those 10. The toughest transition for me is to determine who shares the PF and PNF duties. This historically (3 years) has been the most difficult when the other crew member has transferred from a 3-man cockpit to a 2-man "glass cockpit." This is especially pertinent when the crew member has been on a 3-man crew for a number of years. As F/O, when you are the PNF, you accomplish your normal duties. However, often times when one is the PF, the F/O also has to do the PNF duties because the other crew member has not been used to doing the PNF duties to the extent that it is required on 2-man cockpits, whether they be conventional or EFIS. This

> obviously can lead to a myriad of problems. Add weather or an airport such as Washington National, LaGuardia, or Orange County, and problems can accelerate with alarming rapidity. (ASRS No. 122778)

> Narrative: Aircraft was coupled to autopilot and autopilot was armed for the ILS (8L at Atlanta). Aircraft intercepted and captured localizer at approximately 15 nm from airfield, aircraft at 5000'. I identified localizer. As per company procedures captain rotated heading (HDG) select knob to 340 deg for missed approach HDG, but unknown to either of us, the multifunction knob was pushed in far enough to activate "HDG Hold". I did not notice the flight mode annunciator window change From "LOC TRK" to "HDG HLD". Of course, the ADI (flight director) display remained as before with the pitch bar giving altitude hold at 5000' And the bank bar still centered but centered because we were On HDG not localizer. Obviously we gradually started to drift right. The HSI (nav display) was selected on map mode (20 mile scale). On this scale a small deviation off localizer is too small to detect. I monitored the glide slope (raw data display) and saw it descend through the flight director pitch bar. I looked at the flight mode annunciator (FMA) and realized we were no longer armed for the ILS. I immediately announced to the captain and disconnected the autopilot to start descent and selected arc mode on the nav display. I saw we were full scale localizer deflection so I put in about a 15 deg correction to course. At that moment Atlanta Approach called to tell us we were drifting into the parallel ILS course and he told us to maintain 4500' until established. (He also gave us a HDG to correct). I leveled at 4700' and as I did the localizer centered up and the ILS was resumed uneventfully. Having map mode in HSI instead of arc does not make a localizer deviation immediately obvious. Lack of continuous cross-check of FMA by pilots is a factor. Hdg select knob doubles as HDG hold button and an imperceptible extra push in on it activates HDG hold. To correct the problem: fly ILS with arc (or rose) in map to make deviations immediately obvious. Additionally, multifunction knobs should not be accepted on aircraft. It is simply too easy at night when you are tired or distracted to activate the wrong function. (We have 3 multifunction knobs where different functions are activated depending on how far in you push the knob. It can be very tricky sometimes). (ASRS No. 141226)

However, the evidence is not entirely supportive of the Wiener-Curry hypothesis of automation and error severity. In a recent simulation study which compared performance of crews in a specially designed LOFT (line oriented flight training) session in two aircraft in the same family, one with a traditional cockpit (DC-9-30) and one with an advanced technology ("glass") cockpit (MD-88), there were no statistically significant differences in the severity of errors committed by the crews of the two aircraft (Wiener, Chidester, Kanki, Palmer, Curry, and Gregorich, 1991) This result was confirmed in two independent analyses of error severity.

Contributions of Cognitive Psychology and Systems Engineering

Human error has excited the interest of cognitive psychologists and systems engineers in the last decade, and some very imaginative and creative ideas have resulted (reviewed in Nagel, 1988). The nature of human error has been explored by such experts as Norman (1983, 1984), Rouse and Rouse (1983), Rasmussen, Duncan, and Leplat (1987), Reason (1990), Moray (1988), Woods (1989), and others. Several have developed models and taxonomies of human error (e.g. Rouse and Rouse, 1983; Rasmussen, 1981; and Norman, 1981). These were reviewed by Rogers, Logan, and Boley (1989). Recently, two books on the psychology of human error have appeared (Reason, 1990; Senders and Moray, 1991).

Insightful as the writings of cognitive psychologists may be, they are often highly abstract, and their applicability to aviation is not always clear. However, in recent years some of the leading authors have written far more concretely about cognitive processes and error control in aviation and other domains, notably Norman (1983, 1990), Hutchins and Klausen (in press), Rasmussen and Vicente (1989), and Woods (1986). Despite this, most of the authors have been content to explain the cognitive etiology and psychodynamics of human error, but have been somewhat slower to examine solutions or intervention strategies. Norman (1990), in discussing the "problem with automation" (lack of feedback), has suggested solutions, but mostly by implication. Rouse's writings on how computer technology might play a part (e.g. fault tolerant systems) has given designers some guidance (1990). More will be said about the potential contributions of cognitive psychology and intelligent computer methods in Chapter IV.

C. PURPOSE AND LIMITATIONS OF THIS STUDY

Purpose of This Study

In this report the author examines possible sources of error experienced by humans operating complex systems, and the resources that can be brought to bear on these problems. The goal is to match methods (resources) with demands (potential errors), to determine whether an effective error intervention strategy can be derived (Wiener, 1989a).

A set of guidelines for the design and evaluation of intervention strategies is proposed throughout the text, and collected in Appendix 1. The guidelines provide a "template" against which a proposal can be held. A perfect fit will never be found. The author of any proposed intervention should hope to find a good, or at least satisfactory, fit.

GUIDELINE NO. 1

> *In proposing an intervention strategy, one should ask "is this intervention necessary? Is there a well-defined problem or set of problems that it can prevent or reduce?" It is not sufficient to justify a proposed intervention by merely saying that it is "good for safety."*

Each proposed method of intervention (e.g. error-evident displays) should be examined with respect to its feasibility, applicability, costs, and possible short-comings (e.g. creating a problem elsewhere in the system). Take the following examples.

1. Some error-reducing systems tend to generate other errors, including false alarms. The effectiveness of the early models of the GPWS was marred by high false alarm rates, as well as crew uncertainty about which mode was responsible for triggering the alert (Wiener and Curry, 1980). In the aggregate, GPWS has proven to be highly effective as an intervention against controlled flight into terrain (CFIT) accidents which plagued the industry in the 1970s (Loomis and Porter, 1981; Weener, 1990; Wiener, 1977). The recent crash of an Air Inter A-320 near Strasbourg, France (Lenorovitz, 1992) rekindled the debate over whether the GPWS should be mandatory for passenger aircraft

2. Voice-warning systems can be used to alert crews to hazardous conditions; they also intrude on the cockpit atmosphere and possibly interfere with intra-crew and radio communications.

3. Increasingly crews are encouraged (though not required by FARs) to give detailed readback of takeoff clearances, including stating the runway for aircraft cleared for takeoff. This is an effective cross-check against ATC or crew error, but not without a cost. Any added voice communication requirement potentially increases frequency congestion, which in turn can contribute to communication error. It can also be a source of error.

Limitations of This Study

For the purposes of this study, I have considered only those interventions directed toward the management of human error and the prevention of accidents and incidents. An entire class of interventions which are vitally important to aviation safety will not be addressed. Those are the measures directed toward events that occur in the "post-crash" phase of an accident. They are designed to ameliorate injury and prevent death to the aircraft occupants. Interventions in this area would include such measures as strengthening aircraft floors and seat mounts, improvement of restraint devices, evacuation routes, markings, lighting, and procedures, cabin personnel training, fire suppression, containment of loose objects in the cabin, and many others. Also, this report will be confined to management of errors on the flight-deck, although many of the same principles could apply elsewhere in the aviation system (e.g. air traffic control [ATC], aviation weather, dispatch, passenger cabin, and maintenance), as well in as in other high-risk domains.

I have also excluded from consideration interventions aimed at upper management (including government), for example the possibility of airlines rebuilding their schedules to reduce the likelihood of fatigue, and thus presumably human error. Also excluded from consideration will be pre-employment selection, as this is not clearly an error-management technique.

Organization of This Report

For ease of reference, chapters are denoted by Roman numbers, and tables and figures within a chapter by sequential Arabic numbers. Thus, for example, the first figure in Chapter IV would be referred to as Figure IV-1. The appendices are denoted sequentially by Arabic numerals, and notes (Chapter VII) are cited by square brackets and Arabic numerals, e.g. [2].

II. HUMAN ERROR AND INTERVENTION

A. LINES OF DEFENSE

In this section the concept of lines of defense against human error will be introduced. Lines of defense are seen as a series of imperfect, cascaded filters, each of which may stop an error, or allow it to pass. For any human error or class of errors, there may be a unique set and order of the lines of defense. The purpose of an intervention strategy is to strengthen one or more of the lines of defense. In this chapter the author will discuss various generic opportunities for interventions. Intervention strategies will be covered in detail in subsequent chapters.

On August 16, 1987 Northwest Flight 255, an MD-82, attempted to take off from runway 3C at Detroit. It struggled off the end of the runway, then attained an altitude of approximately 40 feet before striking a light stanchion in a parking lot, and crashing onto a freeway. After a lengthy investigation, the NTSB (1988) concluded that the crew had taken off without slats and flaps deployed, resulting in diminished takeoff performance. An elaborate takeoff warning device, which should have furnished the crew with a voice warning of the misconfiguration, failed to activate, for reasons unknown. The accident's chain of causation was complex, to say the least. In many ways this accident represents a veritable catalog of human factors (Lauber, 1989).

In November of that year the Board's public hearing was held in Detroit. The author was invited to testify as to human factors in general, and automation and warning devices in particular. As part of the testimony, the author proposed six "lines of defense" against human error. These were seen as being essentially arrayed in series, such that any one of the defenses could negate any error and prevent an incident, accident, or undesirable condition (Wiener, 1987c). These are listed in Table II-1 and depicted in Figure II-1. Schwartz (1990) proposed a similar concept which he called the "safety chain."

Note that the items below, and particularly their order, are not proposed as "universal". The order of these lines of defense was proposed by the author, primarily with avoidance of the consequences of a no-slats/flaps takeoff in mind. The order is open to debate, and the reader may propose some other order of the lines of defense, or even other defenses. Furthermore, the order, as well as the inclusion at all, may depend somewhat on the error being defended against. For example, Defense No. 5 may be inappropriate in many cases. In other cases (e.g. altitude deviations), the anomaly is most often detected by an ATC controller (Degani, Chappell, and Hayes, 1991). The order of the lines of defense against a midair collision are considerably different from those that may be established for stall avoidance.

Figure II-1 emphasizes the serial, or cascaded structure of the lines of defense.

TABLE II-1. Lines of defense against human error.
(From Wiener, 1987c)

1. Execution of normal procedures and airmanship, backed up by human vigilance, by the responsible crew member(s).
2. Detection of abnormal condition by other crew members.
3. Secondary indications or displays (e.g. sounds, vibrations or other stimuli impinging on the cockpit that might indicate errors).
4. Warning and alerting devices.
5. Detection of error conditions by persons external to the cockpit (ATC, other aircraft crews, persons on ground, cabin crew or passengers, etc.).
6. Machines that take action on their own (e.g. alpha floor protection against stall in high technology aircraft; autoslats and stick-pushers for stall avoidance and recovery).

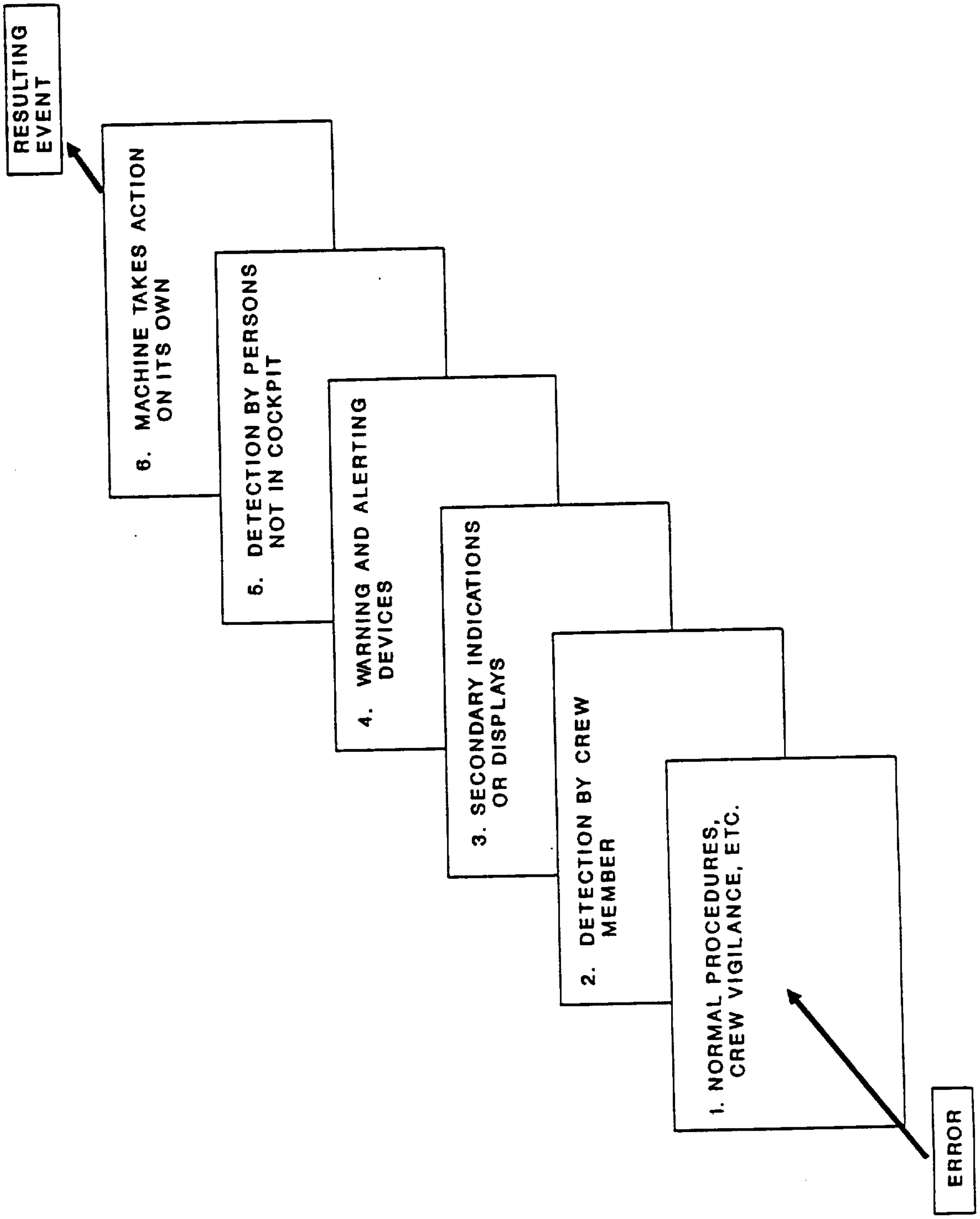


Figure II-1. Lines of defense against human error.

Before discussing interventions, one point needs to be made clear. The first line of defense against human error is, and always will be, product design. This dictum is discussed at several places within this report. Both the author and Norman put the burden on the designer of hardware. Norman (1983), writing on human error, states, "There is little need for most of these errors. Most are system induced, a result of inappropriate system design." Wiener, testifying before Congress (1988b), spoke of his "Iron Law", that if equipment is designed correctly for human use in the first place, the cost is high, but it is paid only once. If poor design must be compensated for in training departments and operations, the price must be paid every day. And what is worse, with weak, potentially error-inducing designs, one cannot be sure that when the chips are down, the correct responses will be made.

The aim of intervention is to strengthen lines of defense at any barrier, or any combination of barriers, and to insert additional lines of defense where possible. It may be helpful at this point to give some examples of interventions, as well as of places where intervention is needed.

B. INTERVENTION STRATEGIES - EXAMPLES

GUIDELINE NO. 2

> *Never implement an intervention or procedure that you feel that the crews will not follow. (This is similar to the military dictum of "never give an order that you do not expect to be carried out.")*

Intervention Through Procedures

One of the carriers studied by the author has a number of procedures that must be completed upon climbing through 10,000 feet. In one aircraft, which has high climb performance, it is very possible to climb rapidly from 10,000, where these duties are initiated, through FL 180 (18,000 feet) where an altimeter adjustment is required (in U.S. airspace). This procedure could easily be ignored in the midst of a demanding workload. It would appear that some of these duties could be reassigned to other points in the flight (and on the checklist), possibly to FL 180 or above, to avoid this potentially serious error. Note that this is not workload reduction: no steps are omitted. This is workload management: the temporal redistribution of workload, with the goal being error control. Workload management, or lack of it, is illustrated by the following ASRS report.

> Narrative: passing ARNES on CIVET 2 profile descent, we both (2 man crew) thought we were cleared after passing FUELR for

> the 25L ILS approach with a sidestep to runway 24R. Approach later asked if we had the airport and we reported we did and we both thought we were cleared for a visual to runway 24R. We switched the ILS to 24R and turned in that direction. Alt was 4000' and descending, then Approach told us to turn 20 deg left and that we had traffic to our right. He apparently was turning into runway 24R. Approach said our original clearance was for runway 25R, not for runway 24R. The rest of the approach and landing was normal on runway 25R. Apparently we misheard the clearance. Contributing factors: tuning in a runway and being forced to change to another runway while trying to make altitude restrictions etc. Also flying an automated, glass cockpit aircraft in this environment pushes workload to the limit, when having to change runways on final, forcing you to reprogram the computer, re-tune the nav radios and change VHF freq and change charts. It becomes very easy to misunderstand clearances. Also no one had time to look for other traffic. (ASRS Report No. 167993)

Intervention Through Regulation

An example of intervention through government regulation can be found in the so-called "sterile cockpit" rule. In the 1970s the airline industry was plagued by a rash of what came to be called "controlled flight into terrain" (CFIT) accidents (Ruffell Smith, 1968; Weener, 1990; Wiener, 1977). In several cases, the cockpit voice recorder indicated a high degree of casual conversation and persiflage in the cockpit, implying a neglect of essential duties. As a result, the FAA promulgated Federal Aviation Regulation (FAR) 121.542, which decreed that while moving on the ground under its own power, or flying below 10,000 feet (MSL), the cockpit was to be "sterile", meaning no non-pertinent conversation could take place. During sterile periods, there can be no entry into the cockpit by the cabin crew for non-essential reasons. Unfortunately, it is not always clear to the cabin crew members what constitutes a warrant to enter the cockpit during sterile periods (Chute and Wiener, in preparation).

The sterile cockpit rule is largely unenforceable, but it does set the tone for a business-like atmosphere in the critical phases of flight, and sets a standard for cockpit behavior at critical times of operation. Some cockpit voice recorder readouts in recent accidents have revealed less than assiduous devotion to the rule (NTSB, 1988, 1989). It will always be controversial since it is invasive on the cockpit working atmosphere and self-expressions of the crew. Although there are no statistics to support the efficacy of the sterile cockpit rule, it is generally seen as a plus for safety. Its benefits not limited to CFIT accidents. With the growing concern over ground collisions at airports, the sterile cockpit rule probably plays a large part in preventing distractive behavior while taxiing.

GUIDELINE NO. 3

> *Politically inspired interventions should be resisted. Although the motivation and intention of the Congress may be correct, legislative bodies do not have the technical expertise to specify and evaluate safety interventions, and at the very least their solutions may involve technically infeasible deadlines (e.g. ELT, GPWS, and TCAS). These may lead to immature hardware and software being installed in aircraft, with the result that effective intervention is delayed rather than hastened. This is particularly true in those cases where Congressional interventions come in the wake of a tragic accident, and political leaders (and possibly their constituents) may feel that the FAA and industry are not moving as quickly as they might.*

Intervention Through Hardware

The author has already mentioned the ground proximity warning system (GPWS), which was mandated by the U.S. Congress as its solution to the CFIT accidents. The early models of the GPWS had their own operational problems, for example high false alarm rates, and alarm modes which were difficult to interpret. In spite of its shaky beginning, the merits of the GPWS have been documented (Loomis and Porter, 1981; Weener, 1990). These authors have shown that in those countries in which the GPWS is required, CFIT accidents have been dramatically reduced, and have virtually disappeared in the U.S. Unfortunately, in other parts of the world GPWS is not required, and each airline may decide whether to equip its fleet with the device. The crash of the Air Inter A-320 near Strasbourg, France in January 1992 emphasized this regrettable fact.

A simple device provides another example of hardware intervention against an all-too-common human error of yesteryear.

1) The device. Conventional aircraft of the World War II era could not be safely left on the ground with their control surfaces unsecured, since wind gusts could move them violently, causing structural damage. As a countermeasure to this, external locks, in the form of crude, V-shaped wedges made of wood, were manually inserted onto the control surfaces, locking them in neutral position.

2) The problem. The reader can immediately see the potential

for disaster. It was not at all infrequent for aircraft to attempt takeoff with the gust locks still installed, usually resulting in a crash off the end of the runway. Countermeasures were devised, such as long red ribbons attached to the locks to make them more conspicuous on the ground, checklist items requiring a response that the locks had been removed, as well as a pre-takeoff check item that required moving the controls through full travel, which would be impossible with the locks installed. Still aircraft managed to get past the lines of defense and take off with gust locks set (NTSB, 1976, 1978).

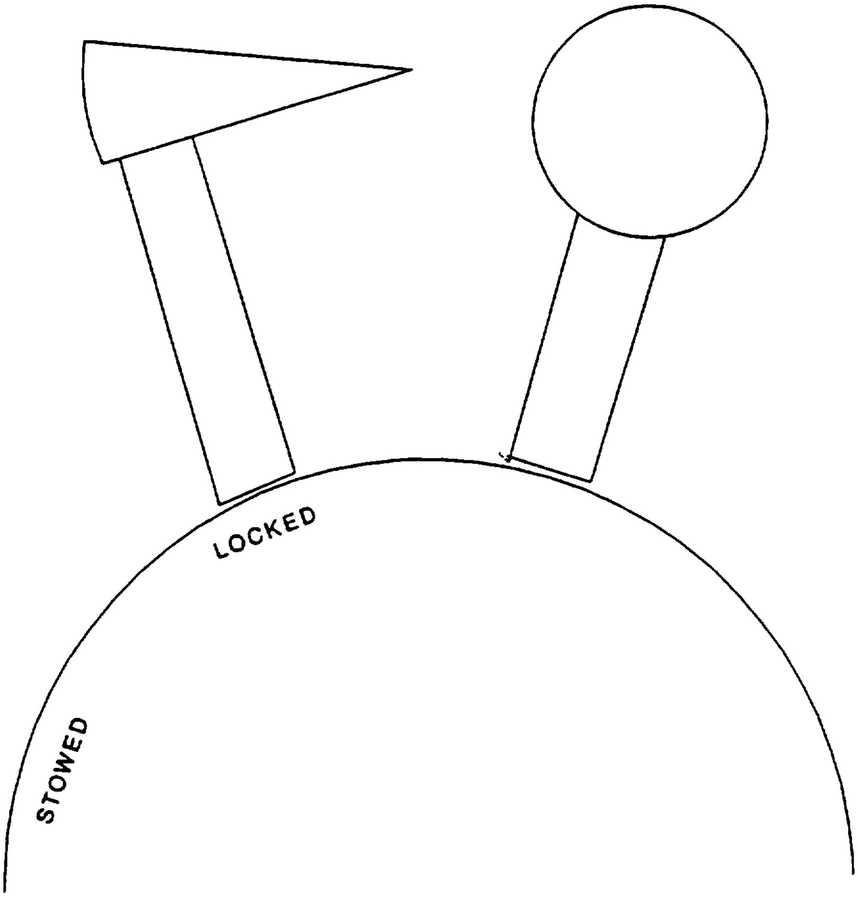


Figure II-2a. Gust lock blocking throttle on C-131 aircraft.

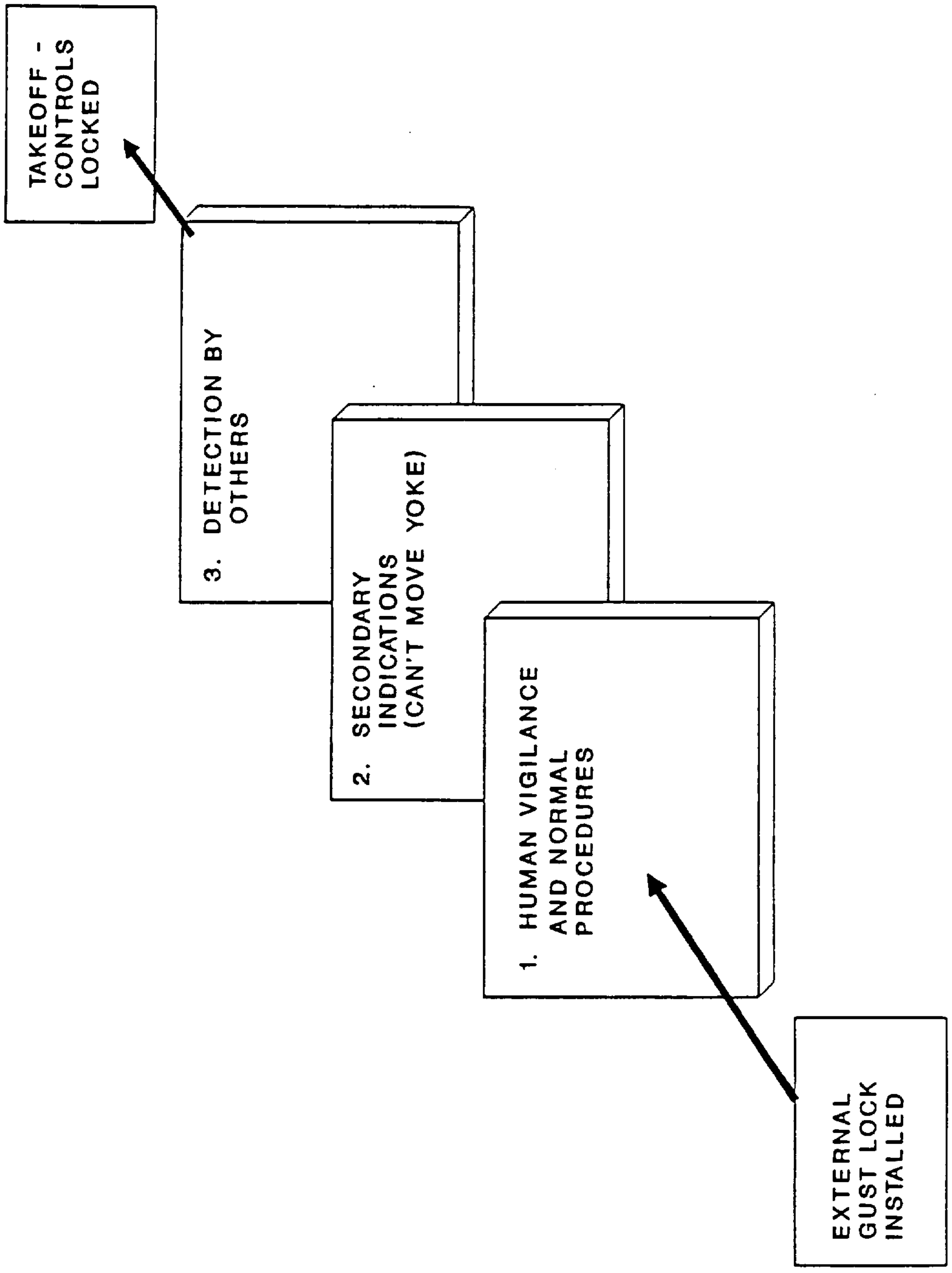


Figure II-2b. Possible lines of defense against taking off with external gust locks installed.

As aircraft grew in size, the control surfaces were often out of reach of the ground crew, and as a result an internal mechanical lock as installed, with the control in the cockpit. The crew would disengage it before taxiing. But the same problem persisted: the crew could still initiate a takeoff with the controls in the locked position.

3) A hardware intervention. In the Convair 240/340/440 series (military designation C-131), designed in the late 1940s, a cockpit control, connected to the control surfaces, replaced the wooden exterior gust locks. The gust lock control was placed on the throttle quadrant forward of the throttles - it was released and moved forward to unlock the control surfaces. To ensure that this would be done prior to takeoff, a simple but ingenious intervention was devised. A small triangular block was attached to the top of the gust lock control, pointing toward the throttle levers (see Figure II-2a). With the controls locked, the block prevented the throttles from being opened past approximately field barometric pressure. In short, the takeoff was mechanically prevented -- the engines simply could not develop anything close to takeoff power with the gust lock handle in place. The intervention was simple, reliable, and economical.

Another example of a hardware intervention is the altitude alerter. Not too many years ago aircraft had no altitude alerter of any kind: the crew depended on short-term memory (STM) to store the target altitude. Since STM is notoriously undependable, the first level of hardware intervention was to add an altitude reminder. The altitude reminder was essentially a digital "scratch pad" into which the crew entered their target altitude; it resided on the panel as a visual reminder, and had no alerting function. This was an improvement over human STM, but was still far from effective in preventing altitude deviations. The next step was make this device an altitude alerter. A certain number of feet (the actual number of feet varying considerably across types and models) prior to the altitude set in the window, an alerting signal is emitted. This was usually an aural tone, but on some models such as the MD-80 it was only a small amber light on the altimeter. The trigger point for the alerting signal has never been standardized, and may vary considerably even within a company's fleet. (See Chapter III, Section A on cockpit standardization)

GUIDELINE NO. 4

Any intervention must be carefully examined to ensure that it does not interfere with other systems, diminish safety elsewhere, or create a problem for the flight crew or other personnel. For example, the early models of the Congressionally mandated emergency locator transmitter (ELT) beacon, which was legislated into service before the

> *industry felt that it had been properly tested, contained batteries that leaked acid and damaged the structure of the aircraft. Another example is the ever-present temptation to add items to the aircraft checklist. Expanding a checklist may decrease the probability that the checklist procedure will be conducted properly (Degani and Wiener, 1990).*
>
> *A final example is the traffic alert/collision avoidance system (TCAS). While the TCAS is undoubtedly a valuable intervention in collision avoidances, especially in protecting again VFR traffic, it does create additional workload and particularly "heads-down" time, which is already recognized as an undesirable by-product of cockpit automation. In such a case, a balance of hazards must be recognized, and secondary interventions may be required.*

The potential value of the altitude alerter may be found in the following two ASRS reports:

> Narrative: We requested and received what for us is a non standard TWR to TWR clearance from ATL to MGM, climb and maintain 4000', expect 10000. When 11 DME from the ATL VORTAC the controller asked us our altitude as we were going through 5000'. Leveled at 5000' and said to the departure controller he thought we had been cleared to 10000'. We had not. The dep controller said to maintain 5000'. We did not hear him give any immediate hdgs or alts to other aircraft so we thought there was no immediate conflict. We subsequently climbed to 10000' and continued the flight w/o incident. My captain had just upgraded from F/O on our company's Part 121 aircraft, which had an altitude alerter installed. Evidently he had subconsciously become dependent on that device because all he has to do as the PF is maintain HDG, altitude and airspeed. I was heads down in the cockpit writing down the dep times in the utilization log instead of monitoring my captain's performance. This is my second altitude bust in 10 months with this commuter, and both times the captain was flying. Both times I was heads down doing paperwork required by the company, or talking to the company on the second radio. From now on, I will only talk to the company once we are at cruising alt. I was an fighter weapons system officer for 10 years and never had an altitude bust. I have been with this commuter for 10 months and I've had 2! If the capts I fly with aren't going to concentrate on flying and stop being so blase about the whole thing, it is destined to happen again. I am frustrated. I don't want to be violated and become unemployable by a major airline. I thought after the first altitude bust it would never happen again, but it did and I allowed myself to be distracted just like the first time. The bottom line is that I have to watch these fallible human

> beings like a hawk. Supplemental info from ASRS No. 144128: I was climbing to 10000' as I thought was had been cleared. This type of occurrence could, I think, be almost eliminated by the mandatory installation of an altitude alerting sys in commuter aircraft operating under FAR 135. (ASRS No. 143963)

> Narrative: I departed DEA on a routine scheduled flight to YKM. We were clred to 5000' and inadvertently went through this altitude by 2000'. My F/O was flying at the time. I was trying to ident a radar return for weather avoidance. I gave him the 1000' call required in our ops specs but he was also involved in the radar tracking of a thunderstorm we were trying to avoid. Consequently, we flew right through our assigned alt. The aircraft we fly are not equipped with altitude alerters which would have prevented this from happening. Recommend that aircraft like these require alerters to prevent this, which will continue to occur because we are only human. It might just save lives. (ASRS No. 145134)

In conclusion, hardware interventions are probably the easiest to evaluate. Regulatory intervention such as the sterile cockpit rule is far more difficult. We further note that an altitude alerter, even correctly set, is no guarantee of a successful leveloff. The ASRS database is replete with examples of crews that failed to hear (process) the aural alert, and busted an altitude.

Intervention Through Documentation

In this report we shall use the term "documentation" to refer a variety of devices employed by the crews, including manuals, checklists, performance charts, flight plans, weather reports, and documents and paperwork of all sorts.

This definition of documentation is consistent with Edwards (1988, page 11), use of the term "software" in his well known SHEL model (software, hardware, environment, and liveware) as "...comprising rules, regulations, laws, orders, standard operating procedures, customs, practices, and habits which govern the manner in which the system operates and in which the information within it is organized. This is software, much - but not all - of which will be set down in a collection of documents". The present author prefers to use the term "documentation" rather than "software," due to the latter's customary usage meaning computer programs.

<u>An example of intervention through computer software</u>. In modern "glass cockpit" aircraft, a vast amount of information is processed and stored in the flight management computer (FMC). This information can be displayed to the crew in text, numeric, and graphic form on selected pages of the control-display unit (CDU), the glass instrument panels, and elsewhere, Some of the information is "automatically" displayed, requiring no request from the crew (e.g. the wind vector on the navigation display); other information is available in the FMC on demand through pilot selection of the correct CDU page. The display of certain valuable information, such as suitable emergency airfields, is switch selectable. Finally, if the FMC detects an abnormal computer condition, a brief message can be displayed in the "scratch pad" line of the CDU, and the pilot is alerted on two other displays that an FMC message awaits him. An example would be a request for a waypoint "not in the database."

GUIDELINE NO. 5

> *If the intervention strategy involves displays, the information should be easily interpretable. For example, the early models of the ground proximity warning system (GPWS) often created confusion as to which trigger mode was responsible for the alarm. Later models of the GPWS improved the situation by identifying alert modes.*

<u>Intervention Through Linguistic Procedures</u>

Miscommunication between aircrews and ATC controllers has long recognized as a leading source of human error (see Billings and Cheaney, 1981). It has also been an area rich in potential for interventions. Examples are the restricted or contrived lexicon (e.g. the phrase "say again" hails from military communications, where it was mandated in order to avoid confusing the words "repeat" and "retreat"); a phonetic alphabet ("alpha", "bravo", etc.); and stylized pronunciations (e.g., "nine-er" due to the confusion of the spoken words "nine" and "five"). Prince and Salas (1993) discuss the need for a standard vocabulary during military operations.

As a result of the tragic ground collision between two B-747s at Tenerife in 1977 (Spanish Ministry of Transport and Communications, 1978), blamed largely on miscommunications between the tower and the two aircraft, the FAA encouraged controllers to restrict the word "cleared" to two circumstances: "cleared to takeoff" and "cleared to land", although other uses of the word is not prohibited (<u>ATC Handbook (FAA 7110.65F)</u>. In the past a pilot might be <u>cleared</u> to start engines, <u>cleared</u> to push back, or <u>cleared</u> to cross a runway. Now the controller typically says, "cross runway 27", and "pushback approved", reserving the word "cleared" for its most flight-critical use.

Likewise, the term "cleared" was dropped from the "position and hold" instruction for the aircraft first in line for takeoff. Previously controllers said "[aircraft identifier] cleared to line up and hold." Because an aircraft in number-one position at the stop line was anticipating takeoff clearance, there were occasional incidents where a takeoff was initiated at this command. Now the controller simply instructs the number-one aircraft, "position and hold" (ATC Handbook 7110.65F).

The need for linguistic intervention never ends, as trouble can appear in unlikely places. For example, pilots reading back altimeter settings often abbreviate by omitting the first digit from the number of inches of barometric pressure. For example, 29.97 (in. Hg.) is read back "niner niner seven". Since baro settings are given in millibars in many parts of the world, varying above and below the standard value of 1013, the readback "niner niner seven" above might be interpreted reasonably but inaccurately as 997 millibars. The obvious intervention strategy would be to require full readback of all four digits when working in inches.

A long-range intervention and contribution to safety would be to accept the more common (in aviation) English system of measurement, eliminating meters, kilometers, and millibars once and for all. Whether English or metric forms should both be used in aviation of course is argumentative, and raises sensitive cultural issues. At this time the English system clearly prevails, as does the English language. In some parts of the world units are mixed: ATC instructions and instrumentation are in feet, weather is reported in meters. In 1983 an Air Canada B-767 ran out of fuel and made a successful dead-stick landing on a small obscure airfield (Ott, 1983). The fuel instrumentation and calculations of most of the planes in the fleet were in pounds; this particular plane was instrumented in metric (kilograms of fuel). An error in conversion occurred, that resulted in insufficient fuel on board by a factor of roughly 2.2, the conversion constant between kilos and pounds.

Intervention By Hardware Retrofit and Redesign

On June 30, 1987, a Delta Air Lines 767 departed Los Angeles International to the west, bound for Cincinnati (Preble, 1987). At approximately 1000 feet above the Pacific, the crew received an EICAS advisory message that the right electronic engine control (EEC) was inoperative. At approximately 1600 feet the captain dealt with the message by retarding the right throttle and reaching for the EEC switch. Instead he grasped the fuel control switch, shutting down the right engine. He then did the same thing to the left engine. The captain realized his error and placed the fuel control switches back on, selected flight ignition, and restarted both engines. During the power loss, the aircraft descended to approximately 500 feet above the Pacific Ocean. The climb was resumed and they flew to their destination without further incident.

Following this incident, the FAA directed the airlines to relocate the EEC switches to the upper left panel, over the captain's position. This was probably an effective intervention, but others were possible. The captain later admitted that he never called for the checklist when the EEC message appeared, and never told the first officer what he was doing. Ironically, no immediate action was required in response to the EICAS message.

As a result of this and other incidents related to crew coordination that occurred the same year, Delta intervened aggressively by developing a crew resource management (CRM) program for its 7000 pilots (Byrnes and Black, 1993). Checklist discipline was stressed at all levels of training. Procedures and checklists were later redesigned. The role of CRM training as an intervention strategy will be discussed elsewhere in this report. A more complete discussion of CRM can be found in various chapters in Wiener, Kanki, and Helmreich, 1993). The effect of both the absence and presence of CRM training in certain accidents investigated by the NTSB is discussed by Kayten (1993). (Note that CRM also stands for cockpit resource management).

GUIDELINE NO. 6

> *Any design, hardware or software, should conform to accepted standards of human factors. The designer of the intervention strategy should be mindful of published design guidelines, whether they are considered official or not [see Wiener and Curry, 1980 for automation guidelines (reprinted in Appendix 2 of this report); Degani and Wiener, 1990 for checklist guidelines (Appendix 3); Williges, Williges, and Fainter (1988) for guidelines for human-computer interaction in aviation), and Wickens (1984) for general guidelines for automated systems]*

Difficult Interventions

Intervention strategies (which meet the guidelines expressed in Appendix 1) are not always apparent; remedies may be elusive. One example is runway incursions and ground collisions, a recognized weak spot in the air safety mosaic, where the lines of defense can easily be breached. In December 1990, a collision occurred on the ground at Detroit Metropolitan Airport when a Northwest DC-9 crew became disoriented taxiing in low visibility and entered a runway in front of a company B-727 that was taking off (NTSB, 1991; Fotos, 1991). Only two months later a collision between a landing USAir B-737 and a Skywest Fairchild Metroliner occurred in Los Angeles (see Appendix 1, Guideline No. 7) (Dornheim, 1991).

Ground collisions present an extraordinarily difficult area for intervention. They are somewhat resistant to technology. Those technologies that could be implemented (e.g. stop lights at the runway threshold) probably violate the guidelines contained in this report, since they may themselves provide an opportunity for human error. The report below is instructive.

> Narrative: on taxi in, last leg of a 4 day trip, I contacted ground control and reported clear of 10. Ground said to hold short of 22 at Charlie. I read back same. During taxi the captain said "after landing," meaning complete the after landing checklist. I completed the checklist, called operations and advised them we were on the ground (a required call) and then called Ramp Control to confirm our gate. I looked back up at the captain (my eyes were down and right toward the radio control panel) and said, "gate is confirmed and we are still to hold short of 22! I reminded him again because I noticed we were not slowing down. He acknowledged me with a nod. I once again diverted my attention to the radio control panel (down and right), maybe for 3 or 4 secs. When I looked up, Ground Control said, "Aircraft XX, hold short of 22." At that time we were within 5′ of RWY 22. The captain slammed on the brakes. A small twin engine plane crossed directly in front of us on a takeoff roll. Had this been a larger aircraft with a greater wing span, there would have been contact! Many times captains bellow out commands. Almost immediately, "after landing checklist," meaning, "I want this right now!" During this approximately 1 minute taxi prior to reaching RWY 22, I was out of the loop three times--solely with non-safety related communications and a checklist that could easily and should have been accomplished only after clearance and on the ramp. I had to leave RND freq twice and read the after landing checklist. Our abrupt stop was beyond the hold short line. If RND Control had not told us again, our 2 aft would have met at the intersection of RWY 22 and taxiway Charlie. F/O's need to remain in the loop and not be involved in non-safety related communications until in a safe zone. (ASRS No. 145483)

Many post-accident suggestions for interventions involve extreme limitations on ATC, which might reduce the already critically limited runway capacities at major airports, creating a potential safety problem in the process. The example cited in Guideline No. 7 speaks to this point.

GUIDELINE NO. 7

> *All interventions should be examined for any adverse effects on air traffic control (ATC). For example, shortly after the accident at Los Angeles where a USAir B-737 landed on top of a Skywest Metroliner awaiting release for takeoff on Runway 24L, it was suggested that towers discontinue their practice of allowing an aircraft to "line up and hold" on an active runway, remaining instead short of the runway until cleared for takeoff. To do so would impose immense delays on the system, for a questionable safety benefit. After reconsideration, this proposal was dropped.*

This is not to say that interventions, some of them quite low on the technology scale, could not improve the situation. These would include standardization of signs and markings, improved maintenance of signs, markings, lighting, and paint stripes, and better guidance devices for very low visibility conditions. A speaker at an Air Transport Association (ATA) meeting in San Diego in May 1991, drew unrestrained applause when he suggested that the situation at most airports could be improved by "a few buckets of paint." The same month the Air Line Pilot, a publication of ALPA, published an article entitled, "A can of paint and a brush" on the same topic (Steenblik, 1991).

C. IS THERE AN INTERVENTION STRATEGY FOR EVERY PROBLEM?

The problem of the unbounded use of the term "intervention strategy" has already been raised. Is everything that is done, every design change, every measure that is taken in the name of safety, every new installation of hardware, or documentation, or policy, regulation, or practice, an intervention?

This question does not have an easy answer. Certainly we can find interventions that have little or nothing to do with safety or human error. These are measures which may improve the operation economically (e.g. fuel conservation; public address announcements to the cabin during flight, etc.). From there we might consider areas that improve the smooth flow of information on the flight deck: minor paperwork changes, ACARS data link for routine company traffic, and elimination or relocation of company-required radio calls. These are interventions -- they are brought to the cockpit to solve a perceived problem, and it is not easy to say which are safety related and which are not. Clearly, most routine PA announcements to the passengers are not. However, measures which improve information flow may also reduce workload, and, in most cases, workload reduction can be linked to safety.

Some interventions are difficult to classify. For example, the

Department of Transportation has recently promulgated an elaborate, controversial, and costly intervention strategy aimed at detecting pilots who take dangerous drugs (DiNunno, 1989). This has angered the pilot community and raised certain constitutional questions, as well as less legalistic questions of fair play. Above all, the use of random drug testing calls into question whether the resources expended by this program are justified by the magnitude of the problem.

GUIDELINE NO. 8

> *Preferably the intervention strategy should be non-punitive. It should not place the crew at an added risk of violation or other punitive action.*

Likewise we must ask if there is an intervention for everything, for every form of human error? Perhaps the question is better stated: for every human factors problem, is there an intervention strategy that meets the requirements of Appendix 1?

The problems of runway and taxiway incursions and the hazard of ground collisions has already been cited as an example of difficult areas for intervention. Others are perhaps even more difficult, due to their unpredictability and low probability. For example, there is a remote possibility of a psychiatric episode occurring to a crew member, which could endanger the aircraft. It has happened before (Dahlby, 1982). Preemptive intervention strategies would include psychiatric screening prior to hiring, and periodic reevaluation of flight crews, perhaps in connection with their semi-annual physicals. Prediction of an sudden episode in an individual whose psychiatric condition is well masked, or not previously existent, is extremely difficult. Intervention at the time of the episode would require immediate action on the part of fellow crew member(s), and may be particularly difficult in a two-pilot cockpit.

One can conceive of other difficult areas for intervention; errors of judgment (e.g. which direction to go to circumnavigate a thunderstorm; whether to accept a flawed though legal aircraft); highly unacceptable behavior such as deliberate, inappropriate silencing of warning and alerting systems; errors of perception and intent (e.g. wrong airport or wrong runway landings, a problem that has had a remarkable persistence). Note that the last example is one of those errors where Line of Defense No. 5 (detection by persons external to the crew) may provide some protection. The brief ASRS report below illustrates a helping hand from outside the cockpit.

Narrative: during ILS approach to RWY 16R TWR advised of a

> low altitude alert, just as I was breaking out of the clouds. I scanned everything only to find an "off" flag on the glide slope. I leveled off and only began descent when the RWY and VASI became visible. There was much turbulence and rain and I never noticed the problem. I landed uneventfully. The next time it appears I am flying a perfect ILS glide slope in rain and turbulence, I will start looking around. (ASRS No. 143781)

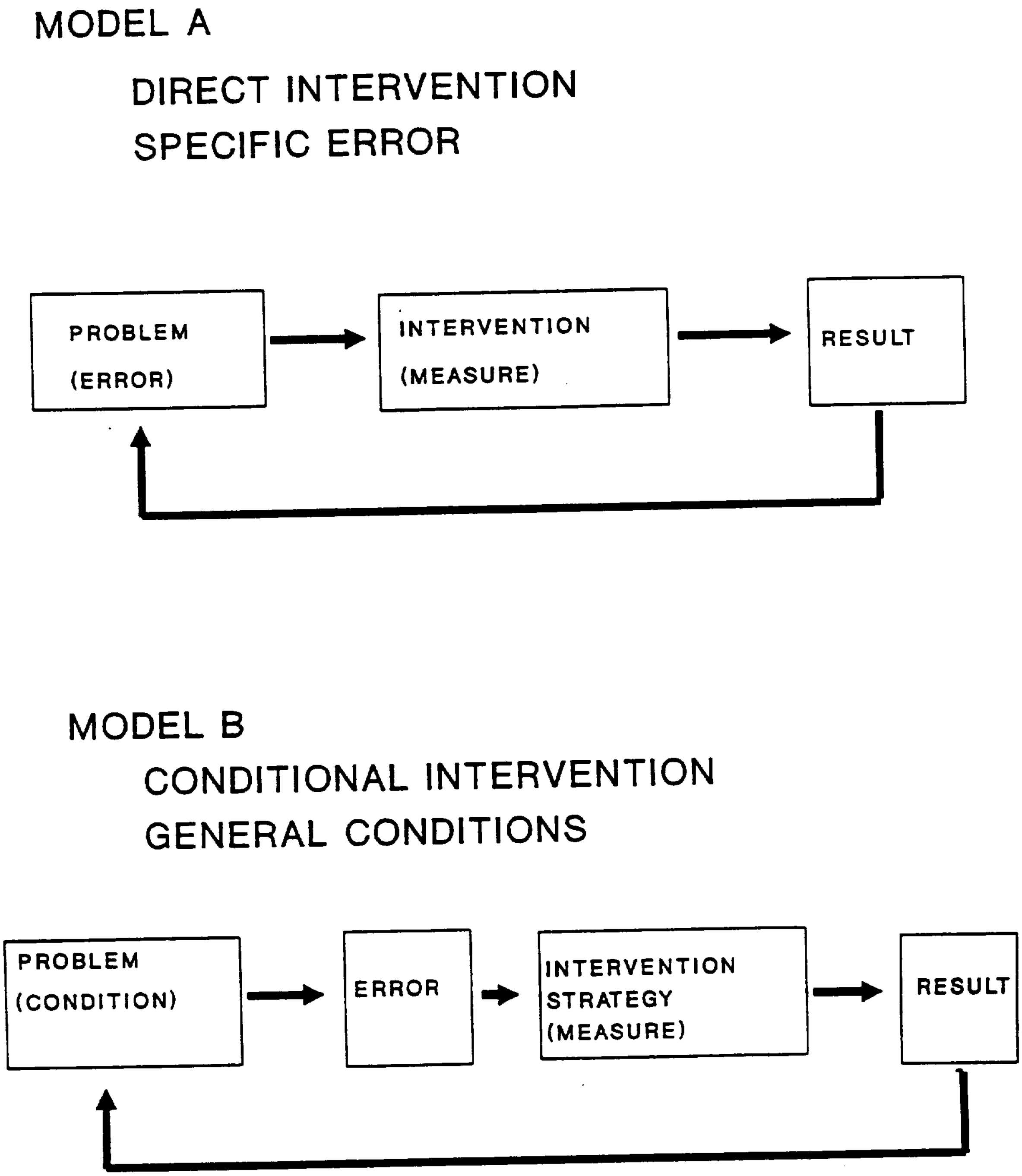
Clearly intervention strategies are not available for every possible form of human error. Some problems may never invite a reasonable intervention; others may have to await the development of some presently unknown or not yet imagined technology. We will restrict the term "intervention strategy" to interventions designed to prevent specific classes or types of human error, not just to generally improve flight safety. Thus we would not call purchasing a new simulator for pilot training an intervention strategy for human error, although the resulting training might be preventive.

In the two chapters that follow, we shall examine various intervention strategies, and errors they were designed to prevent, and comment on the effectiveness of these measures. These chapters are separated with respect to traditional and advanced technologies. In some areas, fairly specific human errors will be discussed. In other areas, such as training, the errors are more non-specific. For example, CRM training is aimed at a constellation of behaviors related to crew coordination, leadership, advocacy, and communication (Wiener, 1989b, pp. 119).

D. TWO MODELS OF INTERVENTION

Two models of intervention strategies are proposed. They differ only in the degree of problem specificity that they are designed to attack. In the first (Model A), the problem is well defined and highly confined (e.g. the error of initiating a takeoff with the control surfaces locked), and the intervention is specific (Model A). The sequence is P-I-R (Problem-Intervention-Result). A specific solution is sought for a specific problem.

In Model B interventions, the problem is broad-scale (e.g. distraction in the cockpit), or is a host of problems, and the intervention is therefore non-specific. A good example is CRM training. This is a broad-scale effort to intervene in a broad-scale, less well defined problem (lack of leadership, poor teamwork, lack of crew coordination). Each of these is not a human error per se, but something that might lead to one (e.g. poor cockpit coordination may result in mismatching altimeter settings). The models are displayed graphically below.



MODEL A
DIRECT INTERVENTION
SPECIFIC ERROR

MODEL B
CONDITIONAL INTERVENTION
GENERAL CONDITIONS

Figure II-3. Two models of intervention.

III. INTERVENTION STRATEGIES: TRADITIONAL TECHNOLOGIES

A. HARDWARE

In this section we shall consider a wide variety of intervention strategies centering around traditional hardware. This is the home court of human factors engineering. The distinction implied by the word "traditional" is to set these interventions apart from those involving advanced technologies found on modern aircraft, and from potentially helpful computer technologies (AI) not yet implemented in civil aircraft. We note that some advanced technologies have been implemented in military aircraft, and these may have potential for civil aviation. Military operations will be the proving ground.

The definition of "traditional" as used here is somewhat arbitrary. For our purposes, the term will mean such aircraft as the B-727, DC-8 and DC-9, and older models of the B-737 and A-300, not equipped with an advanced flight management computer (FMC) such as that found in the glass cockpit aircraft (B-747-400, B-757/767, A-310/320, and A-300-600, F-100, MD-88, etc.). Aircraft such as RVAV-equipped MD-80s, DC-10s, B-747s and L-1011s fall into the boundary land of cockpit automation. Some carriers have equipped models of the L-1011 with an FMC similar to that found in a glass cockpit, with similar capability in the lateral navigation mode, but comparatively limited vertical navigation capability. Also there are currently programs to retrofit traditional cockpits (e.g. DC-8, C-130, B-727) with EFIS instrumentation.

General Human Factors Engineering

Here we aggregate under one heading a vast amount of information and technique with a history of over 50 years. (For an early book on the topic, see Chapanis, Garner, and Morgan, 1949.) Human factors includes the design of controls, displays, codes, and information, communication, and work place layout, just to mention a few. Much of the early work aimed at preventing human error is now disparagingly described by many as "knobs and dials." The interesting thing about knobs and dials is that with all of the sophistication of human factors today, and the contributions toward preventing the types of errors of the past, these errors never seem to completely vanish. The inadvertent shutdown of both engines on a B-767 has been previously mentioned (Preble, 1987). Another example is the shutdown of the wrong engine following an auto-feather on takeoff of a two-engine Nord 262 at Los Angeles (NTSB, 1979). The following report illustrates "knobs and dials" problems in fuel management.

> Narrative: one engine was burning more fuel than the other. So we tried crossfeeding fuel to correct the imbalance. We were distracted with other duties and inadvertently crossfed too long, so we were not able to correct the fuel imbalance as much as desired before landing. The indicator light for crossfeed on this airplane is located in a position on the cockpit panel that is down low and difficult to see. I consider this a design defect. It should be placed at eye level to make it easier for pilots to monitor the crossfeed status. (ASRS No. 121913)

Keyboards, which are gaining increased prominence in cockpits due to the growth of digital systems, are a rich source of human error. As Wiener (1989a) pointed out, after five decades of human factors research and application, keyboard layouts are still not standardized: two or possibly three keyboards of different design can be found in the same cockpit. The vulnerability of aircraft to keyboard errors has been well established (Wiener and Curry, 1980); they have been responsible for some of our more dramatic accidents in recent years (Wiener, 1987a, 1988). Furthermore, data entry via keyboard into a digital system creates the possibility of latent errors which may lie dormant in the system for hours until they finally become active. An example would be lateral navigation waypoints. A discussion of latent errors can be found in Reason (1990). Reason likens such phenomena in human-machine systems to the biological concept of "resident pathogens" - pathological conditions in living beings that may dwell harmlessly until they mature or become triggered, resulting in serious illness.

The problems of crew interaction with keyboard data entry can be seen in the following ASRS report.

> Narrative: while preparing for departure, the captain loaded incorrect position coordinates in the IRS pos. Instead of a correct position of approximately N 50 deg 15 mins, E 00 deg 01 mins, he loaded N 50 deg 15 mins W 00 deg 01 mins. Contributing factors. Rushing to beat a noise curfew; short layover; lack of crew coordination and cross check. This resulted in a NAV map shift of approximately 30 mi. The problem was discovered on initial departure when radar told us we weren't proceeding on the proper course. The problem was discovered quickly and no conflict occurred. We switched to manual nav. However, we couldn't continue our ocean crossing and diverted to Shannon, Ireland, where we made an overweight landing. Human performance considerations: although the captain was supposed to be giving me a nav check he rapidly and without asking for verification programmed the computers himself. We had sufficient time to do the job right but didn't take it. I should have cross

> checked our position, but didn't. (It isn't in our nav checklist to do so). (ASRS No. 150785)

More will be said about the management of such errors in the section on advanced technology. As more highly automated aircraft join airline fleets, keyboards will probably play an increasing role in incidents, accidents, and violations, at least until a substitute for the traditional keyboard can be found. Other devices, including the computer "mouse" are being examined. Boeing plans to include a control employing the pilot's finger on a pad as a pointing device in the B-777. The pointer would give the pilot mouse-like control of the electronic checklist, the electronic library system (when implemented), and some navigational functions (Scott, 1991). However, the practicality of the mouse as an input device has not yet been tested in line operations. Even if successful, it would be premature to forecast an early demise of the keyboard as the primary input device to airborne computers. Keyboards are flexible, reliable, inexpensive, familiar to the user. They are also highly vulnerable to "finger error."

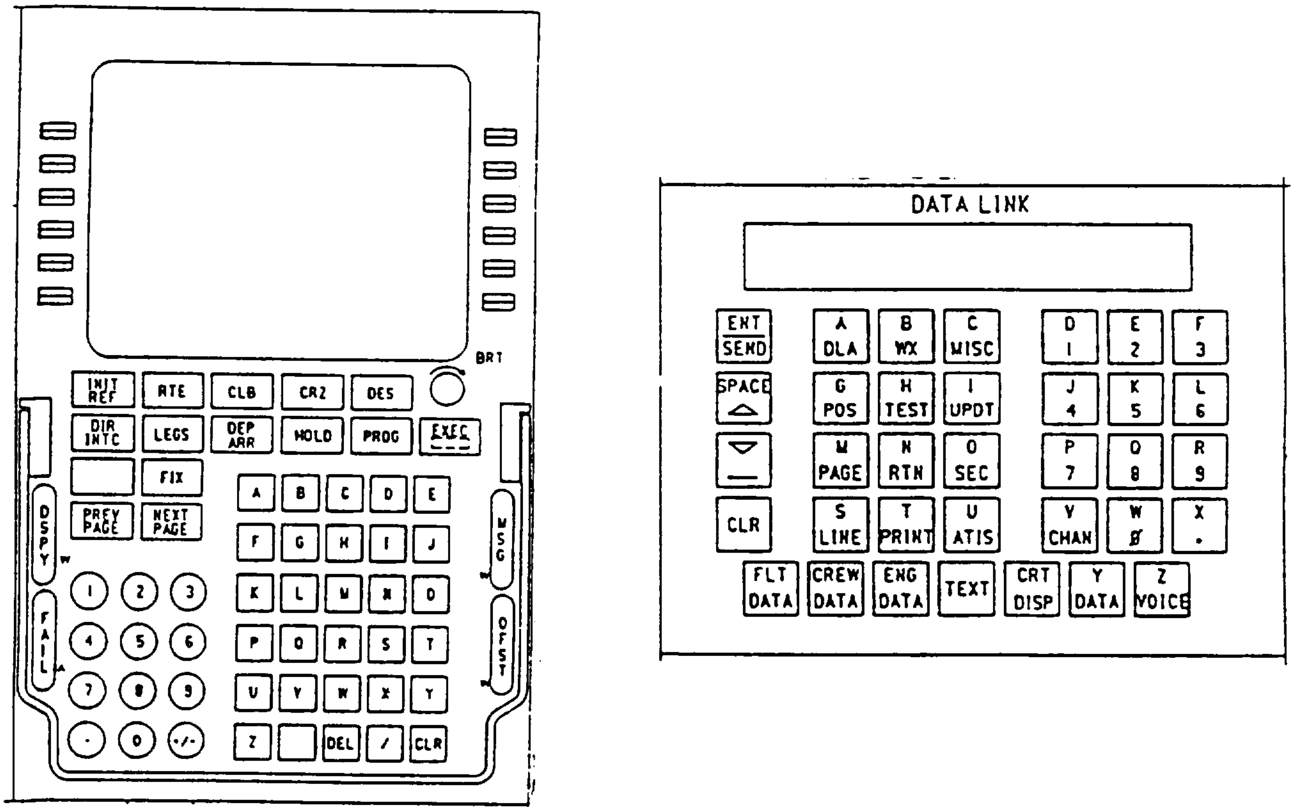


Figure III-1. Two keypad layouts.

Examples of interventions through design, as well as design-induced errors, are endless (see Wiener, 1987b, and almost any textbook on human factors). Cases where errors were induced by advanced automatic systems can be found in Norman, 1983; Wiener and Curry, 1980; and Wiener, 1988a.

Much of the improvement in aviation safety since the dawn of human factors engineering during World War II can be attributed to hardware interventions, which range from simple to complex. The example of the mechanical throttle stop on the gust lock control of the Convair has already been mentioned. Self-illuminating fuel shutoff and engine fire extinguisher handles guide the pilot to the correct handle to be pulled in the event of an engine fire, one of the rare instances where the same device is both control and display The (virtual) replacement of the three-hand altimeter has eliminated the possibility of 10,000 foot errors, although the ideal, error-resistant altimeter face has yet to be designed. The following case speaks to the misinterpretation of the three-hand altimeter.

> Narrative: the appropriate checklists were completed and we took off for Akron, Ohio. We were handed off to Cleveland Center and instructed to climb to 9000' MSL. I contacted Cleveland Center and started out of 8300' MSL for 9000 MSL. The controller said "Cleveland altimeter 29.86, say again alt". At this time I stated Roger 29.86 and level 9000' MSL. He said that he showed 10000 MSL. I said 29.86 and I show 9000' MSL exactly. At this time I glanced at my F/O's altimeter and his said 10000' MSL. On closer inspection of mine I saw the baro pressure set at 28.86 instead of 29.86. The altimeter for some reason was set 1000' high. No maintenance was performed on it and neither me nor my F/O caught it. My F/O also missed his required call of 8000' for 9000'. Had he did this the problem may not have occurred. We have old style 3-hand altimeters installed in the airplanes. Usually setting the instrument on the ground I check the 100' hand for field elevation. I now must also include the 1000' hand. In the checklist we set the altimeter, say the numbers and cross check each other's. Even this operation didn't catch the discrepancy. (ASRS No. 61621)

Regrettably, many of the interventions in hardware design have been implemented after-the-fact, in response to some accident. But happily designers have developed a well-honed awareness concerning error-resistant design, and thus, with each advancing decade, cockpits have increasingly reflected the experiences of the past, and the growing sophistication of human factors engineering (see Sexton, 1988).

What is more regrettable is that error analysis is not a certification requirement. Under Part 25 of the Federal Aviation Regulations (FARs), the only place where a systematic human factors analysis is required is in the area of workload. And this is for the limited purpose of determining whether the workload is excessive for the proposed crew size. Aircraft designers have developed a high degree of sophistication in applying failure analyses techniques (e.g. failure mode and effects analysis -- FMEA) to proposed designs for aircraft structures and components (Miller, 1988). What is obviously needed is the development of similar techniques for evaluating designs for their human error potential, perhaps in the manner that Swain and Guttman (1983) have done in the nuclear industry. From such analyses, interventions could flow before the cockpit design is hardened. One major manufacturer appointed "what if" teams in order to detect potential problems.

GUIDELINE NO. 9

> *The intervention strategy should be economically feasible and otherwise acceptable to management (e.g. minimize contractual implications). It should likewise not impose a cost elsewhere in the overall system (see also No. 7)*

Simplification versus Automation

In the last two decades, with the rapid growth in microprocessor technology, there has been a temptation on the part of some designers to build very complex systems based on the rationale that they could operate automatically. There are two fallacies in this argument. First, almost no major system on an aircraft truly operates fully automatically: the systems must be initialized or set up by the human, decisions about operating modes must be made, and then the systems must be monitored by the humans for obvious reasons. Second, in the event of the failure of automation, it falls to the human to operate the system. This responsibility cannot be avoided or designed away. If the complexity of the systems is unbridled, then the crew may not be able to perform their duties effectively, nor take over in the event of equipment failure.

In response, many design engineers with human factors sophistication have recognized that simplification offers an alternative to automation. If the system can be simplified, there may be no need for complex automation, and the same goal can be achieved without placing the human into a potentially hazardous position. An example is the fuel system on a multi-engine aircraft. Those favoring automation would find no problem with creating a complex tank-to-tank and tank-to-engine relationship, as long as its management could be automated. If, for example, a fuel imbalance were created, automatic devices would detect this, determine a remedy, open the required transfer valves and turn on the appropriate pumps to restore the proper balance. No human intervention would be required.

This example represents a philosophical difference between two major aircraft manufacturers. The Douglas approach, as exemplified by the MD-11, has been to remove the pilot from the loop and turn certain functions over to sophisticated automation (Scott, 1992). Compensation is automatic - the systems do not ask the crew's approval. Boeing's approach is to never bypass the crew: sophisticated devices will inform the crew of a need, and in some cases a step-by-step procedure, but in the end it is the crew that must authorize and conduct the procedure (O'Lone, 1992). Boeing is a strong advocate of simplification before automation. Their designers would look to a less complex relationship. An example would be fewer tanks to feed the engines, creating fewer tank-to-tank and tank-to-engine requirements, requiring less management by the crew, and fewer opportunities for human error (Fadden and Weener, 1984; Aviation Week and Space Technology [AWST], 1988). The report below serves as an example of fuel management difficulties.

> Narrative: fuel crossfeed inadvertently left on after the preflight inspection during a crew change. A fuel imbalance resulted (approximately 3000 pounds) during the short flight from LAX to LAS, which was 37 minutes. The imbalance was first noticed when I disconnected the autopilot during descent for the approach. The captain and I were surprised that so much fuel could feed from the left side when pressure on both left and right should be equal. Given the high tank loading on such a short flight, perhaps some sort of warning light is appropriate to warn the pilots when an imbalance is occurring. No such light presently exists on the aircraft. Every military aircraft I've flown has fuel imbalance caution lights. Why not on civilian aircraft where the effects on weight and balance are more critical? (ASRS No. 115002)

The potential difficulty with over-automation of systems is that the crew simply cannot be aware of the state of the system at all times. Norman (1990) discussed the hazards of automatic devices silently remedying a situation about which the crew was unaware. The difficulty lies in the lack of awareness on the part of the crew that an abnormal condition exists, if the on-board computers are compensating without informing the crew. Efficient automatic compensation for abnormal events and conditions sounds attractive, but there is always a limit to the machine's capacity to compensate. When that limit is reached, something drastic may happen, as in the well-known case of the Air China 747 (NTSB, 1986; Wiener, 1988a). The crew may have no awareness of either the problem or the compensation until the automation reaches the limits of its authority.

As Norman stressed, the problem in highly automated devices is not automation per se, but the lack of feedback. A design principle is apparent here: simplify any system to the extent possible; then and only then turn to automation if it is still needed. When automation is compensating for some worsening condition, the crew must be informed.

Hardware Standardization

In this section we shall consider the standardization of cockpit hardware, both within models and fleets of derivative models, and across fleets. For a similar discussion regarding flight-deck procedures, see Degani and Wiener (in preparation). Standardization with respect to procedures, documentation, and training will be revisited in the section below on procedures. [For a clarification of the two meanings of the term "fleet", see Note No. 3, Chapter VII].

GUIDELINE NO. 10

> *Wherever possible, the intervention strategy should be common to all models within a fleet and across fleets within the same company. When an intervention is recommended or specified by the manufacturer, or imposed by agencies outside of a company (e.g. manufacturer, government) it should be common to all operators of the equipment, wherever possible.*

Between fleets. Between-fleet standardization of hardware is considered desirable in order to reduce training and maintenance costs, as well as to prevent human error that may occur as a result of the pilots moving from one aircraft to another. During periods of rapid expansion of aircraft inventories and pilot personnel, as the airline industry in the U.S. and elsewhere enjoyed in the late 1980's, there is frequent movement between aircraft as pilots bid for more lucrative assignments, more modern aircraft, or desirable bases. Some contracts limit the rapidity with which pilots may bid a new seat, others do not.

Most cockpit hardware is peculiar to the type of aircraft. However, certain cockpit hardware could be common to most or all models operated by a carrier, for example radios, flight directors, certain displays, area navigation equipment, weather radar, etc. Other examples would be devices added after the original manufacture (e.g. TCAS, ACARS). Where the carrier has the opportunity to purchase these add-on units, a common model will most likely be chosen, for all of the reasons stated above.

Where differences already exist between fleets, the airline may intervene by standardizing throughout the airline. For example, some airlines have invested in a common airline-wide model of the flight director.

Between-fleet standardization, if it involves retrofit rather than new equipment purchase, will be extremely costly, and its safety benefits may be modest compared to within-fleet standardization. Nonetheless, when pilots move rapidly through the seats of various aircraft, or complete training for one aircraft and then return to another while awaiting assignment to the new aircraft, between-fleet standardization of cockpit hardware deserves inclusion in the list of intervention strategies.

<u>Within fleets</u>. Far more critical is within-fleet standardization. Long before the Airline Deregulation Act of 1978, carriers purchased aircraft from each other, thus generating mixed configurations within fleets. With the coming of deregulation, the pace of mergers and acquisitions, as well as used equipment purchases and leases, accelerated rapidly This produced fleets of traditional aircraft, such as B-727s, 737s, and DC-9s, that varied greatly with respect to cockpit configuration. These differences included different displays (e.g. various models of flight directors), warning and alerting systems (e.g. a host of altitude warning systems with various trigger points), every imaginable engine configuration, controls in different locations, various directions of movement of switches, and various operating limitations. One carrier, which had been through a number of mergers and acquisitions of other DC-9 operators, had eight different models or locations of altitude alerters. They later invested a very considerable sum in order to standardize the cockpits of their DC-9 fleet. Within fleet standardization is considered a high priority item by the line pilots and their safety committees.

In one rather strange example, a carrier with a large DC-9 fleet had seven DC-9-10 aircraft which it had purchased from another carrier. These aircraft had a 215-knot speed restriction for gear-down flight due to a modified gear door. For the rest of the fleet, it was 270 knots. These were known as the "215 aircraft." Various informal "placards" appeared to remind the pilot that he/she was flying a 215 model. In one aircraft in which the author jumpseated, someone had written on the instrument panel, in inch-high letters, "CCXV".

The most extreme case of non-standardization within a fleet that the author has seen was brought to his attention by ALPA when a U.S. carrier considered buying a small number of DC-9s from a European carrier. The European DC-9s had the slow-fast and the glide slope deviation indicators reversed with respect to their position on the ADI compared to the rest of the purchaser's fleet. The pilots' union took an understandably strong stand against flying the "mixed" instrumentation.

We have already acknowledged that within-fleet standardization of cockpit hardware is an extremely costly. But failure to do so leaves standing in the cockpit a host of potential trip wires for human error, not to mention the increased cost of training, maintenance, and documentation. In addition to the other benefits of common hardware configurations in a given fleet is the fact that only through standardization can the company's simulator(s) faithfully represent every aircraft in the fleet. It is distracting for an instructor to have to remind students that the simulator is different from various models in the fleet. It is easy for one to forget that the purpose of a simulator is to simulate.

> Narrative: during climb out the indicated airspeed registered in excess of 250 kts by about 2000' below 10000' MSL. The captain occupying the left seat was new to the aircraft, the EWR departure area and this was his first trip in this type aircraft. Additionally, the autoplt was giving very slow responses to pitch commands which in my opinion was the primary reason for the excess airspd. The IOE check captain in the right seat was aware of the high spd but was letting the PF work through the prob. To prevent a recurrence, the PF should disconnect the autoplt and hand fly the aircraft until such time spd and altitude are not as critical as they are below 10000'. Also the IOE instructor might have been more vocal in bringing the high airspd to the PF's attention. Supplemental info from ASRS No. 145130. We had been flying Type X on every leg of this IOE training flight. My first exposure was this morning, May, 1980. We were then clred up to 17000'. When I engaged the nose up pos, the pitch change went from level to about a +300 fpm clb, probably. I say probably, because when I engaged the HDG select switch, or rather what I thought was the HDG select, I engaged ALT HLD which is in the exact location on this aircraft as the HDG select switch is on the Type X on which I had been turning. The next thing I hear is my IOE captain very gently saying, "airspd, airspd." Supplemental info from ASRS No. 145128. South of COYLE VOR, PF (IOE student) drifted off course slightly. I pointed out from our computer flight plan that the winds were a 100 kt direct xwind. Student corrected even greater than his 25 deg correction and we reintercepted course. Conducting IOE in a different model aircraft in the very very demanding NYC area is quite

> a challenge. There sometimes is a very fine line between letting a student push a limit and learn and taking the aircraft away. Should I have taken the aircraft? (ASRS No. 145243)

Warning and Alerting Systems

Warning and alerting systems are a middle level line of defense against human error. They may anticipate the possible error or condition (e.g. "insufficient fuel" message in a glass cockpit aircraft). They may warn the crew of an impending hazard (e.g. GPWS), or annunciate the error as it occurs (e.g. mis-configuration takeoff warnings). In many cases they may be considered backups to human vigilance (e.g. out of balance fuel conditions) where the operator has the necessary information available before the system reaches the alarm condition. In other cases warning and alerting systems are not, in the strictest sense, interventions against human error, but are extensions of human sensory capability (e.g. engine fire warnings, baggage compartment doors not closed). These examples represent not a lack of human vigilance, but sensory limitations. Some systems are mixed - human capabilities may or may not be sufficient for detecting the alert condition (e.g. a potential conflict with another aircraft as annunciated by TCAS).

We shall not review in any detail the human factors of warning and alerting systems, as there are many recognized treatises on this subjects (Veitengruber, Baucek, and Smith, 1977; Randle, Larsen, and Williams, 1980), but shall merely place the topic in its proper context as an intervention strategy.

First we suggest that any new warning system should be held up against the applicable guidelines in Appendix 1. It should be required to meet the criteria of economy, feasibility, effective human engineering, acceptance, etc. The proliferation of warning systems in the cockpit has been well documented (Wiener and Curry, 1980), and the trend is difficult to reverse. The design of the B-767/757 was a great step forward in simplifying and unifying the warning systems in the cockpit (Morton, 1982). More will be said later of the potential for warning systems in high technology aircraft.

No warning and alerting system is perfect. None can provide an absolute guarantee against the human error it was designed to prevent, as the crash of Northwest 255 illustrated (NTSB, 1988). The lamentable history of gear-up landings is testimonial to this. A gear-up landing may seem a simple error to prevent, compared to a far more complex error such as a wrong-airport landing, for which no hardware/documentation intervention is obvious. Indeed, we have probably run out of intervention strategies to prevent gear-up landings. They still occur, even to highly experienced pilots.

The imperfection of warning devices is attributable to a variety of problems, from failure of human vigilance to internal failures of the device itself. To begin with, any alerting device is subject to both Type I (commissive) and Type II (omissive) errors. The designer attempts to balance these two types of inevitable error. Deliberate disarming of the device, or deliberate ignoring of the warning are more common than we would wish. In two no-slat/flap takeoffs mentioned previously, the configuration warnings did not trigger. In one case (B-727) it was probably due to a simple mechanical failure (NTSB, 1989); in the other (MD-82), no electrical power was available to the system, for reasons unknown (NTSB, 1988).

Another weakness in crew-warning interaction is what Wiener and Curry (1980) termed "primary-backup inversion." This term reflects the fact that it is not unusual for crews to allow the alarm condition to alert them before they take action. In brief, the primary system (human vigilance) becomes the backup system and the backup system (alerting device) becomes primary. The lines of defense depicted in Figure II-1 are reversed, and human vigilance alone is an insufficient defense. An example of primary-backup inversion can be found in the common practice of an altitude callout 1000 feet prior to reaching target altitude. It is not at all unusual to see the responsible crew member (usually the pilot not flying [PNF]) allow the altitude alerter to sound, and then make his callout (Wiener, 1987c). This practice relaxes a line of defense against altitude deviation. It is especially insidious since there are a great variety of possible trigger points for various models of the altitude alerter. Unfortunately the practice described is very common.

We can end this discussion by simply noting that the human is not a backup system, and should not be used as such. The human remains a vital component in complex systems found in aviation and elsewhere because he/she possesses remarkable perceptual capabilities, among them the ability to detect subtle deviations from normal. This capability should be assigned to the front end of the lines of defense against human error. Human error is the price we pay for the flexibility of the human brain. It is a price that must be minimized by effective intervention strategies and lines of defense.

Error Detection and Error Recovery

Systems designers recognize that human errors cannot always be prevented. Therefore they must construct the system to be impervious to error to the degree possible. Since there are more elaborate opportunities for doing this in advanced technology aircraft, we shall hold the discussion of this approach until the next chapter. However, in the traditional technology cockpits, error detection and error recovery are important topics. The first principle is that if an error is entered into a system, the design should allow the error to be recognized by the crew as quickly as possible. This is what Wiener (1989a) has called an "error evident" design. In brief, errors should be made conspicuous to the operator.

The recovery principle states that when error occurs, and is detected by the crew, a simple recovery should be available. No action should be irreversible, and the crew should not have to accept the adverse consequences of any error, once they have discovered it. To use a familiar non-aviation example, should I make an error and erase text or a file while using my word processor, I have readily available an "unerase" recovery technique, as part of the software. The system does not prevent the error, but it can nullify its consequences. In this case it can render the error totally inconsequential. We should ask as much of the designers of more complex human-machine systems. Without the file and text recovery software, such an error would be unrecoverable and disastrous (in the eyes of the author).

To be sure, some errors are irreversible, particularly those where resources are expended and cannot be recovered (e.g. fuel dumping, triggering engine fire extinguishing agents, etc.) Those cases call for particular care in the design of equipment, procedures, supporting documents, and training protocols.

B. PROCEDURES AND SUPPORTING DOCUMENTATION

Intervention via hardware design and retrofit has long been the concern of the human factors profession; intervention via procedures and documentation has usually been somebody else's problem. The somebody is generally the management of the organization using the equipment. The classic view of human factors has been to design the hardware right in the first place, and everything else will take care of itself. But recent dramatic accidents have shown the inadequacy of this view. Serious questions have been raised about such "soft" areas as checklist behavior, computer-produced flight plans and other flight-deck paperwork, procedures and policies, and flight-deck communication protocol. By the late 1980s, cockpit resource management had become a "household term" in commercial and later in military transports (Wiener, Kanki, and Helmreich, 1993).

Spurred by the advent of the glass cockpit aircraft, several airline managements struggled with the task of developing a philosophy of automation. Experience in the training departments as well as on the line had convinced management pilots that a guiding statement of philosophy was not a bad idea. The statement developed by Delta was, to the author's knowledge, the first in the industry (see below). The efforts of management to develop this policy are detailed in Byrnes and Black (1993).

++

TABLE III-1. Delta Air Lines Automation Philosophy Statement

> The word "Automation", where it appears in this statement, shall mean the replacement of human function, either manual or cognitive, with a machine function. This definition applies to all levels of automation in all airplanes flown by this airline. The purpose of automation is to aid the pilot is doing his or her job.
>
> The pilot is the most complex, capable and flexible component of the air transport system, and as such is best suited to determine the optimal use of resources in any given situation.
>
> Pilots must be proficient in operating their airplanes in all levels of automation. They must be knowledgeable in the selection of the appropriate degree of automation, and must have the skills needed to move from one level of automation to another.
>
> Automation should be used at the level most appropriate to enhance the priorities of Safety, Passenger Comfort, Public Relations, Schedule, and Economy, as stated in the Flight Operations Policy Manual.
>
> In order to achieve the above priorities, all Delta Air Lines training programs, training devices, procedures, checklists, aircraft and equipment acquisitions, manuals, quality control programs, standardization, supporting documents, and the day-to-day operations of Delta aircraft shall be in accordance with this statement of philosophy.

(Reprinted from Wiener, Chidester, Kanki, Palmer, Curry, and Gregorich, 1991)

++

Degani and Wiener sought to examine the softer areas, first concentrating on checklists (1990), later on what we called "The Three P's" - philosophy, policies, and procedures (1991). We pointed out the vulnerability of aircraft (as well as other high-risk systems) to lapses in checklists and the conduct of procedures, and offered guidelines for their design and implementation. We later decided that it was necessary to add a fourth 'P', this one being *practices*, that is, what actually occurs in flight. The difference between procedures and practices is procedural deviation, or error, which is the focus of an expanded report (Degani and Wiener, in preparation). In the next section we shall briefly examine the opportunities for intervention into the soft areas.

Standardization

The importance of hardware standardization was discussed previously. The same principles apply to supporting documentation. Degani and Wiener (1990) discuss the importance of standardization in checklist design and nomenclature. At many carriers there are great differences in the design of checklists across fleets, differences that cannot be explained by the obvious fact that they exist for different aircraft.

Within an organization we found little evidence of unifying principles of checklist design and conduct. Checklists were obviously designed and implemented by various groups at various times, and were thought to be optimal for that aircraft. As to nomenclature, the same piece of hardware had different names in the different fleets (e.g., thrust levers, power levers, and throttles). Just how serious this problem may be is difficult to assess. Some airlines have attempted to standardize hardware nomenclature. We visited a major carrier and were told that they had attempted to standardize nomenclature across fleets and had found it surprisingly difficult. They abandoned the project.

Standardization should not be an end in itself. Standardization exists to establish both in fact and in outlook that the company has arrived on a "best way" to do things, and that this best way may transcend even fleets of very different aircraft. Degani and Wiener (1991) refer to standardization as "the palace guard of procedures." One of the virtues of standardization is that each pilot should know exactly what to expect of another pilot. Standardization also serves as an intervention against human error. Procedures, checklists, and paperwork are established and crews are trained in one consistent, predictable way, in keeping with the company's basic operating philosophy. In theory, transition from one model to another should not be difficult. Although the systems are different, the basic operating methods of various aircraft share much in common.

Standardization of supporting documentation is not cost free. The costs flow from the fact that in order to achieve company-wide uniformity, some equipment may be operated sub-optimally. Degani and Wiener (1990) provide the following example. An operator in the early days of the MD-80 allowed crews to fly mixed lines of DC-9 and MD-80 time. The MD-80's weather radar operated with much lower power than that found in the older sets in the DC-9s, and unlike the DC-9 radars, could be turned on at the gate with no hazard to ground personnel. Fearing that crews flying mixed lines might inadvertently operate the DC-9 radars as if they were MD-80 sets, management decided to intervene by standardizing on the safe side. Checklists for the MD-80 were rewritten to adopt the more conservative DC-9 radar procedures. This may have resulted in somewhat sub-optimal procedures for the MD-80s, but the added protection against human error, with its potential endangerment of ground personnel, was considered worth the price. This was a classic example of employing standard operating procedures as an intervention to control errors.

Procedure Design

Procedures are step-by-step specifications drafted by management and provided to pilots. They are designed to dictate the manner in which tasks and sub-tasks are carried out and to provide a standardization of cockpit duties. In a well standardized and procedurized operation, one of the pilots could be removed from his/her seat in mid-flight and replaced by another, and crew performance would not suffer. Procedures have often been confused with checklists. Degani and Wiener (1991, p. 2) explain the difference: "A checklist is a device (paper, mechanical, audio, or electronic format) that exists to ensure that procedures are carried out. The confusion may come from the fact that 'running' a checklist is in itself a procedure."

Procedures and subtasks are considered here because they are the most elemental steps by which pilots operate their craft. Procedures are fertile ground for human error, and, thus, for intervention strategies. When new equipment is installed, new procedures are needed and checklists must be revised. A recent example is the installation of the first TCAS equipment into the cockpits of airliners in 1990, which necessitated training programs, documentation, procedures, and checklist revisions. It is too early to know how successful these procedures and checklists have been in exploiting the safety potential of TCAS, and avoiding errors in its use. So far the reports on TCAS have generally been favorable, even with the problems that usually accompany the introduction of new systems (Gilmartin, 1991; Smith, 1991; NTSB, 1993).

An interesting example of procedural intervention would be the loading of coordinates for waypoints in area navigation systems. We shall consider here the traditional RNAV equipment, in which each waypoint is defined by a pair of coordinates ("lat and lon"). More modern avionic equipment, utilizing waypoints stored by name in a flight management computer (FMC), will be considered shortly.

The vulnerability of such systems to various human errors, primarily, though not exclusively, those induced by keyboard input error, has been documented by Aarons (1988), Wiener (1988a), and Wiener and Curry (1980). Some of the most dramatic accidents of the last decade can be attributed to RNAV input errors. In brief, it is the task of the crew to take a paper flight plan and establish the waypoints by loading the latitude and longitude for each via keyboard. This task is a breeding ground for error. Errors in this procedure are so common that they have their own nickname: "finger trouble" or "finger error."

Operators have sought to control the errors by intervening procedurally in various ways, for example by establishing redundant input of the same information by the two or three crew members, and by establishing checking procedures once the coordinates are loaded. The procedures vary considerably from one company to another. Specific techniques for cross-checking are covered in FAA Advisory Circular No. 90-79, 7/14/80, "Recommended practices and procedures for the use of electronic long-range navigation equipment." Some companies require that each of the two or three crew members load the data independently from his/her own copy of the flight plan. The system then detects discrepancies. Others specify that one pilot load the data and another check it against the flight plan. Some carriers emphasize error detection by cross-checking against other data on the flight plan, for example, distances between waypoints. The RNAV computer calculates the distance between the waypoints as loaded: the crew checks these against their flight plan. A coordinate error would result in a discrepancy between the paper flight plan and the RNAV readout with respect to waypoint-to-waypoint distances. These checks are particularly important in trans-oceanic operations.

In spite of a variety of intervention strategies, it is still possible to insert erroneous data: a single keystroke can result in an incorrectly located waypoint. In over-water operations some of the lines of defense in Table II-1 are absent. Further, an incorrect waypoint may reside dormant in the RNAV computer for hours, until its time comes to be activated. In one dramatic example, two U.S. wide body jets passed within 30 feet of each other over the North Atlantic in Canadian airspace (Canadian Aviation Safety Board, 1989).

We do not know of any "one best way" to prevent keyboard errors. Hopefully new technologies will soon make RNAV data loading less critical. Satellite navigation and communication will prevent any aircraft from being outside the communication range of ATC, and will provide a "virtual radar" coverage for aircraft wherever they may be, thus restoring vital lines of defense found in overland operations.

Lateral navigation (LNAV) systems found in FMC-equipped aircraft provide more error-free input procedures, and map displays found in the EFIS-equipped aircraft provide error-evident displays that can make a waypoint error obvious to the crew. More will be said about this in the next chapter.

Checklist Design and Usage

The complex issue of the human factors of checklist design, implementation, and usage/non-usage has been explored in detail by Degani and Wiener (1990). Our report included sixteen guidelines for checklist design and use (see Appendix 3 of this document). Basic questions involve what should and should not be included on the checklist; in what order items should appear; whether any items be repeated for redundancy; how items should be subdivided ("chunked") on the checklist; "do it" versus "verification" checklists; and many more. The checklist is far more than a "laundry list" of items and tasks. The checklist serves to prevent error by stating what must be done, when and in what order, and by whom it is done. It also provides the basis for and sets the tone for cockpit discipline and standardization. This document, often a single piece of paper, is the very foundation of flight safety. Procedures, in turn, dictate to the crew how the tasks are done (Degani and Wiener, in preparation).

A distinction must be made between checklist design (what actually goes on the checklist, and how it is displayed) and the "how" of checklist behavior - who does what (e.g. challenge and response), what must be done when a checklist is interrupted, who calls for the checklist, how each sub-task is terminated. Degani and Wiener (1990) explain the difference between a "do" list and a "confirmation" (or "verification") list.

Following three accidents in the U.S. in which airliners took off without flaps and slats set, checklist design became a prominent issue. I was asked during my testimony at the NTSB hearing on the Northwest MD-82 accident what human factors work had been done on checklist design. I had to admit that I had been unable to find any except for some studies of typography and printing layout which would be of minor importance except in the extreme (Wiener, 1987c). The Board's question was the genesis of the Degani and Wiener checklist studies.

Electronic checklists may replace paper versions in future aircraft. Boeing has included such a device in its 777 (Scott, 1991). Electronic checklists have many advantages over conventional versions, particularly when the checklist must be interrupted or items must be taken out of order. The electronic checklist will handle this very well; in the paper checklist, interrupting the process is an invitation to error. However, a recent NASA simulator study of electronic versus standard checklists found that the standard checklists yielded superior performance (Palmer and Degani, 1991). These results may be due to an interface problem in this particular implementation; research on electronic checklists is presently underway at several locations.

For many years to come, the primary intervention strategy against human error in the cockpit will be a conventional paper checklist. It is somewhat ironic that the safety of a modern aircraft worth tens of millions of dollars still depends to a great degree on a device that can be reproduced for pennies.

Methods Improvement

We will next discuss a wide variety of actions that can be viewed, in the industrial engineering sense, as methods improvement. This form of intervention includes actions which simplify paperwork and procedures, reduce the number of steps in a procedure, relocate the steps in a logical manner ("flow"), and generally reduce or manage workload.

In these cases the P-I-R (problem-intervention-result) relationship which was discussed in the last chapter can be fairly direct, or it can be indirect. Examples of each will be offered; both Model A and Model B interventions apply. Where the P-I-R relationship is indirect or vaguely defined (Model B), it is because the interventions may not be necessarily in response to a particular problem, but a general problem. Usually the need is to "clean up" an area, to simplify procedures, and to reduce or better manage workload, wherever possible. This is based on the assumption that reducing workload, particularly during periods of high workload, will reduce human error.

The management of low workload periods of flight (e.g. cruise), possibly by introduction of workload, either genuine or "make work", may also be considered, but it should be viewed as an entirely different problem. Interventions of this type are being examined (Graeber, 1989), due in part to the use of two-pilot crews on increasingly long legs. So far research into this area has not matured to the point where intervention strategies can be recommended. For now, we will confine our consideration of workload management to high levels of workload.

GUIDELINE NO. 11

Examine each proposed intervention and ask if there is an easier, less invasive, or less costly way to accomplish the same thing.

Paperwork engineering. One area that is ubiquitous in methods improvement is paperwork reduction and management. Paperwork of any kind is onerous in the cockpit. As elsewhere, it is subject to steady inflation. We should distinguish between two types of paperwork, that which is necessary for any particular flight (flight plans, NOTAMS, weather, weight and balance advisories, fuel slips, maintenance writeups, etc.), and that which is administrative (e.g. crew pay logs, engine performance logs, and discrepancy reports).

Intervention strategies may consist of reducing cockpit workload by eliminating or simplifying the paperwork not needed for flight, or by assigning it to other personnel in cabin or on the ground. The impact on the workload of these personnel should not be ignored (see Chute and Wiener, in preparation), but it will not be considered here, as the focus on this report is on errors in the cockpit. However, we are not insensitive to the impact, perhaps even safety impact, on the extra-cockpit personnel to whom we are recommending that paperwork be diverted (see Guideline No. 4, Appendix 1).

A related area ripe for methods improvement is the design of the paperwork for compatibility in the cockpit. Paperwork design has not been an attractive area of human factors research and application, even though it can be vitally important. In our report on procedures (Degani and Wiener, 1991), we discuss briefly the incompatibility of paperwork and "computerwork". Much of the paperwork and procedures in use today by airlines were designed for traditional aircraft, and have not been adapted to the advanced technology cockpits.

Illustrative of this is an example from Wiener (1989b) in which the crew of a B-757 was given a flight plan from Miami (MIA) to Washington National (DCA) which included (in part) the following routing: "radar vectors, AR-1 CLB ILM J-40 RIC..." [Atlantic Route 1 to Carolina Beach, direct Wilmington, jet airway 40 to Richmond...] The crew attempted to enter the information on the Route page of the CDU but could progress no further than "CLB". Every time they typed CLB they received a "not in database" error message in the scratch pad of the CDU. Repeated entries yielded the same results. Finally one of the pilots traced the route on his high altitude chart and discovered the problem: CLB is not a VOR as the three-letter designator on the flight plan implied, but is a non-directional beacon (NDB). The entry demanded by the CDU to access this waypoint is "CLBNB".

This flight plan had been stored in the ground computer, and was appropriate for all other types of aircraft in the airline's fleet. This example in itself might not have been a serious matter, but it did frustrate the crew and increase workload. What is more important, it may have pointed toward other examples, perhaps more serious, of paperwork-computerwork incompatibility. The intervention strategy is obvious: carriers operating high technology aircraft should examine every aspect of their operations and paperwork for incompatibility with the new aircraft. It is no small task.

Other methods improvements could be achieved by paperwork simplification and engineering. The author was told recently by a captain that he had made a written request to his company that the stations on a weather sequence printout be in alphabetical order, so he would not have to search for a station, particularly when a diversion might be required. The company's response was one with which we are all familiar: "That's how it comes out of the computer". It is difficult to believe that it would not be a fairly simple matter to build an alphabetical sort into the weather sequence software, thereby reducing cockpit workload, albeit by some small degree.

More serious examples can be found which justify our recommendations that methods improvement be applied to the routine production and handling of flight paperwork. Recently an aircraft prepared to depart Miami and the crew was handed the flight papers. As they loaded the information from the papers into the CDU, an alert crew noticed that some of the numbers did not conform with what they believed to be true, although most of the information seemed logical and correct. Closer examination revealed that they had been provided with the paperwork for the identical flight from the previous day. Of course one may argue that the crew should examine the date on first accepting their flight papers. But one may state with equal verity that this was a "trip wire" incident; no crew expects to be handed yesterday's paperwork. The intervention strategy to ensure that this particular error never occurs again may be more complex than it first appears. The ASRS reports below illustrate that this was not an isolated case.

> Narrative: aircraft number and flight number reversed on dispatch release. Computer then thought aircraft was a new type, instead of the old type. New aircraft burn substantially less fuel at cruise (1294 pounds difference for this leg). During cruise flight we checked fuel against computerized flight plan. Estimated arriving with less than standard fuel (but close to "legal fuel"). After consulting with dispatch it was decided to make a precautionary fuel stop in LAS. Flight was from PDX to PHX. Crew needed to double check release. The correct numbers were there, just in the wrong order. Flight numbers will be rearranged so as not to be same as aircraft number. Don't forget to compute own estimate of fuel needed. I always did before I had computerized flight plans. (ASRS No. 62844)

The intervention appropriate for this problem seems obvious. The author checked the flight schedules of one airline, and found that it had no flight number 727, 737, 757, or 767 (all of which aircraft it operates), though it did have flights with the surrounding numbers (e.g. 726, 728). There is also no flight 747 in the schedule, even though they do not operate this aircraft. The carrier does have a flight 1011, which is a DC-9 trip. Presumably these would not be likely candidates for confusion.

> Narrative: we received final weight and balance just prior to pushback from gate at Orlando. While taxiing to RWY 18R, we received three more weight and balance sheets via aircraft ACARS printer, the last of which varied considerably from correct passenger count. Closer scrutiny and questioning by the captain revealed this computer weight and balance was for the same aircraft, but for a flight originating in Boston. This type of scenario could easily result in use of improper V-speeds and stabilizer trim settings. (ASRS No. 162106)

GUIDELINE NO. 12

> *Examine all paperwork associated with an intervention strategy, or that is in itself the intervention. Does this paperwork actually aid the crew, or does it place unnecessary burdens on the crew? Can the responsibility be assigned elsewhere? If additional paperwork must be implemented, can its form be made more pilot-friendly? Can its design be improved?*

Workload management. There are ample opportunities for intervention by managing (as contrasted with reduction) of workload. If workload cannot be eliminated or reduced, it can be managed. Management consists of reallocating workload to less flight-critical phases (e.g. programming that can be done at the gate, rather than after takeoff); and reallocating duties (particularly in a three-pilot crew) to balance the demands on the individual crew members. For example, it has frequently been suggested that installing a transmitter-receiver or an ACARS in the cabin, for passenger-related communication by the flight attendants, could reduce the radio communication load in the cockpit. This suggestion has been resisted by some pilots, who hold a traditional view that all transmissions from a craft should emanate from the flight deck. (We note the prevalence of cellular telephones in the hands of passengers today). Other pilots see the transfer of passenger-related communication duties to the cabin crew as good riddance.

In some cases the captain may manage workload by simply allocating duties and setting priorities on these duties. For example, captains frequently say (in so many words), "Let's put that off until later, and settle this problem first." The advent of CRM training in recent years has encouraged such interventions by the captain, as well as advocacy by the junior officer(s). Advocacy of workload management by subordinates is often couched as a question: e.g. "What would you think about my building the approach before I call the company about the wheelchairs?"

GUIDELINE NO. 13

An intervention strategy should be acceptable to pilots or other affected personnel. Those who design interventions should recognize that frequently changes in flight-deck regulations and procedures may encounter initial resistance on the part of many. This can often be avoided, or ameliorated, by seeking input from those affected, and making the reason for the intervention and the potential benefits clear to those affected (e.g. the sterile cockpit rule).

C. COMMUNICATION

Linguistic and Para-Linguistic Communication

Aviation is highly dependent on human-to-human voice communication (Kanki and Palmer, 1993). This is also a leading source of error in the system, and one that is difficult to combat. The problems of and opportunities for linguistic intervention were mentioned earlier in this report. Numerous investigators have explored this area both experimentally and by examining incident and accident reports and self-reporting systems. For example, Billings and Cheaney (1981), using the NASA Aviation Safety Reporting System (ASRS) database, explored the general area of errors in information transfer. Monan (1988) employed ASRS reports to examine what has been called the "hearback" problem, the frequent failure of pilots or controllers to detect errors in a message when it is repeated back to them by the recipient. Monan (1983) has also addressed the familiar problem of confusion over similar aircraft call signs.

> Narrative: cleared to 11000', descending through FL180. The preliminary landing checklist was accomplished and the current altimeter setting of 29.54" was challenged by the PNF as ".54 on the altimeters." I (the PF) responded with ".54 checked and set." Upon handoff to Approach Control, the PNF noticed on his altimeter that we were passing through

> 10700′. A quick glance at my altimeter revealed an altitude of 11700′ and an erroneous altimeter setting of 30.54." My altimeter was indicating 1000′ higher than our actual alt. A climb was initiated immediately to 11000′. Since the erroneous altimeter setting was on the captain's altimeter, and the altitude alerter receives its info from this same INS, no altitude deviation alert was sounded. This situation could have been alleviated by calling out all 4 digits of the altimeter setting (with particular emphasis on low settings) and cross-checking to ensure that they are properly set. An approved company ATIS data card for terminal weather info to be written on, would also help correct the situation of having terminal weather read aloud from the PNF or written on napkins and various pieces of paper that are placed in different areas in the cockpit. This would provide standardization with a visual cue card to review terminal weather info when workload permits, and not daring a critical phase of flight where you have to listen to ATC in one ear and ATIS info in the other. (ASRS No. 145761)

We must make a distinction between intra-cockpit communication errors, which have not been studied extensively for lack of convenient data (except in accident investigations and some NASA simulator studies) and extra-cockpit communication by radio. Intra-cockpit communication is being studied by Kanki and her collaborators at NASA-Ames. For a preliminary report, see Veinott and Irwin (1993). Present datalink, such as ACARS, employs highly restricted input domains, composed of numeric data and alphanumeric codes entered via keyboard. Although very brief free-text messages can be composed, the system is essentially non-verbal. Errors in communication with this system would best be described as problems within basic human factors engineering: input hardware (e.g. keyboards versus touch screen devices), formats, and codes.

Much of the intra-crew exchange of information in the cockpit is based not on verbal language, but on para-linguistic communication (Segal, 1990). Movements of the head, hands and arms, holding up fingers to exchange numerical information, and other body language is common in the cockpit. Some specific motions have well understood meanings, as determined by the context: on takeoff a thumb up by the pilot flying (PF) as a non-verbal command to raise the landing gear; in climb or descent, a single finger up means 1000 feet to go to target altitude.

This form of communication is used in place of oral communication because it is efficient, it is impervious to ambient noise, and it can be carried on simultaneously with oral communication, including radio work. However, it is also highly vulnerable to human error. Video tapes recorded in a flight simulator, either for experimental purposes or as part of a LOFT/CRM training program, illustrate the richness of para-linguistic communication.

Para-linguistic communication in the cockpit may be an efficient channel, but it is also highly subject to misinterpretation. It is generally not encouraged in training and quality management, except possibly as a redundant measure accompanying the verbal callout. For example, many pilots call orally for gear up and make a motion with their hand at the same time, as a form of deliberate redundancy for the purpose of error checking. In much the same way a customer entering a noisy restaurant might indicate to the maitre d' the number of persons in his party by both stating the number verbally and holding up fingers. The finger signals would probably be sufficient, and even more efficient under conditions of either high noise levels, or language differences. But the customer adds the redundant verbal channel because it is generally not considered polite, at least in the U.S., to transmit numerical information exclusively by hand signals. The cockpit may be an exception, where a well-established, non-verbal lexicon evolved over the years.

Well-established though the actions may seem, miscommunication by non-verbal means may result in serious consequences. Consider the following example related to the author by an airline captain whose company requires a callout at both 2000 feet and 1000 feet prior to target altitude.

> We were descending rapidly. At 2000 feet prior to our altitude I held up two fingers. The first officer nodded and moved the flap handle to the 2-degree position. We were well above the placard speed for slats and flaps.

It is futile to dream of ever totally removing communication errors, linguistic or para-linguistic, from the aviation system, but certainly effective interventions have been made, and can be made in the future. Para-linguistic communication can be controlled through standardization (e.g. ground-crew to cockpit hand signals), but it is not easy. The richness that makes language so adaptable, the lack of precision that engenders humor and makes speech a pleasure, also lays a trap for the unwary. Oral communication can be engineered, as is widely done in the military, but linguistic engineering and standardization requires never-ending vigilance. For example, a recent copy of NASA's ASRS Callback (May 1991) related the confusion over ATC's use of the verb "circumnavigate", as in "circumnavigate the TCA." One of the readers comments:

> "For instance, the pilot could be thinking, 'I know what circumnavigate means in this situation, but what does the controller think it means...and what does he really want me to do?' The words 'remain clear of' or 'do not enter' are not open to misinterpretation, and are more easily understood than 'circumnavigate'".

One obvious intervention is to eliminate voice communication where possible, replacing it with electronic datalink (Kerns, 1990). Datalink technology is undergoing rapid development at this time. The drivers for replacing voice with datalink are not only error reduction, but reduction of frequency congestion on voice channels, which is a long-standing problem in air-ground communication. Police departments have for some time used both voice and datalink communications to and from patrol cars.

The question of whether datalink will result in an effective intervention is not one of available technology. Clearly the technology exists today, and there are no barriers to its eventual introduction in the system. The problem is whether this intervention will meet the criteria suggested in Appendix 1. Serious questions can be raised about the possibility of trading one form of error for another. While we are well aware of the speaking-hearing errors as documented by Billings and Cheaney (1981), Monan (1983, 1988), and others, and also by examples from accident reports, it would be unwise to assume that datalink is itself error-free. At the transmission end, we are all too aware of the error-inducing properties of keyboard input, especially during high-workload and other adverse conditions. At the receiving end, there are reading errors. System accuracy can be degraded by many of the same errors that exist in radio communication, such as numeral, letter, and word transposition, expectation bias, and many more. We cannot be certain that any of these will be eliminated by switching to electronic datalink, with human input and output at each end.

Critics have raised the question of the loss of a valuable incidental source of information, the so-called "party-line" which allows crews to garner information from over-hearing the transmissions between other aircraft and controllers (Midkiff and Hansman, 1992). The presumption is that party line transmissions convey valuable incidental information, which enhances the "situational awareness" of other crews, particularly as they enter or depart a terminal area. The benefits of the party line have not been systematically studied; they have only been assumed to exist. If they do exist, they come at a price: possible distraction and congestion of human auditory processing channels, which must process the irrelevant as well as the useful party line information. If datalink proves to be an effective form of communication, abandonment of the party line channel may be a small sacrifice.

Linguistic Interventions

We have stated previously that oral communication offers opportunities for intervention strategies. A few examples may help. As early as World War II, human factors scientists saw both the need and the opportunity to intervene into human-to-human voice communication, particularly when noisy channels are employed. Recognizing the confusion of English letters when pronounced, the "phonetic alphabet" ensued, later to be changed to an "international alphabet", and some words changed back again, creating great confusion. The confusion created by this vacillation not withstanding, the phonetic alphabet was a classic case of a linguistic intervention to prevent transmission errors.

Words and phrases were also invented to avoid human error. The contrived term "say again", the restricted use of "cleared" in ATC instructions, and the contrived pronunciation "niner" have already been mentioned as examples of specific interventions. A highly structured ATC lexicon was developed. However, even in this structured and disciplined linguistic environment, misunderstanding of the speaker's intended meaning can occur. The crash of TWA 514 into Mount Weather near Washington, DC in 1974 resulted from lack of an unambiguous interpretation of what it meant to be "cleared for an approach" (NTSB, 1975). A runway collision occurred at O'Hare in 1972 because a single word was omitted from a tower transmission (NTSB, 1973).

Many airlines have established specific, word-for-word expanded checklists, which spell out in meticulous detail not only the steps to be taken, but also the callouts and verbal exchanges. Little is left to the imagination or individual styles of the crews. The emphasis of the jet age has been on rigid standardization. More will be said of this when procedures are discussed in the next section. Still, pilots superimpose their own individualities on the process.

Degani and Wiener (1990; in preparation) discuss the tendency of some pilots to superimpose their own language upon that required by the checklist and company's standard operating procedure. The motivation for this may be the desire to separate themselves apart from the rigid standardization of modern flying, or to inject "humor" into an otherwise monotonous activity (e.g. the word "gasoline" may be substituted for "fuel" in a checklist challenge). The author once observed a first officer who, on making his takeoff "bug" calls, said "V-one-R" (in place of two required calls, "V-1" and "V-R"), and then for the "V-2" call substituted "Two of 'em."

This departure from required procedures is a small matter, but it illustrates the difficulty of maintaining standardization and discipline, even in a generally well standardized airline.

Interventions into behavior of this sort are difficult. Such laxity will always exist, but it must be resisted by all means possible: through training, unswerving emphasis on standardization, and constant attention to quality control through line checks, simulator checks, recurrent training, and LOFT. Needless to say, the first officer would probably not have breached the system with a check airman on board. Cockpit resource management (CRM) training is another feasible intervention strategy. The captain could have later seized the opportunity (out of the presence of the author) to practice his CRM skills by discussing with the first officer, in a constructive manner, the obviously substandard performance in his bug speed callouts.

D. TRAINING

Pilot training may be considered a form of intervention strategy. There is a practical and a regulatory requirement for training. But in addition to these requirements, training managers may wish to make curricular interventions, in order to introduce new equipment, new techniques, or new operating philosophies. In any of these, the link between the intervention and reduction of human error may be quite remote; this provides a good example of a Model B intervention.

There are three levels at which we may consider opportunities for intervention through training.

Overall Training Curriculum

Training curricula are based on statutory requirements of the FARs. These regulations must be interpreted by each company, consistent with its own philosophy and resources, as approved by the FAA. This level would provide only in the broadest sense opportunities for intervention. In the near future, the FAA's Advanced Qualification Program (AQP) will offer greater opportunities for each company to tailor its training program in accordance with its own philosophy and experience. It is difficult to say at this time just what opportunities AQP will offer for interventions aimed at either general or specific human errors.

The distinction between the next two levels is similar to the distinction between Specific and Conditional interventions discussed previously and depicted in Figure II-4.

General Interventions Through Training (Model B)

Training offers flight management the opportunity to intervene in a broad class of problems. The strategy is based on the belief that the class of problems is more easily attacked as a training problem than through discipline, standardization, procedures changes, or the like. An good example is CRM. CRM training offers a remedy for a broad, perhaps poorly defined class of problems, whose origins are inadequate or inappropriate communication in the cockpit (Wiener, Kanki, and Helmreich, 1993). The intervention comes in the form of a training program for all pilots. At some carriers the training is extended to other personnel, such as maintenance, cabin crews, and flight management. It is not remedial training for a handful of personnel who have been singled out as requiring intervention, nor is it psychotherapy. CRM training is a broad-scale approach to social communication-based behaviors and attitudes. It attempts to change cockpit behavior, not personalities (Foushee and Helmreich, 1988; Helmreich and Foushee, 1993). It is even questionable whether attitudes are altered.

CRM training might be an interesting place to apply our list of guidelines, interesting because many of the questions raised by our guidelines could not be easily answered. Furthermore, the value of the intervention must be taken on faith, and a few good examples. CRM training at United Airlines, one of the pioneers in the field, was recognized by the captains in two fatal accidents, a B-747 door separation in flight near Hawaii (NTSB, 1990a); and DC-10 crash in Sioux City, following total loss of hydraulics, (NTSB, 1990b) as a major factor in their success in saving as many lives as they did. Such examples are difficult to come by, since it is usually problems and failures that get reported, not positive outcomes. Though CRM has generally been accepted by flight crews as a worthwhile approach, it may not be able to meet the rigors of our list of criteria. This is be due to the inherent defect in CRM training, but fact that the problems for which CRM was developed are themselves poorly defined, and clear-cut answers are unlikely to be found.

Specific Interventions Through Training (Model A)

Interventions designed to meet more specific problems (Model A) usually fare better than those directed at less well-defined problems. When a specific problem has been identified training can be directed toward a possible solution. An example of training to avoid foreseeable human error is windshear escape maneuvers. During the last decade, windshear became a major safety concern, with little agreement on how pilots should maneuver their aircraft to avoid terrain, while also avoiding low-altitude aerodynamic stalls. One procedure called for increasing the angle of attack until stick shaker stall warnings were obtained, and then "flying the shaker." Training programs for windshear escape were formulated, and introduced to the pilots at their next simulator check. The training requirement for glass cockpit aircraft is simplified by hardware. These aircraft have pitch angle guidance for windshear escape depicted directly on the ADI. A yellow horizontal line commands the nose-up pitch angle to be followed, and the resulting angle of attack is kept just below the level for stick shaker actuation.

We end the discussion of training with a word of caution. There has been some tendency in the past to regard any operational human error as addressable by training. There has been an unfortunate tendency to treat a training department as a dumping ground for inadequate design of hardware or software. The first line against human error must be the designer.

IV. INTERVENTION STRATEGIES: ADVANCED TECHNOLOGIES

A. EMPLOYMENT OF ADVANCED TECHNOLOGIES

In this section we shall discuss intervention strategies for the management of human error. Error management must be distinguished from error reduction or elimination. "Management" in this sense means that one strives to build into systems and operators methods by which one can either eliminate or reduce human error, or if this is not possible, to minimize its consequences. The computer technologies upon which such methods depend are not necessarily new; some have existed in computer-based systems for years. The discussion concentrates upon the on-board computers on the advanced technology aircraft. Assistance from ground-based computers may be required for some interventions. Some of the techniques which we discuss will take us to the doorstep of artificial intelligence (AI), but not beyond.

Our aim is to employ the capabilities of modern on-board computers to negate the effects of human error. The computer takes on the role of being one (or perhaps more than one) line of defense, protecting the system from human error. Our distal goal is to ensure system effectiveness and safety. We seek to achieve this by satisfying a proximal goal, the management of human error.

Some methods of error management are designed to prevent an error from occurring in the first place, or to prevent it from entering the system; others will allow an error to enter the system, but will make the error more apparent to the operator so that he/she can correct it. Still other techniques will trap the error, preventing it from adversely affecting the system: the operator will be alerted by some means and have the opportunity to make the necessary changes. Intelligent warning and alerting systems may also play a role in defending the system from error.

The Impact of Cockpit Automation

The history of cockpit automation has been told by Billings (1991). Wiener (1988a, pp. 444-451) explored the question "Why automate?". Since the role of human factors in flight deck automation is documented by these and other authors, this report will offer only a scant introduction to the subject. Figure IV-1 displays the history of autoflight.

Cockpit automation began in the mid-1930's with the introduction of crude autopilots. Autopilot development has enjoyed uninterrupted growth since the early models. By the 1950's more sophisticated models could be found on aircraft of the Super Constellation and DC-6 era. Development continued into the jet age, as autopilots and flight directors became components of flight guidance systems, which included area navigation (RNAV), and rudimentary autothrottles. Other devices such as autoslats, autospoilers, and autobrakes became part of the automation package.

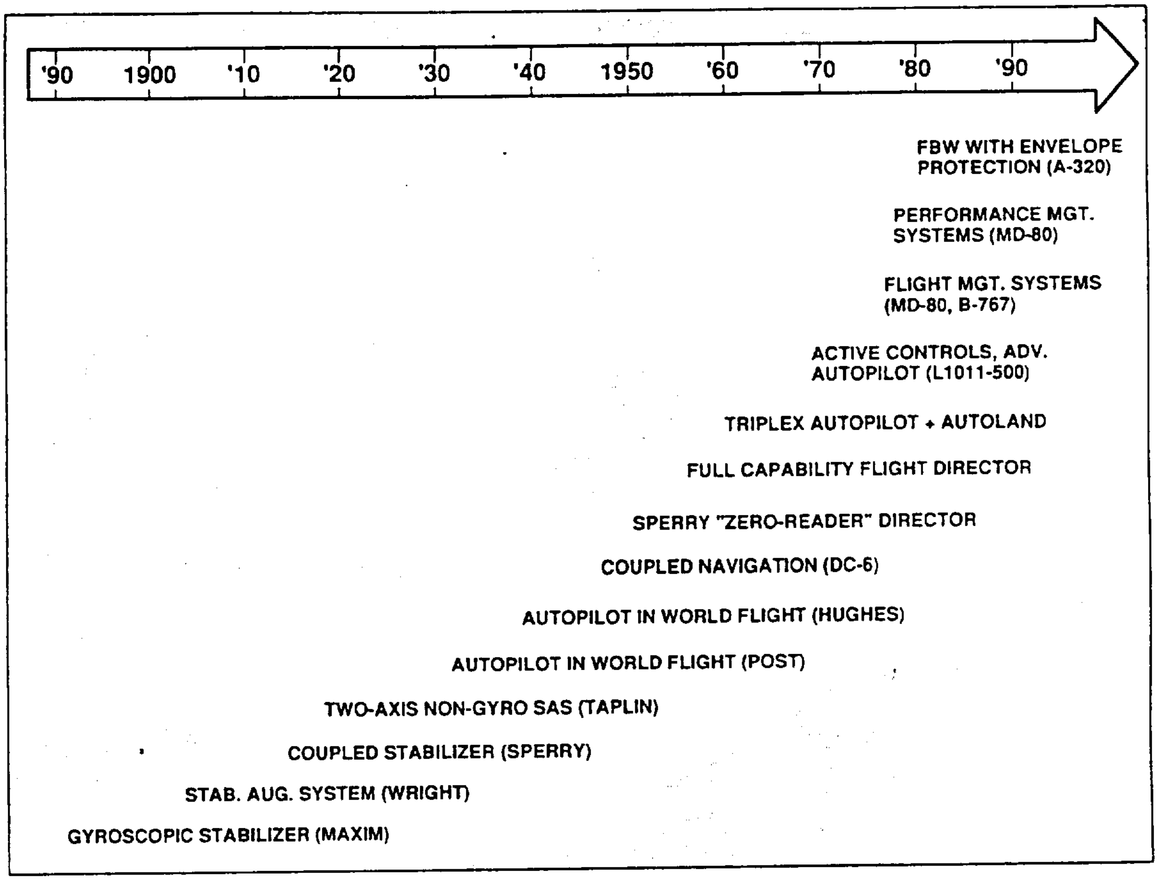


Figure IV-1. A chronology of aircraft automation. From Billings (1991).

It was not until the late 1970's that modern flight-deck automation flourished, driven by the rapid development of the microprocessor. In 1982 Boeing introduced the B-767, the first of the "glass cockpit" (more correctly EFIS - electronic flight instrument system) passenger aircraft. Other Boeing models, and those of other manufacturers followed. By the end of the decade, glass cockpits were offered to the airline industry by all major manufacturers of large airliners, as well as many manufacturers of smaller aircraft operated by the regional carriers. Glass cockpits can also be found in corporate and military aircraft.

The new cockpit designs combined many of the previously existing devices with new features, based on a sophisticated inertial reference system (IRS) and color computer graphic instrumentation. The computer graphic ("glass") displays not only replaced the traditional ("iron") electro-mechanical instruments, but also allowed a wide variety of information to be displayed which had not be available previously, e.g. a wind vector; a path predictor vector; navaids and airports, superimposed color radar; and a moving map on the horizontal situation indicator (HSI). Some of these features can be seen in Figure IV-2, which depicts a glass HSI in the map mode. Note the two shaded areas representing superimposed (color) radar returns. The three-segment line curving forward and to the right of the airplane symbol is the path predictor vector.

In Wiener's study of pilot reaction to the glass cockpit (1989b), the HSI map display was consistently mentioned as the favorite feature of the new aircraft. Furthermore, color radar can be superimposed on the HSI map display, a capability also universally praised by airline crews. These displays also allowed pilot selection and deselection of information (e.g. emergency airfields on the map), and switch-selectable options for instrument configuration, a feature not possible prior to the EFIS era. The pilot has at his/her fingertips a vast storehouse of information which previously was either not available, or had to be extracted from charts, tables, hand-held (mostly analog) computers, and manuals.

Error Protection

The on-board computers also offered some novel features that could be considered interventions for protection against human error. For example, the flight management computer (FMC) could recognize and reject certain cases of input that were outside of its domain. While the FMC of today can recognize and reject inputs because they are stylistically incorrect, it generally lacks the intelligence to detect inputs which are illogical or wildly incorrect, but in the proper form.

Pilots are forced to enter information in a rigid format, which in one sense may be a defense against input errors, but in another sense creates a less user-friendly device. Why should a crew have to worry about whether or not a slash ("/") is required between the latitude and longitude? On one flight in a glass aircraft, the author observed the crew struggle to establish a latitude and longitude ("lat and lon") waypoint (as required by a change in their clearance) to no avail. There were three different types of errors in their input, for a total of five errors in merely establishing a waypoint. The struggle continued until the captain thought of looking on another CDU page to discover the proper format, which he then mimicked in order to establish the waypoint (Wiener, 1993).

Other input errors result in error messages (e.g. "not in database") in the CDU scratchpad. The ability of the FMC to check fuel burn to destination against current fuel load has already been mentioned in Chapter II as an example of machine intelligence. Such an error message also serves as an example of Wiener and Curry's assertion (1980) that, in contrast with the traditional view that the human should serve as a monitor of a machine (Howland and Wiener, 1963), automation has enabled the opposite doctrine: the machine should monitor the human.

The B-767/757, and the glass cockpit aircraft that followed, possessed rudimentary forms of computer-based error elimination and protection. The A-320, introduced in 1988, took error protection a step further. The fly-by-wire feature offered the opportunity to fly maneuvers such as maximum safe angle of attack (AOA) for windshear escape, with no danger of entering a stall. The computer would simply stop the aircraft's increase in pitch short of its computed safe AOA. If the pilot continued to pull back on the stick, no more nose-up pitch would be commanded. An intelligent computer interposes an electronic line of defense between the pilot's control and the aircraft's control surfaces.

Other EFIS aircraft such as the 757/756 offer escape guidance on the attitude director indicator (ADI) in the form of a target line for optimal nose-up pitch, as described in the previous chapter. In contrast with the approach taken in the A-320 design, the pilot remains in the loop (presumably). The pilot controls the pitch angle; the computer merely computes and displays the commanded nose-up pitch.

These two approaches emphasize not only disparate views of cockpit design, but basic philosophical design differences: the A-320 essentially allows the pilot to pull the control stick all the way back and let the computer find the maximum angle of attack which will avoid a stall. Other EFIS aircraft depend on the pilot to follow the windshear escape guidance cues. It is impossible to say which approach is more effective. Only time and experience will settle that question.

Error Prevention Through Automation

It may seem ironic that the author takes the position that while current generation cockpit automation has not lived up to the designers' and operators' dreams of eliminating human error at its source, more use of automation in future generation aircraft may offer a solution.

The answers lie in creating error-resistant designs which reliably (1) employ automation to detect errors; or (2) predict errors before they mature, warn the crews, and suggest solutions. The doctrine can be stated as follows: use traditional human factors methods to prevent error where possible. In those cases where human errors penetrate the first lines of defense, automation must then detect, display, and ultimately "trap" the error and not allow it to adversely affect the system.

Much of what the author proposes requires the development of more intelligent human-computer interfaces, and the expanded use of machine intelligence. This invokes the fundamental human factors question of which functions should be assigned to humans and which to machines. The issue, of course, is not what machine or humans do better, but how the assets of each can be combined to produce an effective system. There is no need to review the question here; the reader is referred to papers by Wiener and Curry (1980), Chambers and Nagel (1985), Fadden and Weener (1984), Price (1987), Speyer (1987), and Billings (1991).

GUIDELINE NO. 14

An intervention should not produce conflicts with present equipment and procedures already in place (e.g. TCAS and GPWS giving conflicting vertical commands).

B. ERROR MANAGEMENT

In this section we shall discuss a variety of error management techniques which depend on at least present-day computer technology. We will consider the capabilities and limitations of this technology, as well as those additional developments which would be required by proposed intervention strategies.

Specific Error Intervention

Under the heading of error management, we will discuss computer-based interventions. Our aim is to find means of employing on-board computers to manage entire classes of errors (e.g. erroneous waypoint locations, illogical navigational requests, or illogical commanded airspeeds). Occasionally techniques are needed for protection from a more restricted class of errors. We would like the flexibility of computer software to be cordial to modification to meet a particular problem.

A current example is a new aural warning system that is being retrofitted onto existing A-320 aircraft, and installed as basic equipment on future A-320/330/340s. The system will warn the flight crew should they enter a low-energy flight regime. The device is the result of two accidents involving A-320s in which the aircraft flew too low and slow to recover before striking terrain. According to an Airbus Industrie official, the system is "designed to protect the aircraft when pilots are flying manually - meaning the autopilot and autothrottle are disconnected." The data used are the aircraft's speed, angle of attack, deceleration rate, and engine thrust (AWST, 1991, p. 30).

Feedback and Feedforward Mechanisms

The ability of the computer to provide feedback and feedforward information enhances the operator's knowledge of the state and future state of the system. Feedback provides the operator with information on the impact of his/her control inputs. Feedforward mechanisms predict and display the future state of the system, which may provide guidance for control inputs. Feedforward is seldom an inherent part of the system; it must be inserted artificially. Feedback may be inherent to the system (e.g. pre-stall buffet), or may be artificially inserted or enhanced (e.g. electronic stall warning devices).

Feedback. One of the virtues of computer graphic systems is their ability to enhance feedback. However, this capability has not always been exploited to its full potential. A persistent complaint about automatic systems is their inherent paucity of feedback. Norman (1990) has written on this subject, and attributes the problem to designers who are not sensitive to the need to deliver feedback to the operators, since it would appear to the designer that everything is working as planned. Norman gives several interesting examples where the aircraft's automation compensated for system's failures. One case involved a gradual power loss in the Number 4 engine of a B-747; the other a potentially catastrophic fuel leak. In both cases, the crew was unaware that anything was wrong. The automation silently and efficiently compensated for the power loss and the fuel imbalance, to the extent that the crew was unaware of both the basic unhealthy condition and the computer's efforts to deal with it.

In these examples, it is clear that the automation is so highly capable of providing compensation that the crew was unaware of the abnormal conditions. There are two dangers here:

1) The crew incorrectly believes that things are normal, when human intervention (beyond the authority of the automation) may soon be required.

2) If automation fails, the crew may have little awareness of the condition that led to the failure, to the possible detriment of recovery.

Norman argues that the problem with systems that seem to be troublesome is not overuse of automation, but lack of feedback. In these two examples it would have been desirable for the system to inform the crew that it was compensating to an unusual degree, as if to say, "Captain, I am steadily increasing aileron to keep this plane on its heading, so something must be creating asymmetric thrust, and what's more it is getting worse." Such a dialogue is not entirely fanciful. With the sophistication of modern flight guidance systems, it should not be difficult to enhance the feedback in this manner. The difficulty would not lie in developing the software or hardware, but in producing a system intelligent enough to provide feedback enhancement for a vast number of conditions that might arise, including those which the designers may not have anticipated.

Norman goes on to state that the problem with today's automation is that its intelligence is at the wrong level; it is both too high and too low. He finds current automation level high enough to do most of the jobs and do them dependably, but not high enough to provide feedback to the crew, or to avoid problems of information transfer when the human must take control. His point is interesting: that we need computer-based systems that are either a little dumber or a little smarter. Cook, Woods, McColligan and Howie (1990), and Wiener (1988b) complain of "clumsy" automation: modern systems that require excessive human monitoring, increasing rather than relieving human workload.

Both of Norman's examples come from traditional jet aircraft. Modern aircraft have their own problems, perhaps at a more sophisticated level. If Norman is correct, the modern glass cockpits offer novel opportunities for human error due to lack of feedback. One such problem is an incorrect positional representation on the HSI map mode. If a programming error is made, for example a non-matching runway and ILS frequency is selected, the HSI map position will not conform to the ILS course. Also if the IRUs are not updating the FMC position of the aircraft, a map shift can occur, where the map is not located correctly with respect to the aircraft. It is not always easy to detect. Many of the pilots interviewed by the author have a map shift story to tell. The difficulty here is also lack of feedback. The HSI map display is so compelling and so helpful that pilots become dependent on it, and perhaps less critical of what they see than they should be. Since the shift may not be geographically great, it may go unnoticed. The pilot would be better off if the map display disappeared entirely. The following ASRS report illustrates a problem with feedback from glass instruments and a map display.

> Narrative: aircraft was coupled to autopilot and autopilot was armed for the ILS (8L at Atlanta). Aircraft intercepted and captured localizer at approximately 15 nm from airfield. At 5000' I identified localizer. As per company procedure, captain rotated hdg select knob to 340 deg for missed approach heading, but unknown to either of us this multifunction knob was pushed in far enough to activate "hdg hold". I did not notice the flight mode annunciator (FMA)

> window change from "loc trk" [localizer track] to "hdg hld" [heading hold]. Of course, the ADI (flight director) display remained as before with the pitch bar giving altitude hold at 5000′ and the bank bar still centered but centered because we were on heading not localizer. Obviously we gradually started to drift right. The HSI (nav display) was selected on map mode (20 mi scale). On this scale a small deviation off localizer is too small to detect. I monitored the glide slope (raw data display) and saw it descend through the flight director pitch bar. I looked at the FMA and realized we were no longer armed for the ILS. I immediately announced to the captain and disconnected the autopilot to start descent and selected arc mode on the nav display. I saw we were full scale localizer deflection so I put in about a 15 deg correction to course. At that moment Atlanta Approach called to tell us we were drifting into the parallel ILS course and he told us to maintain 4500′ until established. (He also gave us a hdg to correct). I leveled at 4700′ and as I did the localizer centered up and the ILS was resumed uneventfully. Having map mode in HSI instead of arc does not make a localizer deviation immediately obvious. Lack of continuous cross-check of FMA by pilots is a factor. Hdg select knob doubles as hdg hold button and an imperceptible extra push in on it activates heading hold. To correct the problem: fly ILS with arc (or rose) in map to make deviations immediately obvious. Additionally, multifunction knobs should not be accepted on aircraft. It is simply too easy at night when you are tired or distracted to activate the wrong function. (In the this aircraft we have 3 multifunction knobs where different functions are activated depending on how far in you push the knob. It can be very tricky sometimes). (ASRS No. 141226)

<u>Feedforward</u>. Some systems have the capability to furnish the operator with a predicted view of the future progress of the system. This provides an opportunity to enhance situational awareness and provide guidance for future actions. This principle has been called "feedforward". [Note: "feedforward" as used in human factors is not equivalent to the term as used in control theory]. Feedforward is also frequently employed in training, where the same mechanism is called "cueing." The trainee is informed, either by a living instructor or an inanimate device, of actions to be taken. Cueing has proven particularly helpful in motor skills training.

The most familiar example of feedforward to be found in aviation is the flight director. This device cues the pilot as to heading and pitch to obtain in order to achieve his short-term goal (e.g. intercept and follow glide path and localizer) as computed from information set into the mode control panel, and in the case of glass cockpits, the CDU.

As with feedback, feedforward can be implemented with relative ease on computer-driven displays. The B-767/757, for example, supports a flight-path predictor vector in the HSI map mode. It is a white, three-segment line displayed ahead of the aircraft symbol (see Figure IV-2). If the aircraft enters a turn, the white line curves in that direction, showing the future trajectory of the aircraft. The segments represent 30, 60, and 90 seconds into the future. To roll out on a given course as depicted on the map (e.g. an ILS localizer), the pilot can easily make use of the feedforward information and adjust the rate of turn. The white vector is continually recomputed and displayed; it provides both feedforward and feedback. The pilot sets an initial angle of bank; the white curved segments on the display feed information forward about the future track of the aircraft for that angle of bank, speed, and wind. Feedforward becomes feedback with respect to the appropriateness of the angle of bank that has chosen for the desired intercept, and the pilot can make an adjustment in bank angle and immediately view the new projected flight path.

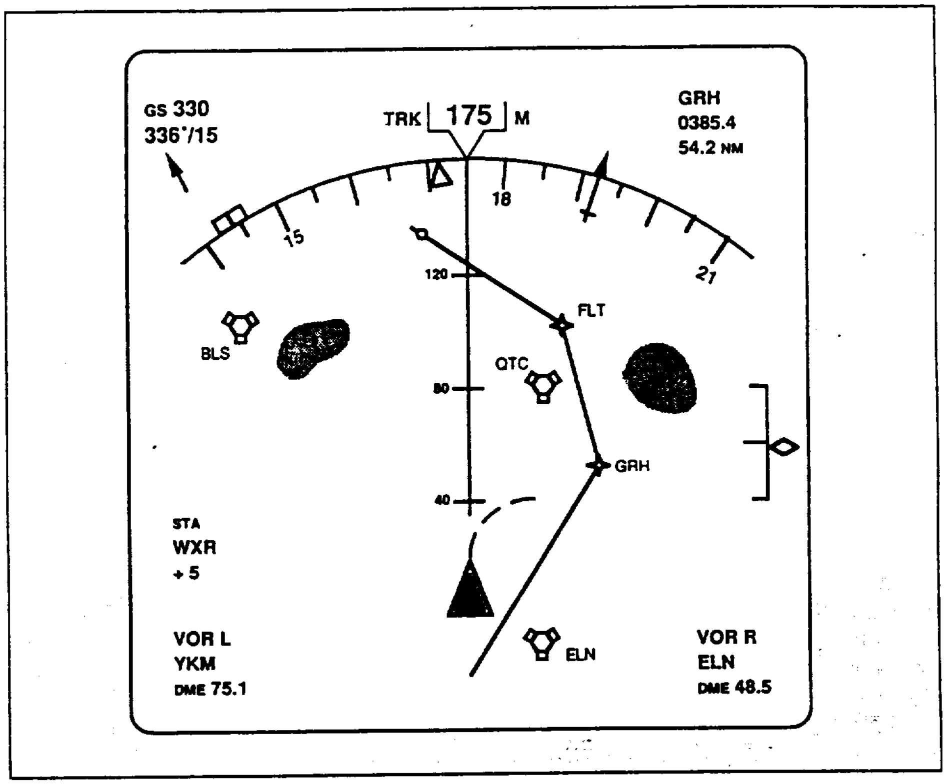


Figure IV-2. Horizontal situation indicator (HSI) display from a generic glass cockpit. Note the three-segment flight-path predictor vector ahead of the aircraft symbol and superimposed radar return. From Billings (1991).

Error-Evident Displays

Another line of defense against error is to make the error, once it enters the system, more conspicuous to the crew. Such an mechanism does not prevent the original error, nor does it ensure error tolerance. What it does is to provide the crew a better opportunity to detect their own error and remove it before it affects the functioning of the system. The author has referred to these as "error-evident displays" (1989a). The map mode of the horizontal situation indicator (HSI) of the EFIS aircraft provides an excellent example. Lateral navigational errors show up very clearly in the map mode. Error evident displays can be thought of as a form of feedback, at times employing feedforward (see example below).

The inter-relationship between feedforward and feedback can be found in the "plan" mode of the HSI map display, which allows the crew to step through the lateral course after it is entered is an error-evident system at its best. In this mode, the crew steps through the lateral flight plan one waypoint at a time. The next waypoint in line appears to move toward the aircraft symbol. Thus, the crew would be alerted if there were an illogical entry, a severe turn, or an inconsistent position on the course. With waypoint-to-waypoint navigation, an erroneously located waypoint would cause the course line to appear on the map with some highly suspect orientation, probably a sharp bend, which would alert the crew.

The author once observed a perfect example of this capability while aboard a B-767 preparing to depart Atlanta for Miami. The clearance included as a waypoint the TEPEE (note spelling) intersection near Tampa. The captain entered TEEPE (note spelling) into the Route page of the CDU. Because there is a TEEPE intersection (near Waco, Texas), the CDU dutifully accepted the erroneous spelling and established it as a waypoint on the route from Atlanta to Miami (see Figure IV-3). The sudden shift in course to the west-southwest toward TEEPE from the southward course toward TEPEE was immediately evident to the crew. A non-EFIS aircraft with the same CDU/FMS (such as some models of the B-737-300) would not have provided this form of error detection capability. The crew would have had to detect the error by some other check, but whatever the method used, it would lack the rich, error-evident depiction found on the HSI map.

Two points should be made regarding this example. First, the willingness of the FMC to accept such a clearly erroneous waypoint is an example of what the author has called the "Two 'D's" of automation: dumb and dutiful. Dumb in the sense that it will readily accept illogical input; dutiful in the sense that the computer will attempt to fly whatever is put in. Had the crew not intervened, the flight guidance system would have attempted to fly to TEEPE. Probably the "insufficient fuel" message would have been triggered: the aircraft would not have had the fuel to fly from Atlanta to Miami via Texas. In this had occurred, the computer would have detected an error and alerted the crew, albeit for the wrong reason. Later in this chapter we shall discuss the potential for on-board computers to act more intelligently and possibly detect anomalies, rather than merely display inputs that do not conform with the stated desires (e.g. original and destination) of the crew.

Then we may ask why the FAA has let stand so many possible pitfalls for crews, of which the TEEPE and TEPEE intersections are such a clear example. In the age of the FMS, the spellings and pronunciations of intersections and VORs has taken on new meaning (see Wiener, 1988a, pp. 454-455, and Figure IV-4 of this report). Intervention strategies for this problem are obvious.

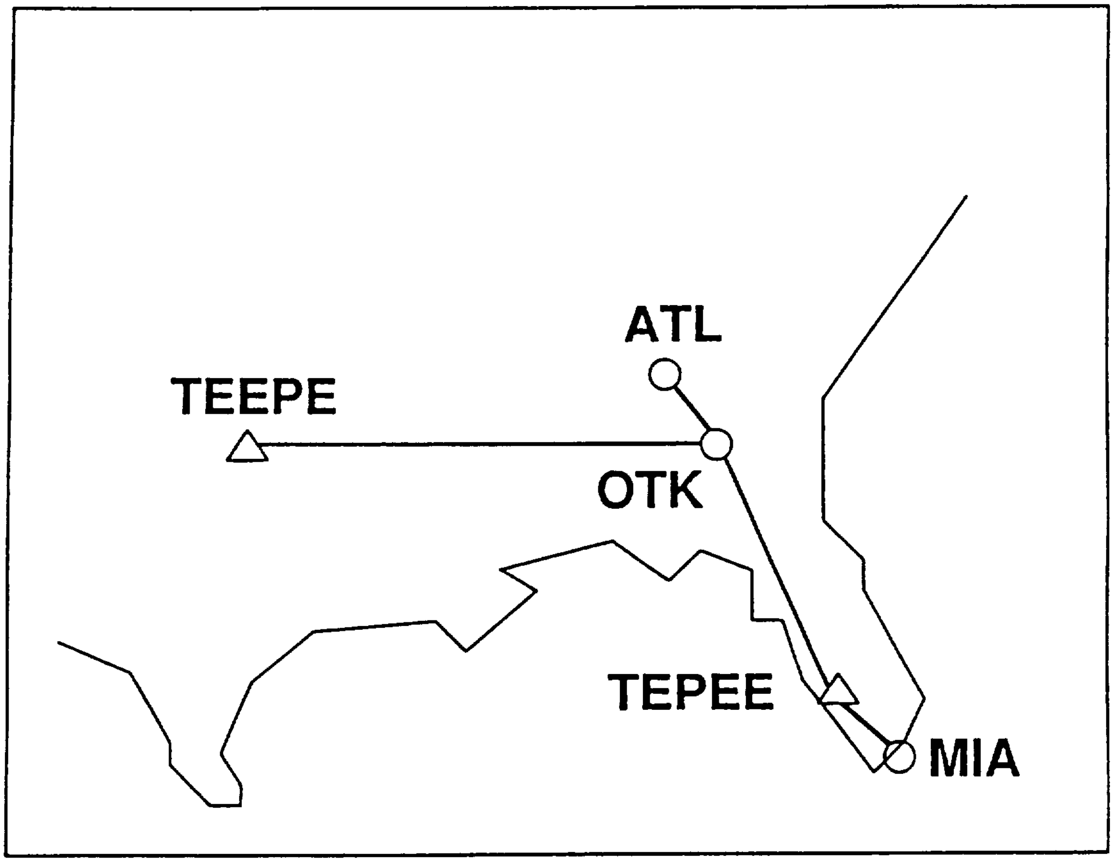


Figure IV-3. Map depiction of the location of TEPEE and TEEPE intersections.

Many of the navigational errors resulting from keyboard input described by Aarons (1988) might have prevented if the course could have been visualized. The example given in Wiener (1988a, p. 454) illustrates the peril of loading an incorrect waypoint, and the means of managing such an error. In this example, two pairs of VORs with identical names (Las Vegas and Farmington) are depicted. If the wrong waypoint were entered, the flight management computer would dutifully attempt to fly the course.

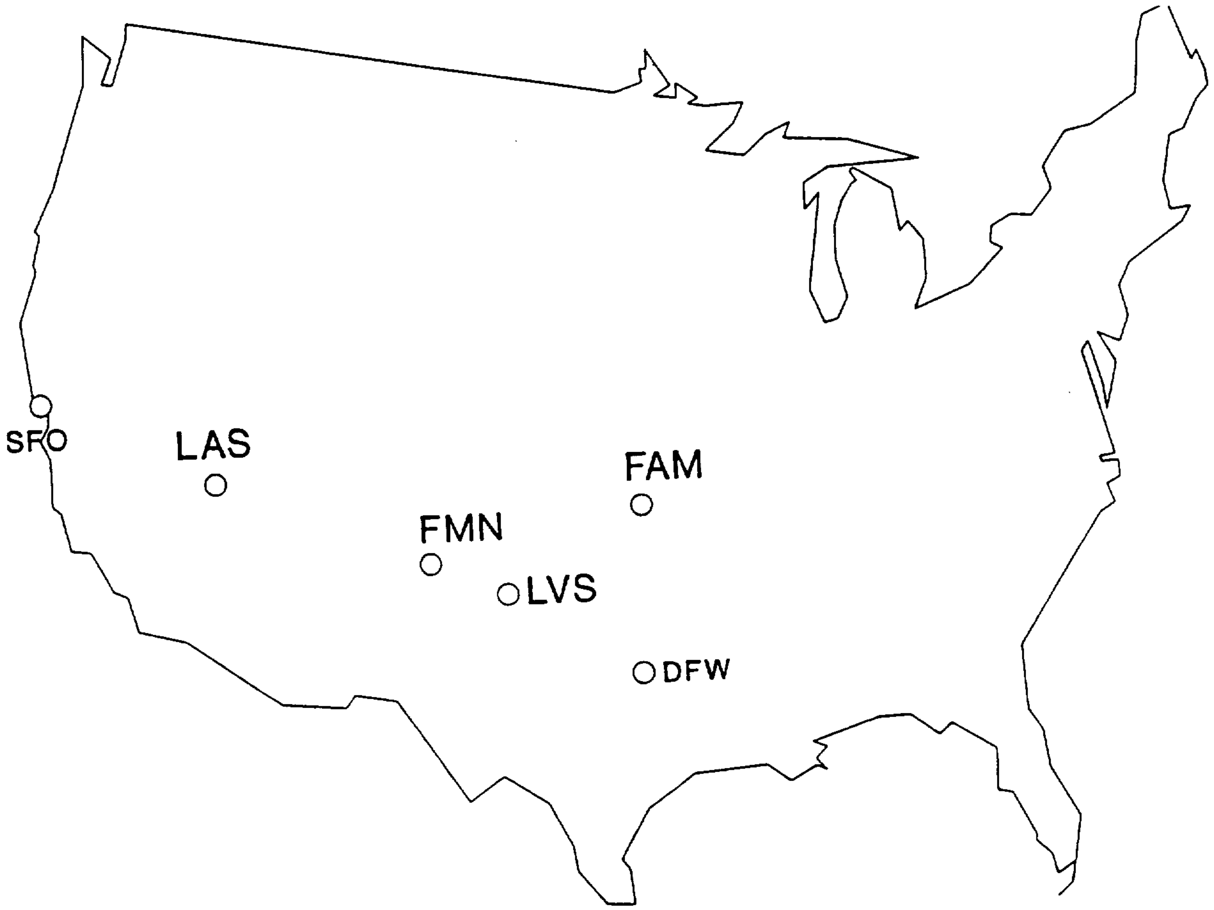


Figure IV-4. Map depiction of two pairs of VORs with same names but different abbreviations. From Wiener (1985b and 1988). Reprinted with permission of Society of Automotive Engineers.

The possibility of such an error is not fanciful. An actual case of entering the wrong Farmington is revealed in the following ASRS report:

> Cleared direct to Farmington. F/O loaded direct intercept to "FAM" and executed same. About a minute and a half later, captain loads direct intercept to "FMN" (also on our filed and cleared route of flight) and comments "it's 1061 miles to Farmington." This aroused my curiosity, and I noticed he had loaded Farmington, New Mexico (FMN) after I had correctly loaded Farmington, Missouri (FAM). Navaids with the same name, or same sounding names, are obvious areas for potential ambiguity, particularly with RNAV aircraft that can navigate direct to any point in the world. (ASRS No. 93876)

In this case it was the ability of the FMC to compute and display the distance to the active (direct intercept) waypoint, not the map display, that saved the day. Some aircraft have stored waypoint capability (FMC) without the glass HSI display; we do not know the type aircraft in the report above. It would be possible that the aircraft's route of flight was, more or less, on a line connecting FAM with FMN. In such a case, course deviation may not be evident on the HSI map.

Crews interviewed in the author's field study of glass cockpit operations (Wiener, 1989b) who had left the 757 to transition back to less advanced aircraft stated that the one feature they miss the most was the HSI map. They saw it as a great advance in safety, partly because of its ability to enhance situational awareness with respect to position, but also for its capability to display suitable emergency airports.

One could speculate that if the error-evidentiary capabilities of the glass cockpit had been present in the L-1011 that came within a few feet of colliding with a B-747 in Canadian air space over the Atlantic (Canadian Aviation Safety Board, 1989), the erroneous waypoint would have been apparent to the crew, and would have been corrected. Although there are error checking methods for traditional stored waypoint RNAV systems (see <u>FAA AC 90-79</u>, July 1980) none can compare with the graphic depiction found in the EFIS cockpit. Some error checking procedures involve doing essentially what the crew did in the Farmington example -- checking the distance to the waypoint against their flight plan, or as in the example above, against their own logic, and their personal stored database of "reasonable" distances.

One distinction needs to be made. The error-evident display does not have the intelligence to detect errors. It is merely a display system, and the management of human error ultimately depends on human intelligence to detect the error. Note that the 767 FMC did not balk at accepting "TEEPE" as a waypoint to be crossed between Atlanta and Miami. The design implication is that displays can be provided to aid in the management of error by increasing the probability that human intelligence will be sufficient to detect the error. In the next section we shall encounter systems that depend on machine intelligence and logic to perform these functions.

Goal-Sharing (Intent-Driven) Systems

It would seem prudent to build into systems the capability for the crew to inform the machine of its strategic intent (e.g. to fly from Paris to Miami), a capability that exists in the modern systems. Then all input would be checked for consistency with this intent, a capability that rarely exists. In such systems, error management would occur, not because errors were excluded, but because they would be automatically detected, and the crew advised of input inconsistent with the stated goal. Thus, using the example from the previous section, a waypoint badly out of line with a reasonable route of flight (the wrong Farmington) would be brought to the crew's attention. Many of the dramatic incidents and accidents reported in recent years might have been avoided had this capability existed. The virtue of goal-sharing and error-evident displays is that they allow the error to be trapped, rather than allowing it to affect the system.

In FMC-based systems, it is possible for the crew to input their strategic goal in very direct and unambiguous language, e.g. entering the origin and destination of a flight. Thus the goal of the operator is entirely clear to the system.

It is essential to maintain the distinction between goal-sharing and error-evident displays. In goal-sharing, it is the machine that must detect and report the anomaly. This might require development of artificial intelligence systems that may not be available today. For lateral navigation, the task may not be difficult. The course entered by the crew could be subjected to a series of logical tests, asking essentially if each waypoint is consistent with the one before and after, and if all are consistent with the stated intent (origin and destination) of the flight. Other types of errors might be more difficult to detect.

Another approach would be to allow an intelligent machine to <u>infer</u> the intent of the crew, based on recent history of the crew's inputs. This subject has been explored by Geddes (date unknown). It is too early to tell whether this procedure truly has promise for error reduction, or whether incorrect inferences might introduce more error than they remove. Also one may raise questions as to (1) why such a capability is needed in transport flight, as possibly contrasted with combat flight; (2) the degree of machine intelligence required to support it; and (3) the probability and effect of errors of inference.

Intent inferencing has enjoyed a certain popularity in the AI community in recent years, particularly in air combat applications, and no doubt will be further researched in the future. Developments in this field bear watching. For the present, the author's position is that error management could be advanced by intelligent machines that depend on the crew sharing its intent with the machine by direct communication. The immediate problem is not the determination of intent, but the development of machine intelligence that can detect and report inputs that are inconsistent with the stated intent, and do so without generating excessive false alarms.

Intelligent Warning and Alerting Systems

Most warning and alerting systems have grown up piecemeal in the cockpit, often being added one-by-one as the result of accidents (Wiener and Curry, 1980). The new glass cockpit warning systems, such as Boeing's EICAS and Airbus' ECAM have halted and reversed the continual upward spiral of the number of alerts in the cockpit. This is depicted in Figure IV-5, using the Boeing 767/757 as an example.

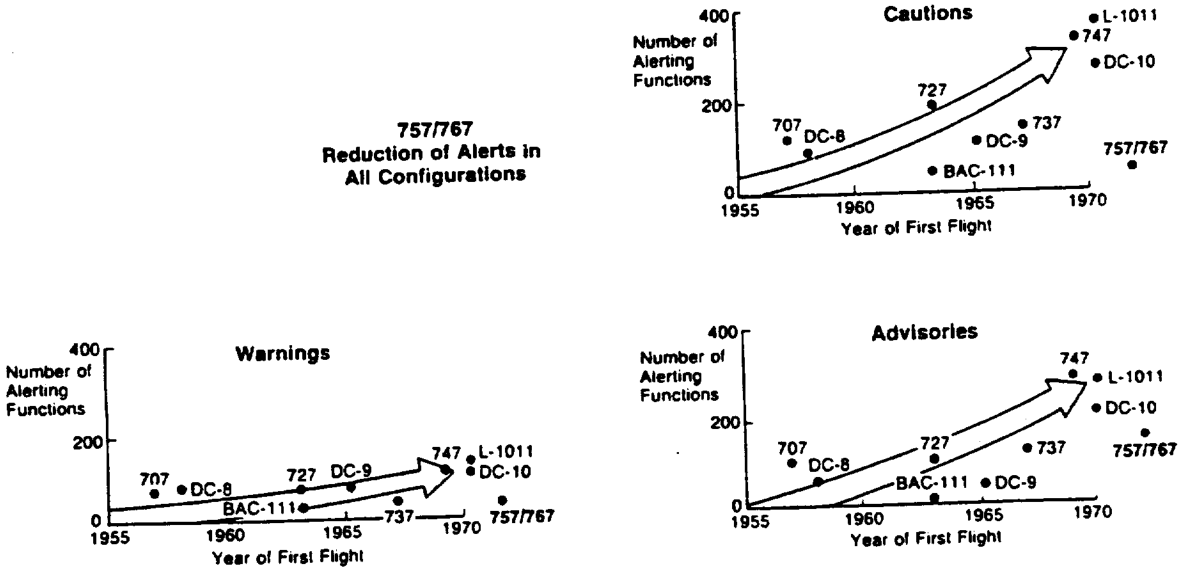


Figure IV-5. The growth of warning devices. From Morton (1982).

There is far more to warnings and alerts than merely the classic human engineering decisions about how they should be displayed. Computers now offer the opportunity for far more intelligent devices, which can analyze systems, prioritize alerts, offer solutions or even probabilistic diagnoses, and display systems schematics for diagnosis and intervention (features currently found in the A-320, MD-11, and B-747-400).

In 1980, Wiener and Curry introduced the concept of the "electronic cocoon", a metaphorical, multivariate protective shell around the aircraft. As long as the plane stayed within the cocoon, the crew would be free to operate as they saw fit, within the bounds of reason. If the aircraft penetrated the cocoon, the crew would be alerted. (See the discussion of "Predictive Systems" below).

The 1980s generation transports (e.g. B-757/767, MD-88, and A-310/320) have made great strides in reducing and simplifying the alerting systems. Today's warning and alerting systems are still essentially unintelligent systems that detect abnormal conditions when they occur, lacking the intelligence to predict problems or to detect erroneous input.

A welcome counter-example is the 767/757 fuel monitoring system previously mentioned. This is a large step in the direction of more intelligent warning systems. The insufficient fuel warning not only monitors the progress of a flight under normal conditions, but it may also, as a "side-effect", detect erroneous course input, as the author pointed out in the TEPEE/TEEPE error. Let us suppose in the example of the VORs with identical names that the crew was flying from Dallas to San Francisco and selected the wrong Farmington (Missouri) (see Figure IV-4). Even in an FMC-equipped aircraft without an HSI map (e.g., B-737-300 non-EFIS), the computer would probably catch the error because the incorrect course would trigger an insufficient fuel message. This would provide crew with a warning of its lateral navigational error, but for the wrong reason. This illustrates "trapping" an error. The incorrect input enters the system, but it is not allowed to affect it, and the crew is notified. At this point the error has not been identified, and crew must find and correct it.

Predictive Systems

In some cases it is not sufficient simply to alert the crew as soon as an alarm condition exists. An intelligent system should be able to predict trouble before alarm conditions are reached, allowing an alert before the "electronic cocoon" is penetrated.

In an earlier paper the author gave as an example the prediction of over-consumption of engine oil (Wiener, 1985b). In a 757 the EICAS set point is five quarts, at which time the crew is alerted. The author wrote that it would seem only wise to allow the computer to do more than merely monitoring and displaying present oil levels. It could continuously forecast future levels, and inform the crew if one might become critical before reaching the destination.

About a year later the author interviewed a 757 captain who related a story involving a flight from New York to San Francisco. In the 757 he had developed his own personal technique of calling up the EICAS (engine indicating and crew alerting system) pages once each hour. (See Degani and Wiener, 1991, and in preparation, for the difference between procedures and techniques.) Upon doing so east of the Detroit area, he discovered that one engine was low on oil. He contacted the company, who advised him to continue monitoring oil quantity. Since the over-consumption continued, and the captain made the decision to divert to Detroit.

Had he not had this "personal procedure", he might have continued into the western part of the U.S., where airports with adequate facilities are far apart, before being alerted at the five-quart set point, causing at least a diversion to an airport less adequate for both maintenance and passenger service. If it had been an over-water flight, the situation would have been more critical. We are long overdue in developing systems that can forecast trouble, rather than merely waiting for it to occur.

Predictive alerts are a special form of feedforward, and should not be a difficult problem for an on-board computer. Sensors already aboard the aircraft feed information on the present state of systems to the FMC. It should not be difficult for the computer to use forecasting algorithms to predict future states of the systems being sampled. An alarm logic would determine the need to alert the crew, based on design decisions such as how far forward (in time) to predict, and how far backward in time to include samples in the forecasting equations. Mathematical forecasting techniques such as exponential smoothing allow the forecasting equation to place relatively higher weights on recent experience than on aging experience, thus looking backward, but mathematically discounting the importance of "ancient history."

System Recovery

A final step in error management is system recovery. This concept requires that once an error is detected, there must be a effective means of removing it and allowing the system to recover. In brief, we want to be certain that our system does not permit irreversible errors.

The first step is detection: this has been covered partially in our discussion of feedback, and error-evident displays.

Detection is a function of the extent to which the system properly displays abnormal conditions, and the ability of the human to monitor the displays. The subject of human vigilance in automated systems has been extensively researched, and is well documented (Mackie, 1987; Wiener, 1987a; Coblentz, 1989).

The next step is to make certain that the crew has an escape for any error they may make, the reversibility criterion. With traditional aircraft, this was usually not a problem. Working with less sophisticated systems, the pilots were closely coupled to the machine; an error once detected could usually be reversed quite easily. The advent of highly sophisticated automation raises the question of escape from error and system recovery. Generally the problem is not that the error is irreversible, but that the recovery process can be difficult, time-consuming, and possibly error-inducing itself.

A familiar example of system recovery from error is file or text restoration in a personal computer. The most vexing error that most of us make (short of erasing an entire disk system) is to erase text, or more seriously an entire file, and then discover that we would like to have it back. Fortunately the software designers usually give us at least a limited way out. Text and files can often be "unerased."

C. SUMMARY OF MANAGEMENT TECHNIQUES

In summary, we would like systems to possess the following characteristics, given that an error has been entered, or that an alarm condition exists:

1. The anomaly is conspicuous.

2. The condition is diagnosable, and the effect of the error on the system is clear.

3. There exists a recovery technique.

4. The recovery technique is (if possible) simple, rapid, and error-resistant.

5. The technique has low probability of error itself (it should not be easy to make things worse).

6. The system is either unaffected during the time that the error was present, or can recover quickly and totally when it is removed.

7. It is clear to the operator when the error has been cleared, and if necessary, that the system is awaiting corrected input.

V. CONCLUSIONS AND OVERVIEW

A. HUMAN ERROR CAN BE MANAGED

To err is human; to manage human error is sublime. Previous chapters have made it clear that it is possible for those who design and operate aviation operations, and other high-risk systems, to erect lines of defense against error, and to intervene in both general and specific ways to protect the systems. Furthermore, we have seen that this is possible in both traditional and advanced technology aircraft. As many authors have pointed out, the high technology aircraft offer new opportunities for human error (Wiener and Curry, 1980; Wiener, 1988a; Billings, 1991; Demosthenes and Oliver, 1991; Woods, 1989, 1990). Cook, Woods, McColligan, and Howie (1990) have discussed the same phenomenon in medical applications.

It is equally important to recognize that the new technologies also offer ways and means for management of error that are not available with traditional aircraft. Any limitations in the exploitation of this technology lie not in technology itself, but in the resourcefulness of persons who can affect intervention. Thus we may conclude that the computers which drive the modern cockpit technology provide opportunities previously unknown for both the commission of and the control of human error.

In Chapter I the concept of cascaded lines of defense against human error was introduced. Chapter IV provides the framework for more global lines of defense, five levels at which technology and humans may combine to <u>manage</u> rather than necessarily prevent error. These lines of defense are:

1. Prevent the error in the first place, or make it as unlikely as possible. This is done through design, training, procedures, management, and quality assurance.

2. If an error is introduced into the system, make it as conspicuous as possible through display design and traditional human factors ("error evident" displays).

3. If the first two methods fail to block or remove the error, design the system, probably through software, to trap the error and prevent it from affecting the system. This level of defense may or may not require further developments in artificial intelligence.

4. Provide sophisticated warning and alerting systems.

5. Make certain that there is a recovery path from any error.

GUIDELINE NO. 15

> *Above all, the intervention strategy should be* *__effective__*. *It must be demonstrated to achieve the safety gain for which it was designed. Its effectiveness should be evaluated in advance by all means possible, including simulation, and post-intervention evaluations should be conducted. This is often far easier to do with hardware interventions than more subtle strategies. For example, though its usefulness is now generally accepted, what proof do we have that the sterile cockpit rule has been effective? Compare this to, let us say, TCAS, where industry could "keep score" on the number of traffic advisories (TA's) and resolution advisories (RA's), allowing it to infer the number of near-midair collisions or collisions avoided.*

B. MANAGEMENT STRATEGIES

In this section we shall discuss the process by which intervention strategies are warranted, designed, and implemented. The reader is again referred to Appendix 1, for the list of guidelines for the design of interventions.

Warrants for Intervention

The first question is how we ascertain that an intervention is required (see Guideline No. 1, Appendix 1). The usual indications for intervention to manage error are:

1. Accidents, incidents, and violations
2. Quality assurance methods (check airmen, simulator instructors, FAA air carrier inspectors and designates)
3. Reporting systems (e.g. NASA's ASRS; company irregularity reports)
4. Reports from pilots outside of established reporting systems, often word-of-mouth (e.g. pilots' union committees, direct contact with company personnel such as chief pilots, supervisors, etc.)

Top-Down vs. Bottom-Up Strategies

Degani and Wiener (1991; in preparation) have proposed a framework for establishment of flight-deck procedures (see Figure V-1). To a great extent the same methodology applies to intervention. These reports stress the role of management in determining its philosophies and strategic goals as a step preliminary to establishing flight procedures.

The novelty of the Degani-Wiener approach is that it emphasizes a top-down methodology, in which flight management first determines its overall operating philosophy; this in turn determines policies (broad statements of the way the company wants things done). From policies flow procedures. Contrast this with a bottom-up process, whereby the equipment or flight requirement itself determines the procedures, as if it exists in isolation. Such an approach leads to inconsistent, possibly conflicting, procedurization. In a later paper Degani and Wiener (in preparation) added a fourth "P" for "Practices" - what is actually practiced in the cockpit where a procedure is called for. The Four "P" model recognizes that all planning is not top-down; that bottom-up influences also exist; practices may affect procedures.

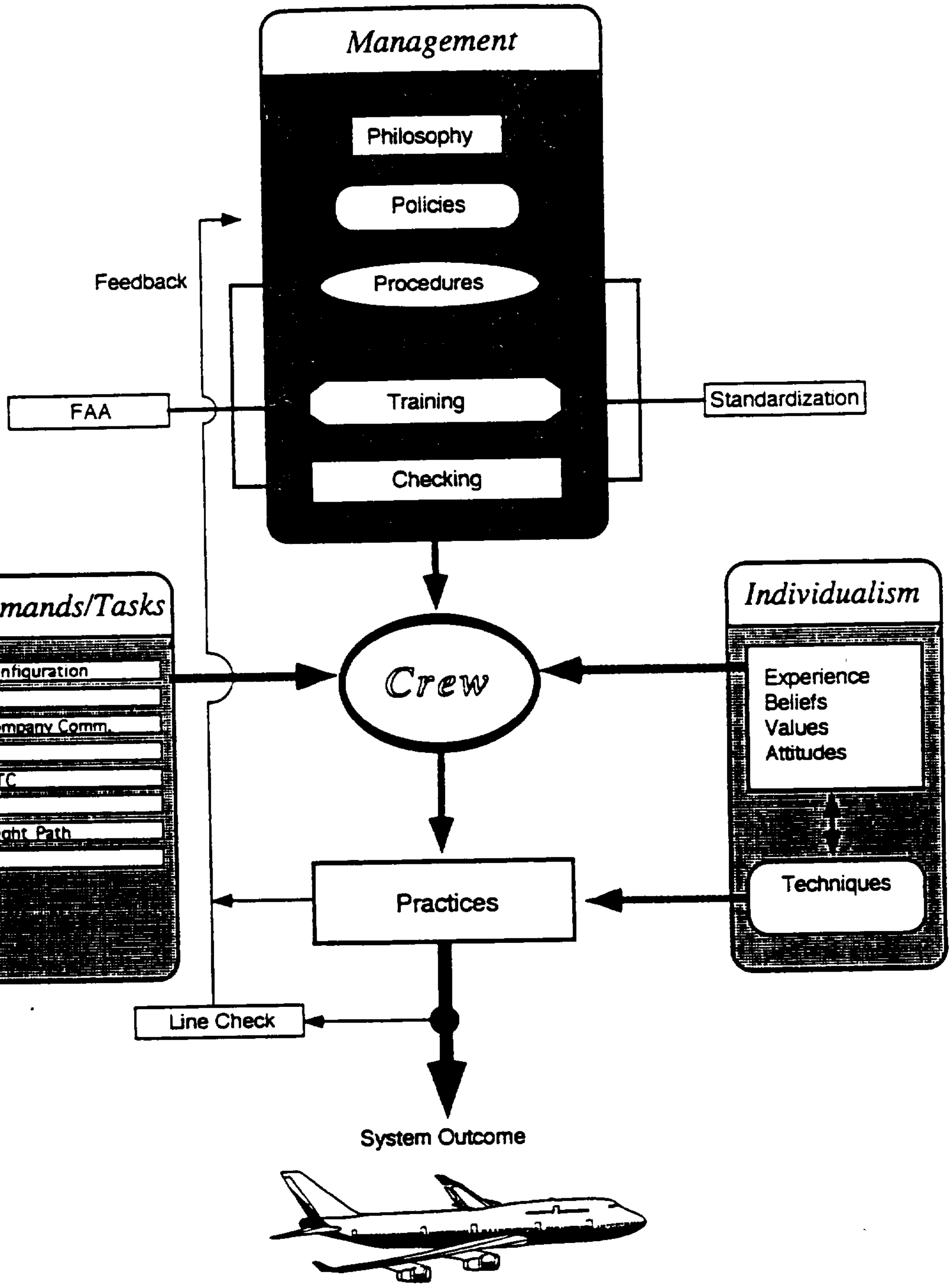


Figure V-1. The top-down design of flight-deck procedures, using the "Four P's": Philosophies, policies, procedures, and Practices. From Degani and Wiener (in preparation).

If one accepts the approach depicted above, it means that each company (perhaps also the FAA and the manufacturer) must proceed in the same way with intervention strategies, yielding philosophies and policies that will guide in the design and implementation of the intervention. For example, one company may favor hardware interventions (e.g. interlocks), another documentation (e.g. checklist modifications), and a third may have a philosophy that leads to behaviorally based methods (e.g. training, discipline, etc.)

Organizations (airlines, governmental agencies, manufacturers) may have philosophies and policies that lead to a preferred method of intervention. In the end each will chose that intervention strategy that is considered most effective, often based on hunches and opinions, rather than on sound human factors principles. Whatever the method, the author recommends that any proposed intervention be held up against the guidelines in Appendix 1. As with any list of guidelines (see also Appendix 2 and 3), there will never be a perfect fit, but the guidelines will provide at least a preliminary assessment of any proposed intervention strategy. Guidelines may also be employed as a method of comparison when there are competing candidates for intervention strategies.

Mechanistic vs. Behaviorally Based Strategies

So far we have discussed a variety of interventions, involving: 1) hardware and documentation, and 2) some behaviorally based methods such as linguistic and para-linguistic communication, training, procedures, and self-discipline (e.g. the sterile cockpit). We have not contrasted the two approaches; the guidelines in Appendix 1 are directed toward both types.

Most persons concerned with system safety would favor mechanistic interventions. These methods are less dependent on the quality and uniformity of human behavior, less vulnerable to lapses, more predictable throughout, and probably require less effort on the part of management. In the example of the physical barrier on the gust lock discussed in Chapter II, a mechanistic approach was taken because there existed so many opportunities for lapses in the behaviorally based methods (discipline, training, checklists, procedures). The outcome of the mechanistic approach was highly predictable. Barring some very unlikely occurrence, the block on the Convair's gust lock (Figure II-2a) would prevent the throttles from being opened to takeoff power with the controls locked, and it would do it consistently and predictably over the entire range of operations that one could conceive of. The same could never be said of any method which depends on standardization of human behavior.

Unfortunately there is not always a hardware interlock or a software trap available, and behaviorally based methods must be employed, imperfect though they may be. One should approach with austere caution any intervention that is behaviorally based. While the well trained and well standardized crew remains the first line of defense against error, it is also one of the most unpredictable (see Figure II-1). The tragedy of the Northwest 255 (NTSB, 1988) accident was that behaviorally based and mechanistic protections failed simultaneously. Had any of the lines of defense held, the accident would not have occurred.

Crews often impose their own mechanistic interventions to prevent behavioral errors. These should be regarded as "techniques", or personalized methods for carrying out standardized procedures (Degani and Wiener, in preparation). One example involves the use of the takeoff and landing speed book as a "flag" to indicate abnormal conditions. Many pilots wish to "hoist a flag" to remind themselves that an abnormal operation is under way that requires their attention, such as during fuel transfer, operations. The pilots place the book between the throttles to indicate that the transfer valve is open. When the operation is complete, they close the valve and remove the book. Boeing 737 pilots use the hinged magnetic compass for the same purpose. During a fuel transfer they rotate it down to the visible position; after the transfer it is stowed in the "up" position out of sight.

Here we see the superimposition of a mechanistic device as a supplement to human memory. It is both amusing and curious that in an airliner costing over 40 million dollars, this is the best device to alert the pilot to continue to check fuel balance and terminate cross-feed operations. One could imagine other possible solutions, anything from a simple electronic "egg timer" to automation of the transfer process. Each would have its own problems.

Another example of creating a mechanistic reminder was observed by the author during a line flight. The captain had developed a technique involving a specialized "flag". When he was cleared to land by the tower, he moved one of the two-position toggle switches on the ADF control box. After landing, he had a ritualistic point at which he reset the switch. Resetting the switch is the crucial operation: one can see in this technique a golden opportunity for error. This particular memory device is included in this report as an example, not a recommendation.

Ill-Defined Areas for Intervention

Certain ill-defined areas are generally believed to contribute to human error, and these may be subject to intervention. These include such poorly defined, but none the less important, constructs as fatigue, boredom, monotony, situational awareness, and complacency, as well as excessive workload. Of these, workload is the most amenable to intervention, and examples of workload reduction and management are discussed elsewhere.

As previously noted in Chapter II, Model B provides the paradigm for intervention in these ill-defined areas. In these cases the intervention is not directed at a specific error (e.g. incorrect waypoint insertion on Route page) or even a class of errors (e.g. inappropriate choice of autopilot or flight director modes), but at "human error" in general. The paradigm suggests that if the offending condition (e.g. fatigue) can be relieved, or the facilitating condition (e.g. alertness) enhanced, errors in general will be reduced. But the connection is vague.

The implementation of interventions of this type is difficult for several reasons. First, the terms themselves are poorly defined and poorly understood as scientific constructs. Take for example, "complacency." It is easy to talk about complacency, and the term enjoys a certain popularity in aviation safety. ASRS reports are replete with self-remonstrations from pilots who attribute some specific error to complacency. The error would not have occurred, in the eyes of the reporter, had he/she not been complacent. There may be general agreement on a non-scientific level about what the term means, or at least implies, but as the author (Wiener, 1981) has pointed out, "complacency" as a scientific construct lacks operational definition, and thus is difficult to measure or to attack experimentally. Intervention strategies for loosely defined and poorly understood terms will remain the most difficult to design.

Recently R. Parasuraman and his colleagues began the first organized attempt to understand and quantify complacency, particularly that portion thought to be induced by over-use of and over-confidence in automation. Their work is based on the assumption that complacency is defined by over-confidence (R. Parasuraman, Molloy, and Singh, 1991; S. Parasuraman, Singh, Molloy, and R. Parasuraman, 1992).

The reader may find the following exercise instructive: design an intervention aimed at managing error by reducing complacency, using Model B.

Fatigue is another construct that is well understood in the minds of pilots and managers, but less well defined in the minds of scientists (Graeber, 1988). To many, the warrant for intervention seems clear: errors occur more frequently when the operators are tired. As with complacency, many pilots report to ASRS and perhaps elsewhere that but for their fatigue, this error would never have occurred.

Applying Model B to "fatigue" is somewhat more tractable than to "complacency," though the two are often thought of as traveling companions. In fact, fatigue is often viewed as a causative agent for complacency. Improvements in crew scheduling are seen by pilots as the obvious intervention strategy. This is a difficult and complex issue, and one beset with strong emotions and potent economic implications. Only recently has the scientific community been able to offer schedule builders help based on experimentation into fatigue (Graeber, 1989; Rosekind, Gander, Miller, Gregory, McNally, Smith, and Lebacqz, 1993).

Scheduling is not the only candidate for intervention to relieve fatigue. Another might be napping in the cockpit on long flights. Although not specifically proscribed under U.S. FARs, the practice is generally frowned upon. Many pilots think that cockpit napping is illegal, or at least that such a thing would be a violation of certain general duty clauses in FAR 91.3.

NASA investigators (Rosekind, Gander, and Dinges, 1991) obtained special permission from the FAA in order to examine napping in the cockpit on actual airline flights. The naps were taken in the cockpit by one crew member at a time, and strictly according to a pre-arranged schedule. The evidence from this study strongly suggests that napping can reduce fatigue, defined operationally as performance on a vigilance task in the cockpit. It also reduces self-reports of fatigue state. Thus we have the elements of a Model B intervention: napping reduces fatigue; reduced fatigue increases vigilance (an early line of defense); and presumably increasing vigilance reduces errors. The case could only be improved by having measures of actual errors in the cockpit as a function of napping regimes versus a control.

In keeping with Guideline Number 4, we note that napping, particularly in a two-pilot aircraft, is not without risks. It could increase the probability that both pilots could be asleep at the same time. It may also reduce the probability.

The NASA fatigue paradigm could be applied to other ill-defined constructs, boredom and monotony being likely candidates. For years authors in the area of vigilance have discussed introducing task-irrelevant stimulation into the work place during long vigils. On the flight deck, the flight management computer could be the agent of monotony reduction.

Only a little imagination is needed to conjure up programs that could be offered to the crew through on-board computers: quiz shows, sports news, financial programs, games, or perhaps as a first step, reviews of aircraft systems. This is not without its perils, and the risks of distraction must be weighed against the possible gain in monotony management (and therefore, presumably, error reduction). One can easily imagine an incident or accident occurring at some distant time in which the probable cause was determined to be distraction during a monotony management session. Most of us would probably prefer to answer to charges of ignoring monotony in the cockpit than to being to author of such an intervention.

At this point scientific evidence offers little help: we would be hard put to quantify either the increase in risk of distraction or the reduction in monotony, and even more difficult, their relative effects on the criterion, human error. Model B interventions can be seen as far more difficult than those governed by Model A. For example, take a very specific human error: leaving the center fuel boost pumps on when the tank has emptied. This error could be attacked in any number of ways with Model A intervention.

But suppose that this very same error occurred and resulted in a fuel tank fire. And suppose further that the crew error, as a result of a thorough investigation, were attributed in part to one of the ill-defined constructs, perhaps complacency (Wiener, 1981) or fatigue (Graeber, 1988, 1989). The safety investigators and regulators would find it more than difficult to attack that portion of the problem. Error management by means of Model B will remain a challenge for the human factors profession.

In a paper on human vigilance, Wiener (1987a) noted that following two accidents that might be attributable to lack of vigilance (NTSB, 1986) the NTSB recommended that the FAA:

"Apply the findings of behavioral research programs and accident/incident investigations regarding degradation of pilot performance as a result of automation, and modify pilot training programs and flight procedures to take full advantage of the safety benefits of automation technology" (NTSB Recommendation A-84-123, November 15, 1984).

Wiener later asks his reader: "If you were assigned to the FAA, and NTSB Safety Recommendation A-84-123 were dropped on your desk, what steps would you take?"

Emerging Technologies

In the previous chapter, the potential for intervention through advanced technologies was discussed. These ranged from fairly straight-forward, computer-based capabilities to the somewhat more exotic devices, such as more sophisticated warning and alerting systems. Many of the interventions discussed could be easily implemented using today's technologies, both in hardware and software; they need not await the development of more sophisticated methods.

Some methods that have been discussed border on artificial intelligence, for example the concept of goal-sharing (intent-driven) systems. The ability to deduce that certain computer inputs, such as waypoints, are not in keeping with the stated goal of the crew (to fly from a stated origin to a stated destination) could be done fairly simply. A logical flight path (course) could be determined, and tolerance limits could be established, somewhat like a traditional control chart is used in industrial quality assurance. If a waypoint falls outside of the limits, the crew is notified.

Other applications would require either intelligent systems or elaborate computer programs. Using the previous example, an incorrect waypoint could be within tolerance for lateral error, but could result in flight through a military operations area (MOA). An intrusion could be detected if the boundaries of the MOAs were included in the database (they are not presently), and if software could check that the course as entered would not penetrate a MOA. This would require considerably more programming. In order for machine intelligence to supplement human intelligence, more eventualities would have to be considered, more data stored, and more instructions written and stored, and of course certified as flight worthy, all of which is an expensive process.

The next level would involve an attempt to model human intelligence by computer, and now we have arrived at the doorstep of artificial intelligence. For such systems to work, they would have to be programmed to operate at least at the rule-based level and to truly mimic human intelligence, at the knowledge-based level. (For a discussion of these levels, see Rasmussen, 1986, Chapter 9). At the rule-based level, specific interventions may take place (e.g. the computer would store a rule saying that the fuel boost pump should not be running in a dry tank) because the rule is stated. The problem in all rule-based systems is the vast dimensions of the required set of rules.

For the system to be knowledge-based, the plans would be continuously compared to the goals which the crew has shared with the computer. The computer would have to store symbolic relationships that would mimic human intelligence. In the example above, the system must "know", as a pilot does, that an electrical pump running in a fuel tank without fuel as a coolant would become hot and become a potential fire hazard. It would "know" this because it, like the human, it knows that electrical energy converted to mechanical energy generates heat, that aircraft fuel is generally cool, dissipating heat, and that heat is a fire/explosion hazard, particularly near combustibles, and so forth. It would know this for the same reason the reader knows it: the rotation-heat-fire relationships have been learned, either through "training" or "experience."

Does artificial intelligence in its full-blown form offer promise for error intervention? Can AI be developed to detect those rare cases and conditions that are the stuff that accident reports are made of, the errors "nobody ever made before?" It is difficult to say at this early stage in the development of the technology. There is always the temptation to point to amazing computer solutions and say, "just turn it over to the computer." As with any intervention, the implementation of AI must also be held up to the guidelines of Appendix 1. We must consider the well established fact that computer-based systems, particularly as their programs become more exotic, can themselves generate never-before errors.

We cannot afford to ignore AI as a potential error management technology. Promising developments in AI applications in combat aircraft suggest the potential for AI in civil aircraft. In combat aircraft, AI assists the crew in complex tasks such as target evaluation, planning, computation of threat-minimizing routes to and from the target, damage evaluation and control, and weapons selection.

C. THE ROLE OF GOVERNMENT

Thus far the focus of the discussion has been on the designer and operator of aircraft. In this section we will explore the role of governmental authorities, primarily the FAA, in devising and implementing interventions. We will concentrate on the regulatory authority of the FAA, and not on its role as operator of the air traffic control system.

Rule-Making Authority

The FAA has the legal responsibility to promote air safety, and the authority to do so through rule-making and enforcement. As such, many of the FARs that exist today may have originated as intervention strategies, some of which were governed by Model A, some by Model B. The FAA also influences human error through its certification process, although this appears to be a weak link. Unfortunately, under FAR Part 25, the only references to human factors engineering deal with the necessity to conduct workload analyses in order to certify the aircraft for the size of the crew for which the design is submitted. There is no FAR requirement to analyze human error potential, although this may take place informally during the certification process.

When errors are discovered by the FAA (through accidents, incidents, check airmen, or FAA's sponsorship of NASA's reporting system), they may intervene through regulations, or informally through emphasis on the matter in its various examinations and inspections of pilots and training centers. They can also intervene at airlines through their principal operations inspectors (POIs), who have considerable authority. It is the POI who must approve training programs, manuals, devices, procedures, checklists, etc.

Some interventions come as a result of a single accident. The speed limitation of 250 knots below 10,000 feet (FAR 91.70) followed the collision of a Constellation and a DC-8 over Staten

Island in 1960. The DC-8 was flying at almost 500 knots on its way to Idlewild Airport (now Kennedy), navigating on a single VOR. The Constellation was flying to LaGuardia.

The speed restriction was thought to make it less likely that an aircrew could overshoot their clearance limits. In addition, ATC modified its method of making handoffs from one controller to another. Previously aircraft were cleared to a fix, at which the radar clearance actually terminated; then another radar controller would pick up the target and clear it to the next fix. Now the radar controller effects a position handoff procedure, transferring authority for his target to the next controller. The handoff point does not terminate the clearance.

The sterile cockpit rule (FAR 121.542) has already been cited. This regulation was the result of a series of accidents in which investigations revealed less than professional approaches toward their duties on the part of the crew, as evidenced by casual conversation during critical flight phases on the cockpit voice recorder (CVR). This could be regarded as a Model B intervention: it was not aimed at a specific error in the cockpit, but a broad area which might be viewed as inattention to duties, which in turn could be responsible for specific errors (e.g. altitude deviations; failure to make callouts, failure to initiate or complete checklists, navigational errors, etc.).

Enforcement and Discipline

The FAA exerts iron-clad discipline over flight crews, with the authority to levy fines or suspend licenses. For example, the FAA has recently cracked down on crews moving their airplane out of the gate or taxiing with a passenger standing in the aisle. Fines of 1000 dollars can be levied against the captain for such an action, although, it can be argued, passenger behavior is often beyond his control. The flight crew depends on the cabin crew for information on passenger behavior, and often a passenger will stand up unexpectedly as the aircraft begins to move.

The ATC System

In this section we shall discuss briefly the influence of the ATC system on human errors in the cockpit. Errors committed by ATC personnel and opportunities to intervene in these errors are outside of the scope of this report.

The FAA has the opportunity to intervene to prevent navigational errors in several ways. They can make changes in:

1. The system itself.

2. Procedures by which the system is operated by ATC personnel (FAA manual 7110.65G).

3. Cockpit procedures.

An example of the first is related in Wiener (1987b, p. 173). An incident was reported to the ASRS in which a pilot was cleared to the TOUTU intersection. After some delay, the pilot called back to the controller and asked, "Am I cleared to DME 22 miles, or Flight Level 220 (22,000 feet)?" The pilot had, quite reasonably, imposed a numerical interpretation on the name TOUTU. ASRS referred the report to the FAA for possible intervention, and the name of the intersection was changed. The incident is amusing, but it also reveals the vulnerability of the system. It also illustrates the great value of a reporting system in bringing potential hazards to the surface where they can be attacked by interventions. TOUTU intersection no longer exists.

Examples of the second type of intervention available to the FAA are easily found in linguistic interventions. The use of the term "cleared" in ATC lexicon was mentioned in Chapter II. An example of how fragile the system can be to linguistics was revealed to the author by an airline first officer. He was flying from San Francisco to Los Angeles with a captain who was highly familiar with the CIVET approach to Los Angeles (from the east), but not the present route. As they approached Fillmore VOR (FIM), the controller cleared them to Los Angeles, "for <u>the profile</u> descent." The captain did not know that there is a profile descent ("Runway 24/25") from Fillmore to Los Angeles. He immediately turned toward CIVET. All the controller had to do to avoid this confusion was to add the words "Runway 24/25" which is the standard terminology for this profile descent, or at least to mention Fillmore, thereby identifying the correct profile descent.

The third type of intervention can also be illustrated by linguistic procedures. It is not unheard of for an aircraft awaiting takeoff clearance to take the clearance of another aircraft and initiate a takeoff. This is particularly easy to do when parallel runways are being used for takeoff. As an intervention to make this less likely, when more than one runway is in use, tower operators are now required to state the runway when issuing takeoff instructions (e.g. "American 123, runway zero-eight right, cleared for takeoff"). The aircraft crew usually acknowledges in kind, stating the runway along with their call sign and clearance, but it is not a requirement to do so.

D. SUMMARY

We have discussed the concept of intervention strategies to prevent, or at least reduce the likelihood of human errors on the flight deck. A framework consisting of lines of defense, an intervention paradigm consisting of direct and indirect strategies, and a set of guidelines have been provided.

Human error on the flight deck can never been totally eliminated. However, through judicious design, constant monitoring of accidents, incidents, and internal reports, and the aggressive use of reporting systems such as NASA's ASRS, the warrants for and the means of intervention can be found. Air transportation enjoys an excellent safety record today largely because no part of the system is ever allowed to rest.

The need to seize every opportunity to intervene was best expressed by Gerald Bruggink, a former NTSB investigator, who wrote, "Aircraft accidents are not caused by villains; they are allowed to happen by those who fail to see, or use, opportunities to reduce the likelihood of their occurrence" (1980, p. 6).

Finally, I leave the reader with an assignment. Design a practical intervention strategy to prevent "once and for all" an inadvertent no-flap/no-slat takeoff. Attack the problem from any angle; use any existing methods and technologies, or any methods that could reasonably be brought into existence. Then test your solution against the guidelines in Appendix 1.

VI. REFERENCES

Aarons, R. N. (1988). Waypoint insertion errors. Business and Commercial Aviation. June, pp. 78, 80, 82, 84-85.

Aviation Week and Space Technology. (1991, April 29). Airbus designs new aural system to warning pilots of low-energy flight regime. p. 30.

Aviation Week and Space Technology. (1988, May 9). Inquiry into 747 emergency landing focuses on fuel distribution system, training. p. 94.

Billings, C. E. (1991). Human-centered aircraft automation: a concept and guidelines. (NASA Tech. Memo 103885). Moffett Field, CA: NASA Ames Research Center.

Billings, C. E., and Cheaney, E. S. (1981). Information transfer problems in the aviation system. (NASA Technical Paper 1875). Moffett Field, CA: NASA Ames Research Center.

Bruggink, G. (1980). Accident sense and the 1978 record. American Airlines Flight Deck. November, 5-11.

Byrnes, R., and Black. R. (1993). Developing and implementing CRM programs: the Delta experience (pp. 421-4430. In E. L. Wiener, B. G. Kanki, and R. L. Helmreich (Eds.), Cockpit resource management. San Diego: Academic Press.

Canadian Aviation Safety Board. (1989). Delta Air Lines Lockheed L-1011 N1739D and Continental Airlines Boeing 747-200 N608PE, North Atlantic 52°14'N 34°00'W, 08 July 1987. (Aviation Occurrence Report No. 87-A74947). Ottawa.

Chambers, A. B., and Nagel, D. C. (1985, November). Pilots of the future: Human or computer? Communications of the ACM, 28, 1187-1199.

Chapanis, A., Garner, W. R., and Morgan, C. T. (1949). Applied experimental psychology. New York: Wiley.

Chute, R. D., and Wiener, E. L. Cockpit-cabin communications: a tale of two cultures. In preparation.

Coblentz, A. (1989). Vigilance and performance in automated systems. Dordrecht, Netherlands: Kluwer.

Cook, R. I., Woods, D. D., McColligan, E., and Howie, M. B. (1990). Cognitive consequences of 'clumsy' automation on high workload, high consequence human performance. Proceedings of Fourth Annual Space Operations, Applications, and Research Symposium. Albuquerque, June.

Curry, R. E. (1985). The introduction of new cockpit technology: a human factors study. (NASA Technical Memorandum 86659). Moffett Field, CA: NASA Ames Research Center.

Dahlby, T. (1982, February 16). Japan widens crash probe amid reports on pilot. Washington Post.

Degani, A. S., Chappell, S. L, and Hayes, M. S. (1991). Who or what saved the day? A comparison of traditional and glass cockpits. Proceedings of the Sixth International Symposium on Aviation Psychology (pp. 227-234). Columbus, OH: The Ohio State University.

Degani, A. S., and Wiener, E. L. (1990). Human factors of flight-deck checklists: the normal checklist. (NASA Contractor Report 177549). Moffett Field, CA: NASA Ames Research Center.

Degani, A. S., and Wiener, E. L. (1991). Philosophy, policies, and procedures: The Three P's of flight-deck operations. Proceedings of the Sixth International Symposium on Aviation Psychology (pp. 184-191). Columbus, OH: The Ohio State University.

Degani, A. S., and Wiener, E. L. (in preparation). The design of flight-deck procedures.

Demosthenes, T. A., and Oliver, J. G. (1991, June). Design principles for commercial transport aircraft: A pilot's perspective. Air Line Pilot, pp. 22-55.

Department of Transport (UK). (1987). *mv Herald of Free Enterprise* (Report of the Court No. 8074). London: Her Majesty's Stationery Office.

DiNunno, G. (1989). Drug test looms closer. Air Line Pilot, 58, November, 10-14.

Dornheim, M. A. (1991, February 11). 737-Metro crash raises controller workload issues. Aviation Week and Space Technology, pp. 27-28.

Edwards, E. (1988). Introductory overview. In E. L. Wiener and D. C. Nagel (Eds.), Human factors in aviation (pp. 1-25). San Diego: Academic Press.

Fadden, D. M., and Weener, E. F. (1984). Selecting effective automation. Paper presented at 1984 ALPA Safety Workshop, July. Washington

Federal Aviation Administration. (1991). FAA aviation forecasts. (FAA-APO 91-1). Washington, DC: Author.

Fotos, C. P. (1991, July 1). NTSB blames DC-9 crew error for Detroit runway collision. Aviation Week and Space Technology, pp. 27-28.

Foushee, H. C., and Helmreich, R. L. (1988). Group interaction and flight crew performance (pp. 189-227). In E. L. Wiener and D. C. Nagel (Eds.), Human factors in aviation. San Diego: Academic Press.

Geddes, N. D. (date unknown). Feasibility of the use of artificial intelligence techniques in pilot-related tasks: Goal understanding in the advanced concepts flight station simulator. Unpublished working paper (Contract NAS 2-12381). Norcross, GA: Search Technology, Inc.

Gilmartin, P. A. (1991, October 14). Aviation interests urge upgraded TCAS pilot and controller training. Aviation Week and Space Technology. p. 32.

Graeber, R. C. (1988). Aircrew fatigue and circadian rhythmicity (pp. 305-344). In E. L. Wiener and D. C. Nagel (Eds.), Human factors in aviation. San Diego: Academic Press.

Graeber, R. C. (1989). Long-range operations in the glass cockpit: Vigilance, boredom, and sleepless nights. In A. Coblentz (Ed.), Vigilance and performance in automated systems (pp. 67-76). Kordrecht, Germany: Kluwer Academic Publishers.

Helmreich, R. L., and Foushee, H. C. (1993). Why cockpit resource management? Empirical and theoretic bases of human factors training in aviation (pp. 3-45). In E. L. Wiener, B. G. Kanki, and R. L. Helmreich (Eds.), Cockpit resource management, San Diego: Academic Press.

Howland, D., and Wiener, E. L. (1963). The system monitor. In D. N. Buckner and J. J. McGrath (Eds.), Vigilance: A symposium (pp. 217-223). New York: McGraw-Hill.

Hutchins, E., and Klausen, T. (in press). Distributed cognition in an airline cockpit. In D. Middleton, and Y. Engestrom (Eds.), Cognition and communication at work. Cambridge, UK: Cambridge University Press.

Kanki, B. G., and Palmer, M. (1993). Communication and crew resource management (pp. 99-136). In E. L. Wiener, B. G. Kanki, and R. L. Helmreich (Eds.), Cockpit resource management. San Diego: Academic Press.

Kayten, P. J. (1993). The accident investigator's perspective (pp. 283-314). In E. L. Wiener, B. G. Kanki, and R. H. Helmreich (Eds.), Cockpit resource management. San Diego: Academic Press.

Kerns, K. (1990). Data link communication between controllers and pilots: A review and synthesis of the simulation literature. MITRE Corporation Report No. MP-90W00027, McLean, VA.

Lauber, J. K. (1989) Anatomy of a human factors accident. In Proceedings of the Flight Safety Foundation 34th Annual Corporate Aviation Safety Seminar (pp. 19-29). Dearborn, MI: Flight Safety Foundation.

Lautman, L., and Gallimore, P. L. (1987). Control of the crew caused accident: Results of a 12-operator survey. Boeing Airliner, April-June, 1-6.

Lenorovitz, J. M. (1992, February 3). Confusion over flight may have a role in A320 crash. Aviation Week and Space Technology, pp. 29-30.

Loomis, J. P., and Porter, R. F. (1981, April). The performance of warning systems in avoiding controlled-flight-into-terrain (CFIT) accidents. Paper presented at the First International Symposium on Aviation Psychology, Columbus, Ohio State University.

Mackie, R. R. (1987). Vigilance: Are we ready for countermeasures? Human Factors, 29, 707-723.

Meshkati, N. (1988). Human factors in complex technological systems disasters: The Iranian Airbus, Three Mile Island, Bhopal, Chernobyl. Submitted for publication.

Midkiff, A. H., and Hansman, R. J. (1992, October). Identification of important "party line" information elements and implications for situational awareness in the datalink environment. Paper presented at SAE Aerotech Conference, Long Beach, CA.

Miller, C. O. (1988). System safety. In E. L. Wiener and D. C. Nagel (Eds.), Human factors in aviation (pp. 53-80). San Diego: Academic Press.

Monan, W. P. (1983). Addressee errors in ATC communications: The call sign problem. (NASA Contractor Report 166462). Moffett Field, CA: NASA Ames Research Center.

Monan, W. P. (1988). Human factors in aviation operations: The hearback problem. (NASA Tech. Contractor Report 177398). Moffett Field, CA: NASA Ames Research Center.

Moray, N. (1988). Can decision aids help to reduce risk and human error? A program for research on the management of risk. (Report No. EPRL-88-20). Engineering Psychology Research Laboratory, University of Illinois, Urbana, IL.

Morton, P. M. (1982; revised 1983). The 757/767 engine indicating and crew alerting system: It's history, philosophy, and future. Paper presented to the Royal Aeronautical Society, London Airport Branch, and the Society of Licensed Aircraft Engineers and Technologists. London.

Nagel, D. C. (1988). Human error in aviation operations. In E. L. Wiener and D. C. Nagel (Eds.), Human factors in aviation (pp. 263-303). San Diego: Academic Press.

National Transportation Safety Board. (1973). North Central Airlines, Inc., McDonnell-Douglas DC-9-31, N954N, and Delta Air Lines, Inc., Convair CV-880, N8807E, O'Hare International Airport, Chicago, Illinois, December 20, 1972 (Report No. NTSB/AAR-73-15). Washington: Author.

National Transportation Safety Board. (1975). Trans World Airlines Boeing 727-231, Berryville, Virginia, December 1, 1974 Report No. NTSB-AAR-75-16, Washington: Author.

National Transportation Safety Board. (1976). Aerotransportes Entre Rios S.R.L. Canadair CL-44-6, LV-JSY, Miami International Airport, September 27, 1975. (Report No. NTSB-AAR-76-9). Washington: Author.

National Transportation Safety Board. (1978). National Jet Services, Inc., Douglas DC-3, N51071, Evansville Dress Regional Airport, Indiana, December 13, 1977. (Report No. NTSB-AAR-78-10). Washington: Author.

National Transportation Safety Board. (1979). Swift Aire Lines Nord 262, Marina del Rey, California, March 10, 1979 (Report No. NTSB/AAR/79-13). Washington: Author.

National Transportation Safety Board. (1984). Scandinavian Airlines Systems, DC-10-30, John F. Kennedy Airport, New York, February 28, 1984 (Report No. NTSB/AAR-84-15). Washington: Author.

National Transportation Safety Board. (1985). US Air, Inc., Flight 183, McDonnell Douglas DC9-31, N964VJ, Detroit Metropolitan Airport, Detroit, Michigan (Report No. NTSB/AAR-85/01). Washington: Author.

National Transportation Safety Board. (1986). China Airlines 747-SP, N4522V, 300 Nautical Miles Northwest of San Francisco, California, February 19, 1985 (Report No. NTSB/AAR-86-03). Washington: Author.

C-2

National Transportation Safety Board. (1988). Northwest Airlines, Inc. McDonnell Douglas DC-9-82 N312RC, Detroit Metropolitan Wayne County Airport, Romulus, Michigan, August 16, 1987 (Report No. NTSB/AAR/88/05). Washington: Author.

National Transportation Safety Board. (1989). Delta Air Lines Boeing 727-232, N473DA. Dallas-Fort Worth International Airport, Texas, August 31, 1988 (Report No NTSB/AAR-89/040). Washington: Author.

National Transportation Safety Board. (1990a). United Airlines Flight 811, Boeing 747-122, N4713U, Honolulu, Hawaii, February 24, 1989 (NTSB/AAR-90/01). Washington: Author.

National Transportation Safety Board. (1990b). United Airlines Flight 232, McDonnell Douglas DC-10-10, Sioux Gateway Airport, Sioux City, Iowa, July 19, 1989 (NTSB/AAR-90/06). Washington: Author.

National Transportation Safety Board. (1991). Northwest Airlines, Inc. Flights 1482 and 299 runway collision, Detroit Metropolitan/Wayne Countrry Airport, Romulus, Michigan, December 3, 1990 (Report No. NTSB/AAR-91/05). Washington: Author.

National Transportation Safety Board. (1993, March 25). Safety Recommendation No. A-93-46 [regarding TCAS and TCAS training].

Norman, D. A. (1981). Categorization of action slips. Psychological Review, 88, 1-15.

Norman, D. A. (1983). Design rules based on analyses of human error. Communications of the ACM, 26, 254-258.

Norman, D. A. (1984). Working papers on errors and error detection. Unpublished draft, Institute for Cognitive Science, University of California, San Diego.

Norman, D. A. (1990). The 'problem' with automation: inappropriate feedback and interaction, not 'over-automation'. Philosophical transactions of the Royal Society of London, 327, 585-593.

Norman, S., and Orlady, H. W. (1989). Flight-deck automation: Promises and realities. Final report of a NASA/FAA/Industry joint workshop on cockpit automation. Carmel Valley, CA, August 1988. Moffett Field, CA: NASA Ames Research Center.

O'Lone, R. G. (1992, March 23). Boeing works to keep pilot in decision loop on board advanced 777. Aviation Week and Space Technology, p. 61.

Ott, J. (1983, August 1). Air Canada 767 lands dead stick. Aviation Week and Space Technology, pp. 23-25.

Palmer, E., and Degani, A. S. (1991). Electronic checklists: Evaluation of two levels of automation. Proceedings of the Sixth International Symposium on Aviation Psychology (pp. 178-183). Columbus, OH: The Ohio State University.

Parasuraman, R., Molloy, R., and Singh, I. L. (1991). Performance consequences of automation-induced "complacency." (Technical Report No. CSL-A-91-2). Cognitive Science Laboratory, Catholic University, Washington.

Parasuraman, S., Singh, I. L., Molloy, R., and Parasuraman, R. (1992). Automation-related complacency: A source of vulnerability in contemporary organizations. (Technical Report No. CSL-A-92-1). Cognitive Science Laboratory, Catholic University, Washington.

Perrow, C. (1984). Normal accidents. New York: Basic Books.

Preble, C. (1987, July 20). Delta Air Lines officials baffled by series of unrelated mishaps. Aviation Week and Space Technology, pp. 31-32.

Price, H. E. (1987). The allocation of functions in systems. Human Factors, 27, 33-45.

Prince, C., and Salas, E. (1993). Training for teamwork in the military aircrew: Military CRM programs (pp. 337-366). In E. L. Wiener, B. G. Kanki, and R. L. Helmreich, (Eds.), Cockpit resource management. San Diego: Academic Press.

Proctor, P. (1988, August 8). Traffic cap may be needed to assure safety margins. Aviation Week and Space Technology, pp. 74-75.

Randle, R. J., Larsen, W. E., and Williams, D. H. (1980). Human factors guide to evaluating cockpit alerting and warning systems. (NASA Reference Publication NO. 1055). Moffett Field, CA: NASA Ames Research Center.

Rasmussen, J. (1981). Human errors: a taxonomy for describing human malfunction in industrial installations. (Report Riso-M-2304). Riso National Laboratory, Roskilde, Denmark.

Rasmussen, J. (1986). Information processing and human-machine interaction. Amsterdam: North Holland.

Rasmussen, J., Duncan, K., and Leplat, J. (1987). New techniques for human error. Chichester: Wiley.

Rasmussen, J., and Vicente, K. J. (1989). Coping with human errors through system design: Implications for ecological interface design. International Journal of Man-Machine Studies, 31, 517-534.

Reason, J. (1990). Human error. Cambridge, UK: Cambridge University Press.

Rogers, W. H., Logan, A. L., and Boley, G. D. (1989). Classification and reduction of human error. (NASA Contractor Report 181867). NASA Langley Research Center, Hampton, VA.

Rosekind, M. R., Gander, P. H., and Dinges, D. F. (1991). Alertness management in flight operations: Strategic napping. In Proceedings of Aerospace Technology Conference and Exposition. Long Beach, CA. September. Warrendale, PA: Society of Automotive Engineers.

Rosekind, M. R., Gander, P. H., Miller, D. L., Gregory, K. B., McNally, K. L., Smith, R. M., and Lebacqz, J. V. (1993). NASA fatigue countermeasures program. FAA Aviation Safety Journal, 3, 20-25.

Rouse, W. B. (1990). Designing for human error: Concepts for Error tolerant systems. In H. R. Booher (Ed.), MANPRINT: an approach to systems integration (pp. 237-255). New York: Van Nostrand Reinhold.

Rouse, W. B., and Rouse, S. A. (1983). Analysis and classification of human error. IEEE Transactions on Systems, Man, and Cybernetics, SMC-13, 539-549.

Ruffell Smith, H. P. (1968). Some human factors of aircraft accidents during collision with high ground. Journal of the Institute of Navigation, 21, 1-10.

Schwartz, D. (1990). Reducing the human error contribution to mishaps through identification of sequential error chains. Safety Liner. 13-19.

Scott, W. B. (1991, June 3). 777's flight deck reflects strong operations influence. Aviation Week and Space Technology, pp. 53, 57-58.

Scott, W. B. (1992, March 23). Douglas uses MD-11 cockpit success as springboard for designing MD-12. Aviation Week and Space Technology, pp. 58-59.

Sears, R. L. (1989, February). Prevention strategies for the crew-caused accident. Paper presented at Egyptian Aircraft Accident Investigation and Prevention Seminar, Cairo.

Segal, L. D. (1990). Effects of aircraft cockpit design on crew communication. In E. J. Lovesey (Ed.), Contemporary ergonomics 1990, (pp. 247-252). London: Taylor and Francis.

Senders, J. W., and Moray, N. P. (1991). Human error: Cause, prediction, and reduction. Hillsdale, NJ: Lawrence Erlbaum.

Sexton, G. A. (1988). Cockpit-crew systems design and integration (pp. 495-526). In E. L. Wiener and D. C. Nagel (Eds.), Human factors in aviation. San Diego: Academic Press.

Smith, D. (1991, March). TCAS 2 is working. Professional Pilot, pp. 54-57.

Spanish Ministry of Transport and Communications. (1978). Report of collision between PAA B-747 and KLM B-747 at Tenerife, March 27, 1977 (in Spanish). English translation published in Aviation Week and Space Technology, November 20 and 27, 1978.

Speyer, J-J. (1987, May). Cockpit design-induced error tolerance. Paper presented at 9th Orient Airlines Association flight safety seminar. Manila, Philippines.

Steenblik, J. W. (1991, May). A can of paint and a brush. Air Line Pilot, pp. 26-31.

Swain, A. D., and Guttman, H. E. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications. (NUREG/CR-1278, SAND80-00200). Washington: U.S. Nuclear Regulatory Commission.

Veinott, E. S., and Irwin, C. M. (1993). Analysis of communication in the standard versus automated aircraft. Paper presented at Seventh International Symposium on Aviation Psychology. Columbus, OH.

Veitengruber, J. E., Baucek, J. P., and Smith, W. D. (1977). Aircraft alerting system criteria study, Vol I: Collation and analysis of aircraft alerting systems data. (Report No. FAA-RD-76-222). May 1. Seattle: Boeing Commercial Airplane Company.

Weener, E. F. (1990). Control of crew-caused accidents. Paper presented at Third Annual Society of Automotive Engineers symposium on human error. December. Dallas.

Weener, E. F. (1991). Key elements of accident avoidance. Seattle: Boeing Commercial Airplane Company.

Wickens, C. D. (1984). Engineering psychology and human performance. Columbus, OH: Charles E. Merrill.

Wiener, E. L. (1977). Controlled flight into terrain accidents: System-induced errors. Human Factors, 19, 171-181.

Wiener, E. L. (1981). Complacency: Is the term useful for air safety? Proceedings of the Flight Safety Foundation Seminar on Human Factors in Corporate Aviation. Denver.

Wiener, E. L. (1985a). Beyond the sterile cockpit. Human Factors, 27, 75-90.

Wiener, E. L. (1985b). Cockpit automation: In need of a philosophy. In Proceedings of Society of Automotive Engineers Aerotech 85 Symposium (pp. 369-375). Warrendale, PA: SAE.

Wiener, E. L. (1985c). Human factors of cockpit automation: a field study of flight crew transition. (NASA Contractor Report No. 177333). Moffett Field, CA: NASA Ames Research Center.

Wiener, E. L. (1987a). Application of vigilance research: Rare, medium, or well done? Human Factors, 29, 725-736.

Wiener, E. L. (1987b) Fallible humans and vulnerable systems: Lessons learned from aviation. In J. Wise and A. Debons (Eds.), Information systems: Failure analysis. Berlin: Springer-Verlag.

Wiener, E. L. (1987c). Testimony before the National Transportation Safety Board in the accident of a Northwest Airlines MD-82 at Detroit on August 16, 1987. pp. 1032-1073.

Wiener, E. L. (1988a). Cockpit automation. In E. L. Wiener and D. C. Nagel (Eds.), Human factors in aviation (pp. 433-461). San Diego: Academic Press.

Wiener, E. L. (1988b). Congressional testimony before the Subcommittee on Transportation, Aviation, and Materials of the Committee on Science, Space, and Technology, U. S. House of Representatives, June 16, 1988. (Report No. 109). Pp. 65-71. Washington.

Wiener, E. L. (1989a). Errors and error control in high technology transport aircraft. Proceedings of the 7th Meeting on Aeronautic and Space Medicine. Paris.

Wiener, E. L. (1989b). Human factors of advanced technology ("glass cockpit") transport aircraft. NASA Contractor Report No. 177528. Moffett Field, CA: NASA Ames Research Center.

Wiener, E. L. (1989c). Reflections on human error: Matters of life and death. Presidential address at annual meeting of the Human Factors Society, Denver.

Wiener, E. L. (1993). Crew coordination and training in the high technology cockpit (pp. 199-229. In E. L. Wiener, B. G. Kanki, and R. L. Helmreich (Eds.), Cockpit resource management. San Diego: Academic Press.

Wiener, E. L., Chidester, T. R., Kanki, B. G., Palmer, E. A., Curry, R. E., and Gregorich, S. A. (1991). The impact of cockpit automation on crew coordination and communication: I. Overview, LOFT evaluations, error severity, and questionnaire data. (NASA Contractor Report No. 177587). Moffett Field, CA: NASA Ames Research Center.

Wiener, E. L., and Curry, R. E. (1980). Flight-deck automation: Promises and problems. Ergonomics, 23, 995-1011. Also published in R. Hurst and L. Hurst (Eds.). (1982). Pilot error: the human factors (pp. 67-86). New York: Jason Aronson.

Wiener, E. L., Kanki, B. G., and Helmreich, R. H. (1993). Cockpit resource management. San Diego: Academic Press.

Wiener, E. L., and Nagel, D. C. (1988). Human factors in aviation. San Diego: Academic Press.

Williges, R. C., Williges, B. H., and Fainter, R. G. (1988). Software interfaces for aviation systems (pp. 463-493). In E. L. Wiener and D. C. Nagel (Eds.), Human factors in aviation. San Diego: Academic Press.

Woods, D. D. (1986). Cognitive technologies: The design of joint human-machine cognitive systems. The A.I. Magazine, 6, Winter, 86-92.

Woods, D. D. (1989). Modeling and predicting human error. In J. I. Elkind, S. K. Card, J. Hochberg, and B. Messick (Eds.), Human performance models for computer-aided engineering. Washington: National Academic Press.

Woods, D. D. (1990). Risk and human performance: Measuring the potential for disaster. Reliability engineering and system safety, 29, 387-405.

VII. NOTES AND ACKNOWLEDGMENTS

1. This project was supported by a research grant, Number NCA2-441, from the NASA-Ames Research Center to the University of Miami. It was funded by the Federal Aviation Administration. The contract monitors were Vernol Battiste and Douglas Sweet of NASA, and Dr. Ronald Lofaro of the FAA.

2. The author was assisted at the University of Miami by Elvira Laredo, Vanessa Donahue and Lynn Russell. The author gratefully acknowledges the following persons who reviewed the manuscript: Capt. Michael Smiley, Drs. J. Victor Lebacqz, Stephen Casner, and Everett Palmer, and Ms. Sandra Hart.

   The author also acknowledges the support of the staff of the NASA Aviation Safety Reporting System, whose help was also invaluable.

3. The term "fleet" has two meanings in the airline industry. In one sense it has the usual meaning, similar to that of sea-going vessels, of all of the aircraft of all models and types in a given company's inventory. The other sense means all of those aircraft of a given type, including all models and derivatives, in inventory (e.g. the B-737 fleet). Many airlines have a management pilot designated as a "fleet manager" or "fleet captain", consistent with this usage. In this report, "fleet" usually refers to the latter meaning. In those cases where the intended meaning is all of the aircraft operated by an airline, this will be made clear.

   A distinction must be made in the case of the DC-9 and the MD-80 series aircraft. The MD-80 series aircraft are derivatives of the DC-9; the MD-80 was originally designated the DC-9-80. In this report the author considers the DC-9 models and the MD-80 series as separate fleets, even though pilots flying them have a common type rating.

   At most airlines which operate both the B-757 and 767, they are considered one fleet, due to the commonality of their cockpit.

4. The units of measure in this report are in feet and miles, as appropriate to air navigation in the U.S. and most of the world. For those wishing to convert to metric units, 1000 feet approximately equals 300 meters, and one mile approximately equals 1600 meters.

5. It is assumed that the reader is familiar with common aviation terminology and abbreviations. A glossary of some of the less familiar abbreviations and acronyms, particularly those used in the high technology aircraft, is included in Appendix 4.

6. The opinions expressed here are those of the author, and not of any agency, institution, or organization.

VIII. APPENDICES

1. Guidelines for intervention strategies 104
2. Wiener-Curry automation guidelines (1980) 107
3. Degani-Wiener guidelines for checklists (1990) 109
4. Glossary of abbreviations 111

APPENDIX 1

Guidelines for intervention strategies

1. In proposing an intervention strategy, one should ask "is this intervention necessary? Is there a well-defined problem or set of problems that it can prevent or reduce?" It is not sufficient to justify a proposed intervention by merely saying that it is "good for safety."

2. Never implement an intervention or procedure that you feel that the crews will not follow. (This is similar to the military dictum of "never give an order that you do not expect to be carried out").

3. Politically inspired interventions should be resisted. Although the motivation and intention of the Congress may be correct, legislative bodies do not have the technical expertise to specify and evaluate safety interventions, and at the very least their solutions may involve technically infeasible deadlines (e.g. ELT, GPWS, and TCAS). These may lead to immature hardware and software being installed in aircraft, with the result that effective intervention is delayed rather than hastened. This is particularly true in those cases where Congressional interventions come in the wake of a tragic accident, and political leaders (and possibly their constituents) may feel that the FAA and industry are not moving as quickly as they might.

4. Any intervention must be carefully examined to ensure that it does not interfere with other systems, diminish safety elsewhere, or create a problem for the flight crew or other personnel. For example, the early models of the Congressionally mandated emergency locator transmitter (ELT) beacon, which was legislated into service before the industry felt that it had been properly tested, contained batteries that leaked acid and damaged the structure of the aircraft. Another example is the ever-present temptation to add items to the aircraft checklist. Expanding a checklist may decrease the probability that the checklist procedure will be conducted properly (Degani and Wiener, 1990).

   A final example is the traffic alert/collision avoidance system (TCAS). While the TCAS is undoubtedly a valuable intervention in collision avoidance hazards, especially in protecting again VFR traffic, it does create additional workload and particularly "heads-down" time, which is already recognized as an undesirable by-product of cockpit automation. In such a case, a balance of hazards must be recognized, and secondary interventions may be required, e.g. restricting some use of TCAS at low altitudes.

5. If the intervention strategy involves displays, the information should be easily interpretable. For example, the early models of the ground proximity warning system (GPWS) often created confusion as to which trigger mode was responsible for the alarm. Later models of the GPWS improved the situation by identifying alert modes.

6. Any design, hardware or software, should conform to accepted standards of human factors. The designer of the intervention strategy should be mindful of published design guidelines, whether they are considered official or not (see Wiener and Curry, 1980 for automation guidelines (reprinted in Appendix 2 of this report); Degani and Wiener, 1990 for checklist guidelines (Appendix 3); Williges, Williges, and Fainter (1988) for guidelines for human-computer interaction in aviation), and Wickens (1984) for general guidelines for automated systems.

7. All interventions should be examined for any adverse effects on air traffic control (ATC). For example, shortly after the accident at Los Angeles where a USAir B-737 landed on top of a Skywest Metroliner awaiting release for takeoff on Runway 24L, it was suggested that towers discontinue their practice of allowing an aircraft to "line up and hold" on an active runway, remaining instead short of the runway until cleared for takeoff. To do so would impose immense delays on the system, for a questionable safety benefit. After reconsideration, this proposal was dropped.

8. Preferably the intervention strategy should be non-punitive. It should not place the crew at an added risk of violation or other punitive action.

9. The intervention strategy should be economically feasible and otherwise acceptable to management (e.g. minimize contractual implications). It should likewise not impose a cost elsewhere in the overall system (see No. 9).

10. Wherever possible, the intervention strategy should be common to all models within a fleet and across fleets within the same company. When an intervention is recommended or specified by the manufacturer, or imposed by agencies outside of a company (e.g. manufacturer, government) it should be common to all operators of the equipment, wherever possible.

11. Examine each proposed intervention and ask if there is an easier, less invasive, or less costly way to accomplish the same thing.

12. Examine all paperwork associated with an intervention strategy. Does this paperwork actually aid the crew, or does it place unnecessary burdens on the crew? Can the responsibility be assigned elsewhere? If additional paperwork must be implemented, can its form be made more pilot-friendly? Can its design be improved?

13. The intervention strategy should be acceptable to pilots or other affected personnel. Those who design interventions should recognize that frequently changes in flight-deck regulations and procedures may encounter initial resistance on the part of many. This can often be avoided, or ameliorated, by seeking input from those affected, and by making the reason for the intervention and the potential benefits clear to those affected (e.g. the sterile cockpit rule).

14. Intervention strategies should not be at odds with other mandated items (e.g. TCAS and GPWS giving conflicting vertical commands).

15. Above all, the intervention strategy should be <u>effective</u>. It must be demonstrated to achieve the safety gain for which it was designed. Its effectiveness should be evaluated in advance by all means possible, including simulation, and post-intervention evaluations should be conducted. This is often far easier to do with hardware interventions than more subtle strategies. For example, though its usefulness is now generally accepted, what proof do we have that the sterile cockpit rule has been effective? Compare this to, let us say, TCAS, where industry could "keep score" on the number of traffic advisories (TA's) and resolution advisories (RA's), allowing it to infer the number of near-midair collisions or collisions avoided.

APPENDIX 2

Automation Guidelines from Wiener and Curry (1980)

Control Tasks

1. System operation should be easily interpretable or understandable by the operator, to facilitate the detection of improper operation and to facilitate the diagnosis of malfunctions.

2. Design the automatic system to perform the task the way the user wants it done (consistent with other constraints such as safety); this may require user control of certain parameters, such as system gains (see Principle No. 5). Many users of automated systems find that the systems do not perform the function in the manner desired by the operator. For example, autopilots, especially older designs, have too much "wing waggle" for passenger comfort when tracking ground based navigation stations. Thus, many airline pilots do not use this feature, even when traveling coast-to-coast on non-stop flights.

3. Design the automation to prevent peak levels of task demand from becoming excessive (this may vary from operator to operator). System monitoring is not only a legitimate, but a necessary activity of the human operator; however, it generally takes second priority to other, event-driven tasks. Keeping task demand at reasonable levels will ensure available time for monitoring.

4. For most complex systems, it is very difficult for the computer to sense when the task demands on the operator are too high. Thus the operator must be trained and motivated to use automation as an additional resource (i.e. as a helper).

5. Desires and needs for automation will vary with operators, and with time for any one operator. Allow for different operator "styles" (choice of automation) when feasible.

6. Ensure that overall system performance will be insensitive to different options, or styles of operation. For example, the pilot may choose to have the autopilot either fly pilot-selected headings or track ground-based navigation stations.

7. Provide a means for checking the set-up and information input to automatic systems. Many automatic system failures have been and will continue to be due to set-up error, rather than hardware failures. The automatic system itself can check some of the set-up, but independent error-checking

equipment/procedures should be provided when appropriate.

8. Extensive training is required for operators working with automated equipment, not only to ensure proper operation and set-up, but to impart a knowledge of correct operation (for anomaly detection) and malfunction procedures (for diagnosis and treatment).

Monitoring Tasks

9. Operators should be trained, motivated, and evaluated to monitor effectively.

10. If automation reduces task demands to low levels, provide meaningful duties to maintain operator involvement and resistance to distraction. Many others have recommended adding tasks, but it is extremely important that any additional duties be meaningful (not "make-work") and directed toward the primary task itself.

11. Keep false alarm rates within acceptable limits (recognize the behavioral impact of excessive false alarms).

12. Alarms with more than one mode, or more than one condition that can trigger the alarm for a mode, must clearly indicate which condition is responsible for the alarm display.

13. When response time is not critical, most operators will attempt to check the validity of the alarm. Provide information in a proper format for that this validity check can be made quickly and accurately and not become a source of distraction. Also provide the operator with information and controls to diagnose the automatic system and warning system operation. Some of these should be easy, quick checks of sensors and indicators (such as the familiar "press to test" for light bulbs); larger systems may require logic tests.

14. The format of the alarm should indicate the degree of emergency. Multiple levels of urgency of the same condition may be beneficial.

15. Devise training techniques and possible training hardware (including part- and whole-task simulators) to ensure that flight-crews are exposed to all forms of alerts and to many of the possible conditions of alerts, and that they understand how to deal with them.

Copies of this report can be obtained from E. L. Wiener, Box 248237, University of Miami, Coral Gables, FL 33124.

APPENDIX 3

Guidelines for checklist design and implementation from Degani and Wiener (1990)

In this appendix the authors propose several guidelines for designing and using flight-deck checklists. These considerations are not specifications, and some when applied individually may conflict. Therefore, each should be carefully evaluated for its relevance to operational constraints and the checklist philosophy-of-use in any specific airline operation. The section in the original report which explains the rationale for each guideline is given in parenthesis.

(1) Every effort should be made to avoid using the checklist as a "site" for resolving discipline problems. (3.2.3.)

(2) Standardization of checklists between fleets has many advantages, but this should be done carefully to prevent inappropriately imposing a checklist sequence and concept of one aircraft type on another. (3.3.)

(3) Airlines should attempt to standardize the names assigned to controls and displays between different fleets. (6.2.4.)

(4) Checklist responses should portray the desired status or the value of the item being considered (not just "checked" or "set"). (6.2.3.)

(5) The use of hands and fingers to touch appropriate controls, switches, and displays while conducting the checklist is recommended. (7.2.2)

(6) The completion call of a task-checklist should be written as the last item on the checklist, allowing all crew members to move mentally from the checklist to other activities with the assurance of all pilots that the task-checklist has been completed. (5.3.)

(7) A long checklist should be subdivided to smaller task-checklists or chunks that can be associated with systems and functions within the cockpit. For example, a BEFORE START checklist can easily grow to be very lengthy. If so, it can be subdivided as suggested above. (7.1.1.)

(8) Sequencing of checklist items should follow the "geographical" organization of the items in the cockpit, and be performed in a logical flow. Training departments should provide a pictorial scheme of this flow for training purposes. (7.1. and 7.2.)

(9) Checklist items should be sequenced in parallel to internal and external activities that require input from out-of-cockpit agents such as cabin crew, ground crew, fuelers, and gate agents. (7.2., 5.4., and 8.2.2.)

(10) The most critical items on the task-checklist should be listed as close as possible to the beginning of the task-checklist, in order to increase the likelihood of completing the task before interruptions may occur. We note that this guideline could be in conflict with Nos. (8) and (9) above. In most cases where this occurs, this guideline (10) should take precedence. (7.2.)

(11) Critical checklist items such as flaps/slats, trim, etc., that might be reset prior to takeoff due to new information should be duplicated between task-checklists. (7.2.)

(12) Checklists should be designed in such a way that they will not be tightly coupled with other tasks. Every effort should be made to provide buffers for recovery from failure, and a way to "take up the slack" if checklist completion does not keep pace with the external operation. (8.2.)

(13) The TAXI checklist should be completed as close as possible to the gate and as far away as possible from the active runway(s) and adjacent taxiways. (8.2.)

(14) Flight crews should be made aware that the checklist procedure is highly susceptible to production pressures. These pressures "set the stage" for errors by encouraging substandard performance, and later may lead some to relegate checklist procedures to second level of importance, or not use them at all in order to save time. (8.2.3.)

(16) FAA officials, particularly Principal Operations Inspectors, should be sensitive to cultural, traditional, and philosophical factors in airline companies and their effect on checklists submitted for their approval. There should be no compromise, however, regarding the critical "killer" items. (3.)

(17) Likewise, when a merger occurs, checklists of the acquired airline should be carefully examined for their differences. Knowledge gained by the acquired airline in operating a specific model should not be ignored. Differences in concepts and operating procedures should be resolved in a manner that enhances safe checklist behavior of all crew members. (4.)

Copies of this report can be obtained from A. S. Degani, MS 262-4, NASA-Ames Research Center, Moffett Field, CA 94035.

APPENDIX 4

Glossary of abbreviations

ACARS	ARINC communication and reporting system
ADI	attitude director indicator
AFCS	automatic flight control system
AI	artificial intelligence
AOA	angle of attack
AQP	advanced qualification program
ARINC	Aeronautical Radio, Inc.
ASRS	Aviation Safety Reporting System (NASA)
CDU	control-display unit
CFIT	control flight into terrain (accident)
CRM	cockpit resource management; crew resource management
CRT	cathode ray tube
CVR	cockpit voice recorder
ECAM	electronic centralized aircraft monitor (Airbus)
EEC	electronic engine control
EFIS	electronic flight instrument systems
EICAS	engine indication and crew alerting system (Boeing)
ELS	electronic library system
ELT	emergency locator transmitter
FAR	federal aviation regulation
FMA	flight mode annunciator
FMC	flight management computer
FMEA	failure mode and effects analysis
FMS	flight management system
GPWS	ground proximity warning system
HSI	horizontal situation indicator
INS	inertial navigation system
IRS	inertial reference system
IRU	inertial reference unit
LNAV	lateral navigation
LOFT	line oriented flight training
LOS	line oriented simulation
MOA	military operations area
MSAW	minimum safe altitude warning
PF	pilot flying
PNF	pilot not flying
RNAV	area navigation
TCAS	traffic alert/collision avoidance system
TMC	thrust management computer
VNAV	vertical navigation

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY ***(Leave blank)***

2. REPORT DATE
August 1993

3. REPORT TYPE AND DATES COVERED
Contractor Report

4. TITLE AND SUBTITLE
Intervention Strategies for the Management of Human Error

5. FUNDING NUMBERS
NCA2-441

6. AUTHOR(S)
Earl L. Wiener

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Miami at Coral Gables
Department of Management Science
P. O. Box 248237
Coral Gables, FL 33124

8. PERFORMING ORGANIZATION REPORT NUMBER
A-93120

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
NASA CR-4547

11. SUPPLEMENTARY NOTES
Point of Contact: Victor Lebacqz, Ames Research Center, MS 262-4, Moffett Field, CA 94035-1000;
(415) 604-0013

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified — Unlimited
Subject Category 03

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 words)***

This report examines the **management** of human error in the cockpit. The principles probably apply as well to other applications in the aviation realm (e.g. air traffic control, dispatch, weather, etc.) as well as other high-risk systems outside of aviation (e.g. shipping, high-technology medical procedures, military operations, nuclear power production).

Management of human error is distinguished from error prevention. It is a more encompassing term, which includes not only the prevention of error, but also a means of disallowing an error, once made, from adversely affecting system output. Such techniques include: (1) Traditional human factors engineering, (2) Improvement of feedback and feedforward of information from system to crew, (3) "Error-evident" displays which make erroneous input more obvious to the crew, (4) Trapping of errors within a system, (5) Goal-sharing between humans and machines (also called "intent-driven" systems), (6) Paperwork management, and (7) Behaviorally based approaches, including procedures, standardization, checklist design, training, cockpit resource management, etc.

Fifteen guidelines for the design and implementation of intervention strategies are included.

14. SUBJECT TERMS
Human error, Flight safety, Intervention, Glass cockpit, Automation

15. NUMBER OF PAGES
115

16. PRICE CODE
A06

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT

20. LIMITATION OF ABSTRACT