NASA Technical Memorandum 110381

Human-Centered Aviation Automation: Principles and Guidelines

Charles E. Billings

February 1996

National Aeronautics and
Space Administration

NASA Technical Memorandum 110381

Human-Centered Aviation Automation: Principles and Guidelines

Charles E. Billings, Ames Research Center, Moffett Field, California

February 1996

National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California 94035-1000

Table of Contents

Figures

Glossary of Acronyms and Abbreviations

Where appropriate, acronyms and abbreviations used here conform to FAA-approved acronyms as used in the Airman's Information Manual and other regulatory and advisory material. Acronyms and abbreviations used for cockpit devices by specific manufacturers or in specific aircraft are indicated.

AAS — Advanced automation system (FAA): the constellation of hardware, software and procedures to be implemented during the 1990s for air traffic control and management in United States national airspace.

AC, A/C — Abbreviation for "aircraft".

ACARS — ARINC Communications and Address Reporting System.

ADI — Attitude director indicator: a gyroscopic aircraft attitude display, also known as an artificial horizon. See also EADI.

ADS — Automatic Dependent Surveillance: means whereby an airplane's position, altitude and other data are automatically reported to ground control stations at frequent intervals.

AERA — Automated En Route Air Traffic Control, the FAA's advanced ATC system concept. There is no longer as clear-cut a separation between enroute and terminal automation and use of this term is declining; see also AAS, FAS.

AFSS — Automated Flight Service Station: an interactive automated facility which makes flight-relevant information available to general aviation and other pilots. See also FSS.

AI — Artificial intelligence.

ALPA — Air Line Pilots Association, a labor organization for air carrier pilots.

ALT* — (ALT-STAR): Altitude acquisition mode of flight management system, in which the airplane is commanded to climb to and level off at a pre-selected altitude.

APU — Auxiliary Power Unit, a small turbine that provides electrical power, compressed air and a source of power for airplane hydraulic systems.

ARAC — Aviation Regulations Advisory Committee, set up by FAA to secure user input to the regulatory process.

ARINC — Aeronautical Radio, Incorporated, provides international and domestic data transmission, receiving and forwarding services for air carriers and other subscribers.

ARTCC — Air Route Traffic Control Center (USA): provides enroute tactical control of air traffic.

ASC — Aircraft Systems Controller: a computer which controls the operation of an aircraft subsystem (McDonnell-Douglas MD-11).

ASD — Aircraft Situation Display, an information element of the U.S. traffic management system.

ASDE — Airport Surface Detection Equipment (radar).

ASRS — NASA Aviation Safety Reporting System, a voluntary, confidential incident reporting system operated by NASA for FAA.

ATA — Air Transport Association of America, the U.S. air carrier industry organization.

ATC — Air Traffic Control system: tactical control of air movements (in USA) by Towers and Air Route Traffic Control Centers.

ATCRBS — Air Traffic Control Radar Beacon System: a surface transponder-interrogator system which obtains information from aircraft.

ATCSCC — Air Traffic Control System Command Center (USA): FAA organization whose mission is to balance air traffic demand with system capacity (strategic traffic management). Also referred to here as SCC.

ATCU — Air Traffic Control Unit: the forerunner of today's air route traffic control centers.

ATM — Air traffic management: strategic direction of air movements (in USA, by ATC System Command Center). Also a planned NASA research and development initiative.

AWST — *Aviation Week and Space Technology:* an aerospace industry technical periodical.

CAA United Kingdom Civil Aviation Authority; the UK's equivalent of the FAA.
CAB Civil Aeronautics Board (U.S.), the organization that formerly controlled air transport in the United States, and also investigated aircraft accidents. Now defunct.
CADC Central air data computer.
CD-ROM A means of storage of documents on laser computer disks with read-only memory.
CDU Control and display unit: the flight management system human-system interface (in general usage).
CFIT Controlled flight into terrain.
CFMU Central Flow Management Unit: the European equivalent of the U. S. System Command Center.
CFR Code of Federal Regulations (U.S.).
CFTT Controlled flight toward terrain.
CRM Crew or cockpit Resource Management: a concept to improve the resource management skills of pilots, cabin crews and others in the aviation system.
CRT Cathode ray tube.
CTAS Center-Tracon Automation System: a set of software modules designed to assist terminal area controllers in the management of air traffic.
CVR Cockpit Voice Recorder, a device that preserves 30 minutes of voice comments and transmissions to, from and within the cockpit.
CWS Control Wheel Steering: an autopilot mode which permits pilot input to the autoflight system using the control yoke.

DA Descent Advisor, a component of CTAS which assists controllers to order descending traffic.
Dead reckoning A means of navigating using time, estimated distance traveled and headings, all corrected for estimated winds.
DME Distance measuring equipment, an element in the common navigation system.
Doppler Aircraft-based navigation system making use of Doppler radar to sense rate of change of position.
DOT Department of Transportation, the Cabinet Agency which supervises the FAA.
DRAPHYS Diagnostic Reasoning About Physical Systems: a model-based AI diagnostic system for aircraft faults.
DUAT Direct User Access Terminal: an automated means whereby pilots can obtain weather and flight planning information from FAA resources.

E-MACS Engine Monitoring and Control System.
EAD Engine and Alert Display (McDonnell-Douglas MD-11).
EADI Electronic attitude director indicator: provides aircraft attitude information on an electronic display (CRT or other EDU).
ECAM Electronic Centralized Aircraft Monitoring system (Airbus Industrie term) .
EDU Electronic display unit (generic): a screen which displays data or graphics by any means, including CRTs, light-emitting diodes, liquid crystal or plasma displays, or other display technology.
EEC Electronic Engine Controller (Boeing 757/767).
EGT Exhaust gas temperature.
EHSI Electronic horizontal situation indicator, using a CRT or other EDU.
EICAS Engine indication and crew alerting system (Boeing 757/767, 747-400, 777).
ELS Electronic Library System: an automated system for the storage and retrieval of documents in an airplane.
EM Electromagnetic.
ES Expert System: a type of artificial intelligence reasoning and inference system.
ETMS Enhanced Traffic Management System: the advanced software system to be utilized by the FAA's System Command Center.

ETOPS Extended Twin-engine Operations: a regulatory scheme for control of overwater flights by twin-engine transport aircraft.

F-PLN Abbreviation for "flight plan".
FAA Federal Aviation Administration.
FADEC Full authority digital engine controller.
FAS Full Automation System (FAA): the advanced air traffic control system to be implemented in U.S. airspace, including conflict detection and resolution.
FAST Final Approach Spacing Tool: a component of CTAS for control of aircraft during final approach to landing.
FCC Flight Control Computer (Airbus A320/330/340 aircraft).
FCU Flight Control Unit (Airbus Industrie): the tactical mode and input data control panel for the autoflight system; located centrally at the top of the aircraft instrument panel. See also MCP.
FDP Flight Data Processor: a computer component used in air traffic control facilities.
FDR Flight data recorder: a crash-survivable recorder for aircraft data.
FLIR Forward Looking Infra-Red: sensors that detect infra-red emissions ahead of an airplane.
FMA Flight Mode Annunciation panel or function: in older aircraft, a dedicated panel, usually above or near the attitude indicator; in glass cockpit aircraft, a display of flight modes located at the top of the primary flight display.
FMC Flight management computer.
FMS Flight management system.
FSF Flight Safety Foundation: an international voluntary, user-supported air safety research and educational organization.
FSS Flight Service Station: a class of facility operated by FAA to provide flight-relevant information for general aviation pilots.

GA General Aviation: all civil aviation other than air transport.
Glonass Global positioning system, a satellite-based navigation system (Russia).
GNSS Global navigation system by satellites, a generic term.
GP Glide path, derived from any surface or airborne navigation system.
GPS Global positioning system, a satellite-based navigation system (USA).
GPWS Ground proximity warning system.
GS Glide slope, the vertical path generated by a surface transmitter for instrument approaches; an element of the instrument landing system. (Also G/S).

HDG/VS Heading/Vertical Speed, a flight management system mode in which the airplane's flight path is determined by these two parameters.
HF High frequency, a portion of the electromagnetic spectrum used for aeronautical voice and data communications. Unlike VHF and UHF bands, HF is not limited to line-of-sight; it is, however, much more susceptible to weather and solar event disruption. Until the advent of satellite communications systems, HF communications were virtually the only form of real-time voice communications in transoceanic flying.
HFES Human Factors and Engineering Society: a professional organization.
HSCT High Speed Civil Transport: a future supersonic transport airplane (generic).
HSI Horizontal situation indicator, either electromechanical or glass cockpit display. See also EHSI.

IATA International Air Transport Association, the representative organization of international air carriers, headquartered in Montreal, Canada.
ICARUS A Flight Safety Foundation technical committee set up to explore ways to reduce human factors accidents in aviation.

ICAO International Civil Aviation Organization, an arm of the United Nations; headquarters in Montreal, Quebec, Canada.
IFF Identification Friend or Foe: the military aircraft identification system adapted for use by civil air traffic management organizations.
IFR Instrument Flight Rules: a system of rules for the conduct of air traffic under conditions of limited visibility. Essentially all transport flying is done under these rules.
ILS Instrument landing system, consisting of localizer and glide slope transmitters on the ground. Also used to describe an approach conducted using ILS guidance. (Obsolete: ILAS).
IMC Instrument Meteorological Conditions: visibility below specified minima which require that aviation operations be conducted under instrument flight rules (IFR).
INIT Initialize: a flight management system mode and function.
INS Inertial navigation system, an airborne system of gyroscopes and accelerometers that keeps track of aircraft movement in three spatial axes.
IR Infra-red portion of the electromagnetic spectrum.
IRS Inertial reference system, provides inertial data for navigation, as does INS, but also provides other data to pilot and aircraft systems.
IVSI Instantaneous vertical speed indicator, an electromechanical instrument using air data quickened by acceleration data; also the display of such information on a primary flight display in a glass cockpit aircraft.

KLM The Royal Dutch flag airline.

LAF Load Alleviation Function (Airbus Industrie), automation that acts on wing control surfaces to smooth the effect of gusts in flight.
LCD Liquid crystal display.
LED Light Emitting Diode: an electronic display technology.
LGS Landing guidance system, a localizer transmitter offset from a runway's geographic orientation; used to assist aircraft to a position from which a visual landing can be accomplished. See also LOC.
LNAV Lateral navigation; also a navigation mode in flight management systems.
LOC Localizer, a surface transmitter that delineates a horizontal path to an instrument runway; a component of the ILS. Also, the path so delineated.
LORAN Long-Range Navigation system: uses ground-based low-frequency radio aids to provide triangulation-based position derivation for aircraft, marine and surface vehicles. The LORAN system in the United States is operated by the U.S. Coast Guard.

Mach, M A scale put forward by Ernst Mach which states speed relative to the speed of sound in air. M. 1=the speed of sound. The speed of sound varies with absolute temperature.
MCP Mode control panel: the tactical control panel for the autoflight system; almost always located centrally at the top of the aircraft instrument panel. Most airframe and avionics manufacturers except Airbus use this acronym. (See also FCU.)
MFD Multi Function Display: an electronic display which can be used to show various types of data or information.
MITRE MITRE Corporation, an engineering firm that conducts systems analyses and provides engineering technical support and guidance to the FAA, Department of Defense and others.
MLS Microwave landing system, a high-precision landing aid which provides the capability for curved as well as straight-in approaches to a runway, and conveys certain other advantages. The system is in advanced development and verification testing by FAA and is the future standard precision landing system presently endorsed by ICAO.
MMW The millimeter-wave portion of the electromagnetic spectrum.
MONITAUR The monitoring "front end" of the DRAPHYS and related fault diagnosis systems.

MSAW Minimum Safe Altitude Warning: a software module in air traffic control computers which warns of aircraft operating below a safe altitude above the ground.

NAS National Airspace System.
NASA National Aeronautics and Space Administration.
NATS National Air Traffic System (United Kingdom): equivalent of the United States Air Traffic Control system.
NC Numerical Control: automated machine control system using input data for production processes.
NOTAM Notice To Airmen: information concerning potential hazards to flight.
NTSB National Transportation Safety Board (U.S.), investigates all aircraft accidents.

PERF Abbreviation for "performance".
PFD Primary flight display, usually electronic. See also ADI, EADI.
PIC Pilot in command.
PIREP Pilot Report: a report concerning hazards to flight submitted by pilots to ATC facilities.
PMS Performance Management System: a forerunner of the flight management system.
PVD Plan View Display: the controller's primary display of air traffic.

QRH Quick reference handbook, a booklet containing aircraft operating procedures, especially abnormal and emergency procedures.

RA Resolution advisory: an avoidance maneuver provided by TCAS systems when another aircraft poses a serious threat.
RBES Rule-based expert system; see ES.
RDP Radar Data Processor: ATC computer modules that synthesize, from a number of radar sources, planview displays for air traffic control.
RMI Radio magnetic indicator, an electromechanical instrument showing magnetic heading and bearing to VOR or low frequency nondirectional radio beacons. Also, this information presented on an electronic display.
RNAV Area Navigation system, a generic acronym for any device which is capable of aircraft guidance between pilot-defined waypoints, such as LORAN, Doppler, INS, etc.
RVR Runway Visual Range: a measure of visibility in a runway's landing zone.

SAE Society of Automotive Engineers, a professional organization.
SAS Scandinavian Airlines System.
SBO Specific Behavioral Objectives: a method of constructing training programs oriented toward specific tasks and activities rather than general system knowledge.
SCC System Command Center (FAA): the strategic air traffic flow management organization and facility.
SID Standard instrument departure procedure.
SOC Systems Operations Center (air carriers): flight operations management organization.
SSR Secondary Surveillance Radar: radar which makes use of ATCRBS to obtain data from aircraft.
STAR Standard Arrival Route: an FAA-approved arrival route and procedure (see also SID).

T/FPA Track/Flight Path Angle, a flight management system mode in which the airplane's flight path is guided by these two parameters. See also HDG/VS.
TA Traffic advisory: an indication that another aircraft poses a potential threat, provided by TCAS systems.
TATCA Terminal Air Traffic Control Automation research and development program (FAA).
TCA Terminal Control Area: the former designation for Class B airspace.
TCAS Traffic alert and Collision Avoidance System. TCAS-II, now installed in most U.S. and many foreign air carrier aircraft, provides vertical maneuver guidance for the

resolution of serious potential conflicts; this system is mandated for U.S. transport aircraft. TCAS-III, in development, will provide both vertical and horizontal avoidance maneuvers. TCAS-I, a less expensive system, provides information concerning potential conflicts but does not provide resolution advisories.

TM — Technical memorandum (NASA)

TMA — Traffic Management Advisor, a component of CTAS.

TOGA — Take Off Go Around: an aircraft automation mode which controls and displays information about the takeoff or go-around maneuvers.

TRACON — Terminal Radar Approach Control facility (FAA).

UHF — Ultra-high frequency, a portion of the electromagnetic spectrum used for aeronautical communications and navigation. It is limited to line-of-sight.

UK — United Kingdom.

USAF — United States Air Force.

VDU — Video Display Unit, a display device.

VFR — Visual Flight Rules: the rules which govern aircraft operations under conditions of good visibility (see also IFR).

VHF — Very high frequency, a portion of the electromagnetic spectrum used for line-of-sight aeronautical communications and navigation.

VMC — Visual Meteorological Conditions: visibility conditions that permit VFR flight.

VNAV — Vertical navigation; ordinarily refers to a navigation mode used for climbs and descents in flight management systems.

VOR — Very high frequency Omnidirectional Range, a surface radio navigation beacon transmitter which forms the core of the common overland navigation system for aircraft.

VS — Vertical Speed.

VSI — Vertical Speed Indicator (generic).

WSAS — Wind Shear Advisory System: a system that provides warnings of wind shear to pilots. The system may be passive (reactive), using airborne inertial sensors which react to accelerational forces on an airplane, or active, searching the environment for evidence of shears. If the latter, it may be located either on the ground (e.g., Doppler radar) or in an airplane (Lidar and radar are both under study).

Dedication

This book is dedicated to the memory of Hugh Patrick Ruffell Smith, who introduced me to the excitement of aviation human factors in 1955 when he was a Royal Air Force Group Captain in charge of the medical flight test group at the RAF Institute of Aviation Medicine. He was a valued teacher and friend for 24 years.

Dr. Ruffell Smith's research presaged work still in progress today. His studies of visual and auditory display media, his work on improved navigation displays, and his determined (though unsuccessful) efforts to standardize flight displays and controls stand as monuments to his understanding of the tasks of pilots and the difficulties often placed in their way. His research project while a senior post-doctoral associate at the NASA Ames Research Center, "A Simulator Study of the Interaction of Pilot Workload with Errors, Vigilance, and Decisions" (1979), performed with Dr. John K. Lauber, was the primary stimulus for an enormous volume of research on and application of the principles of cockpit and crew resource management which has taken place over the past 15 years. Pat received too little credit during his lifetime for his monumental contributions, but he understood better than most in our profession the importance of what he was doing.

Acknowledgments

I am most grateful to the management of NASA's Ames Research Center for its support of my continuing studies of aviation automation during and after my tenure at Ames. C. Thomas Snyder and J. Victor Lebacqz have greatly facilitated the research. My colleagues in the Flight Systems and Human Factors Division have been most generous with their comments, criticism and encouragement.

Since my return to The Ohio State University in 1992, Professors David Woods and Philip Smith have greatly strengthened my understanding of cognitive engineering and have given much time to helping me organize, plan and execute the revised document. I must mention with special gratitude the help of Sidney Dekker, my graduate research assistant, and Dr. Nadine Sarter, whose insights into aviation automation have shaped my understanding of the cognitive bases of the human-machine interaction process.

Throughout the development of the original document and this revision, Delmar Fadden, of the Boeing Commercial Airplane Group, has been a superb teacher and constructive critic of my attempts to understand why today's aircraft have developed as they have. The Air Transport Association of America has also been most supportive of these efforts. The ATA Flight Systems Integration Committee Chair, Capt. Robert Buley, and its Executive Secretary, Will Russell of ATA, have been particularly helpful and encouraging over a long period of time. I am also indebted to others who have reviewed portions of the revised document, among them John Enders, Ted Demosthenes, Kevin Corker, Donald Armstrong, Guy Thiele, and personnel of the NASA Aviation Safety Reporting System, especially Vincent Mellone. I am deeply grateful for the invaluable assistance provided by Dr. John Lauber, who has shared his unique insights into the realities of aviation operations and aviation safety throughout the twenty years of our collaboration. Finally, I acknowledge with special gratitude the indispensable support of my dear wife, Lillian, who has made all of my endeavors worthwhile.

Foreword

Origins of this document

Automation technology, used in the control of aircraft and many industrial processes for many years, has been revolutionized by the development of the digital computer. The invention of the transistor in 1947 and subsequent miniaturization of computer components enabled widespread application of digital technology in aircraft. The period since 1970 has seen an explosion in aircraft automation technology. In 1987, the Air Transport Association of America (ATA) Flight Systems Integration Committee established an industry-wide task force to consider aviation human factors issues.

In its "National Plan to Enhance Aviation Safety through Human Factors Improvements", (Air Transport Association, 1989) the Human Factors Task Force stated that "During the 1970s and early 1980s...the concept of automating as much as possible was considered appropriate. The expected benefits were a reduction in pilot workload and increased safety...Although many of these benefits have been realized, serious questions have arisen and incidents/accidents have occurred which question the underlying assumption that the maximum available automation is ALWAYS appropriate or that we understand how to design automated systems so that they are fully compatible with the capabilities and limitations of the humans in the system". The ATA report went on, "The fundamental concern is the lack of a scientifically-based philosophy of automation which describes the circumstances under which tasks are appropriately allocated to the machine and/or to the pilot. Humans will continue to manage and direct the NAS (National Aviation System) through the year 2010. Automation should therefore be designed to assist and augment the capabilities of the human managers...It is vitally important to develop human-centered automation for the piloted aircraft and controller work station".

During the same year, NASA's Office of Aeronautics and Space Technology approved a new research initiative, "Aviation Safety/Automation" (National Aeronautics and Space Administration, 1989). Under this initiative, the Ames and Langley Research Centers were to examine human-machine interactions in aviation and future aircraft automation options. As a response to the need for a philosophy of aircraft automation expressed by the ATA, I prepared a NASA Technical Memorandum (Billings, 1991). The TM's focus was deliberately confined to aircraft, rather than aviation, automation. This constraint was appropriate at that time, but it has become less appropriate (or even possible) as each passing year has seen increases in the tightness and complexity of the integration between the airborne and surface elements of the national aviation system. I have therefore attempted to discuss air traffic control automation in some detail in this revision, recognizing that both ATC and aircraft are critical elements of a single aviation system.

The original Technical Memorandum has served a number of useful purposes, the primary one being to stimulate a dialogue among professionals in the aviation community about automation philosophy. It is my hope that this revised and expanded document will serve to further that dialogue. I have incorporated lessons learned from the considerable operational experience in advanced aircraft which has accrued since 1990, a more systematic consideration of air traffic control and management automation, and discussion of the integration of the airborne and surface elements of the aviation system.

Rationale

One need only look back over the developments of the last twenty years to realize how much has already been done to integrate advanced automation into the aviation system. Advanced, highly automated aircraft are more productive, more reliable and safer than their predecessors when managed properly. The aviation system has been strained beyond its presumed limits, yet remains safe and fairly resilient. The system is carrying more people, in more airplanes, to more places than at any time in its history.

Why, then, is this document needed? If the ATA Human Factors Task Force were beginning its work today, would it still place automation at the top of its list of concerns? Is there any substantive evidence that what we have built to date, and what we are planning to build during the remainder of this decade, will not continue to improve upon the progress of the past two decades?

The Task Force has continued its activities. Its discussions suggest that aviation automation remains as important a topic today as it was five or ten years ago. The stresses that the aviation system has experienced have exacted a price in terms of decreased residual capacity of that system to cope with inexorable demands for still greater throughput. Much more of the system's design capacity is being used; all credible projections indicate more serious capacity problems in the years ahead. The hub-and-spoke system has also created much greater traffic concentrations, and thus greater flight crew and controller workloads, at hub terminals at certain times. Hub-and-spoke implementation has also made the system less tolerant of delays and cancellations.

Automation has freed the crews of newer aircraft from dependence on point-to-point systems of navigation aids, but this freedom from defined route constraints has increased air traffic coordination requirements and has complicated conflict prediction. Economic constraints have increased the pressure on every human and machine element of the system. Each of these factors has played a part in increasing the demand for greater system precision and reliability, and each has shaped, and continues to shape, the behavior of the human operators of the system.

Technology improvements have increased aircraft and system complexity and cost. Some, like Ground Proximity Warning Systems, have conveyed substantial benefits; for some others, like electronic library systems, the benefits appear thus far to be marginal at best. It can be confidently predicted that other new technology solutions will be proposed in the future if they appear likely to improve safety or utility. It is certain that they will impose additional tasks upon the humans who operate the system. It is only slightly less certain that some or many of these novel technologies will not operate quite as planned, and that humans will be required to adapt to, compensate for, and shape the new artifacts, as they have always had to do when new technology was provided.

Readers should keep in mind that the "future" aviation system, to a considerable extent, is with us today. It will rely upon aircraft already in line service (and future derivatives of those aircraft), just as the vast majority of today's modern aircraft are themselves derivatives of machines developed as long as three decades ago. The general outlines of the future system can be seen today at any major airport. Even supersonic transport aircraft, which may well represent the most radical future technology departure from today's system, are presaged by the Anglo-French *Concorde,* which has been safely flying trans-Atlantic routes for 20 years.

This is not to say that the system will necessarily operate as does today's system. Though the aircraft may appear to be similar, today's aircraft represent vast advances over their progenitors. Their automation, in many cases, is two generations advanced, and the requirements upon the humans who operate them are considerably different. The Air Traffic Control system today operates much as it has for the past two decades, but this is about to change. Over the next decade, radical changes in hardware, software and procedures will result in much more highly automated systems for air traffic management. These changes will have profound implications for the pilots and controllers who manage and operate the national aviation system. Today's system works well, but significant problems exist, some of which relate directly to the automation that has become an increasingly important element in its operation.

This document is not only about technology, nor only about the human users of technology. Like its predecessor, it is about humans and technology, working together in highly dynamic and potentially dangerous environments to accomplish social goals, subject to a multitude of social, political and technical constraints.

Aviation is not yet one century old, yet the system it supports has grown over this time to become an absolutely essential part of our global economy. Those of us who have been privileged to work within this dynamic, rapidly-advancing system know that we can make the system do more, more effectively. The demands that will be placed on the aviation system during the next two decades make it quite obvious that we *must* do more; we must develop a still safer, more efficient and more productive aviation system, and do it quickly. The increasing needs of the users of the system demand that the system continue to improve. The improvement of the aviation system through more effective coordination between humans and automation is the goal of this document.

Charles E. Billings
Columbus, Ohio
March, 1995

Part 1: Aviation Automation: Past, Present and Future

Part 1 contains the premises of this document and most of the factual bases for the conclusions drawn in it. It describes the technology that has been applied in aviation and considers the implications of those technologies for the human operators of the aviation system.

In chapter 1, the problem is presented, the purpose of the document is explained, and definitions and assumptions are discussed. Chapter 2 briefly describes problems associated with today's aviation automation, and goes on to present a concept of human-centered aviation automation. Some "first principles" of human-centered automation are discussed. Chapters 3 discusses aircraft automation since its beginnings; the technology and its effects on human operators are described. In chapter 4, future aircraft automation is presented and its effects considered. Chapters 5 and 6 discuss air traffic control and management automation to this time and in the future. Chapter 6 also presents proposals that have been advanced for the architecture of the future automated air traffic management system.

(*Note for readers:* Most of the serious incidents and mishaps cited with a place name and year in the text are summarized in appendix 1. Investigation reports are also cited in the References.)

1. Statement of the Problem; Definitions

Introduction

This document describes the development of aviation automation, its likely evolution in the future, and the effects that these technologies have had on the human operators of the aviation system. It suggests concepts that may be able to enhance the human-machine relationship in the future system. The focus is on the interactions of human operators with the constellation of machines they command and control. I have not attempted to consider either the humans, or the automation, in isolation, because it is the *interactions among* these system elements that result in the success or failure of the system's mission.

The aviation system is a technology-intensive, spatially distributed system in which skilled human operators accomplish the goal of moving passengers and cargo from place to place utilizing complex, variably-automated machines. In no endeavor has technology been brought to bear more effectively than in the aviation enterprise, and no enterprise has more effectively stimulated the advance of technology. In the space of a century, we have moved from wood and fabric gliders to aircraft carrying hundreds of people and tons of cargo halfway around the earth at near-sonic speeds in comfort and safety.

In the course of this development process, we have learned how to automate this remarkable machinery nearly completely. The newest long-range airplanes can operate almost unassisted from shortly after takeoff in New York until coming to rest after a landing in Tokyo. The considerable psychomotor and cognitive skills of their human operators are hardly called upon unless some element of the automation fails or unanticipated environmental circumstances arise. But when the environment does not behave as expected, or when the very reliable machinery does not function correctly, we expect these human operators to do whatever is required to complete the mission safely. Is it reasonable to expect human operators in a highly automated, dynamic system always to do "the right thing" when they are called upon? Are today's aircraft designed to facilitate effective cooperation between the humans and the machines they manage? Aviation automation has conveyed great social and technological benefits, but these benefits have not come without cost. In recent years, we have seen the emergence of new classes of problems which are due to failures in the human-machine relationship.

In particular, we have seen the appearance of failures to understand automation behavior, mode errors, lack of mode awareness, and inability to determine what automation was doing. Common to these occurrences have been complex, tightly-coupled automated systems which have become more autonomous and authoritarian, and which provide inadequate system feedback to human operators. These are not isolated problems, and they will not be fixed by "local" measures. They are *system* problems, and they require systematic correction.

It is these accidents and incidents that have motivated this inquiry into aviation automation. I will suggest here that a different approach to automation, which I have called "human-centered automation", offers potential benefits for system performance by enabling a more cooperative human-machine relationship in the control and management of aircraft and air traffic. This approach requires, and encourages, more effective coordination among system elements, so that there is less likelihood of misunderstanding or misinterpretation of system state, or which element is performing what functions, and a more cooperative relationship among system elements.

Background

It has long been an article of faith that from 65-80% of air transport accidents are attributable in whole or part to human error. The figure has been relatively stable throughout the jet era. Indeed, one of the motives for increasing automation in transport aircraft has been the desire by manufacturers and operators to decrease the frequency of human errors by automating more of the tasks of the pilot (Wiener, 1989). Similar motives underlie, at least in part, the interest in automating the Air Traffic Control system. While one can argue with the usefulness or appropriateness of the retrospective attribution of "human error" in aviation accidents, all of which have multiple overt and latent cause factors (Lauber, 1989; Reason, 1990; Hollnagel, 1993), the aviation community and the public clearly believe that the human is potentially a "weak link" in the chain of accident causation (Boeing, 1993). What has been our experience with aviation automation to date? Is there good evidence that the considerable amount of automation already in place has affected accident or incident rates? The answer to this question, briefly, is, "yes and no". But the question is also too simplistic, for "automation" is not a single entity.

Examination of aviation incident and accident data from the past two decades reveals two seemingly contrary trends. On the one hand, there have been sharp declines in certain types of accidents that appear almost certainly to be due to the introduction of automatic monitoring and alerting devices such as the ground proximity warning system (GPWS), introduced in 1975. On the other hand, there is clear evidence that despite the application of automation technology to this problem, controlled flight into terrain accidents still represent perhaps our most serious safety problem. Collision avoidance systems (TCAS) and wind shear advisory systems (WSAS) have more recently been installed in transport aircraft. Like GPWS, these devices can detect environmental conditions that may not be obvious to the unaided human senses. All make use of sophisticated sensors and algorithms to detect, evaluate and provide timely warning of critical threats in order to permit avoidance action by pilots. TCAS has almost certainly prevented collisions, though it, like GPWS, is plagued by nuisance warnings and it has caused serious problems for air traffic controllers. At least 20 fatal wind shear accidents have occurred since the introduction of jet transports and WSAS has the potential to assist in preventing such catastrophic microburst encounters, though in at least one recent case it failed to provide timely warning of a microburst event which caused a disaster.

There is also a contrary trend in accident data. Several mishaps and a larger number of incidents have been associated with, and in some cases may have been caused by, aircraft automation, or more properly by the interaction between automation and the human operators of aircraft. In some cases, automated configuration warning devices have failed or been rendered inoperative and flight crew procedures have failed to detect by independent means an unsafe configuration for takeoff. In other cases, automation has operated in accordance with its design specifications, but in a mode incompatible with safe flight under particular circumstances. In still others, automation has not warned, or flight crews have not detected, that the automation was operating at its limits, or was operating unreliably, or was being used beyond its limits. Finally, we have seen incidents and a few accidents in which pilots have simply not understood what automation was doing, or why, or what it was going to do next.

It is clear, as the ATA report stated (see Foreword), that aviation automation has conveyed important benefits. It is also clear that certain costs have been associated with automation, and that the presence of automated devices has changed human operator behavior, often for the better but, in a few cases, for worse. If we observe Wiener's (1993) maxim that automation does not eliminate human error, but rather changes its nature and possibly increases the severity of its consequences, it is necessary to understand how these devices influence the humans who work with them, and how humans use and shape automated devices as tools with which to accomplish their work.

Purpose of this document

My purpose in writing this document is to describe and exemplify several classes of problems that are associated with the implementation of advanced automation in the aviation context. These problems interfere with the effective operation of the aviation system and in some cases degrade the safety and reliability of the system. I shall attempt to show that these problems arise at the conjunction of humans and automated devices in this human-machine system, and I shall propose that a philosophy or construct which I call "human-centered automation" may be of assistance in resolving these problems in the future system by improving the cooperation between humans and machines.

Definitions

"*Automation*", as used here, refers to systems or methods in which many of the processes of production are automatically performed or controlled by autonomous machines or electronic devices. I consider automation to be a tool, or resource—a device, system or method by which a human operator or manager can accomplish some task that would otherwise be more difficult or impossible, or a device or system which the human can direct to carry out more or less independently a task that would otherwise require increased human attention or effort. As used here, the word "tool" does not foreclose the possibility that the device may have some degree of intelligence—some capacity to learn and then to proceed independently to accomplish a task. Automation is simply one class of resource among many available to the human operator or manager. "*Human-centered automation*" means automation designed to work cooperatively with human operators in the pursuit of stated common objectives.

"*Piloting*" is the use by a human operator of a vehicle (an aircraft) to accomplish a *mission* (to deliver passengers or cargo from one point to another). A mission consists of a number of functions, each involving from one to many tasks and sub-tasks, which are accomplished using a variety of human and machine resources. Most attempts to decompose the piloting function have adopted a functional hierarchical architecture of this sort.

Resources available to pilots include their own perceptual, cognitive, social and psychomotor skills, the knowledge and skills of other flight and cabin crew members, and the knowledge and information possessed by other persons with whom the pilot may be able to communicate, especially airline flight dispatchers, who share with the pilots responsibility for the safe planning and conduct of their flight. They are aided by a variety of information sources and control devices, including automated devices, within the aircraft. In aircraft designed for multiple crewmembers, these resources are controlled and managed by a *pilot in command (PIC)*, who is ultimately responsible for safe mission accomplishment.

"Controlling" is the function of directing aircraft, on the ground or in flight, in ways that assist the aircraft to move from point to point in conflict-free trajectories. Control may be *tactical*, involving the direction of specific aircraft through a specified part of the airspace; or *strategic*, involving the provision of general instructions and constraints for the movement of masses of aircraft within a much larger volume of airspace. Tactical control is referred to as air traffic *control (ATC)*; strategic control of air traffic is referred to here as air traffic *management (ATM)*.

Air traffic controllers are responsible for the safe direction and separation of air traffic. The resources available to them include their perceptual and cognitive skills (psycho-motor skills are less important than in piloting), their knowledge of and ability to recall quickly a large body of procedures and regulations governing the control and movement of air traffic, the knowledge, skills and abilities of other controllers who may be assisting or immediately supervising them, and the support of controllers and team supervisors controlling adjacent airspace. Their material resources include the airspace itself, airports, surface or airborne navigation aids, and a variety of surveillance, communications, and data processing systems and devices.

"Managing:" Strategic management and coordination of, and assistance to, tactical air traffic controllers is designed to maximize airspace usage while preventing overload of individual air traffic control facilities. This function is provided within the United States by an air traffic management organization called the Air Traffic Control System Command Center (ATCSCC), located near Washington and connected to all control facilities (and to many air carriers) by various means of voice and data communication.

Comment

To summarize: this document is about a human-machine system in which highly-skilled human operators use tools of varying complexity to perform cognitively difficult and exacting work in a very demanding, sometimes dangerous and always highly dynamic physical environment. Their work is tightly constrained by a highly-developed, well-integrated operational environment and a complex organizational environment. These environments are also the source of most of the variability within the system, some of it inherently unpredictable and uncontrollable by the humans who control and manage the system. A great deal of automation has been introduced in aviation to assist and support human operators and managers in the performance of their duties (though many of the older aircraft in the system today are not heavily automated and the air traffic control system is still largely unautomated, pending an extensive rework now underway). It is highly likely that the airborne and surface components of the aviation system will become much more tightly coupled in the near future. Whether the tighter coupling, as well as the continuing integration, of the various system elements will be accomplished in ways that permit human operators to remain in effective command of the system is not yet clear, and this is one of the major issues raised in this document.

Most knowledgeable observers agree that future social and political demands on the aviation system cannot be satisfied without more automation, but the form of that new automation, how it will interface with the humans who remain responsible for system safety, and whether it will materially assist those humans to improve overall system performance, are open questions. I will attempt to bound these questions more precisely and to answer those for which principled answers are possible.

2. A concept of human-centered aviation automation

Introduction

There are disquieting signs in recently-issued accident investigation reports that in some respects, our applications of automation technology may have gone too far too quickly, without full understanding of their likely effects on human operators. In this document, I will discuss some of the shortcomings of today's automation, trying not to lose sight of the benefits conveyed by these remarkable technologies. The automation itself, however, in some cases, and procedures governing its use in other cases, has impinged on the authority of its operators. As always with new tools, automation has shaped the behavior of those operators, sometimes in ways not foreseen by its designers.

The progress of automation technology will accelerate during this decade, and more rather than less automation will be needed (both in aircraft and in air traffic management) as we confront new capacity demands. Does this new automation (and further development of the automation now in use) have to be as complex, opaque, brittle and clumsy as the present generation? I think not, for we have learned a great deal about these problems from observation of today's automation. Can we solve the human-machine interface problems without compromising the utility of these remarkable tools? I believe we can, by carefully examining what we have learned and applying it to the design and operation of new systems. This will not be easy or cheap, but it will be easier and a great deal less expensive than continuing to tolerate aircraft accidents caused by inadequate human-system interfaces.

Problems associated with the evolution of automation

Most of this document describes problems associated with aviation automation. In chapter 1, I listed some automation attributes that have been found in a number of aviation mishaps (figure 2-1). These and other attributes are discussed in later chapters, but among the most important are:

- *Loss of state awareness, associated with:*
    - *complexity*
    - *coupling*
    - *autonomy*
    - *inadequate feedback*

MISHAP	COMMON FACTORS
DC-10 landing in CWS mode	Complexity; mode feedback
B-747 upset over Pacific	Lack of mode awareness
DC-10 overrun at New York	Trust in autothrust system
B-747 uncommanded roll	Trust in automation behavior
A320 accident at Mulhouse-Habsheim	System coupling and autonomy
A320 accident at Strasbourg	Inadequate feedback
A300 accident at Nagoya	Complexity and autonomy
A330 accident at Toulouse	Feedback; system complexity
A320 accident at Bangalore	System complexity & autonomy
A320 landing at Hong Kong	System coupling
B-737 wet runway overruns	System coupling
A320 overrun at Warsaw	System coupling
B-757 climbout at Manchester	System coupling
A310 approach at Orly	System autonomy and coupling

Fig. 2-1: Common factors in some aircraft incidents and accidents

What are the effects of these characteristics on human operators?

Complexity makes the details of automation more difficult for the human operator to understand, model, and remember when that understanding is needed to explain automation behavior. This is especially true when a complex automation function is utilized or invoked only rarely. (See Woods, 1994b, on "Apparent simplicity, real complexity" of aviation automation.)

Coupling refers to internal relationships or interdependencies between or among automation functions. These interdependencies are rarely obvious; many are not discussed in manuals or other documents accessible to users of the automation. As a result, operators may be surprised by automation behavior, particularly if it is driven by conditional factors and thus does not appear uniformly. (Perrow, 1984, discusses coupling and its potential for surprises.)

Autonomy is a characteristic of advanced automation; the term describes real or apparent self-initiated machine behavior. Today's flight management systems, once programmed to conduct a flight and activated, can accomplish autonomously all or nearly all of the tasks required thereafter. When autonomous behavior is unexpected by a human monitor, it is often perceived as "animate"; the automation appears to have "a mind of its own". The human must decide, sometimes rather quickly, whether the observed behavior is appropriate or inappropriate. This decision can be difficult, in part because of the coupling mentioned above and in part because the automation may not provide adequate feedback about its activities. (See Billings (1991) and chapter 8.)

Inadequate feedback describes a situation in which automation does not communicate, or communicates poorly or ambiguously, either what it is doing, or why it is doing it, or, in some cases, why it is about to change or has just changed what it is doing. Without this feedback, the human operator must understand, from memory or a mental model of the automation, the reason for the observed behavior. As a pilot has remarked, "If you can't *see* what you've gotta know, you gotta *know* what you gotta know" (Demosthenes, personal communication, 1994).

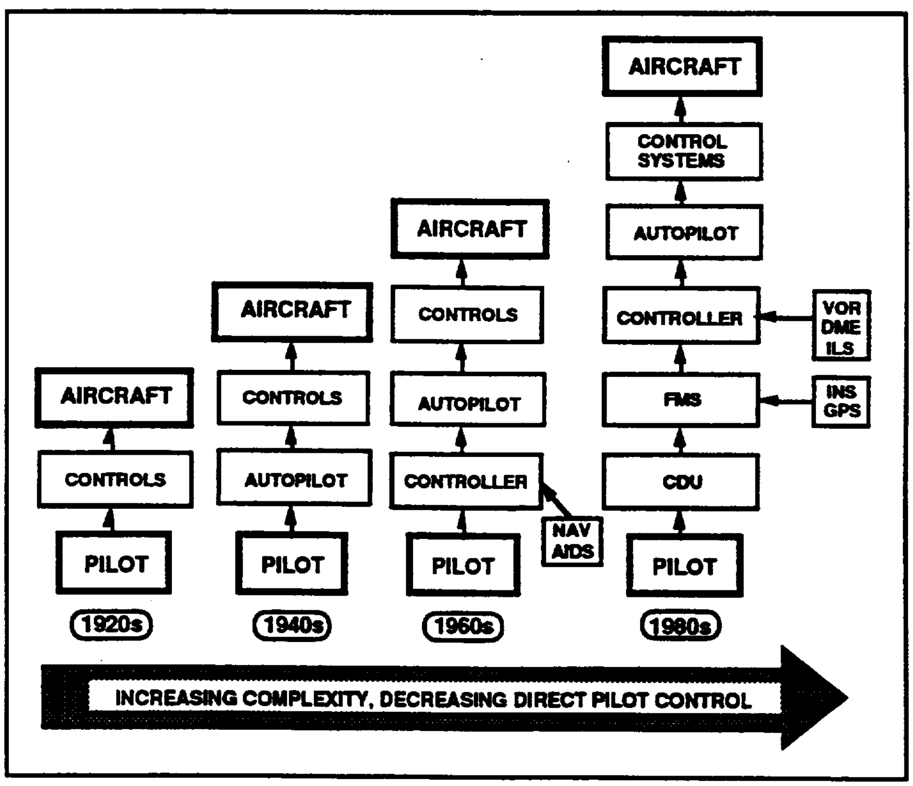

Fig. 2-2: Increasing complexity of aircraft automation decreases direct pilot control

The interposition of more and more automation between the pilot and the vehicle tends to distance pilots from many details of the operation (fig. 2-2). Over time, if the automation is reliable, pilots may become less concerned with the details of their tasks. Though this may have the desirable effect of lessening flight crew workload, it has an undesired effect as well, in that pilots may be, and may feel, less involved in the mission. The newest technologies nearing application: digital data link, automatic dependent surveillance and direct digital data transfers between flight management system (FMS) and air traffic control (ATC) computers, have the potential to accentuate this tendency toward peripheralization of the flight crew. The effects of less verbal interaction with ATC as data link comes into wider service may, I believe, also tend to distance the flight crew, and the air traffic controller as well, from a sense of immediate involvement in the team venture (as well as depriving pilots of the ability to hear what other pilots are saying, and thus the ability to infer what they are doing).

Recent accidents, among them those listed above, have demonstrated how easily pilots can lose track of what is going on in advanced aircraft. Though some new aircraft types have had better experience than others, these types differ more in degree than in kind. The mishaps that have occurred must serve as a warning of what may lie ahead unless we learn the fundamental conceptual lessons these accidents can teach us. One of the most important lessons is that we must design flight crew, and controller, workstations and tasking so that the human operator is, and cannot perceive himself as other than, at the *locus of control* of the vehicle or system, regardless of the automation or other tools being used to assist in or accomplish that control.

No regulator, aircraft manufacturer or operator talks aloud about totally replacing the human operator with automation in the aviation domain, and I think that few people in the industry believe it can be done, if only for sociological and political reasons. To the extent that pilots and controllers are distanced from their operations by automation, it is an unintended side-effect of the way their systems have evolved. I do not believe that a sense of diminished involvement is prevalent—yet—but it may well be if we continue along our present course of automating everything that can be automated, moving the human more and more toward a "back-up" or ancillary role. The AERA and "free flight" concepts of air traffic management now under consideration exemplify this trend (see chapters 6 and 7 for discussion of these concepts.).

It is these threats to the loci of control of the system as we know it that lead me to suggest that we need to reevaluate the human-machine interactions in this system at a fairly fundamental level. The concept of "human-centered" automation outlined below is an attempt to do just that. Its thesis is that by beginning with the human and designing tools and artifacts specifically to *complement* his capabilities (Jordan, 1963), we can build more effective and robust systems that will avoid or ameliorate many of the "automation problems" that now confront us. Most of these problems, of course, are neither "automation problems" nor "human error" problems. They are human-machine *system* problems, and they must be attacked as such.

A concept of human-centered automation

The remainder of this chapter is devoted to an explanation and defense of some of the principles I believe constitute the essence of human-centered automation in aviation. The term is not mine, and I have been unable to find out who first conceived it. Sheridan, Norman, Rouse, Cooley, and many others have written for many years about "human-centered" or "user-centered" technology.

First Principles of Human-Centered Aviation Automation

PREMISES:

The pilot bears the responsibility for safety of flight.

The controller bears the responsibility for traffic separation and safe traffic flow.

AXIOMS:

Pilots must remain in command of their flights.

Controllers must remain in command of air traffic.

COROLLARIES:

The pilot and controller must be actively involved.

Both human operators must be adequately informed.

The operators must be able to monitor the automation assisting them.

The automated systems must therefore be predictable.

The automated systems must also monitor the human operators.

Every intelligent system element must understand the intent of other intelligent system elements.

Fig. 2-3: First principles of human-centered aviation automation

Some people have criticized this term because it appears to emphasize the human rather than the human-machine system, but in the aviation domain, in which humans are fully responsible for the outcome, the human must be the primary focus of our attention. The tools are there to assist the *human operators* in carrying out the mission.

Figure 2-3 is a brief summary of some "first principles" that I believe are central to this concept. In later chapters, I will apply these general principles to specific automation problems and functions that I think will be implemented in future aircraft and the future air traffic system.

These "first principles", of course, are stated as absolutes. In reality, they are matters of choice to which system designers may or may not wish to adhere. An aviation system in which pilots and/or controllers were *not* at the loci of control is possible, but it would represent a radical departure from today's system. It might convey new benefits, but they would be accompanied by new costs and problems. Nonetheless, radical departures from today's system design have been actively considered, and they must be considered here in terms of the role and authority of the operators. This is discussed further in chapter 7. Here, I shall briefly discuss each of these "principles".

Responsibility and command authority

In their determinations of the probable causes of several recent aircraft accidents, the members and staff of the NTSB have made a commendable effort to recognize explicitly that there is much more to aviation system problems than "the sharp end": that pilot or controller errors are usually enabled by management, design and other latent defects in the system (Cove Neck, NY, 1990; Los Angeles, 1991; Sydney, 1991). There is a growing, though sometimes fragile, consensus that factors throughout the system must be considered before assigning causation for a mishap. By law, however, the human operators: pilots and controllers, are still responsible for the safety of each flight and for the safety of air traffic movements. The same precept applies in other transportation modes; it is reinforced by an enormous body of statute and case law. The law also provides the responsible operator with very broad discretion in the execution of this heavy responsibility. While the authority of a pilot or controller operating under normal conditions is circumscribed by a great variety of regulatory and procedural constraints, the operator's authority to use his or her best judgment in an emergency is not usually questioned, even after the fact, if the outcome is successful.

Automation is able to limit the operator's authority, and in some cases it is not obvious to the operator that this has occurred. In chapter 3, I will discuss envelope protection or limitation as an example of circumscribing control authority, but homelier examples are found in older aircraft as well. All complex aircraft have "squat" switches on their landing gear struts that sense wheels on ground; the switch, alone or in combination with a wheel spin-up sensor, enables (or disables) a number of important control functions including (in various aircraft) thrust reverser deployment, ground spoiler actuation, and autobraking. It is very important that these functions not occur in flight; the only fatal B-767 accident occurred after a thrust reverser deployed during climb at high altitude. (Thailand, 1991) On the other hand, there have been several incidents in which pilots landed gently on a water-contaminated runway and were unable to use deceleration devices for some time because of delayed wheel spin-up due to hydroplaning (Marthinson & Hagy, 1993a,b; Warsaw, 1993). In the Warsaw case, there was an 8-second delay during which the airplane traveled almost 2000 ft.

Newer autothrust systems, usually activated early in the takeoff roll, limit engine power to maximum rated thrust or a lower value depending on aircraft weight, runway length, temperature and other variables. The purpose of this is to minimize engine wear and fuel consumption. The desired takeoff thrust is selected through the thrust management system. Occasionally, an aircraft on takeoff encounters a situation in which all available power reserves are needed to climb over a runway obstacle or to maintain acceleration on a contaminated runway. In older aircraft, pilots simply "firewalled" their throttles to obtain maximum thrust. Engine overheating usually resulted, but the technique was often successful in avoiding a far more critical threat. (Unfortunately, there are also incidents in which pilots did not utilize all available power when it was needed, perhaps because they feared overheating their engines.) In some of today's aircraft, it is not possible for pilots to obtain more than rated thrust from the engines. "Full throttle" instructs engine computers to provide rated thrust; no reserve is available. Should a pilot be permitted to "burn up" an engine, or overstress an airplane? It is the pilot, after all, who is responsible for a successful outcome. On the other hand, it is predictable that some pilot will unnecessarily overheat some very expensive engines if given the means with which to do so.

In the air traffic control domain, concepts for advanced enroute ATC systems will be able, either through automation design or procedures, to limit the scope of controller authority appreciably, though the responsibility for a safe operation will remain with the human. If the human operator cannot effectively oversee and retain management authority over his tools, he has lost authority over the entire operation. Will this be a tenable situation?

I believe it comes down to a matter of trust. Will we provide pilots with full authority, train them carefully, and trust them to do "the right thing", whatever it is in particular circumstances? Or will we circumscribe pilot authority by making it impossible to damage the airplane, and in the process perhaps make it impossible to use its ultimate capabilities if they really need them, or circumscribe controller authority to do whatever is necessary in contingencies? My bias, based on a number of cases in which pilots have been able to recover from extreme emergencies, and other cases in which they did not recover but could have had they used all available resources (e.g., Washington, 1982), is that command authority should be limited only for the most compelling reasons, and only after extensive consultation with both test and line pilots or controllers at "the sharp end" of the system.

Operators must be involved

No one questions the necessity for operator involvement in flight and air traffic operations at some level; the questions relate to the degree of involvement. The tenets of situation awareness, a concept with which the aviation community is much preoccupied, correctly state that it is easy for pilots to become preoccupied with detail at the expense of maintaining "the big picture" of their operations (Gilson, Garland, Koonce, 1994). This concept underlies the design philosophy characterized as, "If it is technically and economically feasible to automate a function, automate it" (Douglas, 1990).

My questions regarding involvement are rather whether pilots of newer aircraft are indeed sufficiently "drawn in" (the definition of involvement) to their operations by having an active and necessary role apart from simply monitoring the course of the operation. That role may involve active control, or decision-making, or allocation of resources, or evaluation of alternatives, but it should not be passive, as it too often is today. The Flight Safety Foundation ICARUS Committee has also emphasized the need for more "disciplined" training to ensure that both technical and human factors needs are met (Flight Safety Foundation, 1994). I believe that pilots must be given meaningful and relevant tasks throughout the conduct of a flight, and that these tasks must be designed into the aircraft automation. This will not be easy, for we have spent the last decade making the automation self-sufficient. The change from passive monitor to active problem-solver can be abrupt and difficult. *If humans are to remain involved (and without such involvement they will not always remain in command), they must be an essential part of the normal operational flow, not only the resolvers of anomalies.*

One operator has seriously considered asking its pilots to engage in a continuing process of flight replanning to take advantage of changing wind and weather conditions by revising their flight plans while they are being executed. This approach has merit—but technology is now under development to accomplish this automatically on the ground, using automatic dependent surveillance to provide the real-time data! One is reminded of Wiener and Curry's (1980) statement: "Any task can be automated. The question is whether it should be..."

This question has not yet come up with respect to controllers, because automation of air traffic control processes is not yet available to them. It will be, however, in the near future. It is hoped that the lessons taught in aircraft by assuming "that the maximum available automation is always appropriate" (ATA, 1989) will not be lost on ATC system architects, but there is little reason thus far for optimism.

Operators must be informed

For many decades, neither pilots nor controllers ever had as much information as they needed to conduct operations optimally under changing and often unpredicted circumstances. During the last two decades, however, there have been quantum increases in the amount of data available in the cockpit and in ATC facilities. Glass cockpit technology has made it possible to provide much more of this data in aircraft; information management technology has all but erased the problem of insufficient data in the system. *Data, however, is not information. It becomes information only when it is appropriately transformed and presented in a way which is meaningful to a person who needs it in a given context.*

The secret to compressing and transforming data into information lies in a designer's understanding of the operator's needs, cognitive models and operating styles under a wide variety of circumstances. It is absolutely crucial that the designer be able to assume the line pilot's or the controller's role and way of thinking when designing information displays or representations. Further, the designer must understand information needs not only through the minds of the highly experienced test and certification pilots or managers with whom he or she ordinarily interacts, but must also understand the broad range of cultures and capabilities in the population of operators who will fly the airplane in line service, and the broad range of environmental circumstances under which it will be flown. The most capable pilots are able to "make do" with displays that are far from optimal; it is one measure of their capabilities. But the same displays in service must support fatigued pilots of below-average ability operating under difficult conditions: what Charles Schultz's Snoopy calls the "dark and stormy night" in his never-finished novel about world war I flying. Similarly, ATC systems cannot be designed only for the "aces"; they must assist the inexperienced trainee as well.

Without adequate information (and what is adequate depends to a great extent on the context and the human operator), neither pilots nor controllers can make uniformly wise decisions.

Without correct and timely information, displayed in a way that minimizes operator cognitive effort, even the best pilots and controllers cannot remain constructively involved in an operation, and thus cannot maintain command of the situation. The designer must ask how he or she is affecting the *processes* that it takes to extract meaning from the data or information provided.

Humans must be able to monitor the automation

In automated aircraft, one essential information element is information concerning the status and activities of the automation itself. Just as the pilot must be alert for performance decrements or anomalous behavior in the human crew members (self included), he or she must be equally alert for such decrements in the automated systems that are assisting in the conduct of the operation. The first principles state that "The humans must be able to monitor the automation." This sounds obvious, but it has been observed that advanced automation is often "strong and silent" (Sarter & Woods, 1994) about its work, leaving humans to wonder about what it is doing, and sometimes why.

In part, this situation reflects the commendable desire of aircraft manufacturers to avoid burdening the pilot with information unless something is wrong. The "quiet, dark cockpit" concept reflects this philosophy by giving a positive indication only when some system is not operating properly. The equally important issue today is how to inform the pilot (or controller) that the automation is performing each of the functions it has been commanded to perform.

When automation performed only tactical chores in response to direct commands from pilots, it was reasoned that the pilots could monitor the automation by simply observing the correctness of the airplane's responses to autopilot inputs. Today's automation, however, is far more capable and ubiquitous; it accomplishes more functions over a longer period of time, often with only strategic guidance from pilot inputs to the FMS. The number and seriousness of mode errors (Boston, 1973; Los Angeles, 1979; Strasbourg, 1992; Paris, 1994) that occur despite information on the flight mode annunciator panel at the top of the primary flight display suggest strongly that pilots of modern aircraft must be given more salient *affirmative* evidence that their automation is indeed doing what they told it to do, perhaps many hours earlier (Sarter & Woods, 1992b; 1994).

Automation must therefore be predictable

In many redundant aircraft systems, the human operator is informed only if there is a discrepancy between or among the units sufficient to disrupt or disable the performance of their functions. In those cases, the operator is usually instructed to take over control of that function. *To be able to assume control without delay, it is essential that the pilot be aware on a continuing basis both of the function (or dysfunction) of each critical automated system and of the results of its labors to that point, as well as what it was going to do next and when.* This, of course, requires that the pilot have an accurate mental model of how the automation is expected to behave.

The formation of such internal models occurs, or should occur, during training, when the pilot learns what "the book" says about particular automation functions and then uses those functions in a simulator or part-task training device. The models are reinforced when the pilot successfully invokes the functions in line operations. They may be modified if the functions are found to be "buggy" or to work in ways not expected, and such behavior, which is fortunately rare, can cause severe disruption to the pilot's mental image of the system. An example in the 757/767 was an occasional turn to an outbound instead of inbound heading when converging on a localizer course, or more simply, the lack of a display of the inbound heading in the pilot's field of view in the same aircraft.

The pilot's model may be an accurate representation of a function, or it may be a drastically simplified construct of a complex function. If accurate and reasonably complete, the model may help the pilot to detect and diagnose aberrant automation behavior if it occurs. If the model is a grossly simplified or metaphorical representation, the pilot is more likely to be surprised by anomalous behavior of the real system, since its detailed behavior may not be a part of his or her mental model.

Because of the logical complexity of modern digital systems, they may fail in ways that are quite different from "physical" systems. This increases the probability that the pilot's mental model will not fully account for its actual performance. Only if the automation's normal behavior is predictable, given a certain input or circumstance, will pilots be able to detect subtle signs of failure. It is for this reason that automation must be predictable, so that pilots will be able to observe and respond to unpredicted behavior of these systems. This fact also emphasizes the importance of helping pilots to build adequate mental models of automated systems during training, and the importance of simplicity in functional design. It is difficult for pilots to remember the "normal behavior" of functions that are used only infrequently. (See chapter 7, Training.)

Automation must monitor the human

Just as machines are prone to failure, so are the human components of the human-machine system. Human error is thought to contribute to roughly 80 percent of aviation accidents (Lauber, 1989). Though we now recognize that a great many of these human failures are enabled by other system factors, there is clearly a need to monitor human behavior at the "sharp end" of the system. Indeed, much of our elaborate safety surveillance apparatus is designed specifically for this purpose.

One of the major reasons air transport is so safe is the ongoing monitoring of the flying pilot by a non-flying pilot in the cockpit. This duty is spelled out in the operating procedures of every air carrier and nearly all other organizations that conduct multiple-pilot operations. Flight dispatchers monitor pilot decisions, and pilots monitor dispatcher planning. Pilots monitor the actions of air traffic controllers, and those controllers monitor the behavior of the aircraft they control. ATC automation monitors both pilot and controller actions. Error detection, diagnosis and correction are integral parts of the aviation system, and a great deal of effort has gone into making all parts of the system redundant.

Despite everyone's best efforts, however, human errors continue to occur, are missed, and occasionally propagate into a catastrophic system failure. There are many reasons for this; one is that humans are not very good monitors of infrequent events (Mackworth, 1950; Broadbent, 1971) and may fail to detect them when they occur. This is an area in which automation technology can be extremely useful, for computers do not become fatigued or relax their vigilance when a long period elapses between events of interest, and they fail much less frequently than do human operators.

Automated devices already perform a variety of monitoring tasks in aircraft, as indicated throughout this document. Incident reports confirm their effectiveness in preventing mishaps (and also confirm, unfortunately, the failure of pilots to detect configuration problems when the automated monitors fail, as in takeoffs without flaps in the face of an undetected configuration warning system failure (Detroit, 1987; Dallas-Ft. Worth, 1988)). Designing warning systems to detect failures of warning systems can be an endless task, but it is necessary that we recognize the human tendency to rely upon reliable assistants and consider how much redundancy is therefore required in essential warning systems. The tradeoff, of course, is increased automation complexity and decreased reliability.

Data now resident in flight management and other aircraft systems can be used to provide more comprehensive and effective monitoring of both pilots and controllers, if specific attention is given to potential failure points that have been well-documented in aviation operations. Automation, in the air and on the ground, can and should be thought of as a primary monitor of human behavior in exactly the same way that humans are the primary monitors of machine behavior. In the more tightly-integrated system of the future, such cross-monitoring will be the key to improved system safety. The use of aircraft automation, especially the FMS, for flight crew monitoring has not been given the attention it deserves; air traffic control automation has done a better job in this area.

Communication of intent

Cross-monitoring (of machines by humans, of humans by machines, and ultimately of human-machine systems by other such systems) can only be effective if the monitoring agent, whether a person or a machine, knows what the monitored agent is trying to accomplish, and in some cases, why. The intentions of the automated systems and the human operators must be explicit, *and they must be communicated* to the other intelligent agents in the system.

A great deal of this goes on already. Pilots (or airline Systems Operations Centers, SOCs) communicate their intent to Air Traffic Control by filing a flight plan. Pilots communicate their intent to the FMS by inserting the flight plan into the computer or calling it up from the navigation data base. Controllers, in turn, communicate their intent to pilots by granting a clearance to proceed; in the near future, data link will transmit this information to the FMC as well. During flight, clearance changes are communicated to pilots by ATC; they acknowledge their understanding of ATC's intentions by reading back the revised clearance as they heard it (though on busy communication channels, this procedure is far from faultless (Monan, 1986)).

It is when circumstances become abnormal, due either to problems in the physical or operating environment or to in-flight anomalies, that communication of intent among the various human and machine agents becomes less certain. An Avianca B707 accident (Cove Neck, NY, 1990) was a classic example of failure to communicate need and intent between pilots and air traffic controllers, but there have been many others, some as serious. Further, the communication of intent makes it possible for all system participants to work cooperatively to solve the problem. Many traffic control problems occur simply because pilots do not understand what the controller is trying to accomplish, and the converse is also true, as in the Avianca case. Finally, automation cannot monitor pilot performance effectively unless it "understands" the pilot's intent, and this is most important when the operation departs from normality. This problem has the potential to become more pressing as new ATC automation is introduced, for there will be linked human and machine systems both in flight and on the ground, all of which will have to work harmoniously to resolve tactical problems as they arise.

Comment

Though humans are far from perfect sensors, decision-makers and controllers, they possess three invaluable attributes. *They are excellent detectors of signals in the midst of noise, they can reason effectively in the face of uncertainty, and they are capable of abstraction and conceptual organization.* Humans thus provide to the aviation system a degree of flexibility that cannot now, and may never, be attained by computers. Human experts can cope with failures not envisioned by aircraft and aviation system designers. They are intelligent: they possess the ability to learn from experience and thus the ability to respond adaptively to new situations. Computers cannot do this except in narrowly-defined, completely-understood domains and situations.

The ability of humans to recognize and bound the expected, to cope with the unexpected, to innovate and to reason by analogy when previous experience does not cover a new problem are what has made the aviation system robust, for there are still many circumstances, especially in the weather domain, that are neither controllable nor fully predictable. Each of these uniquely human attributes is a compelling reason to retain human operators in a central position in aircraft and in the aviation system. Those humans can function effectively, however, only if the system is designed and structured to assist them to accomplish the required tasks. I believe that as technology continues to advance, it will become increasingly urgent that its applications in aviation be designed specifically around the human who must command them; in short, that future aviation automation must be human-centered if it is to be a maximally effective tool.

At the same time, many machines today are capable of tasks that unaided humans simply cannot accomplish. This is true in both the perceptual and cognitive realms. An example today is the calculation of optimal orbital trajectories for systems such as the Space Shuttle; another is the determination of a great circle navigation route. For these tasks, computers and automated systems are an absolute requirement. Competitive pressures in aviation being what they are, it is likely that still more complex automation may be offered in the marketplace, even in subsonic aircraft, and there will be a tendency to accept it. If this tendency toward greater complexity is to be countered, it must be by the customers: airlines and other operators must decide whether the potential gains are worth the certain costs. Some air carriers, among them Southwest Airlines, have decided that "simpler is better" with regard to cockpit automation. Others, as recommended by the ICARUS Committee (FSF, 1994), are "minimiz(ing) crew confusion by selecting the automation options and methods best suited to their own operations, and training for those options/methods as 'preferred' methods", rather than requiring that the full capabilities of their flight management systems be used in line operations. Given the problems associated with automation complexity, this seems a prudent approach.

3. The evolution of aircraft automation

Introduction

This chapter discusses aircraft automation. It is not possible to discuss the interaction of humans with the machines they control without some understanding of the machines themselves, which is why this discussion is oriented around the technology. But the overriding issue, as noted in chapter 1, is not just the machines, nor the people; it is the processes by which they interact to get the job done.

The earliest flying machines were extremely unstable and often barely controllable. Aircraft automation was invented to complement and assist human operators in carrying out tasks which were difficult or even impossible without machine assistance. Later, it became obvious that automation could appreciably offload pilots, who had increasing numbers of tasks to perform as aircraft utility and aviation system complexity increased.

Until the late 1960s, automation was largely devoted to maintaining aircraft control, leaving navigation, communications and management functions to the flight crew. The 1970s saw the onset of a technological revolution as the expanding utility of digital computers stimulated the development of miniaturized "microprocessors" with new solid-state circuitry based on the transistor. In aviation, the changes enabled by the new technology were as revolutionary as had been those during the previous 15 years when faster, larger, higher-flying jets began to replace propeller-driven transport aircraft. Microprocessors have had profound effects on the ways aircraft are flown, on the ways the aviation system is managed, and on the human pilots and air traffic controllers who operate the system.

Aircraft functions

The range of functions that an airplane can perform is really quite limited. Properly controlled, an airplane can move about on a prepared surface. It can take off from that surface and once above the earth's surface, it is free to move in all spatial axes. It can be directed from one location to another, where it can land and again move about on a prepared surface, coming to rest at a predetermined spot.

Several categories of tasks must be performed by pilots in pursuit of their objectives. They must *control* the airplane in three translational and three angular axes. The autopilots discussed immediately above were designed to assist with this task, which requires nearly continuous adjustment of the airplane's control surfaces unless the air is perfectly smooth and air speed remains constant. They must remain cognizant of their airplane's position relative to their objectives, and must direct, or *navigate*, the airplane from one location to another. These functions may be performed by reference to external objects on the ground, celestial bodies, by dead reckoning, by use of data from radio-frequency navigation aids, or by making use of geographic reference information from onboard aircraft sensors or satellites. In today's operational environment, they must also *communicate* with air traffic control, airline operations control and other facilities to receive and acknowledge instructions, consult regarding changes, and receive advice concerning malfunctions or changes in the external environment.

These three invariant requirements are often referred to colloquially in flight safety literature as "aviate, navigate, communicate". Their successful accomplishment under all circumstances is the hallmark of the capable pilot. To these three functions must be added another, that of aircraft, flight and subsystems *management*. This became a major task as reciprocating-engine transport aircraft became larger and more complex and their engines became more powerful and temperamental during the 1930s, requiring the full-time attention of flight engineers who became an essential part of the cockpit crew. For overwater flights, navigators and radio operators were also carried, though newer technology developments have made all flight crew except pilots superfluous.

The beginnings of aircraft automation

In 1908, Sir Hiram Maxim published a book discussing his experiments in aeronautics. He described a gyroscopic stability augmentation device connected to the fore and aft elevators of a large, highly unstable airplane built and tested while tethered during the 1890s (fig. 3-1). This device, believed to be the first example of aircraft automation, was patented in England in 1891.

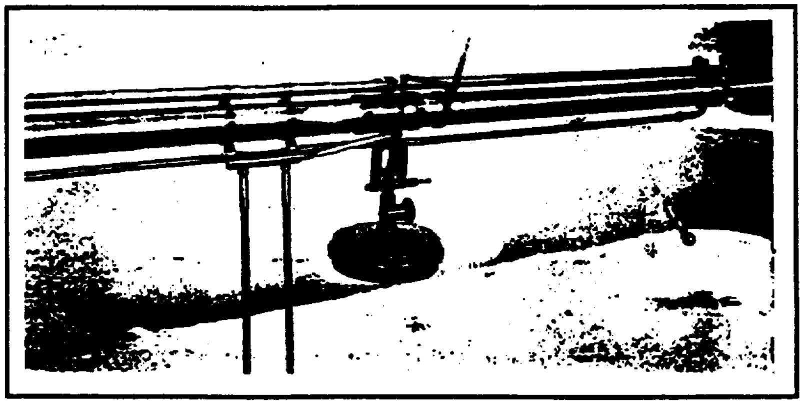

Fig. 3-1: Maxim gyroscopic stability augmentation system (Maxim, 1908)

In their flight experiments, Orville and Wilbur Wright also recognized the extreme instability of their aircraft; they independently developed stability augmentation devices for their machines, for which they received the Collier trophy in 1913.

Lawrence Sperry developed a more advanced gyroscopic stability augmentation system which was demonstrated in flight (while a "mechanician" walked back and forth on the lower wing of a seaplane and the pilot stood with both hands over his head, fig. 3-2) at the *Concours l'Union pour la Securité en Aeroplane* in France in the summer of 1914. The "Automatic Pilot" was awarded First Prize at the event.

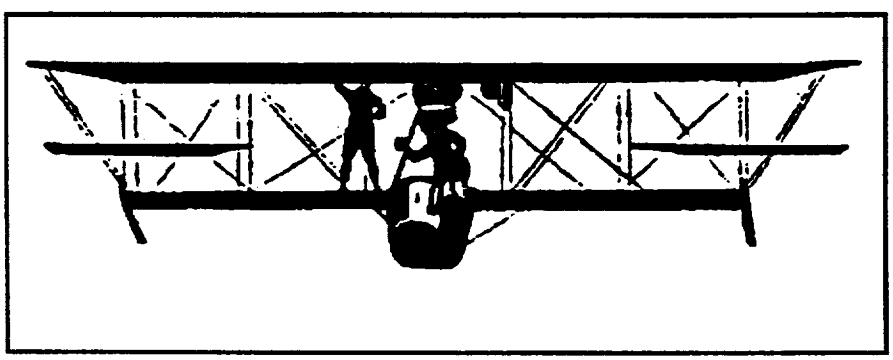

Fig. 3-2: Flight demonstration of Sperry Automatic Pilot in France, 1914 (Sperry Company).

The Sperry name was associated with aircraft automation for the next 60 years. Sperry automatic pilots (called "autopilots") became available during the 1920s. In 1918, H. J. Taplin patented a non-gyroscopic two-axis stabilization device that relied on differential aerodynamic pressures. His device was successfully flown in the United States in 1926 (Taplin, 1969). With this exception, as far as is known, all successful autopilots during this period are believed to have utilized the gyroscopic principle.

A capable three-axis autopilot actuated solely by hydraulic and pneumatic power was an essential part of the equipment installed in Wiley Post's Lockheed Vega, *Winnie Mae*, for his solo round-the-world flight in 1933 (fig. 3-3; Mohler & Johnson, 1971). The flight's successful conclusion was marked by the *New York Times* with the observation that "By winning a victory with the use of gyrostats, a variable-pitch propeller and a radio compass, Post definitely ushers in a new stage of long-distance aviation...Commercial flying in the future will be automatic" (July 24, 1933).

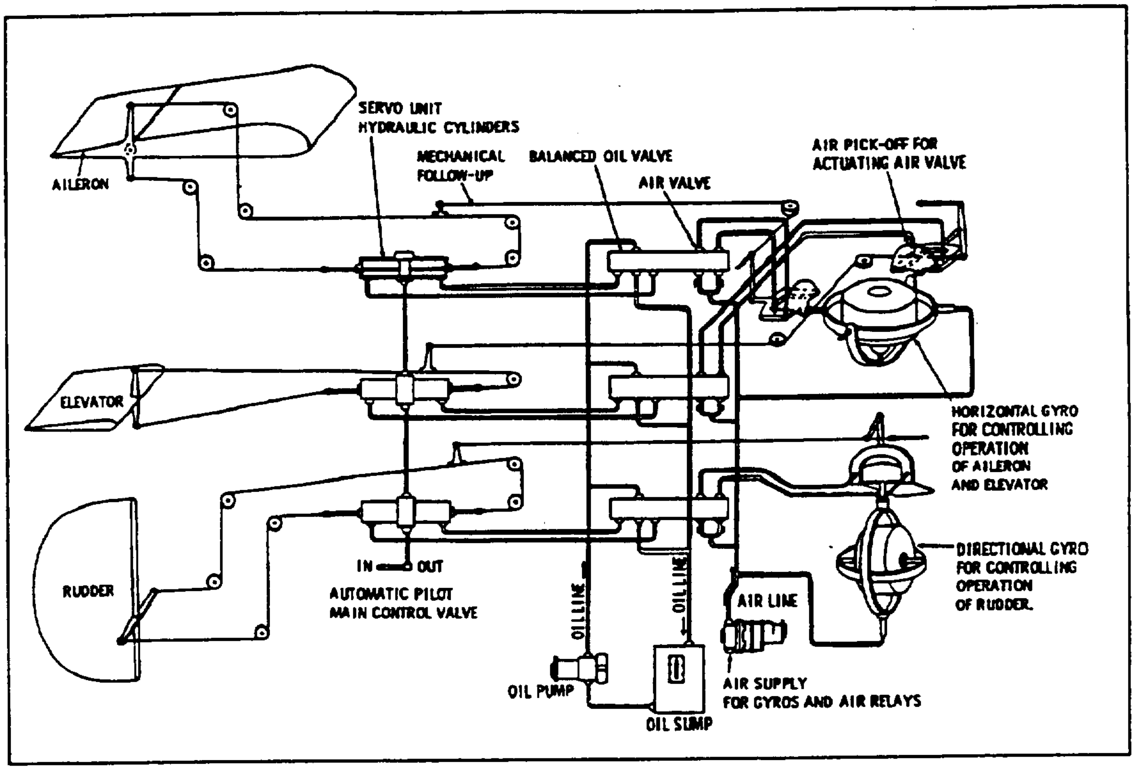

Fig. 3-3: Diagram of autopilot used in *Winnie Mae* (Mohler & Johnson, 1971, from Sperry data)

In 1938, Howard Hughes established a new round-the-world speed record in conjunction with the opening of the New York World's Fair. His Lockheed model 14 was also equipped with a Sperry autopilot. Long-range civil aircraft during the late 1930s, and military transport and bomber aircraft throughout World War II, were similarly equipped. By that time, aerodynamic understanding and engineering practice had improved; most of these aircraft were relatively stable platforms under normal conditions. The automatic devices were installed to relieve pilots of the manual labor of hand-flying on long flights. They provided inner-loop control of the aircraft in response to direct pilot instructions (see below) but left the pilot to perform all navigation and other essential piloting tasks. Virtually all reciprocating-engine transport aircraft introduced after world war II were equipped with autopilots of this sort.

The jet era

The introduction of jet aircraft into civil aviation marked the beginning of a technological revolution (fig. 3-4). The DeHavilland *Comet*, introduced in 1954, provided air passengers with transportation at much higher altitudes and greater speeds than had been available previously. It was followed in 1958 by the Boeing 707, an outgrowth of the military C-135 transport and tanker designed for the U.S. Strategic Air Command. Douglas was not far behind with its DC-8, introduced in 1960. During the early 60s, both American manufacturers introduced smaller jets, the DC-9, B720 and the second-generation B-727.

Generations of Civil Jet Transport Aircraft	
First generation	DeHavilland Comet
• Simple systems	Boeing 707
• Many manual tasks	Douglas DC-8
• Manual navigation	Douglas DC-9
Second generation	Boeing 727
• Systems redundancy	Boeing 737-100, 200
• Pilot navigation	Boeing 747-100, 200, 300
	Douglas DC-10
	Lockheed L-1011
	Airbus A-300
Third generation	Boeing 767/757, 747-400
• Digital systems	McDonnell-Douglas MD-80
• Two-person cockpit crews	Airbus A-310, 300-600
• Graphic displays	Fokker F-28-100
• Flight management systems	McDonnell-Douglas MD-11
• Integrated alerting	(transitional to 4th Gen.)
Fourth generation	Airbus A-319/320/321
• Fly by wire	Airbus A-330, A-340
• Integrated systems operation	Boeing 777

Fig. 3-4: Evolution of civil jet transports (Fadden)

In 1967, the second generation Boeing 737 entered line service. Its systems were generally similar to those of the larger 727 introduced three years earlier, but to keep cockpit workload within reasonable limits for a crew of two rather than three persons, Boeing automated the operation of a number of airplane systems to a limited degree and simplified other systems. During the 1970s, the reliability of microprocessors improved to the point that Douglas, Boeing and the new Airbus Industrie consortium all felt themselves ready to take advantage of digital technology in the design of new airplanes. Douglas enlarged upon its DC-9 series with the 135-passenger DC-9-80, introduced in 1978. Though the airplane made use of conventional electromechanical cockpit instruments, the manufacturer introduced considerably more automation of aircraft systems than in previous models.

Boeing introduced its 767 wide-body twin in 1982. The findings of a Presidential Task Force on Crew Complement (1981) allowed the airplane to be certified for two-person operation and this crewing was adopted as the standard for all new types. Boeing also put into production its 757 series, a narrow-body airplane with a virtually identical cockpit and systems; a common type rating covered both. The latter type caught on more slowly but is now in wide use throughout the world, as are various models of the larger 767. These aircraft and the Airbus A310, introduced slightly earlier, were the first "glass cockpit" aircraft in civil service. They made extensive use of microprocessors (the 767 and 757 had over 100 in their cockpit avionics suites), though all three types retained some electromechanical instruments along with the cathode-ray tubes that provided primary flight, navigation and systems information and motivated the "glass cockpit" descriptor.

During the 1980s, considerable operational experience was gained with these third-generation aircraft. As manufacturers gained confidence in the new automation technology, it was incorporated and its uses extended in new designs. This decade saw the development and introduction of the Airbus A320 (1989), the first of the "all-glass" cockpit airplanes, the Boeing 747-400, a greatly advanced two-person crew version of the venerable 747 in service since 1970, the development of the McDonnell-Douglas MD-11 which entered service in 1991, and the Fokker F-100, an enlarged and highly automated outgrowth of the earlier F-28 regional jet. These aircraft, and several corporate jets developed during the same time period, represent the state of the art in cockpit technology at this time.

Fadden (1990) described two categories of aircraft automation; he called them "control automation" (automation whose functions are the control and direction of an airplane) and "information automation" (automation devoted to the management and presentation of relevant information to flight crew members; this category includes communications automation). To these categories, I have added a third, "management automation" (automation designed to permit strategic, rather than tactical, control of an operation). When management automation is available, the pilot has the option of acting as a "supervisory controller" (Sheridan, 1987). In aircraft, automation is directed by the pilot to accomplish the tactical control functions necessary to accomplish the objective. This most useful taxonomy is used throughout this document. Under each category, I will describe the technologies, discuss benefits and problems associated with them, and try to characterize their effects on human operators.

Control Automation

Throughout most of the history of aviation, automation has fulfilled primarily inner-loop *control* functions (fig. 3-5). Control automation assists or supplants a human pilot in guiding an airplane through the maneuvers necessary for mission accomplishment. In this document, the term also includes devices devoted to the operation of aircraft subsystems, which are complex in modern aircraft.

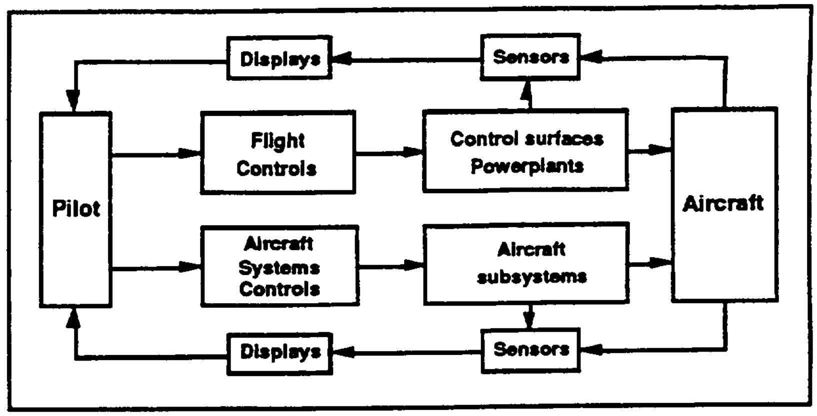

Fig. 3-5: Flight and systems inner control loops

Aircraft attitude control

Maxim's 1891 device maintained pitch attitude, but other early automated controllers maintained attitude in the roll axis (fig. 3-2). Later generations of such single-axis stability augmentation devices have been called "wing levelers" and they continue to be available for general aviation aircraft today. Later, autopilots added other axes of control; the device used in the world flight of the *Winnie Mae* maintained the aircraft attitude in pitch, roll and yaw by controlling the positions of the elevators, the ailerons and the rudder (figure 3-3).

Flight path control

In early generations of autopilots, the gyroscope which controlled roll was also used as a heading, or directional, gyro in the cockpit. Some autopilots of this period also incorporated a barometric altitude sensor which could be used to hold altitude as well, once the proper altitude was attained and set into the sensor. In these developments, we see the beginnings of *intermediate loop* control, in which the pilot could specify a *goal:* a heading and altitude to be maintained, rather than roll and pitch attitude.

As aircraft performance increased, air mass data became necessary for precise control of aircraft speed and height. Central air data computers were provided when jet-powered transport aircraft entered service in the 1950s; these devices provided integrated precision sensing of static and dynamic air pressures. The analog computers likewise incorporated rate sensors which enabled precise climbs and descents.

Swept-wing jet aircraft are susceptible to Dutch roll, a lightly-damped roll-yaw interaction that can be suppressed only by well-coordinated pilot or machine inputs. Early jet transport control required very precise coordination to counter this tendency. When the 707 was introduced, yaw dampers were provided to counter the problem. Though nominally under control of the pilot (they can be turned off), yaw dampers in fact operate autonomously in all swept-wing jet aircraft. The same can be said of pitch trim compensators, used to counter the tendency of jet aircraft to pitch down at high Mach numbers. These devices likewise operate essentially autonomously.

Spoilers or wing "fences" were installed on jet aircraft to increase control authority and reduce adverse yaw, to assist in slowing these aerodynamically clean aircraft, to permit steeper descents and to decrease aerodynamic lift during and after landings. Early jets had manually-controlled spoilers; later aircraft had spoilers that were activated either manually, in flight, or automatically after main wheel spin-up during landings. The Lockheed L1011 introduced direct lift control by means of automatic modulated spoiler deflection during precision approaches.

Jet transports also required more precise control to compensate for decreased stability and higher speeds, particularly at high altitudes and during approaches to landing. Flight by reference to precision navigational data was made easier by the development of flight director displays which provided pilots with computed pitch and roll commands, displayed as shown in figure 3-6. The directors were much easier to fly than unmodified instrument landing system (ILS) localizer and glide slope deviation data, which were presented on the periphery of the instruments used for the director displays. Such displays rapidly became a mainstay of transport aviation. They made it possible for pilots of average ability to fly with high precision, though concern was expressed about "losing sight of the 'raw' data" while relying upon the directors for guidance. A Delta DC-9 impacted a seawall short of a runway at Boston; its crew is believed to have followed the flight director, which was mis-set in "attitude" rather than "approach" mode, without adequate cross-checking of localizer and glide slope data (Boston, 1973).

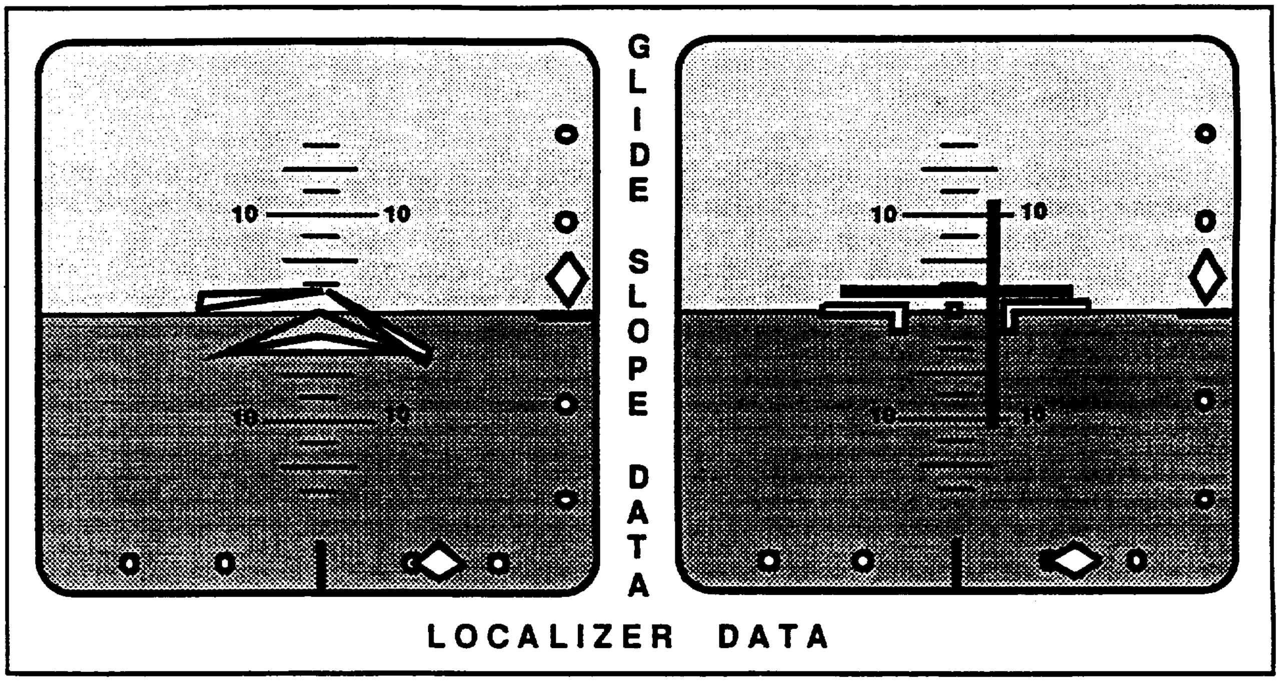

Fig. 3-6: Single-cue (left) and dual-cue (right) Flight Director displays. Deviation data is at right and bottom of presentations. Aircraft is left of localizer centerline and slightly low on glide slope; the directors are commanding a right turn and climb to regain ILS centerline.

Navigation systems

The advent of precision radio navigation systems capable of providing both azimuthal and distance information occurred during the late 1940s and early 1950s. Very high frequency (VHF) navigational radios were developed during world war II. When introduced in civil aviation beginning in 1946, they eliminated problems due to low frequency interference from thunderstorms, but they were limited to line-of-sight coverage.

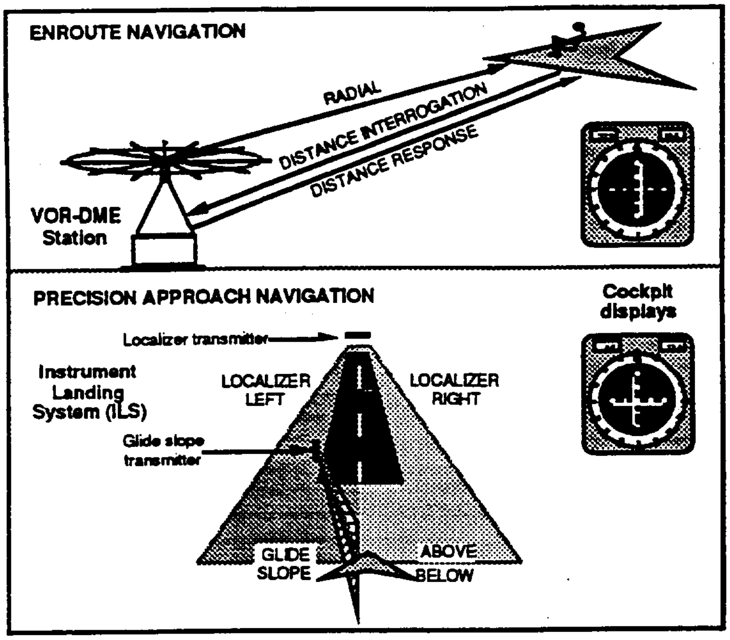

Fig. 3-7: Enroute and approach navigation aids

VHF omnidirectional range (VOR) transmitters became the foundation of overland aerial radio navigation in the United States; ICAO soon adopted a similar standard. Distance measuring equipment (DME), consisting of airborne interrogators and ground transponders, was co-located with VORs and provided range data.

For approach guidance, VHF directional "localizer" transmitters and ultra-high frequency glide slope transmitters were located on airport runways; together they formed the basis for the instrument landing systems (ILS) which are still the standard of the current system (figure 3-7). Later, DME units were co-located with ILS to improve precision.

These devices provided aircraft with positional information of high precision. Their signals provided azimuthal and distance information which could be used either by pilots or by autopilots to provide intermediate loop control of aircraft paths. ILS signals, which provided glide slope guidance as well, were used to permit both manual and automatic ("coupled") precision approaches to runways. They enabled the design and implementation of autopilots with a wide range of capabilities including control of pitch, roll and yaw, maintenance of a track to or from a surface navigational aid, and the capture of localizer and glide slope centerlines followed by the conduct of automatic approaches.

To improve schedule reliability, carriers began to study automatic landings ("autoland"). After automatic landing demonstrations in 1965, the British Aircraft Corporation *Trident III* (a three-engine medium-range transport) was the first production-series transport to be approved for automatic landings in category III weather (figure 3-8). The airplane utilized three autopilots with flare capability and roll-out guidance, and a voting system to ensure concordance in the control outputs from the three analog autopilot computers. This equipment enabled the Tridents, operated by British European Airways from 1965 to the mid-1980s, to continue flying their routes when nearly all other aircraft were grounded.

Many newer transport aircraft have autoland capability, though pilots as well as aircraft and navigation facilities must be certified for such bad-weather approaches. In recent years, some carriers have utilized head-up display equipment to provide pilots with a better means to transition to a visual landing during extremely low visibility.

Precision Approach (ILS) Categories

Category	Decision Height	Visibility or RVR*
I	200 ft.	2400 ft. (1/2 mile)
II	100 ft.	1200 ft.«
IIIa	50 ft.	700 ft.«
IIIb	†	150 ft.«
IIIc	†	††

* Runway visual range (RVR).
† No decision height specified. Visibility is the only limiting factor.
« No fractions of miles authorized when determining visibility. The runway served by the ILS must have operable RVR equipment.
†† No ceiling or visibility specified. Aircraft must be equipped with autoland.

Fig. 3-8: Weather limits for ILS approaches

Integrated flight control systems

Aircraft control automation was well-advanced by 1970. Analog computers of considerable sophistication were the basis for autopilots which performed all inner-loop and many intermediate-loop functions (see figure 3-12), though pilots were still responsible for providing the devices with tactical instructions and monitoring the performance of the automation. Since the outputs of the autopilot and autothrottles were reflected both in control movements and airplane behavior, the pilots' monitoring task required only the displays also used by them for manual flight. A few new instruments provided surveillance of autopilot functions and indications of autopilot modes when automatic navigation was in use.

Two wide-body airplanes introduced during the 1960s and early 70s, the Douglas DC-10 and Lockheed L-1011, introduced more complex autopilots with comprehensive mode annunciation and a broader range of options for both lateral and vertical aircraft control. Mode control panels (figure 3-9), located in the center of the instrument panel glareshield, commanded autoflight and autothrottle functions and the flight directors whose computers provided flight path commands to the integrated autoflight systems. The L-1011, which entered service in 1973, was the first commercial type to incorporate direct lift control, which controlled lift automatically during landing approaches by means of partial spoiler deployment and thus improved landing precision (Gorham, 1973). This feature, the forerunner of gust alleviation and lift modulation seen in some of the most modern transports, was an integral part of a Category III fail-operational autoland system designed and incorporated when the airplane was initially certified—a first in transport aviation.

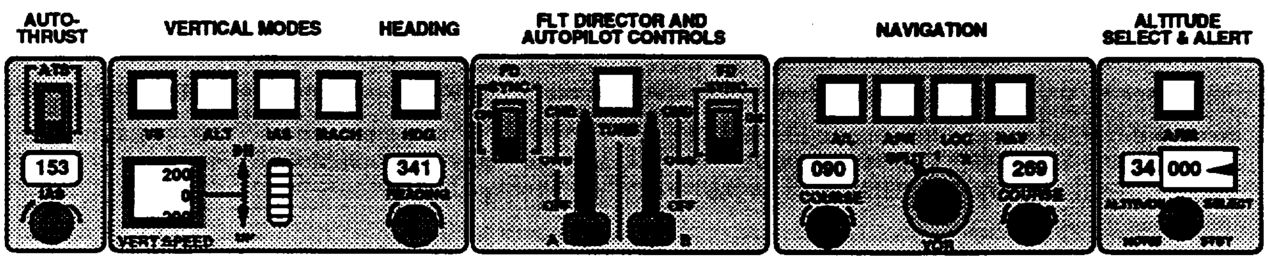

Fig. 3-9: Lockheed 1011 Avionic Flight Control System Mode Control Panel (Gorham, 1973)

The 1011 flight control system was more highly integrated than any other in service at the time and provided a number of autoflight modes (fig. 3-10), which were generally similar to those incorporated in the DC-10's automation suite. These systems provided pilots with more sophisticated tools than had previously been available (at the cost of considerably more complexity). Training officers noted that some pilots and flight engineers had difficulty in learning the new systems, as their forebears had when first-generation jet transports entered service during the late 1950s.

PITCH AXIS	ROLL AXIS
• Control wheel steering • Altitude hold • Vertical speed hold • IAS hold • Mach hold • Altitude capture	• Control wheel steering • Heading select • VOR hold • R-nav coupling • Localizer hold
DUAL AXIS • Approach • Approach/land • Go-around • Take-off • Turbulence	

Fig. 3-10: Lockheed 1011 Avionic Flight Control System functions (adapted from Gorham, 1973)

Advanced flight control systems

Until 1988, control of large aircraft, whether manual or automatic, was carried out through hydraulic actuators. The conventional large, centrally-located control columns ("yokes") and rudder pedals controlled the hydraulic actuators; they moved when actuated by the autoflight systems or the pilots and thus provided visual and tactile feedback of flight control inputs. Throttles (actually thrust levers: they were now connected to electronic control systems rather than fuel valves) were electrically driven; they likewise moved when actuated by the pilots or the autothrust system.

The 1988 Airbus A320, whose flight controls are unconventional ("fly-by-wire"), represented a departure from previous civil designs. Attitude control in the A320 is by hand controllers ("sidesticks") located outboard of each pilot. The two sidesticks are not coupled to each other, nor do they move to provide tactile (touch) feedback during autopilot control inputs or when the other pilot is making manual inputs. Likewise, the "throttles" in the center console do not move during autothrust inputs, though they can be moved by the pilots to provide instructions to the full-authority digital engine controllers (FADECs) which control the power systems (figure 3-11). Electronic Centralized Aircraft Monitor (ECAM) visual displays indicate both power commanded and power delivered, but ancillary tactile or visible feedback is not provided by the levers themselves.

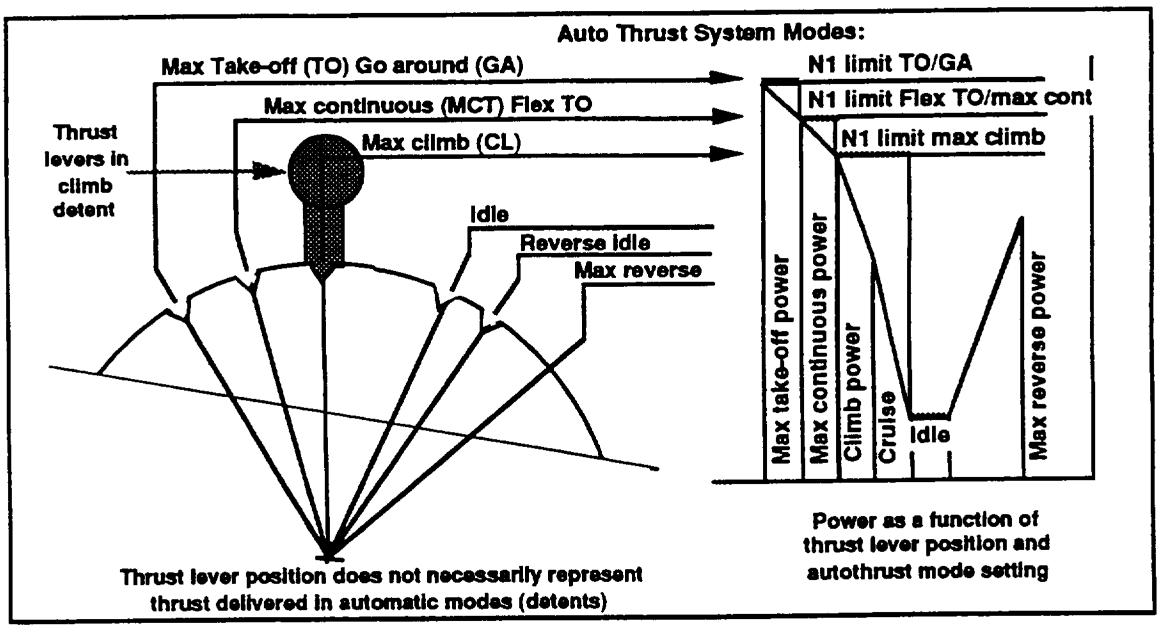

Fig. 3-11: Diagram of dual-function thrust levers on A320/330/340 aircraft showing detents for autothrust modes. Thrust levers may also be moved to intermediate positions for manual power control.

The introduction of fly-by-wire systems in the A320/330/340 and B-777 has provided control system engineers with more flexibility to tailor aircraft control responses to match desired characteristics through software in the flight control computers. An inherently unstable airplane can be made to feel, to the pilot, like an extremely stable platform. Indeed, some modern aircraft (such as the MD-11) incorporate reduced longitudinal stability to reduce control surface weight, which is compensated for by a stability augmentation system. Even manually-controlled flight in such aircraft is actually accomplished by one or more computers interposed between the pilot and the machine. This control architecture offers other opportunities to the designer, who may now limit the flight envelope by making it impossible for the pilot to exceed certain boundaries, or provide precisely tempered degradation of flying qualities as safe operating limits are approached. This is called "envelope protection"; it is discussed in detail in chapter 8.

Effects of control automation on human operators

Figure 3-12, an expansion of 3-5, suggests some of the effects of adding control automation to the pilot's resources. It indicates that the pilot has an additional means of controlling his aircraft attitude and flight path. In this sense, it relieves the pilot of inner loop control tasks, which require a relatively high level of activity and considerable attention on a more or less continuous basis. Providing an alternative means of accomplishing the control functions gives the pilot considerably more time to devote to other functions and tasks essential to safe flight.

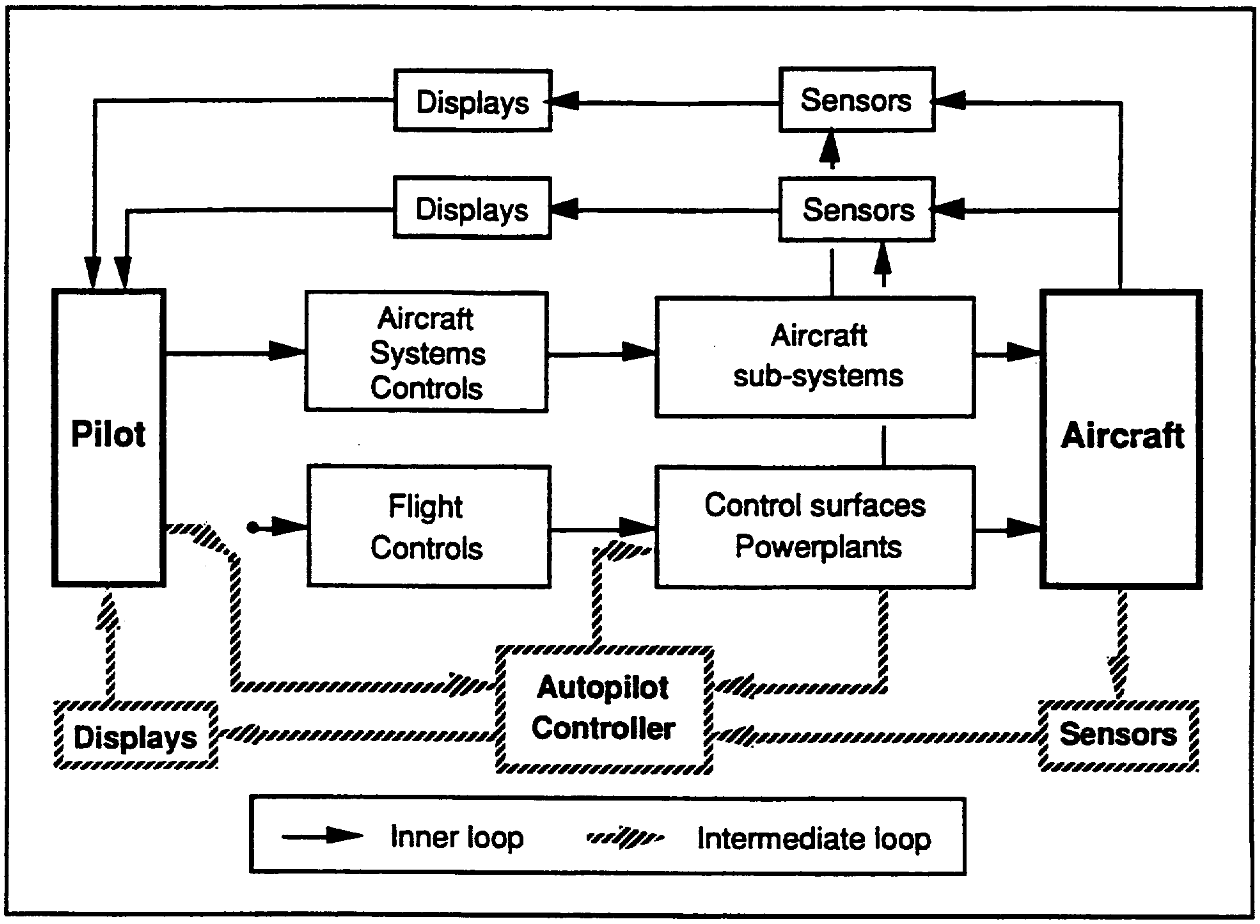

Fig. 3-12: Flight and systems control loops with autopilot.

On the other hand, note that the pilot must now give at least intermittent attention to additional equipment and displays. The pilot must understand the functioning of an additional aircraft subsystem, remember how to operate it, and decide when to use it and which of its capabilities to utilize in a given set of circumstances. When it is in use, its operation must be monitored to ensure that it is functioning properly, If it begins to malfunction, the pilot must be aware of what it is supposed to be doing so he or she can take over its functions. Finally, the pilot must consider whether the failure impacts in any way the accomplishment of the mission and whether replanning is necessary; if so, the replanning must be done either alone or in communication with company resources.

Issues raised by integrated flight control systems

While the considerable psychomotor workload of the pilot is reduced by an autopilot, *the cognitive workload is increased by the introduction of automated devices, and the pilot' tasks are always changed by the provision of such devices.* The addition of an autopilot provides the pilot with additional resources which can offload high-bandwidth, flight-critical tasks, but the addition is not without cost in terms of the attentional, knowledge and information processing requirements placed on the flight crew. Note also that the pilots' management tasks increase.

The decrease in pilot workload when an autopilot is in use can be dramatic, but even this benefit is a two-edged sword. As an example, there have been several instances in which early series Boeing 707 and 747 autopilots have malfunctioned subtly by disconnecting or introducing a gradual uncommanded roll input to the airplane controls. In at least some of these, pilots have first noticed the uncommanded maneuver only when the airplane was in a steep bank and dive from which level flight was regained eventually only after severe maneuvers (Atlantic Ocean, 1959; Nakina, 1991). It has long been known that humans are not very good monitors of uncommon events, especially when they are tired, bored, or distracted by other tasks (Mackworth, 1950; Broadbent, 1971). Autopilot functioning is annunciated in the cockpit, but a subtle system interaction such as this, with or without a failure, may produce little in the way of obvious visual signals aside from the gradual attitude change, and the human vestibular system is unable to perceive a very gradual roll acceleration.

These systems are more complex and tightly coupled than their predecessors. They require that pilots know more about system behavior under both normal and abnormal circumstances. Since the systems are very reliable, many system anomalies will occur only rarely, presenting the pilots with behavior that may not be understood when it occurs. It is difficult for pilots to keep all knowledge about uncommon system states and failures available in memory, and equally difficult for them to access such information when it is needed. This is sometimes called "inert" knowledge.

Moreover, even if the systems exceed the limits of their design envelopes, there may be little information provided aside from an alerting message, if the pilot is expected to take action. If the fault is one for which corrective action is not thought necessary by the designer, the system may provide no explanation of its behavior. While this approach serves to keep pilots from improvising solutions to problems that may not require them, it does little to increase their confidence in the automated systems.

Issues raised by advanced flight control systems

The major differences from previous aircraft control systems in recent Airbus aircraft have evoked fairly widespread concern in the operational and human factors communities, though it should be said that the concern does not appear to be serious in airlines operating this aircraft type. After a survey of pilots operating these aircraft, British Airways concluded "that the A320 (thrust lever) design provides advantages in respect to engagement and selection of power settings, (but) that (thrust lever) movement provides better disengagement and information on system function...from a Flight Operations perspective a future system should consider providing movement between the idle and climb power positions, retaining the A320 thrust setting and engagement 'detents' technique" (Last & Alder, 1991).

The lack of tactile feedback to the sidestick controllers either from autopilot inputs or between the two pilots' controls in the A320/330/340 has been a matter of concern to human factors engineers because these airplanes differ from all other civil aircraft in this respect. Reports indicate that there have been a few situations in which opposing inputs from the two pilots have summed to produce no change in airplane flight path (e.g., incident at Sydney, 1991), though a button on each sidestick permits either pilot to remove the other from the control loop. This control arrangement would be likely to present problems only if a non-flying pilot were to initiate a go-around or an evasive maneuver because of an emergency before being able to tell the flying pilot that he or she was assuming control. Simultaneous inputs from both control sticks are not annunciated in the cockpit except on the ground. To cover such a case, it is possible that procedures and training should be modified to include using the lockout when the non-flying pilot assumes control, to insure that only one pilot is flying the airplane.

Based on operating experience to date, it appears that pilots are usually able to obtain all needed information concerning flight and power control either with, or without, tactile feedback of control movements initiated by the automatic systems. This may be a case in which there is not "one best way", based on empirical or analytical knowledge, to automate a system, and in which, therefore, any of several methods of providing feedback may be equally effective provided that pilots are given sufficient information to permit them to monitor the systems effectively. Unfortunately, information concerning the rare cases in which a particular innovation is *not* effective in providing adequate feedback may not come to light until a mishap occurs. How much feedback is enough? It depends on the context, as will be discussed in future chapters.

Power control

Reciprocating engine aircraft had only limited inner-loop automation of power control systems. Automatic mixture controls which utilized barometric altitude data to adjust fuel-air ratios were installed in the DC-3 and later transports. Automated control of propeller pitch (by means of governors) was also introduced during the 1930s, not long after controllable-pitch propellors. Later multi-engine aircraft required precise synchronization of propeller speeds to minimize vibration and annoying beat frequency noise; propeller autosynchronizers were developed to match the propeller speeds of all engines. Some superchargers, installed in high-altitude aircraft, had automatic sensing devices which controlled the amount of air pressure or "boost" provided to the engine air inlet. Throttles, propeller and mixture controls were not integrated, however.

Following world war II, surplus military aircraft were purchased in considerable numbers by civil operators. Some of these aircraft were extremely demanding to fly after an engine failure at low speed during or shortly following takeoff. To lessen the asymmetric drag caused by a windmilling propeller and assist pilots in maintaining control during the critical moments after takeoff, automatic propeller feathering systems were introduced in some aircraft. These devices sensed a loss of thrust in a malfunctioning engine and rapidly aligned its propeller blades with the airstream to reduce drag.

Autofeathering devices provided critical assistance when they functioned properly, but several accidents occurred after functional engines were shut down autonomously. Autofeathering systems, once armed by pilots just before takeoff, are independent of pilot control and they do not notify the pilot before taking action. To that extent, they remove a portion of the pilot's authority while leaving him with the responsibility for the outcome, a topic on which more will be said in chapter 9.

Control of aircraft subsystems

In early generations of jet aircraft, the many aircraft subsystems were operated in the conventional way, with switches in the cockpit controlling most aspects of system operation. The flight engineer's primary task was the operation and surveillance of power, electrical, fuel, hydraulic, and pneumatic systems. Discrete controls for every system were located on the flight engineer's panel.

In aircraft designed for a crew of two pilots, attempts were made to simplify system operations somewhat to decrease flight crew workload. Passenger alerting signs were activated automatically; automatic load shedding was introduced to simplify electrical system reconfiguration following a generator failure; air conditioning pack deactivation was automatic following an engine failure on takeoff, etc. These and other measures represented a piecemeal approach to the problem, however; subsystems were still considered in isolation by designers, and until recently, manual systems operation during failures was still complex.

Automated flight path control systems usually provide immediate feedback to pilots concerning their continued functioning. Feedback concerning aircraft subsystem status may be much less obvious. Older three-person aircraft incorporated a multiplicity of lights and gages to provide the flight engineer or pilots with such information; cockpit automation and simplification efforts have attempted (with considerable success) to minimize the amount of system information which the crew must monitor. The provision of simpler interfaces, however, has not always been due to the design of simpler aircraft subsystems. On the contrary, system complexity in some cases has increased greatly.

Cockpit simplification has included drastic reductions in the number of subsystem controls and also standardization of those controls, nearly all of which are now lighted pushbuttons with legends. Critical buttons may be guarded. The switches are usually located in subsystem diagrams. The use of pushbuttons of identical shape and size in place of a variety of toggle switches has cleaned up the overhead panel, but it has made more difficult the location by feel of a given switch. Manufacturers state that their "dark cockpit" concept, in which buttons are lighted only if they require attention, indicates those that must be used, and that buttons should be actuated only after visual confirmation of which button to press. Douglas Aircraft Co. has automated large segments of the subsystems management task in its MD-11.

Information Automation

Though control automation followed a generally evolutionary path until the introduction of the A320, information automation is largely a product of the digital revolution. The period from 1970 to the present has been marked by major changes in the appearance of the flight deck due to the introduction of electronic display units (EDUs) in the 767/757, the Airbus A310 and following types.

For those unfamiliar with glass cockpit terminology, figure 3-13 is a generic instrument panel layout, showing the panels that are discussed here. Six electronic display units, together with backup flight instruments (liquid crystal displays or electromechanical instruments) and a few critical systems indicators, are found on the main instrument panel. Aircraft systems controls are located on the overhead systems panel. A mode control panel (also called flight control unit) is located centrally on the glare shield below the windscreens. Other flight management system control units and communications control units are located on the pedestal between the pilots, together with power and configuration controls. These displays, together with paper documents, verbal communications, aural signals, and the pilots' own knowledge, provide all real-time information to the pilots.

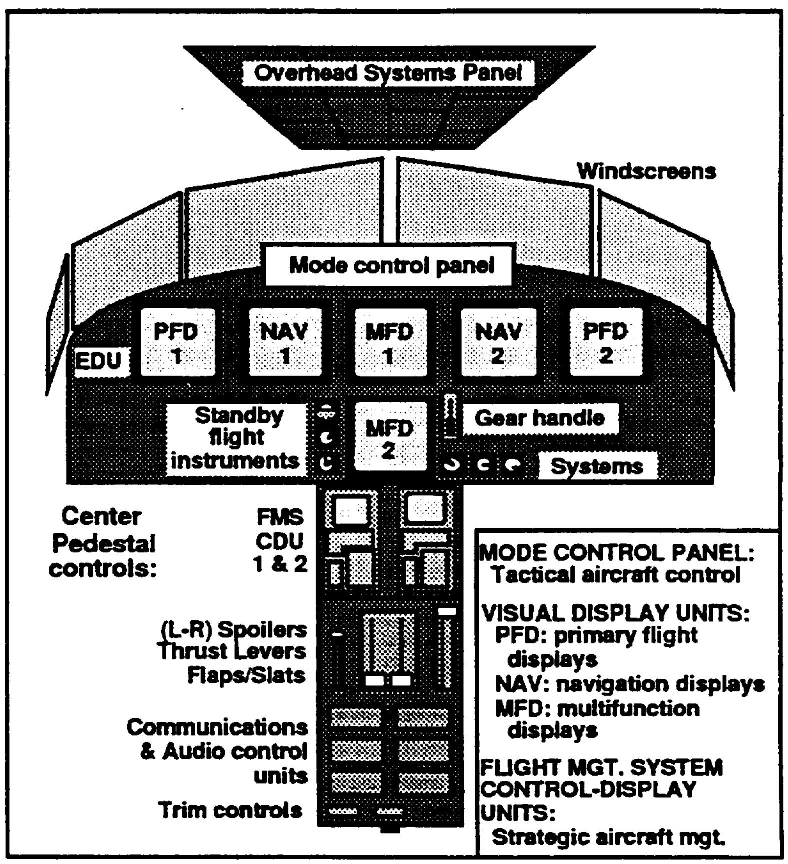

Fig. 3-13: Generic "glass cockpit" layout

The flexibility of "glass cockpit" displays has made it possible to provide any sort of information in new and different formats, and to modify that information in any way desired by designers to fit any need.

Attitude and flight path displays

Electronic primary flight displays (PFDs) have generally shown aircraft attitude and state information in much the same ways it was earlier presented on electromechanical displays (fig. 3-14), though in the latest generation of aircraft all of the formerly available information is shown on a single large display directly in front of the pilots (fig. 3-15). This representation adds additional information, in particular trend information, but few attempts have been made to alter radically the format of the data aside from the use of linear "tape" presentations of altitude, airspeed and vertical speed in place of the former round dial displays (as was done on electromechanical instruments in the USAF C-141 and C-5 transports). The British Aircraft Corporation (now British Aerospace) earlier implemented a simulator cockpit based on CRT displays in which these data were presented in a conventional circular display format. There is still some argument about whether linear or circular displays are preferable, though linear tapes are now the rule.

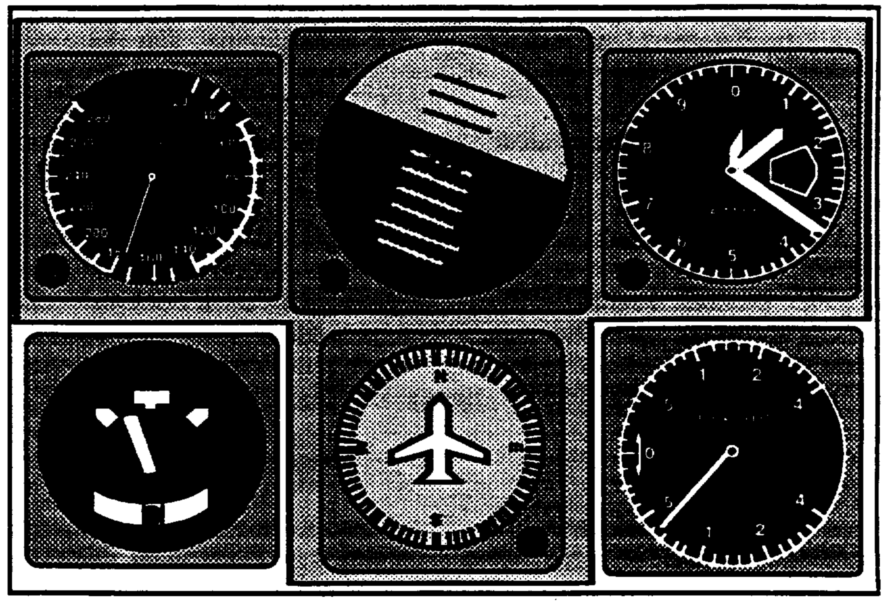

Fig. 3-14: Primary flight display on electromechanical instruments; standard "T" arrangement is boxed and shaded. In upper row: airspeed indicator, attitude indicator,, altimeter; in lower row: turn and slip indicator, heading indicator, vertical speed indicator.

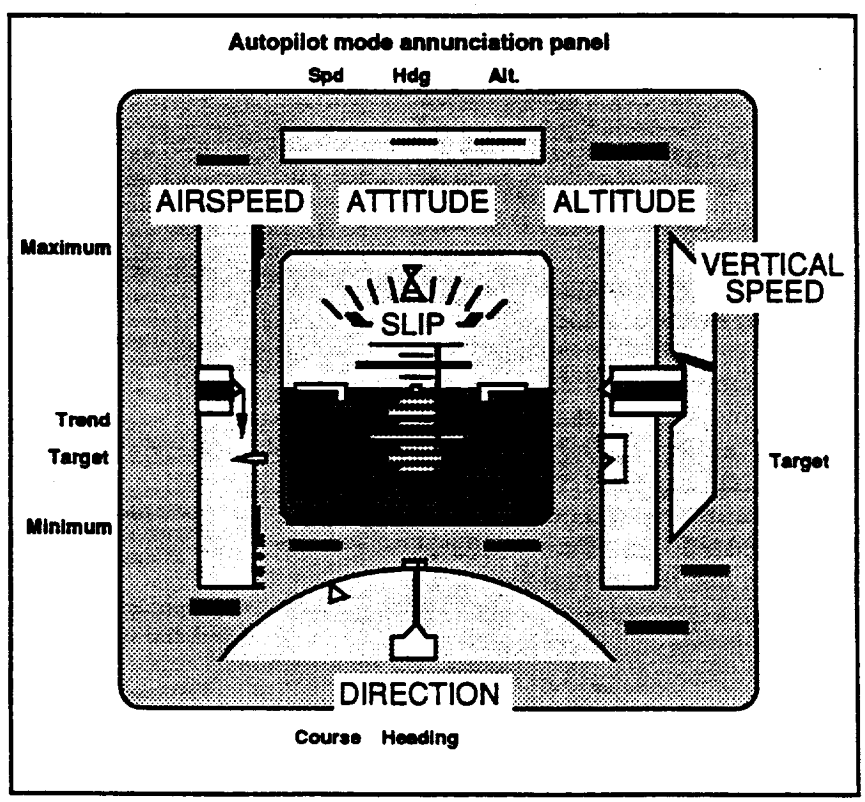

Fig. 3-15: Electronic primary flight display, generic. Note that in general, the "T" arrangement of most essential information has been preserved in this electronic display.

Over the years, human factors researchers and design engineers have brought forth a variety of concepts for the simplification and integration of the information presented on the primary flight displays. Most of these have involved some sort of "pathway (or tunnel) through the sky" concept (figure 3-16). Such displays, based on concepts developed in Germany during the 1950s, have been tested in simulation and flight, and are still under development (Grunwald, Robertson, & Hatfield, 1980). Other displays with the same intent are under development by Langley Research Center, the Air Force Armstrong Laboratory and various airframe manufacturers. In all cases, the intent is to provide integrated information concerning attitude and flight path, similar to the integrated navigation displays which have been so successful in glass cockpits.

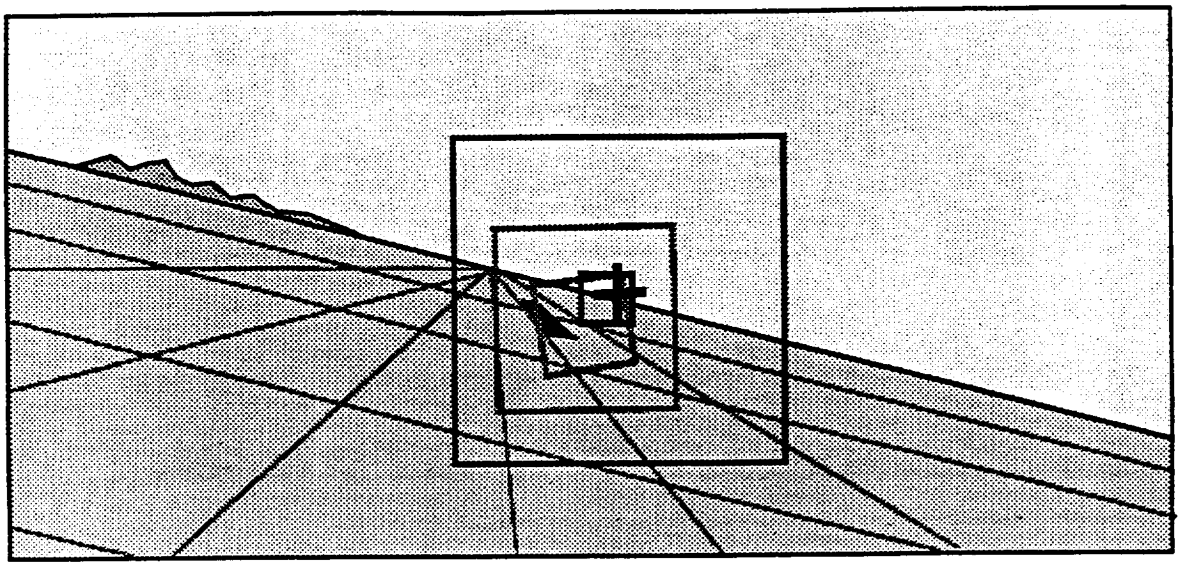

Fig. 3-16: "Tunnel in the sky" flight path display, generic. Flight director guidance is generally incorporated in these displays, with alphanumeric speed and altitude data.

Air Force human factors experts have conducted an intensive search for simpler, more intuitive means by which to convey primary flight information, navigation information and threat alerting (Stein, 1986). Airframe manufacturers have shown interest in such concepts but have been inhibited in bringing them to service use, in part by financial constraints and in part by the mix of aircraft in nearly all fleets. Pilots fly a variety of aircraft during their careers, some with advanced cockpits, some with conventional electromechanical instruments. There has been considerable concern among operators that transitioning back and forth between the older displays and advanced, more integrated, primary flight displays could increase training requirements and perhaps compromise safety. At least two U.S. air carriers, each operating various B-737 models, have gone so far as to install electromechanical instruments rather than EDUs in their -300 and -400 models to insure uniformity of displays across their fleets.

Navigation displays

Nowhere has information automation been used more effectively than in aircraft navigation displays. Glass cockpit navigation displays are a radical departure from their electromechanical forebears. All aircraft manufacturers have integrated the information formerly presented on electromechanical instruments into a single planview map display to which has been added other features derived from the flight management system database. Terrain detail, explicit location of ground navigation aids and pilot-constructed waypoints, airports locations and other data can also be portrayed on a large EDU, together with the programmed route, alternative routes if they are under consideration, and other data. Figure 3-17 shows how such information was formerly presented to pilots, while fig. 3-18 shows a contemporary map display.

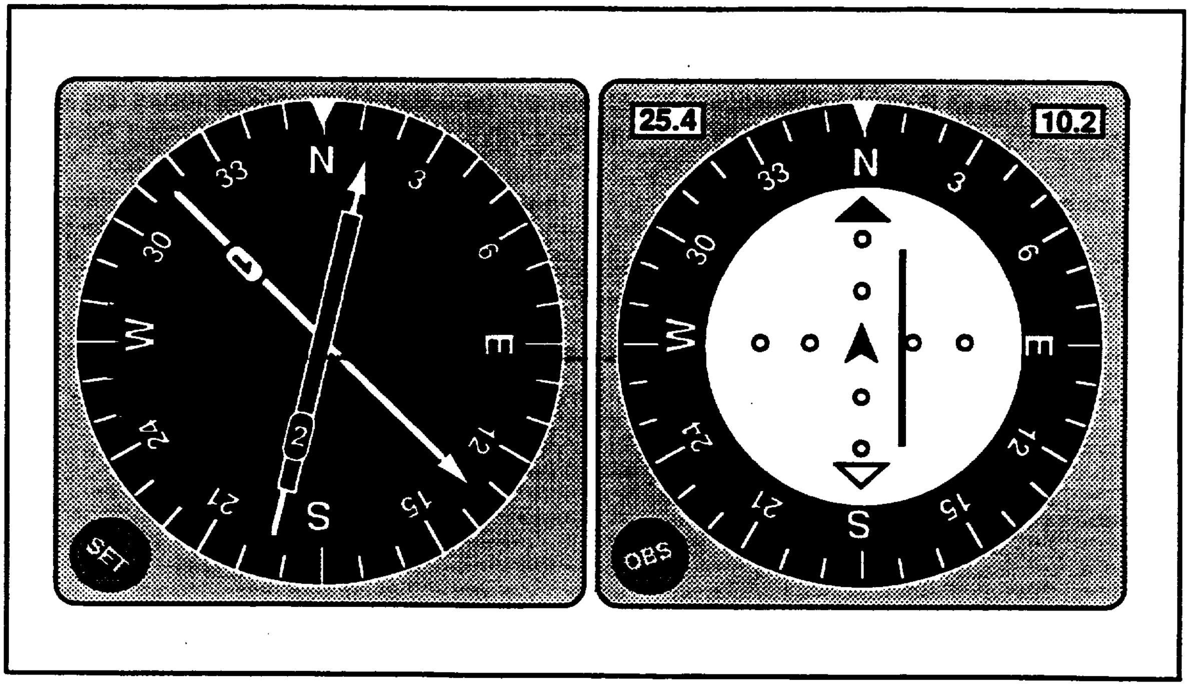

Fig. 3-17: Electromechanical navigation displays: radio magnetic indicator (RMI) at left, horizontal situation display (HSI) at right. The 180° radial of the #2 VOR is 4° to the right; that VOR is 10.2 miles away. Aircraft is flying parallel to that radial. The HSI also shows ILS glide slope deviations, to-from indications and DME range from the two VOR stations.

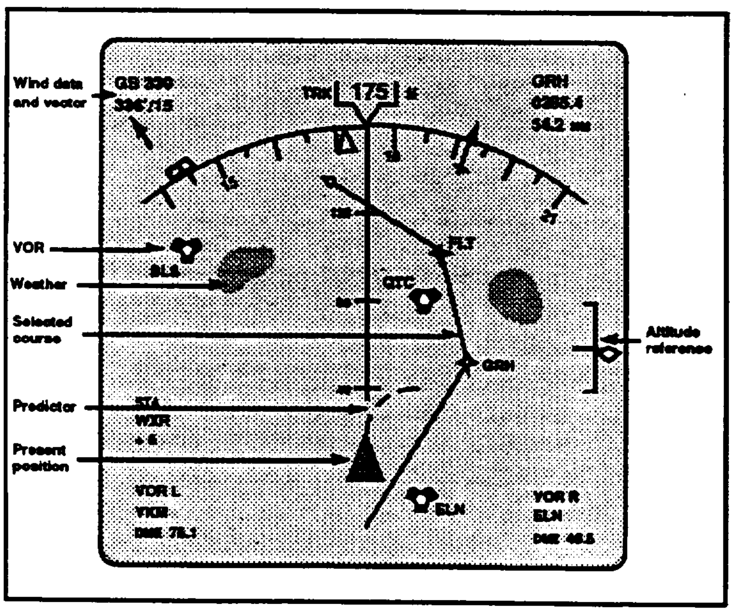

Fig. 3-18: Navigation display (Boeing 747-400)

Map displays are the feature most liked by pilots transitioning to the glass cockpit (Wiener, 1985; 1989), and with good reason. No single feature has mitigated flight crew cognitive workload as much as these new displays, and it is probable that no technological advance has done as much to make the modern airplane more error-resistant than its predecessors. In several advanced aircraft, these displays permit the pilots to preview the flight plans they have entered in the flight management system on a large scale map display, to assist in detecting errors in FMS waypoint insertion.

Current navigation displays integrate a considerable variety of complex data into a clear, precise and intuitive representation of aircraft position with reference to a pre-planned course. As such, they are an information management tool of considerable power. In the Map mode, they also assist in flight path management by displaying the results of FMS entries. They are extremely compelling, though they hide a great deal of data. Unfortunately, they are not always correct, though this is not obvious to pilots unless they invoke special functions designed to show the raw data from which the integrated display was constructed (see figure 4-4 for an example). An example of a potentially serious problem that can be created by the non-observability of source data occurred for a period of time a few years ago at Kai Tak Airport in Hong Kong, an exceptionally difficult airport because of very close high terrain and man-made obstacles. The problem was caused by a navigation transmitter in nearby mainland China which caused spurious location data to be input to aircraft flight management systems and thus map shifts on navigation displays.

Issues raised by advanced flight path displays

The principal issue raised by flight display innovations is that of feedback of automation actions and intent to pilots. Complex data become informative only when they are transformed in an effective representation, and the representation is effective only if it tells the operator what is required to be known at a certain point in an operation. Navigation displays are an excellent representation of what the pilot needs to know. They are not perfect, because the data used in their generation are not infallible. The complexity of the process which produces the map display is not observable unless the pilot becomes suspicious and utilizes the functions that also show raw data (see figure 4-5).

Given the effectiveness of the map displays and their reliability under all usual circumstances, however, the tendency of pilots to rely upon usually reliable information may weigh against the likelihood of checking the raw data when they are busy preparing for an approach to landing. There may be no entirely satisfactory answer to this automation conundrum, but pilots must be taught to be suspicious of *all* of the very capable automation under their control. This is not an easy "sell" in today's aircraft and environment, and it will only become harder in the future.

Power displays

System performance displays generally have two objectives: to inform the pilots of the state or status of the system on an ongoing basis, and to aid the pilots to detect anomalous system performance. The first objective links system performance to some value or state having external significance. The second objective links performance to some value or state having internal significance (Fadden, personal communication, 1995).

In older aircraft, power displays, by their arrangement, permitted pilots to compare the performance of one engine to the other(s). It was easy for pilots to compare needle positions on the electromechanical analog instruments to determine whether all engines were behaving the same, though an implicit weakness in this approach is that it may fail to show the effects of a problem that affects both or all engines equally. In an Air Florida takeoff from Washington National Airport (1982) with engine inlet icing which affected the engine pressure probes, both engines were developing only a fraction of takeoff power, but (incorrect) exhaust pressure ratio indications were the same from both engines and the pilot flying failed to detect the problem during the takeoff roll (NTSB, 1982). One way of circumventing this problem is to compare measured performance with a model of expected performance; an example is shown in figure 3-20.

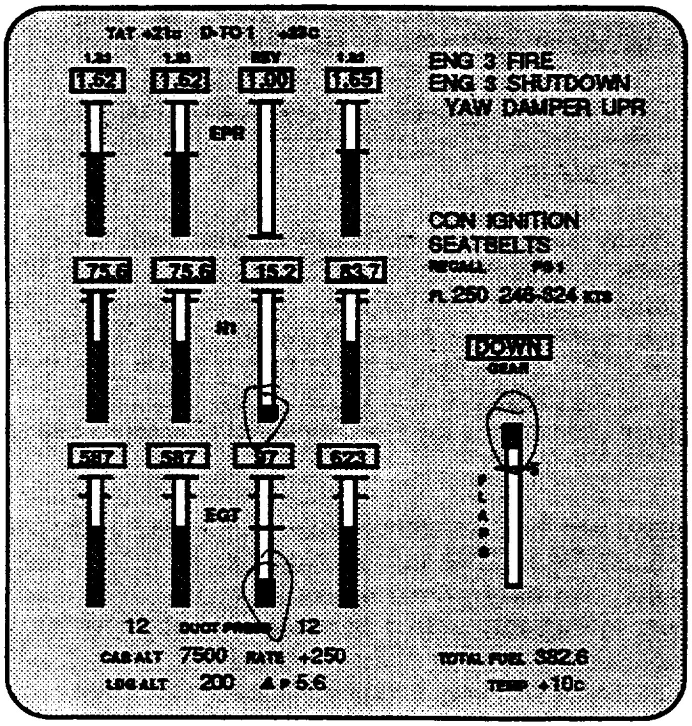

Figure 3-19: Primary EICAS display of power, aircraft configuration and alerts, Boeing 747-400.

The Boeing 757/767 and A310 introduced electronic engine status displays. They depicted information that had previously been available on electromechanical instruments, together with adaptive EGT limits, data on commanded vs. actual thrust for autothrust operation, etc. The later Airbus A320 provided a similar set of electronic displays and alphanumeric information. The Boeing 747-400 power displays were the first to utilize a simplified tape format on a primary and secondary display (figure 3-19). The format eases the task of comparing engine parameters, The MD-11 primary and secondary power displays are again CRT representations of the earlier electromechanical displays.

T. Abbott and coworkers have proposed and evaluated a concept for a simplified set of power displays using bar graphs which show relative data *vs.* expected values for engine parameters (Abbott, T., 1989; 1990). This display is similar to that shown in 3-19, but it compares engine power with a model of expected power.

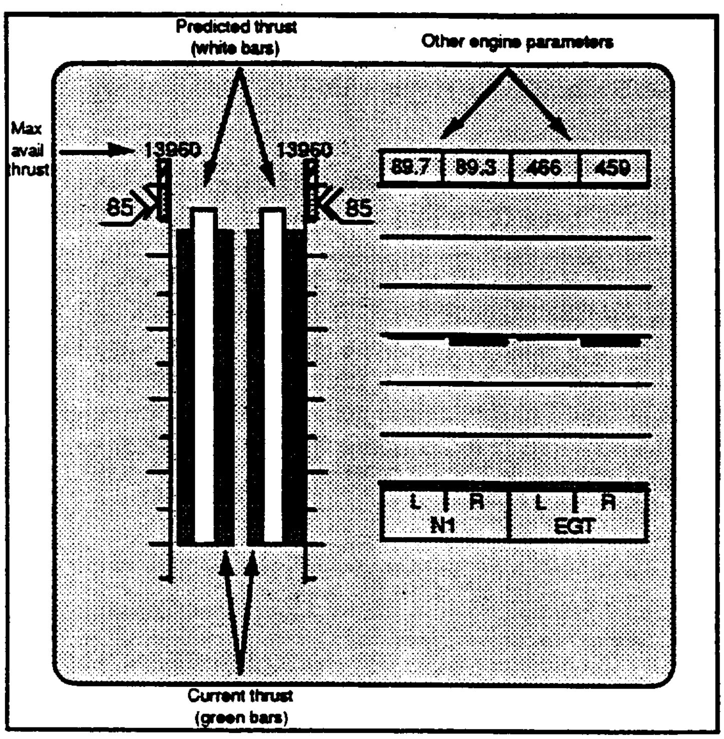

Fig. 3-20: Engine Monitoring and Control Display (from Abbott, T., 1990, p. 27)

E-MACS represents an attempt to reduce cognitive workload by providing a simplified, more integrated representation of power being delivered, using simple dynamic bar charts. The processed information is based on a simplified functional model of the monitored engines, derived from the engine parameters shown in figure 3-19, among others. A glance at the graphics (figure 3-20) is sufficient to inform a pilot about engine condition and whether the requested thrust is being supplied. The concept has been tested in simulation and yielded a decrease in operator errors (all faults were detected vs. 43% of faults on a conventional EICAS display).

The E-MACS concept performs the several cognitive steps necessary to translate raw data into a concept of engine condition and thrust available, and presents summary results to the pilot. It should be noted, however, that its usefulness depends on the adequacy of the system's internal engine model. If actual engine behavior were to differ from the model's predictions, the result could be more confusing than that from a display having a simpler design concept.

The E-MACS display, like the navigation display, is an example of a general trend toward more integrated, pattern-oriented representations to help human operators deal with increasing volumes of data. The concern about overloading operators with information is also the motivating factor for attempts to provide more integrated representations of flight attitude, as noted above with respect to the primary flight display (though a practical display that incorporates all necessary information for this application has not yet been implemented). Similar concerns exist with regard to aircraft subsystem displays, the topic of the next section.

Aircraft subsystem displays

Though there is still a philosophical controversy about the necessity or desirability of providing synoptic (summarized diagrammatic) subsystem information in the cockpit, many pilots and operators clearly find it desirable to have such displays and they are provided in many glass cockpit aircraft. Some designers believe that synoptics of simple systems may increase the risk of misinterpretation. Part of the controversy relates to certification issues; manufacturers wish to incorporate as few essential systems as possible to avoid grounding airplanes when they fail, and the overhead panels on these aircraft permit full manual operation of all subsystems without the aid of the synoptics. On the other hand, pilots are not normally required to operate in this manner and do not practice it; flight crew workload could increase considerably during the time required to reconfigure the affected systems. The Boeing 757/767 cockpit does not provide subsystem synoptics, though the EICAS messages provide information on aircraft system status. Subsequent Boeing aircraft (B-747-400, B-777) do incorporate synoptics, but their designers, and FAA in its certification of the -400, did not consider them essential and the aircraft can be dispatched without them.

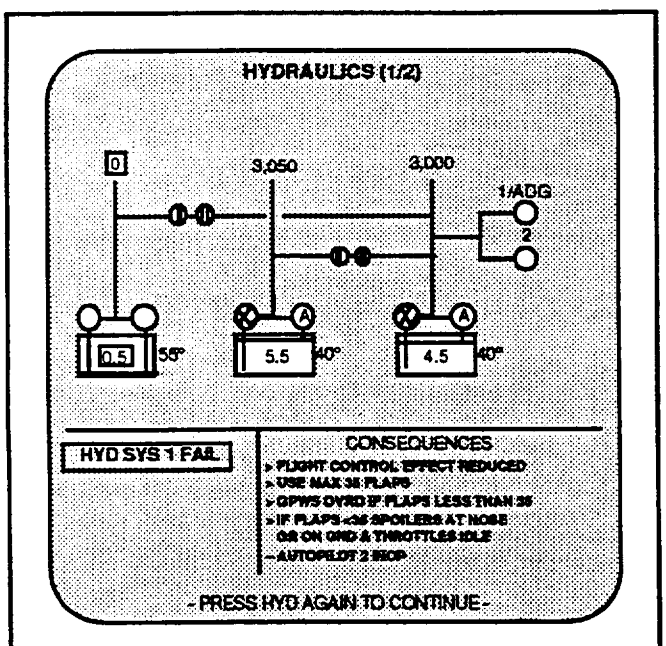

Figure 3-21: Hydraulic system synoptic page, MD-11.

As noted above, Douglas Aircraft has taken a different approach to subsystem management in that it has automated most normal and abnormal actions in the MD-11 subsystems. The synoptics in the MD-11 are simplified diagrams of each subsystem. When an abnormal condition is detected, the appropriate system controller takes action autonomously; an alerting message is displayed on the engine and alert display. The appropriate subsystem pushbutton on the systems control panel is also lighted. When actuated, this pushbutton brings up the synoptic, which will show the system diagram with altered icons indicating the fault, what action has been taken, and a list of the consequences for the conduct of the remainder of the flight.

Figure 3-21 shows an example of a level 2 alert (number 1 hydraulic system fluid loss) which has been resolved automatically by inactivation of the two system 1 hydraulic pumps (the system at the left of the synoptic diagram) after low system 1 hydraulic quantity was detected. The depleted system 1 reservoir is also shown.

Issues raised by automated subsystem displays

Subsystem synoptic displays (see figures 3-20, 3-21, 3-22) can be very complex, though most manufacturers have tried to make them as simple as possible. Multiple faults, however, still require careful pilot attention to several screens to understand fully the nature of the problems (the "keyhole" problem is discussed in chapter 5): more information is available, but more navigating through the menus and representations is necessary to access it). Herein lies another facet of the controversy over what the pilot "needs to know". Modern airplanes are designed to require specific actions (usually as few as possible) in response to any fault or combination of them. The required actions are spelled out in checklists which are designed to be followed precisely. These aircraft are also designed to require no more than checklist adherence for safe flight completion.

There is continuing concern among designers that providing too detailed information on subsystem configuration may lead some pilots to adopt more innovative approaches to solve complex problems, and thereby negate the care the manufacturer has taken to simplify fault rectification. Such behavior has caused serious incidents in the past, among them the destruction of a engine in flight, and will probably continue to do so in the future despite the best efforts of designers to achieve simplicity and clarity in their designs and procedures. Pilots argue, however, with justification based on experience, that faults not contemplated by the manufacturer may well occur in line operations. They point, as one instance, to a L-1011 that landed safely at Los Angeles (1977) after its crew was faced with a compound set of faults for which no book solution existed (McMahon, 1978). They do not wish to be deprived of any information that could assist them in understanding and coping with such problems. The problem for the system designer is to strike the right balance between too little information and too much, recognizing that the pilot's actual needs may not be clear in advance.

Proponents of each approach argue vigorously for their positions regarding display of synoptic information, but since not all information can be presented, the question that must be answered is at what point an appropriate compromise can be found. Better models both of system behavior and of cognitive responses to malfunction information are needed to answer this question. In these and other areas, an important issue is the increasing complexity and coupling of automated systems and the potential for surprises (for both the designer and the pilots) due to the opacity of such systems (Perrow, 1984; see also chapter 7).

Practices with respect to the provision of information regarding subsystems have varied, from tightly-coupled linking of systems, procedures and displays in the Boeing 767/757, to the provision of synoptics simply for pilot information in the 747-400 (figure 3-22) to synoptics that are the primary means of subsystem feedback in the MD-11 and A-310/320 types. The A320 and MD-11 also present a limited number of normal checklists on their ECAM screens; a broader implementation of electronic checklists with automatic sensing of skipped actions is implemented in the Boeing 777, and will likely be seen in other future transport aircraft. Such automation will permit the flight crew to alternate among several checklists when necessary to resolve compound faults. Automated prioritization schemes for such faults are under consideration by NASA and other human factors researchers.

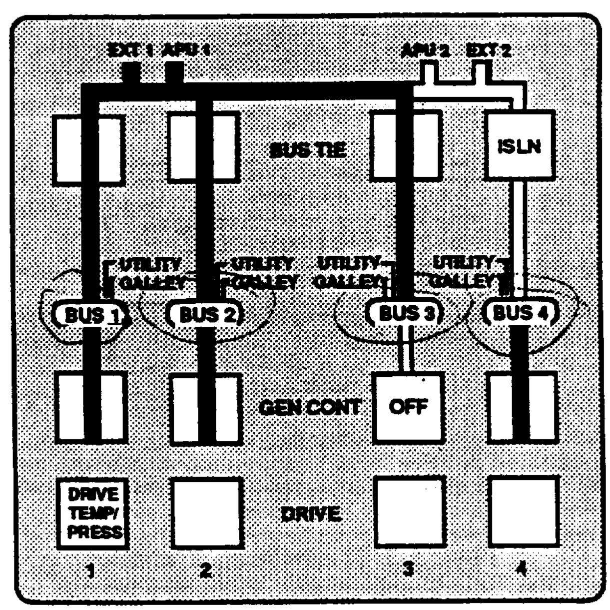

Fig. 3-22: Synoptic display of AC electrical system (Boeing 747-400).

In the MD-80 and B767/757, airplane subsystem control was considerably simplified wherever possible to reduce flight crew workload, though the systems remained conventional. The only alerts that were permitted to appear were those that required pilot decisions or actions, which were carried out largely by actuating lighted push-button switches on the overhead panel. Legends on the buttons showed switch position and, where necessary, related system state. Failure to differentiate switch position from system state has led to problems for operators; this ambiguity was a contributory factor in the nuclear power station accident at Three Mile Island (Woods, personal communication, 1994). In recent aircraft designs, serious efforts have been made to keep the number of corrective or compensatory actions required to a minimum.

Douglas has taken a different approach to subsystem management in the MD-11. Many of its subsystems are automatically reconfigured by an Automated System Controller (ASC) if a fault occurs. The Douglas design philosophy, motivated by a desire to decrease flight crew workload, was stated by its Chief of MD-11 operations: "One of our fundamental strategies has been, if you know what you want the pilot to do, don't tell him, do it" (Hopkins, 1990). Many normal subsystem functions formerly performed by the flight crew have also been automated. Douglas has made no attempt to automate any function which can irreversibly degrade aircraft capability.

The failure to display the basic causes of the faults in the MD-11 implementation of this philosophy presents the potential for pilot confusion or surprises, particularly in the case of a very complex system. Douglas has found it necessary to provide ASC "task lists" in its abnormal/emergency checklists to enable pilots to determine possible malfunctions and the actions the ASC takes when such malfunctions are detected, to clarify possibly ambiguous system states following ASC rectification of faults.

Alerting and warning systems

Configuration displays

Landing gear and other configuration warning systems have been used since it was first discovered by a hapless pilot that retractable gear aircraft could be landed with the gear retracted. Even with these systems, gear-up landings continue to occur occasionally and incidents involving gear up near-landings occur more commonly, usually due to distractions or interruption of routine cockpit task flow. Early warning systems simply provided an aural alert if throttles were pulled back to idle. The use of idle power routinely during descents in jet aircraft required that the landing gear warning system be modified to take account of barometric altitude or other factors that could indicate that landing was not contemplated at the time. Aircraft without such modifications provided large numbers of nuisance warnings to pilots and therefore tended to desensitize them to the importance of the warnings.

Configuration warning systems probably represented the first information automation of any consequence. They date from the early 1930s. In later aircraft, additional surveillance was performed by these systems. In all jet aircraft, a configuration warning system operates prior to takeoff (inferred by landing gear on ground and throttles set at high power) if the airplane wing's leading edge slats or trailing edge flaps are not in appropriate positions for takeoff, or the elevator trim is not positioned within limits determined in flight test to be appropriate for the takeoff maneuver. Before landing (as inferred from throttle and flaps positions), configuration warning systems operate if either gear is up or slats and flaps are in positions other than those permitted for landing.

Nearly all current-generation aircraft have configuration displays that provide aircraft status information in graphic form, though Airbus Industrie has gone farther than other manufacturers in showing graphically the configuration of components of these systems as well as the systems as a whole.

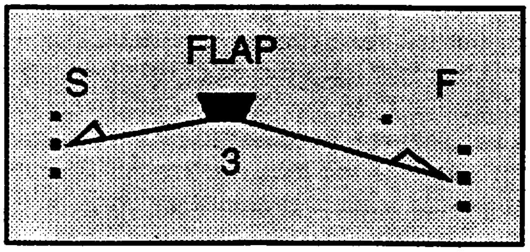

Figure 3-23: Flap-slat position in A320.

Figure 3-23 shows an elegant graphic representation used in the A320 to indicate flap and slat position. The diagram appears on the engine display screen together with engine data, status and alerting messages. The number "3" refers to a flap selector position. The flap and slat indices move as each new device position is selected.

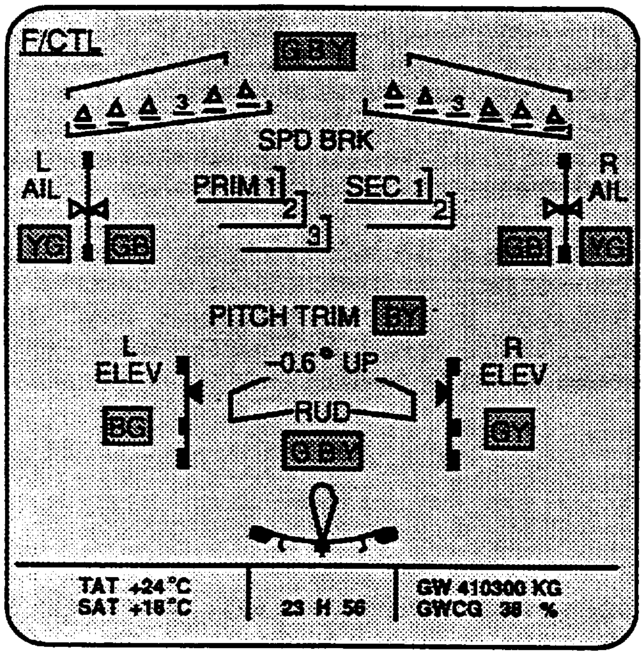

Fig. 3-24: Control configuration display, A340.

The complexity of configuration displays can be high because of the number of items that are pertinent, and the ease with which complex graphics can be generated. Though color can help to direct a pilot's attention to parameters that are abnormal, a good deal of information must still be scanned (fig. 3-24). Cockpit designers have done an excellent job of eliminating large numbers of discrete "lights, bells and whistles", within limits imposed by certification regulations, but they have substituted large amounts of discrete data integrated into a smaller number of displays. Operational constraints often require pilots to review, by whatever means, a great deal of important status information prior to takeoff and during approach, periods that are already busy. (The letters "G", "B", "Y" refer to the three hydraulic systems that power the various control surfaces.)

Altitude alerting systems

In the early 1970s, it was noted by regulatory authorities that the high rates of climb and descent of jet aircraft were causing substantial numbers of altitude deviations (commonly referred to as "altitude busts"), in which aircraft either exceeded the altitude to which they were cleared or failed to reach it. A backup altitude alerting system was mandated for transport aircraft. The altitude alert system consisted of a window on the panel in which the altitude cleared to could be set, and sensors to detect actual altitude. When in a climb or descent, visual and momentary aural signals were actuated approximately 900 feet before reaching the set altitude; the visual signal remained illuminated until 200-300 feet before reaching the new altitude, then extinguished. If the airplane thereafter strayed from the assigned altitude by more than 200-300 feet, the aural and visual signals again appeared.

Malfunction alerting systems

The central multi-function displays in glass cockpit aircraft accommodate alerting and warning information (as shown in an amber boxed legend "HYD SYS 1 FAIL" in fig. 3-21). Older transports had warning and alerting message lights in so many locations that centrally located master warning (red) and master caution (amber) lights were placed on the glare shield in the pilots' direct field of view. Later, dedicated alerting and warning panels with lighted segments containing alphanumeric legends were incorporated wherever there was room for them. As aircraft became more complex, the number of discrete warning signals became progressively greater, reaching several hundred in the early B-747s (Randle, Larsen, & Williams, 1980). In the analysis following a fatal Trident takeoff accident at Heathrow Airport (London, 1972), the investigators cited "a plethora of warnings" that overwhelmed the remaining flightcrew after the Captain's incapacitation and a serious configuration error occurred almost simultaneously (Ruffell Smith, 1974). Newer aircraft have eliminated nearly all of these discrete warning indicators, though the master warning and master caution lights have remained. Alerting information is now presented on the central cockpit screens, usually in the form of alphanumeric messages in a dedicated location (fig. 3-21 shows an example).

While the number of discrete alerting devices has decreased markedly, the number of discrete alerting *messages* that may be displayed and may require action is still large, though the number of level 3 (emergency) warnings has been kept as small as possible. Non-essential warnings and alerts are routinely inhibited during takeoff and final approach. Nonetheless, fault management may still be complex, and newer aircraft are operated by a crew of two instead of the former three persons, so there may be more for each crew member to do during busy periods. It is largely for this reason that Douglas has automated many MD-11 sub-systems management tasks.

Other displays

Aircraft equipped with flight management systems but electromechanical instruments utilize a small monochromatic display in the flight management system for the presentation of alphanumeric information (see fig.3-27, 3-28). Control-display unit (CDU) screens may also be used in the future for ATC messages received by data link units in such aircraft.

TCAS incorporates a planform display of traffic in the vicinity of one's own aircraft. In some installations a dedicated EDU is used. In others, TCAS information may be shown on a color radar screen, while in still others, a new color LCD display combines a presentation of the instantaneous vertical speed indicator (IVSI) with a small planform display of traffic. This instrument replaces the conventional IVSI. In nearly all future glass cockpit aircraft, it is expected that traffic information will be shown on integrated primary flight and navigation displays.

Wind shear advisories in older aircraft are aural and visual, as are GPWS alerts. In new aircraft, wind shear advisories may be displayed on the primary flight display, as are TCAS alerts; in these aircraft, the permitted maneuvering range is shown on the IVSI tape.

Issues raised by automated alerting and warning systems

Configuration alerting systems: Ways of summarizing configuration and subsystem data that can alert pilots to a potential problem are highly desirable. Indeed, in many newer aircraft, pilots have no alternative means of accessing this information. As an example, pre-flight exterior inspection will not show abnormal control surface positions if the hydraulic systems are not powered, because unpowered surfaces drift. There have been cases in which extended wing spoilers on one wing, not indicated on the control surfaces position indicator in the cockpit, were detected before takeoff only by an alert pilot in a following airplane. In at least one case, reported to ASRS, an airplane took off with two spoilers extended and locked on one wing. Fortunately, the airplane was light in weight and the pilot managed to maintain control while returning for an emergency landing.

Alerting messages and aural signals are still used in newer aircraft for critical items prior to takeoff and approaching landing, as noted above. These takeoff and landing configuration warning systems have prevented many accidents, but their occasional failure, and their ability to generate spurious or nuisance warnings, raise a problem of a more general nature. *Devices that are extremely reliable will come, over time, to be relied upon by pilots.* In the rare cases when they fail, or are disabled, pilots may not be sufficiently alert to detect the condition for which the device was originally provided.

Altitude alerting systems: Reports to the NASA Aviation Safety Reporting System (ASRS) indicated that many pilots, after they once became accustomed to the automatic altitude alerter, tended to relax their previously required altitude awareness and to rely on the alerter to warn them that they were approaching a new altitude assignment. If the ordinarily reliable system malfunctioned, or if the pilots were distracted by other tasks and failed to attend to its signals, they "busted" the new altitude. These reports were dramatic evidence that devices installed as a secondary or backup alerting system had become instead the primary means by which pilots derived information. Wiener and Curry (1980) have called this "primary-backup inversion".

Pilots also complained about aural alerts that did not represent an anomalous condition (the signal approaching altitude) They considered these alerts as "nuisance warnings", like the frequent inappropriate configuration warnings referred to above. In response to these complaints, FAA modified the regulations to require only a visual signal before reaching the assigned altitude. From those airlines that thereafter modified the systems to remove the alert approaching altitude, it was noted that reports began to be received indicating that some pilots, accustomed to the unmodified systems, began to report altitude "busts" because of the absence of the aural alert approaching altitude! These reports further reinforced the hypothesis that at least some pilots had come to rely on the alerter as a substitute for altitude awareness.

A similar phenomenon has been observed with respect to configuration warning devices. Though they were intended as backup systems, at least some pilots came to depend on them. This was demonstrated in two mishaps in which takeoff configuration warning devices malfunctioned or had been disabled; in both cases, flight crews failed to detect that flaps and slats had not been deployed prior to takeoff. Both aircraft crashed immediately after leaving the ground, with substantial loss of life (Detroit, 1987; Dallas-Ft. Worth, 1988).

Hazard and malfunction alerting systems: Devices that produce too many "false alarms" will be mistrusted by flight crews. In the extreme case, they will simply be ignored after pilots have become accustomed to them. The earliest models of the ground proximity warning system (GPWS) were prone to nuisance warnings; at least two accidents have occurred because crewmembers ignored, disabled or were slow to respond to warnings that were appropriate (Kaysville,1977; Pensacola, 1978). Later GPWS models incorporated more complex algorithms and the number of nuisance warnings dropped dramatically, although the false alarm problem is still very real at certain locations.

We are now seeing similar problems with large-scale implementation of TCAS-II. This collision avoidance system, mandated by Congress after many years of development by FAA, has unquestionably prevented a number of collisions, but it is an extremely complex device whose control algorithm, now well over 60,000 lines of source code, is not flexible enough to have been able to cope with new ATC procedures to speed the flow of traffic in high-density terminal areas, nor with the large number of aircraft in certain airport areas. As a result, pilots have been burdened with large numbers of "nuisance" warnings in the vicinity of certain airports such as Orange County, California, and during departures from certain terminals, among them Dallas-Fort Worth, Texas. The result has been erosion of confidence in the system, and concern that in certain cases, TCAS may actually worsen the situation (Mellone, 1993). These new mandated functions have been "add-ons"; they are not always integrated with the remainder of the warning systems, and may require quite different responses.

TCAS was mandated by the Congress, as were GPWS and WSAS. They were designed as self-sufficient, add-on systems; in older aircraft, they are not integrated with other cockpit systems, nor with each other. We are already seeing the emergence of new traffic surveillance requirements for TCAS, particularly in over-water navigation where radar surveillance is not available. The

TCAS displays were not designed for these purposes and they may or may not provide information in a form that assists flight crews to perform the additional functions implicit in the new requirements. This is likely to become a more serious problem if pilots are required to take over more functions now carried out by air traffic controllers (see discussion of "free flight", chapter 6).

It is also clear that the use of TCAS in line operations has caused considerable concern among air traffic controllers, who are faced with sudden pilot deviations from cleared altitudes without advance warning under circumstances they cannot control. Their ability to maintain effective command of air traffic rests upon the assumption that pilots will do what they are told to do, and the interjection of this source of uncontrollable variance has caused them great discomfort.

There are *fundamental tensions* between systems capabilities and limitations and human characteristics. False warnings always diminish human trust of warning systems, yet the danger of a missed potentially catastrophic situation requires that conservative warning limits be embodied in such systems. Such situations can arise suddenly and can require immediate action, yet controllers, without an understanding of the immediate problem, cannot function effectively without a knowledge of pilot intent (nor, for that matter, can pilots function effectively without knowledge of controller intent). Communication of intent in advance of action by both humans and machines is an important issue in any real-time dynamic system if all players, or agents, are to remain informed of system status and progress.

Management Automation

During the 1960s, area navigation ("RNAV") systems independent of surface radio aids began to be introduced into aviation. The earliest such system made use of Doppler radar to determine relative movement over the earth's surface. The system was more accurate over water than over irregular terrain, but it provided considerable assistance during the long overwater portions of intercontinental flights and did not require of its operators the highly-developed skills required for celestial navigation. During this period also, inertial navigation systems (INS), first developed for long-range missiles, began to be adapted to air navigation. Like Doppler, all required equipment was carried onboard the aircraft.

INS systems used highly accurate gyroscopes and accelerometers to determine the movement of the system (and the airplane which carried it) after being given a very accurate statement of its initial position prior to flight. INS, like Doppler, was totally reliant on this initialization. If an inaccurate initial position was input, it could not be corrected after the aircraft took off. Several trans-oceanic flights had to be aborted after it was determined that the initial position entry was incorrect.

Both of these early area navigation ("RNAV") systems permitted pilots to enter a series of latitude and longitude waypoint specifications, after which the systems would provide navigation data to the autoflight systems. To this extent, these systems represented the beginnings of flight, or at least navigation, *management* automation. The systems provided pilots with much greater flexibility, but at the expense of greater complexity. They also enabled new types of human error associated with manual entry of waypoint data into navigation computers, a cumbersome and error-intolerant process.

The most revolutionary changes brought about by the introduction of digital computers into aircraft automation have been in the area of flight management. Flight management systems (FMS) in the contemporary sense have been in service for little more than a decade, but they have transformed the pilot's tasks during that time. This section contains a brief description of the modern flight management system, the functions it performs, and its interfaces with the flight crew.

Flight management systems

The introduction of the MD-80 and the Boeing 767/757 marked a fundamental shift in aircraft automation, as noted above. In these machines, the first systematic attempts were made to integrate a variety of automated devices into a seamless automation capability designed for routine use in line operations. Though pilots had been able to program overwater flight paths using inertial navigation systems in older aircraft, the new flight management systems were designed to be the primary means of navigation under all conditions.

Figure 3-25 again shows the control loops diagrammed above, but with the addition of an outer loop which represents management functions. Once again, automation has relieved the pilot of certain tasks, but has added other tasks involving additional cognitive workload. These tasks are the product of the complexity and self-sufficiency of the new functionality, flexibility and complexity of flight management systems. They impose additional knowledge requirements, even while they relieve the pilot of tactical management chores. Most important, there is more information to be gathered and processed to ascertain the state of the aircraft and its automation.

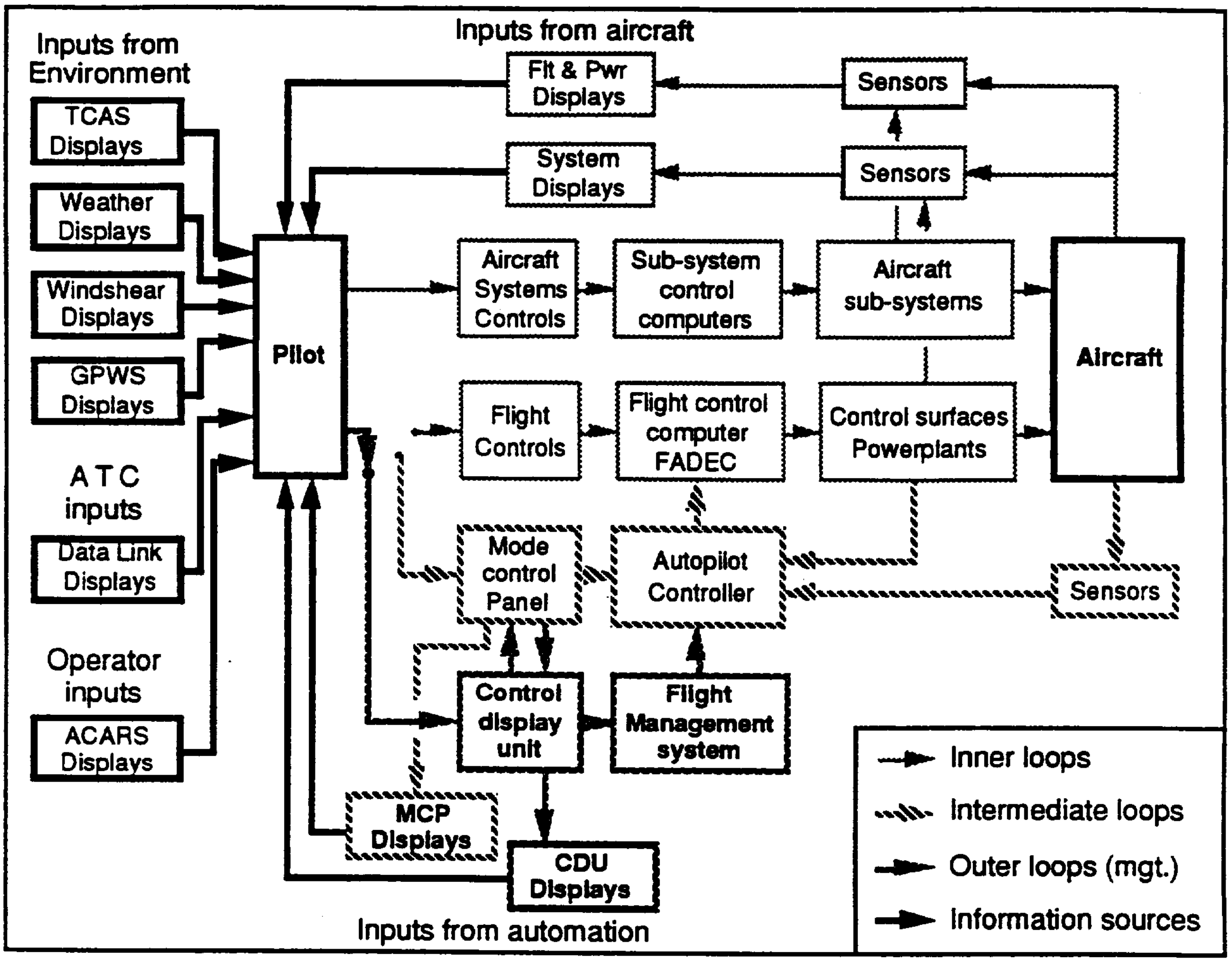

Fig. 3-25: Outer control loops involved in strategic management and information processing.

Flight management system functions

Contemporary flight management systems are complex computational devices linked to and communicating with a great many other aircraft systems as well as with the pilots. Figure 3-26 shows this diagrammatically for the MD-11 FMS (Honeywell, 1990) and the following discussion describes this system, though others have similar capabilities.

FMS software, resident in a flight management computer (FMC), includes an operational program (containing, in this case, over 1400 software modules), a navigation data base, and a performance data base for the aircraft in which it is installed.

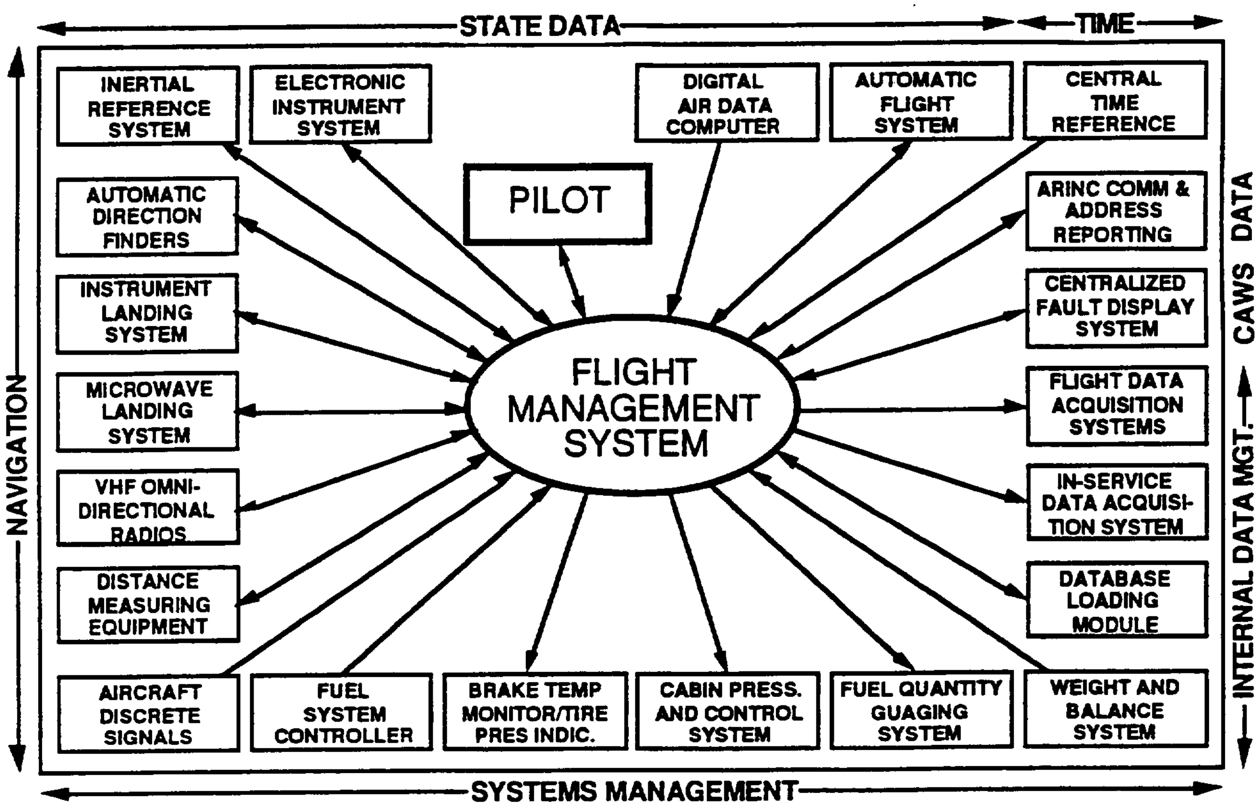

Figure 3-26: Interaction of flight management computer with other aircraft avionics (Honeywell).

The FMC navigation data base includes most of the data the pilot would normally access by referring to navigation charts. This information can be displayed on the CDU or CRT map. The geographic area covered includes all areas where the airplane is normally flown. The data base, tailored to specific airline customers, contains 32,500 navigation points and airway route structure data. The stored data includes the location of VHF navigation aids, airports, runways, geographical reference points, and other airline-selected information such as standard instrument departures, standard arrival routes, approaches and company routes. Up to 40 additional waypoints can be entered into the data base by the pilots. The FMS software executes these functions:

Navigation	Determination of position, velocity and wind; management of navigation data sources.
Performance	Trajectory determination, definition of guidance and control targets, flight path predictions. Time and fuel at destination.
Guidance	Error determination, steering and control command generation.
Electronic instrument system	Computation of map and situation data for display.
Control-display unit	Processing of keystrokes, flight plan construction, presentation of performance and flight plan data.
Input/output	Processing of received and transmitted data.

Built-in test	System monitoring, self testing and record keeping.
Operating system	Executive control of the operational program, memory management, and stored routines.

The FMC performance data base reduces the need for the pilot to refer to performance manuals during flight; it provides speed targets and altitude guidance with which the flight control computer develops pitch and thrust commands. The performance data base is also used by the FMC to provide detailed predictions along the entire aircraft trajectory. The data stored in the data base includes accurate airplane drag and engine model data, maximum altitudes, and maximum and minimum speeds. Functions performed by the FMS include navigation using inertial data from inertial reference units aboard the airplane, updated by a combination of surface and/or satellite navigation aids when available. It provides lateral guidance based on a stored or manually entered flight plan, and vertical guidance and navigation during climb and descent based on gross weight, cost index, predicted winds at cruise altitudes, and specific ATC constraints.

Flight management system controls

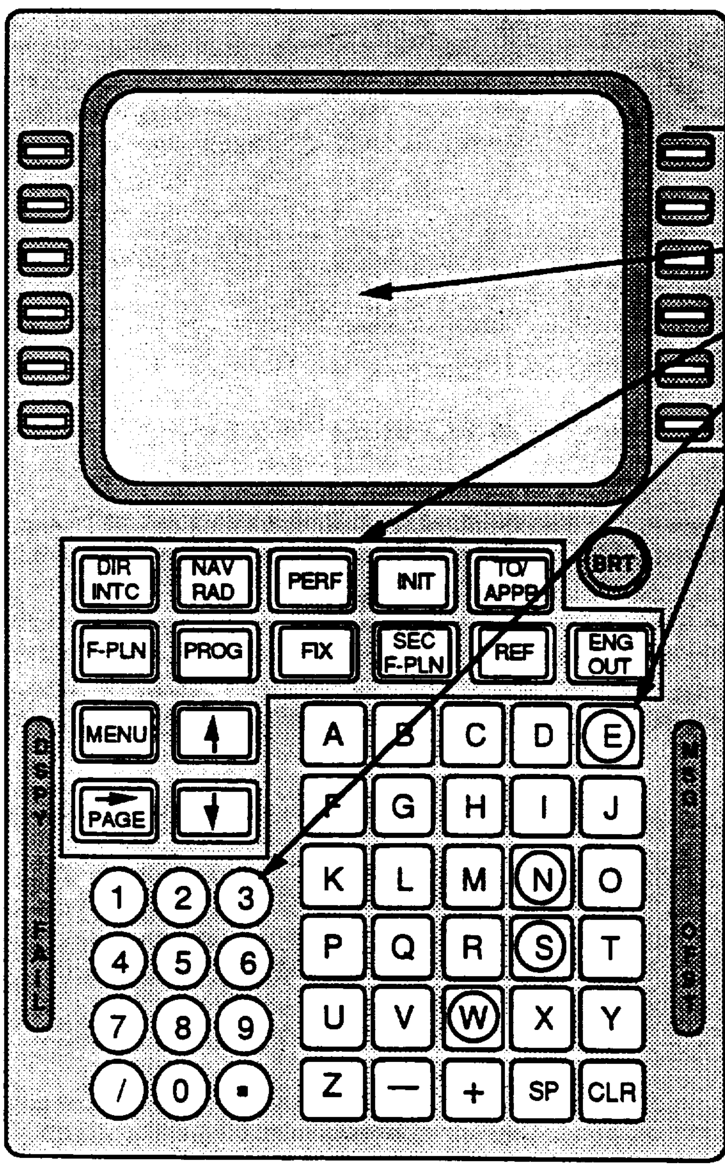

Figure 3-27: Honeywell FMS control and display unit.

Interaction with all flight management systems is through a control and display unit (CDU) which combines a monochromatic or color CRT or LCD screen with a keyboard. An example of a CDU is shown in figure 3-27. The unit contains a CRT display screen, line select keys on each side of the CRT, 15 mode select keys, a numeric keypad, and an alphabetic keypad. The mode select keys provide access to FMS function pages and data; the alphanumeric keypads permit entry of data into the computer.

Newer FMSs provide modes and functions to minimize pilot workload. Among them are the "ENG OUT" function, which provides automatic or manual access to the flight plan (F-PLN) or performance (PERF) pages to assist in evaluating and handling an engine failure condition. Entry of data is accomplished by using the keypads. The entered data are shown on a scratchpad line (see below); when a line select key is pushed, the data are transferred to the indicated line if they are in a format acceptable to the computer.

Flight management system displays

The CDU display consists of a large number of "pages", each containing up to 14 lines of alphanumeric information as shown in figure 3-28.

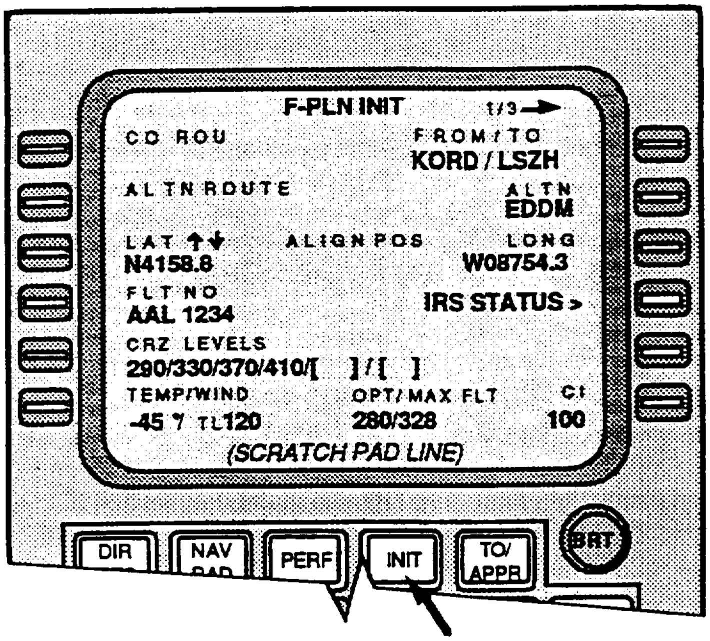

Figure 3-28: Control and display unit screen, MD-11.

The CDU screen shown here appears when the "INIT" (initialize) mode select key is actuated. The title line shows that this is the first of three flight plan screens; others may be accessed with the PAGE key. The scratch pad line is at the bottom of the display. Vertical arrows indicate that the arrow keys may be used to increment values. The small font displays are predicted, default or FMC-calculated values, and labels. The 50 CDU pages are arranged in a "tree" architecture. A portion of this logical, but complex, architecture is shown below in figure 3-29.

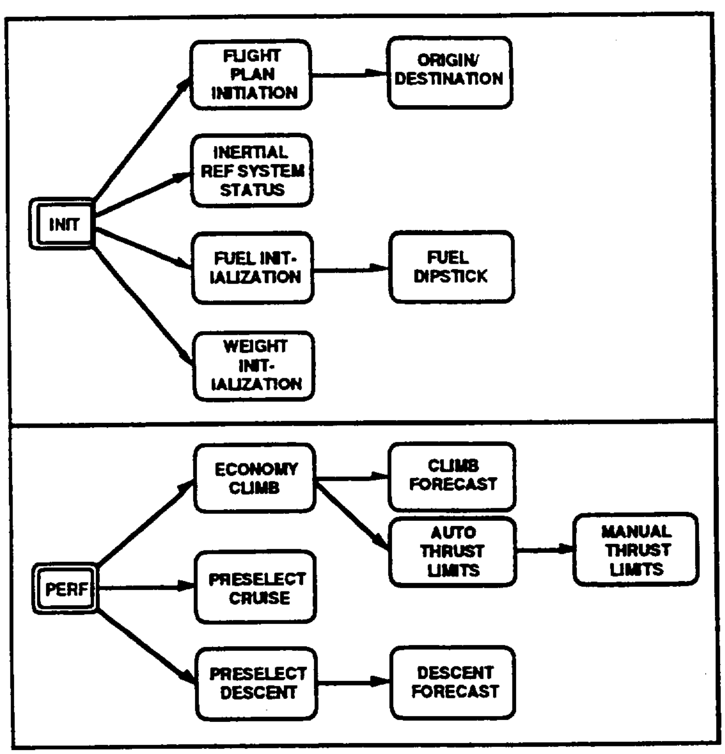

Figure 3-29: FMS mode screens, MD-11.

These diagrams show the tree structure for two modes of this FMS. There are 12 such structures, but in a study of another FMS of the same generation, it was found that the number of sequences was several times the number planned for by the manufacturer (Corker & Reinhardt, 1990). These data structures, as well as the displays, vary greatly among aircraft types and avionics manufacturers. This large number of potential trees involves a considerable attentional demand upon the pilot even if he or she is fully proficient in the use of the FMS. Since flight plan changes are most commonly required during departure and arrival, re-programming the FMS can divert a significant amount of attention that may be needed for outside scan and for cross-cockpit monitoring.

Flight management system operation

The two CDUs are redundant. In the MD-11, both pilots may interact with the FMS simultaneously; however, the system will accept flight plan modifications only one at a time. There are two FMCs, each of which may accept data from either CDU; one FMC is designated as master, and both must confirm data entry before new data will be accepted. The two computers communicate with each other through a private data bus.

Effects of management automation

Programming of INS and Doppler units is an exacting task, requiring precise and accurate entry of many alphanumeric characters. Slips (Norman, 1981) were not uncommon and once made, sometimes went undetected. Air carriers instituted a variety of procedural requirements to detect such errors both during data entry and thereafter during overwater flight, utilizing various crewmembers to read, enter and confirm data and special progress charts to be filled out enroute, in the hope of trapping undetected errors before they affected traffic separation over water where no other means of position evaluation was available.

A few serious errors still crept through the procedural barriers, however, and some led to near-collisions many hours after the initial programming was accomplished, as in an incident between a Delta Airlines L-1011 and a Continental 747 over the North Atlantic Ocean (1987) (Preble, 1987). Also, autopilots had to be properly coupled to the navigation systems; if this was not done, the aircraft could fly a long distance in heading mode rather than in the intended navigation mode. Based on data made available by Russia in recent years, it is now thought that this may have been the error that led to the destruction by Soviet fighters of a Korean Air Lines B-747 after it flew many miles over Soviet territory (Kamchatka Peninsula and Sakhalin islands) enroute to Seoul from Anchorage, Alaska (Sakhalin Island, 1983). It was also the cause of a more recent near-collision between an El Al 747 and a British Airways 747 south of Iceland (Atlantic Ocean, 1990; Pan American, 1990).

Fundamental issues posed by management automation are discussed more fully in chapter 8, but it should be noted that even the early attempts at management automation sometimes distanced pilots from the tactical details of their operations. This, of course, depended on whether the human operators maintained a high degree of alertness concerning the progress of their missions. The safety record indicates clearly that most did, regardless of whether automation was in use. What the increasingly capable automation provided, however, was the *opportunity* to become somewhat less involved, an opportunity which could easily permit tired, fatigued or preoccupied pilots to lose track of their situation if they were not on guard against it. We shall see in chapter 4 the degree to which more modern automation has increased this danger.

Issues raised by flight management automation

In all FMSs, the complexity of the mode and display architecture poses substantial operational issues. Much has been done to simplify routine data entry, but recovery from errors in programming (an acceptable but incorrect entry, for example) can be difficult. Entry of certain types of data remains cumbersome and diverts attention from other flying tasks, as discussed below. If an unacceptable entry is attempted, it is rejected, but without explanation of the error that led to the rejection, as one instance.

Interaction with the FMS is through one of two or three identical CDUs mounted on the center console. Even with color to assist, operation of the FMS requires close visual attention to the screen, and precision in entering data on the keypads. Alphanumeric data entry is known to be subject to human errors: numbers may be recalled incorrectly from short-term memory, they may be input incorrectly, or they may be misread when the entries are verified in the scratchpad before entry into the computer. Some data must be entered in a specific sequence which imposes additional memory load on the operator; screen prompts are not always clear, when they are available.

Avionics and aircraft manufacturers have made many efforts to make interaction with the FMS more error-resistant. Standard or frequently-used routes are stored in the navigation data base and may be recalled by number. SIDs and STARs are also in the data base; if a change is required by ATC, only the name of the procedure need be entered. Changing the arrival runway automatically changes the route of flight. Appropriate navigation radio frequencies are auto-tuned as required. Perhaps most important, newer FMSs interact directly with navigation displays; pilots are shown the effect of a change of flight plan in graphic form. They can thus verify that an alternative flight plan is reasonable (though not necessarily what was requested by ATC) before putting it into effect.

In most newer aircraft, entry of tactical flight plan modifications (speed, altitude, heading, vertical speed) can be done through the mode control panel (MCP) (see figure 3-30) rather than the CDU. These entries may either supersede FMS data temporarily, or may be entered into the FMS directly from the panel.

It is likely that these improvements may resolve some problems with tactical data entry, though pilots must keep track of more potential mode interactions. Mode control panels now contain numerous multi-function control knobs (turn to set; pull to activate, push to transfer data to FMC), which has posed problems of a different sort when pilots have inadvertently activated a mode other than that intended.

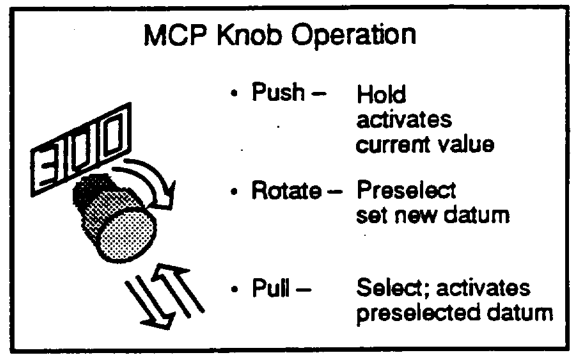

Fig. 3-30: MCP operation (Fokker 100)

Vertical navigation profiles generated by the FMS take account of standard ATC altitude constraints as well as airplane performance constraints, though the air traffic control system is not, at this time, able to take full advantage of the capabilities of management automation which calculates profiles based on actual rather than average aircraft weight. Optimal descent profiles will therefore differ enough to cause sequencing problems for ATC.

In some newer aircraft, manual tuning of navigation radios is possible only by interacting with the CDU. Many pilots have complained that alphanumeric entry of frequency data is more time-consuming and requires more prolonged attention inside the cockpit than setting the rotary selector knobs in older aircraft.

Though flight management systems truly permit pilots to manage, rather than control, their aircraft, the dynamic nature and increasing complexity of today's operational environment has strained the capabilities of the human-machine interface (see below). Despite this, the systems are extremely effective and have enabled many improvements in operational efficiency and economy.

The greatest improvement in FMS display capability has been its integration with aircraft navigation displays, improving visualization and freeing the systems from some of the constraints imposed by small alphanumeric CRTs. The addition of colors, matched with those used on the navigation displays, to the CDU display may help (early displays were invariably monochromatic), though the resolution of the color displays is somewhat less and the usefulness of color in this application has not received much systematic study. The design of pages, however, still represents a compromise between the amount of alphanumeric data per page and the number of pages necessary to enable a particular function. Pilots must look at a very large amount of data through a relatively small "keyhole" (Woods, 1994a).

Initial FMS designs were based on the notion of FMS use at high altitude in cruise flight. The success of the concept resulted in extension of the "cruise" concept into use throughout flight, without redesign of the interfaces, a common problem with successful automation (Fadden, personal communication, 1995). The attention required for reprogramming has led to undesirable *ad hoc* procedures in the cockpit; appreciable numbers of pilots prefer not to interact with the systems below 10,000 feet during descent, in order not to compromise aircraft management and scan for other traffic (Curry, 1985; Wiener, 1989). This approach permits human resources to be devoted to more important tasks, but at the cost of losing some of the benefits of the FMS during flight in the terminal area (such as its knowledge of altitude restrictions). As noted by Fadden, this is a problem of human-system interface design, rather than a problem in the functionality of the systems themselves. Research and development efforts are underway to improve these interfaces and specifically to make them less totally dependent on cumbersome alphanumeric data entry, but considerable attention to the CDU displays is also warranted. There remain important questions about the integration of these systems into the overall cockpit and automation design, and it is these integration issues that most need to be resolved.

Comment

Aircraft automation's major benefits, among them improved fuel economy and operating efficiencies, have been accompanied by certain costs, including an increased cognitive burden on pilots, new information requirements which have required additional training, and more complex, tightly-coupled, less observable systems. To some extent, both benefits and costs are inherent in these highly automated systems. Other costs have accrued because today's automated systems are not optimally designed to work cooperatively with their human operators. Finally, some costs have accrued because the automation was designed to operate in an ATC system that is constantly evolving, forcing human operators to adapt and tailor their uses of and responses to the automation and the changed requirements.

Plus ça change, plus la mème chose—the system changes (as usual); the pilots and controllers adapt (as usual). This is not new, but as elements of the system become more complex and less transparent, the task of adapting becomes more complex and more difficult. The further changes likely to be seen in future aircraft, and their likely effects on operators, are the subject of the next chapter.

4. Aircraft automation in the future

Introduction

This chapter considers aircraft automation proposed or already developed for use in the near-term future system. Airframe and avionics manufacturers and operators alike are constantly on the watch for emerging technology that can widen their scope of operations. Satellite navigation, as an instance, offers the promise of freeing aircraft from constraints imposed by ground navigation facilities, especially if those same satellites can enable landing at any suitable airport, whether or not it is served by precision approach systems. On the other hand, new technology is expensive, and air carriers are only beginning to emerge from a period in which they have suffered the greatest losses in the history of commercial aviation.

Given this economic climate, new aircraft will have to be more efficient, more reliable, and less expensive to maintain than those presently on the market. It will not be easy for airframe and powerplant manufacturers to meet these goals. If new automation functionality can improve efficiency or productivity, it will be embraced. If not, it is not likely to find its way onto future aircraft, at least in the near term. Let us look for a moment at some of the enhancements that have been proposed for near-term (1995-2015) implementation (figure 4-1).

Enhancements proposed for future transport aircraft

- **Control Automation**
  - Low-visibility taxiing assistance or guidance
  - High-precision in-trail operations in terminal areas
  - Automated collision avoidance maneuvers
  - Automated wind shear avoidance maneuvers
- **Information Automation**
  - Electronic library system–"paperless cockpit"
  - Satellite navigation and flight following
  - Digital data link–high bandwidth communications
  - Satellite communications world-wide
  - Automatic dependent surveillance
  - "Big picture" integrated cockpit displays
  - Enhanced head-up displays
  - Enhanced or synthetic vision systems
- **Management Automation**
  - Easier, more intuitive FMS interfaces
    - Cursor modification of flight plans
    - Improved error-checking
  - Direct FMC-ATC computer communication
  - Improved error tolerance
    - Enhanced error monitoring and trapping
  - Improved electronic checklists
  - Improved mental activities models for design

Fig. 4-1: Proposals for future aircraft automation

Control automation is already highly sophisticated; its future applications will probably extend its capabilities rather than making new functions available. An exception to this generalization is the possible requirement for automatic flight during approaches to closely-spaced parallel runways.

Information automation is an area in which many new functions have been proposed; some are now in test or demonstration. Navigation functions will be revolutionized during the next decade by the implementation of satellite navigation for guidance and ADS for flight following.

In the area of management automation, efforts will be directed toward the improvement of the human-machine interfaces and (hopefully) toward new functions or modification of existing functions to improve the error tolerance of the human-machine system.

In *Trends in Advanced Avionics*, Curran (1992) provides a review of avionics evolution throughout the history of aviation and discusses present and future trends in avionics. In one chapter, Perspectives on the Future, Curran states (p. 160) that "Past avionics advances have permitted the elimination of the radio operator, flight navigator, and the flight engineer positions in the cockpit. Future improvements should result in better avionics functional capability, integrity, and availability for the remaining crewmembers." He concludes (p. 172), "Avionics designers must find ways of keeping flight crews more involved as the need for automation increases. Avionics designers must become more aware that there is a kind of automation that improves situation awareness and there is a kind that diminishes this awareness. The challenges for avionics designers are many...These improvements must be accomplished without creating unacceptable workload and information overload."

Curran is quite correct that automation can either enhance, or diminish, situation awareness, and that there is a real need for designers to understand the difference between them. As Woods (1993a) has pointed out, representations are never neutral. Unfortunately, neither Curran nor most other authors have stated how this understanding comes about, or even what the critical differences are. This is a question of some gravity, for without such understanding we cannot improve the design of future automation or the performance of the human-machine systems in which it will be embedded.

Aircraft automation today

If we wish to examine future aircraft automation, the Boeing 777 and Airbus A330 are convenient benchmarks. Both are flying today; together they represent the state of the art in transport aircraft and to a considerable extent, the future of aircraft automation. The A330's cockpit, however, is as nearly identical as possible to that of the A320 and the four-engine A340 to minimize problems in transitioning among these aircraft, another factor driven by economic pressures (see chapter 14 for discussion). The 777 is a new aircraft type and its cockpit is not a derivative, though it has much in common with the slightly older 747-400. Since I have discussed the A320 in chapter 3, I shall spend some time here in an examination of the 777, using various Boeing materials as primary sources.

The Boeing 777

The Boeing 777 is the world's largest twin-engine transport airplane. It was designed for extremely long-haul routes ("B" version), though a shorter-range "A" market variant was the first to enter production. The A330 is slightly smaller than the 777; the Airbus consortium's A340 is its longer-legged companion. The B777 will cover and exceed the range spectrum of the 747-400, though with a smaller capacity.

A330-300 and B777-200 Specifications and Performance

	A340-300	A330-300	B777-200 A-Market	B777-200 B-Market
Size				
Wingspan	198 ft	198 ft	200 ft	200 ft
Length	209 ft	209 ft	209 ft	209 ft
Tail height	55 ft	55 ft	61 ft	61 ft
Cabin width	17'4"	17'4"	19'3"	19'3"
Max. TO weight	558,900 lb	458,600 lb	515,000 lb (1)	632,500 lb (2)
Performance & capacity				
Range	6,750 n.m.	4,550 n.m.	4,240 n.m.	7,380 n.m.
Maximum speed	M 0.86	M 0.86	M 0.87	M 0.87
Fuel capacity	35,660 gal	24,700 gal		
Passenger capacity	295	335	375	305
Cargo volume	5751 cu ft	5,751 cu ft	5,656 cu ft	5,656 cu ft

Notes:
(1): A 535,000 lb variant with a range of 4,820 n.m. carrying 305 passengers will also be offered.
(2): Data shown are for the largest of three variants planned.
Data from Airbus Industrie, 1/1990, and *Aviation Week & Space Technology*, 4/11/94, p. 48.

Fig. 4-2: Comparative specifications of modern transport aircraft

Pilot's Role and Responsibility

- The pilot is the final authority for the operation of the airplane.
- Both crewmembers are ultimately responsible for the safe conduct of the flight.
- Decision making on the flight deck is based on a goal hierarchy.

Pilot's Limitations

- Expected pilot performance must recognize fundamental human performance limitations.
- Individual differences in pilot performance capabilities must be accommodated.
- Flight deck design must apply error tolerance and avoidance techniques to enhance safety.
- Flight decks should be designed for crew operations and training based on past practices and intuitive operations.
- Workload should be balanced appropriately to avoid overload and underload.

Pilot's needs

- When used, automation should aid the pilot.
- Flight deck automation should be managed to support the pilots' goal hierarchy.
- Comfortable working environment.

Fig. 4-3: Boeing 777 cockpit design philosophy (Kelly et al., 1992)

The overall philosophy espoused by the 777 cockpit design team was "crew-centered design and automation" (Kelly, Graeber, & Fadden, 1992, p. 1). This philosophy had been under development for some time before the program was launched (Braune and Fadden, 1987). It is based on the principles set forth in figure 4-3.

Kelly et al. point out the similarity of these principles to those presented in chapter 2 of this document. They are a distillation of experience—what has worked well and what has not—in earlier aircraft. They have pointed out, however, the difficulties inherent in translating these principles into the specifics of a particular flight deck design, in part because of their lack of specificity and because economic and market issues heavily impact the operational features which will actually appear on a new flight deck. "Recently, for example, head-up displays, electronic library systems, and some improvements to flight management functions have been difficult to justify because they did not appear to provide new capabilities which would result in return on investment".

The 777 is Boeing's first commercial fly-by-wire airplane. Large control columns have been retained; the two columns are cross-linked and are back-driven by the autopilots to retain tactile feedback to pilots of control inputs either by the other pilot or the automation. Similarly, the thrust levers are back-driven by the autothrust management system. Control laws provide speed stability; manual trimming is required when speed or pitch is changed. This approach also provides more feedback to pilots, though at the expense of somewhat greater workload during "manual" flight (actually "assisted": all flight control is through the electronic systems).

Perhaps the most obvious innovation in the 777 cockpit is a cursor control used to respond to electronic checklist items, to navigate through menus, and to interact with data link functions when these are implemented. (It does not interact with the FMS or the navigation display at this time.) There are several other innovations, however, including flat panel display technology rather than CRTs; LED lighting for switches and light plates, a master brightness control, and improved LCD displays.

An electronic checklist function has been implemented. The system senses many checklist items and indicates their completion during checklist execution; other functions are marked through the cursor control when completed. The checklist system also keeps track of checklist items not completed and indicates these on command. Both normal and abnormal/emergency checklists are incorporated in the system, to minimize the number of "memory items" required to be performed by the pilots.

Other significant innovations have been provided for but can be implemented only when industry standards are developed. There is a data link interface, for instance, but its final form will depend on the standards set by the FAA in the future for its Automated Telecommunications Network. Similarly, the airplane is equipped for satellite navigation using GPS, but primary reliance on GPS depends on development and implementation of a navigation satellite integrity monitoring and alerting system, as well as the installation of differential GPS stations at or covering airports to be served by GPS precision approaches.

The flight management system on the 777 is not new, though certain aspects of its operation have been simplified to ease programming (and particularly re-programming) workload, a design effort that has been in progress for several years. The FMC automatically detects certain anomalies such as an engine failure and recalculates aircraft capabilities. It also constructs a flight path back to a departure airport if an engine fails during the initial climbout. When instructed by a single keystroke, the FMC builds a transition from a selected runway approach course to another at the same airport and retunes the navigation radios automatically to those appropriate for the new runway, relieving pilots of significant distraction when ATC requires a runway change.

The 777 control-display unit is the first airline unit to use a color screen; colors correspond to those used to highlight specific data on the navigation display, which is generated from the FMC when routes are programmed. This is an excellent use of color and another effective step in the integration of cockpit interfaces. Though the primary displays in the cockpit do not differ greatly from those in the 747-400, many small design innovations have been introduced.

Both the 777 design philosophy and its implementation are more conservative than in some other new aircraft. Though Boeing has always been a conservative company, this may in part be due to an unprecedented effort by the firm to involve customers (as well as human factors experts) in the design process from the outset. United Air Lines, British Airways and All-Nippon Airways had operations and maintenance staff on the Boeing premises throughout the design and development of the airplane. A full-time human factors group was a part of the flight deck design team, and Boeing also utilized human factors consultants from government and industry at intervals during the design phase.

Perhaps most important, and unique in civil transport development programs, engineering simulators were available from early in the process. The first simulator, though not then complete, became available at the beginning of 1991; it was fully functional before the flight deck functional definition was complete and was heavily utilized for familiarization by consultants as well as by the design team. A second simulator was operational before the end of 1993. These devices made it possible to evaluate not only individual devices and functions, but how they were integrated, before the first cockpit was actually built.

Beyond the 777

What lies beyond this point in transport aircraft automation? As noted above, many features thought desirable for tomorrow's flight decks have not been implemented in the 777 because of economic factors: they have not been able to "buy their way" onto the airplane. Nevertheless, several innovations are under active development at this time, either by airframe or avionics manufacturers or in a few cases by air carriers. Some nearly made their way into the 777 design, such as an Electronic Library System. Others were prepared for in that design, to save the expense of later retrofit: data link modules are an example. Still others are being tested in aircraft now flying the line; satellite navigation, communication and automatic dependent surveillance fall in this category.

Other innovations now under development include synthetic vision systems designed to provide pilots with an adequate view of the runway and airport environment during conditions of extremely poor visibility. Finally, there is a set of innovations under consideration or early development whose future use is uncertain. Among them are very large-screen integrated displays incorporating synthetic or "enhanced" views of the aircraft surround and also information concerning aircraft state and status. These devices are sometimes referred to as "big picture" displays; originally considered for military aircraft, they are also under serious consideration for future civil aircraft in which outside visibility will be limited, notably a future high-speed (Mach 2+) civil transport without a forward view from the cockpit (this is discussed below).

Future aircraft automation

Much of this chapter is devoted to technology trends, but the reader must not lose sight of the real issue: the relationship of humans and machines in a complex human-machine system. Each new technology element discussed here, if introduced, will shape human operator behavior. Will the technology *and* the humans who operate it significantly improve the safety, reliability or economy of the overall operation? New devices must have that potential, or they would not be introduced, but it is sometimes a far cry from what should happen to what will happen. This thought pattern must be at the forefront of our minds as we consider new technology for the future system.

I shall continue to categorize technology as control, information, and management automation, though the separation among these categories becomes blurred by the increasing integration of various functional elements. It is a comparatively short step, as an instance, from the provision of a wind shear advisory system (information automation) to the provision of an autoflight module that responds autonomously to such an alert with a predetermined avoidance maneuver (control automation).

Control automation in the future

Because control automation is already so advanced in the newest aircraft, one would expect less further innovation in this area of aircraft automation. Rather, I would anticipate that near-term efforts may be directed toward making existing functionality yet more self-sufficient and autonomous, a trend which would further bound pilot authority with the intention of avoiding execution errors under difficult circumstances. Such a trend, of course, would also increase automation complexity and would probably increase the opportunity for surprises.

Minimizing separation requirements in terminal areas

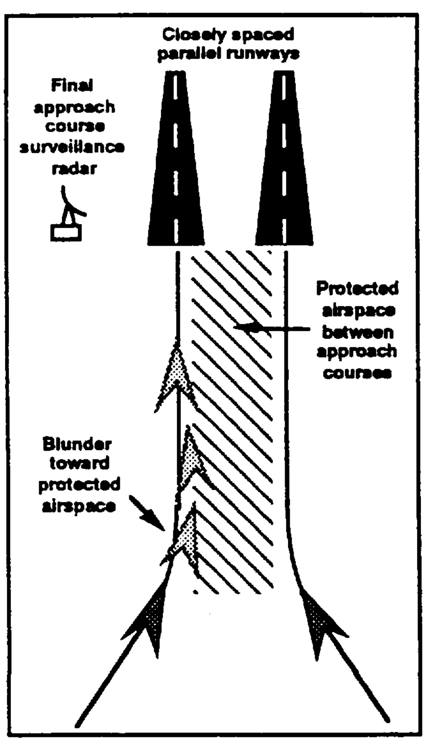

Fig. 4-4: Closely-spaced parallel approaches

The need for increased capacity and throughput has already stimulated the FAA, with NASA, to begin an intensive examination of how technology may be used to increase airport acceptance rates by enabling parallel independent approaches to converging or closely-spaced parallel runways (fig. 4-4). At present, independent approaches to parallel runways at the same airport are not permitted under instrument meteorological conditions unless the runway centerlines are 4300 ft apart. Parallel runways at many major airports are spaced more closely than this because of land restrictions; at San Francisco, as an example, runways 28 left and 28 right, the major landing runways, are only 750 ft apart. The overall acceptance rate for this airport is roughly halved when instrument conditions exist, as they often do because of fog or low cloud. While it is not likely that independent operations will be permitted to runways this close together, FAA and NASA have conducted simulation experiments to determine whether the 4300 ft limitation can be reduced by the use of surveillance radar with a one-second rather than the present 3-second scan rate.

These studies indicated that with improved ATC and radar surveillance, pilots can consistently conduct approaches to two or even three parallel runways whose centerlines are separated by less than 3500 feet, though tight control is required and the problem of blunders or slow turns to the final approach course becomes more serious as separation decreases. The most difficult aspect of such operations, even under VMC, is the "belly-to-belly" cockpit visual restriction when aircraft bank for the turn to the final approach course from opposite sides of the extended centerlines.

Issues raised by reduced traffic separation concepts

If these types of operations are approved for general use at equipped airports, they will be combined with minimum safe longitudinal spacing to make maximum use of the capacity of each runway, possibly using TCAS displays or radar for station-keeping. The Air Force has used station-keeping radar very effectively for in-trail formations. The dual tasks of very precise station-keeping and lateral control will be demanding, and control automation may be introduced and even required to obtain maximum flight path precision under these circumstances. I would also expect that automated alarm systems will be developed to augment controller surveillance of such operations.

Whether manually or automatically flown, tightly-spaced final approaches under IMC will impose considerable cognitive workload both on pilots and on controllers, especially when unforeseen circumstances force departures from nominal flow. If a leading aircraft is slow to clear the runway, following aircraft will have to execute missed approaches, possibly toward aircraft taking off on crossing runways. Design of procedures must insure that one or several aircraft have clear escape paths from any point on the approach. (These contingencies have not always received sufficient attention in the past.) With closely spaced aircraft under IMC, this may not be easy.

The temptation to use such innovative technology to the fullest will be difficult to resist; indeed, increased throughput is the motivation for this technology and these procedures. *Human operators must not be placed, however, in a situation from which they cannot safely and reliably extricate themselves and their aircraft if some element of the automation fails,* which may mean that the full benefits of the technology cannot be realized without eroding safety margins. This dilemma will become commonplace as we attempt to squeeze every possible increase in capacity from our finite airspace; methods to insure that it is done without decreasing safety must be developed where they do not now exist.

Protection against environmental threats

Three types of automated environmental alerting and warning functions are now implemented in transport and some corporate aircraft. They are ground proximity warning systems, traffic alert and collision avoidance systems and wind shear advisory systems. Each is designed to detect threats that may not be obvious to pilots, especially under instrument meteorological conditions. At this time, each is an information system; pilots must respond manually to the warnings. Each requires a pitch mode response; for TCAS-II warnings, the pilot may be required to descend or climb, while GPWS and WSAS advisories require a maximum rate climb to a safe altitude.

Each of the older systems (GPWS, TCAS) has appreciably enhanced safety. GPWS, though not universally effective, has a documented safety record (e.g., Porter & Loomis, 1981). Even at its present state of development, TCAS-II is perceived by pilots and the FAA to have prevented at least several midair collisions—just how many is impossible to tell. WSAS is too new to have accumulated such a record, and newer devices (active sensors in aircraft to improve detection capability, as compared with passive inertial sensors, and Doppler radar at airports, the first of which was commissioned at Houston in July, 1994) are under development, but there is good reason to believe that some form of WSAS will be helpful to pilots, especially during takeoff and approach in the vicinity of convective turbulence. During tests of the Doppler system at Denver in 1993, a considerable number of airplanes were able to avoid severe wind shears.

Issues raised by environmental protection systems automation

Both GPWS and TCAS have produced variable numbers of false and nuisance alarms, particularly early in their periods of line service. Though Ground Proximity Warning Systems have been greatly improved since they were mandated in 1976, they still give rise to nuisance warnings—in the case of one large carrier, 247 of 339 GPWS warnings during a recent 12-month period were false or nuisance alarms (73%). Like all new technology, TCAS has also caused new problems, most importantly for air traffic controllers (see below). Inadequacies in the TCAS software have also burdened pilots with nuisance alerts in considerable numbers, and with a few resolution advisories that if followed would have put the aircraft in danger.

The problem of false/nuisance warnings is not trivial. If a substantial fraction of the warnings received are evaluated by pilots in hindsight as false or unnecessary, they *will not* trust these systems, even if some of the warnings are correct and could save the aircraft. Pilots' (or controllers') perceptions (whether correct or not) about the inaccuracy of warning systems will shape their behavior toward trying to verify whether the warnings are correct–yet delays in responding to appropriate or true warnings may negate their effectiveness. Airlines have mandated full responses to GPWS warnings, but have had to backtrack on these procedures in the face of numerous nuisance warnings at certain specific locations. Procedures may be required in the short run, but they are not the best answer.

To my knowledge, no aircraft now flying in line service responds automatically to these warnings, though autonomous responses could be implemented and would have some theoretical advantages. Manually-flown TCAS responses, in particular, often exceed the vertical plane separation boundaries established by ATC, and this has been a source of intense discomfort to controllers who are faced with sudden altitude excursions without advance warning. The initial operational simulation evaluation (Chappell et al., 1988) indicated the likelihood that such excursions would be observed, and operational evaluations have confirmed it. It is likely that automated resolution advisory responses could minimize such excursions.

The great danger of an inadequate response to a true GPWS warning has motivated nearly all air carriers to require a full procedural response unless it is visually obvious to the crew that no danger of controlled flight into terrain exists (see, for example, Kaysville, UT, 1977). Cases continue to crop up, however, in which an inadequate crew response failed to avert the condition that motivated the warning, and this has been an accident cause in equipped aircraft. Like TCAS avoidance maneuvers, GPWS responses could easily be automated, and it has been suggested that this be done. On the other hand, false or nuisance GPWS alerts occur under a variety of circumstances, among them in holding patterns when an aircraft passes directly over another below in the same pattern. A GPWS response under these conditions could cause the maneuvering airplane to climb into the path of yet another aircraft holding 1000 ft above. (It is worth noting that ATC, which has only a planform view of traffic, cannot detect such an excursion in a holding pattern, so an important element of redundancy is not available. TCAS should warn of a potential conflict, but it is not infallible either.)

Severe wind shears, often caused by microbursts, have been responsible for many aircraft accidents over the years (Caracena, Holle & Doswell, 1989; Boeing, 1994). The most recent occurred only a few months ago, at Charlotte, NC (1994). They are particularly dangerous to aircraft flying slowly in a relatively high-drag configuration; such configurations occur routinely during approach to landing. Wind shear advisories, like GPWS alerts, require an immediate maximum-performance climb, trading kinetic energy (airspeed) for potential energy (altitude) if appropriate. There is little doubt that this escape maneuver could be more precisely performed by automation than by the human operator, simply because not all of the inertial and air data information necessary for the performance of the maneuver is available in the cockpit and a very rapid response is required. This would seem, therefore, to be an ideal candidate for control automation. Although wind shear avoidance systems have been under development for several years, there is not yet, to my knowledge, sufficient information to indicate how frequently false or nuisance alarms may be generated by such systems.

In each of these cases, however, the false alarm problem, together with the many other variables not known to or accounted for by the logic in these systems, suggests a considerable measure of caution with respect to automating escape maneuvers. Leaving aside issues of passenger comfort, a secondary consideration when safety is threatened, the record to date suggests that very substantial numbers of unnecessary and sometimes dangerous escape maneuvers would occur if pilots were not in the loop, and given the time-criticality of these threats, it is likely that pilots would not be able to moderate or inhibit automated response maneuvers.

Further, the initiation of an unannounced escape maneuver by the autopilot when a pilot was flying manually would almost certainly be countered (at least initially) by the pilot, who would consider the maneuver initiation to be a turbulence or other input which required corrective action. At least one recent accident has involved pilots attempting unsuccessfully to counter automation inputs (Nagoya, 1994; see also Paris, 1994). If escape maneuvers were to be automated, highly salient displays to inform the pilot of the intervention would be required, and pilots, as well as ATC, would have to have special procedures available to cover conflicts that might be introduced by the performance of the maneuver.

Automated warning systems have saved lives and aircraft, but they are good example of the dictum stated earlier: that what *should* happen and what *will* happen when new technologies are introduced are often at variance. If new systems are introduced without considering the full range of behaviors they may evoke and the new problems they may create, they are liable to do more harm than good.

Ground maneuvering assistance

A third area in which control automation (together with information automation) may be introduced is on the ground at airports, to assist pilots in guiding their aircraft between parking gates and active runways under conditions of poor visibility. Today's aircraft can land automatically, or even manually, under visibility conditions that are inadequate to permit them to taxi safely from the runway to a gate. This fact and the serious problem of incursions of aircraft into airport movement areas without clearance (Billings & O'Hara, 1978; Detroit, 1990) has stimulated a serious search into how aircraft may be assisted in surface navigation on airports when unaided visibility is inadequate. Some proposals have included either manual or automatic steering with reference to taxiway centerline guidance devices, usually cables buried just beneath taxiway surfaces. Steering guidance during takeoffs has also been considered. (The incursion issue is more serious than just getting lost; avoidance of conflicts between aircraft and other aircraft or surface vehicles is another vexing facet of the problem.) Most such proposals have assumed that pilot vision will also be aided by devices that can produce enhanced or synthetic views of their immediate surround (see below), though some simulator experiments have been conducted using airport maps and enhanced GPS navigation aids.

Advanced navigation systems

Satellite-based position determination systems are rapidly reaching a level of maturity that can permit them to serve as the primary basis for aircraft navigation. One can dispute whether these systems should be considered as control or information automation; in fact, they can serve either purpose depending on the way in which a pilot chooses to couple them to onboard control automation. Such systems are in wide use, though they are not yet approved as a sole or primary means of navigation because adequate monitoring systems (for satellite signal integrity) are not yet available.

As described by Paulson (1994), two satellite navigation systems are now in place. The U.S. Department of Defense Global Positioning System (GPS) is now essentially complete, with 28 Navstar satellites in 55° orbits. The system transmits two codes, a coarse acquisition (C/A) code and an encrypted precision (P) code which thus far has not been made available for other than military use.

The Russian Glonass orbital plan will encompass 24 satellites in 65° orbits; 15 satellites were functional in early 1994 and more have been launched since. The Glonass system, like GPS, is under the control of military authorities, and this fact has caused considerable apprehension among civil operators who are concerned about reliability and guaranteed access. ICAO's Future Air Navigation Committee (FANS) has espoused a Global Navigation Satellite System (GNSS) for civil aviation worldwide, augmented either by signals from geostationary satellites or by transmitting position corrections from precisely located ground transmitters (differential GNSS) to provide the accuracy required for all-weather approaches and landings.

Both the United States and Russia have declared their system's availability for civil use. The Inmarsat organization, recognizing the need for a "health warning system" for satellite signals, agreed to include navigation transponders on its four third-generation geostationary communications satellites; signals from these transponders would provide both wide-area differential capability and an integrity monitoring service, broadcasting warnings to aircraft and ATC in the event of a satellite failure or malfunction. These satellites (or another means of accomplishing this function) will be deployed in 1995-96.

From a technical viewpoint, either or both systems could be made available for precise enroute navigation. Northwest Airlines has conducted long-range navigation tests over China using receivers that utilized both. GPS antennas and decoders are widely available at reasonable cost and several newer aircraft have made provisions for GPS navigation in their flight management systems. ICAO final standards are not yet in place, but FAA has given its permission for use of GPS provided it is not the sole means of navigation, and Europe's Joint Airworthiness Authority has certified the A330 and A340 avionics suites for satellite navigation.

The use of GPS, augmented by inertial data, for precision approaches is under test at this time. Though it is not yet clear whether such a system, enhanced either by differential signals or by other means, can routinely meet the standards for category II or III approaches, there is general agreement that it can provide at least category I accuracy (see fig. 3-8). Whether ILS will be retained for lower-visibility approaches is uncertain. The FAA spent many years developing microwave landing systems (MLS), though it has recently cancelled its MLS production contracts; ICAO has adopted the U.S. MLS standard, and Europe is committed to MLS as its future landing system. The wide availability of the GPS technology, however, has led to much uncertainty about the landing systems of the future. Economic variables will be important; MLS is an expensive system, but some means of conducting category III approaches will be an absolute necessity.

Issues raised by advanced navigation systems

As far as pilots are concerned, the source of their guidance signals is of less importance than the accuracy and reliability of those signals. They will continue to require a way of monitoring signal integrity, but they will accept whatever guidance brings them dependably to a position from which a landing can be assured. It is believed that GPS, like MLS, can be used for more complex approaches than the long straight-in approach paths required with ILS. The FAA has experimented with very complex curved-path approaches for use in noise-sensitive and confined areas (Scott et al., 1987), but it is not clear whether such approaches will be widely used except in very difficult locations such as the New York (LaGuardia/Kennedy/Newark) area.

I mentioned earlier that while pilots of advanced aircraft are able to evaluate the sources of the information on their map displays, it is not obvious what raw data are being used to synthesize the integrated information. When GPS alone is used, it is impossible for the pilot to determine either the source or the accuracy of the data because of the complexity of the calculations used to derive instantaneous position from 4-6 satellites. About all the pilot can do is to compare the satellite-derived position with the inertial position, once VOR-DME data become unavailable. It must also be said, however, that GPS will free pilots from the constraints of surface navigation aids, which are not always reliable. If both GPS and Glonass are integrated into the future navigation system, the positions derived from each independent satellite system can serve as a new source of redundancy; each will have about equal precision. If the ability to compare them is made available, this redundancy will be available almost anywhere over the earth's surface.

Information automation in the future

This is an aspect of automation in which many innovations will be offered in the near future. Some are already in test; others await technology advances such as large flat panel displays. All will be able to make still more information available in the cockpit at a time when there may already be more than many pilots can attend to in the time available. But the new technology, if properly implemented, can simplify rather than complicate the pilot's task. I will review some of the new functionality that has been proposed and then examine the likely effects on flight crews.

Digital data link

Digital data link, combined with satellite communication, has been under evaluation in civil aviation for several years. At present, ACARS transceivers are used; in the future, mode S transponders may become the preferred medium for exchange of ATC data. At this time, the usefulness of automatic dependent surveillance (ADS) on overwater routes seems assured. Several carriers have participated in tests over the Pacific ocean. Russian authorities are also considering ADS for primary use over large portions of its land mass, where radar air traffic surveillance is not available.

ADS involves the frequent reporting, without crew intervention, of position, altitude, and often wind speed and direction. In recent tests, reports have been issued every five minutes. These data are received by ARINC or a similar communication service and retransmitted to air traffic control facilities, where they are automatically plotted and can be used by controllers to survey traffic under their control. At present, voice communication with aircraft in oceanic airspace still depends on largely HF radio equipment, but all parties hope that satellite communications, already available for passenger telephonic communications on a few air carriers, will soon become available for the pilots of those aircraft as well. As one pilot remarked, "I hate to be using a lousy HF channel when the passenger behind me is talking to his wife on the phone!".

Data link provides the capability for high-bandwidth data communication; the issues relate not to the technology but to its uses. The FAA is working on standards for integrated data and voice communications services for the future, the Aeronautical Telecommunications Network, which will tie the entire aviation communications system together. A host of issues concerning communications architecture, protocols, vocabularies, standards, policies and procedures remains to be enunciated, however, and equipment manufacturers cannot provide equipment without these details. This is a major reason why ATC data link is not yet implemented in the 777 and other new aircraft, and why aviation communications technology is still a patchwork.

Data link may eventually enable nearly all routine communication between ATC and aircraft to be carried out without recourse to voice contact, leaving voice for urgent messages and non-routine transactions between pilot and controller. Weather enroute and terminal airport information are among the types of data that will be sent in this way. Through ACARS, two-way data link is already used for much company communication, and the ACARS system has been used experimentally for pre-flight clearance delivery (Air Canada, American, Delta) and other non-time critical data transfers. Many new aircraft have printers in the cockpit, so that ATC messages can be saved as hard copy when desired. It is likely that such devices will be needed to spare crews the need to page forward and backward through many stored messages when a particular datum is needed, and give them the ability to refer to such information quickly. The flexibility of the display systems should permit pilots with differing cognitive styles to adapt information-handling to their own preferences.

Thus far, I have not discussed new functions that may be enabled by data link. I will discuss error tolerance and error resistance below, but it should be said here that the high-bandwidth capability of digital data link permits it, at least in theory, to be used to downlink a considerable amount of aircraft data not now made available to ground facilities. This offers the potential for error-checking by ATC computers of clearances that have been uplinked, accepted and executed by pilots, as well as the exchange of more aircraft data with the ground, as was done in the UK CAA trials in 1991 (see page 111).

Among the functions that are routinely performed by ACARS data link are the transmission of "out-off-on-in" data (times of departure from gate, takeoff, landing, and gate arrival), diversion or delay information, engine performance data, arrival gate data and airplane malfunction information to assist ground maintenance personnel in planning for repairs or parts replacement without causing delays. Passenger needs upon arrival are also communicated. Other data could also be transmitted, including performance data and non-routine events, though the transmission in real time of such data is of concern to pilots. Transmission of sensitive data over broadcast channels also brings up questions of data security, especially if the data concerns identifiable flights or persons.

Issues raised by data link

The lack of standard procedures for pre-departure clearance delivery has posed some problems; ASRS reports indicate that aircraft have occasionally taken off without flight clearances when hard copies of the initial clearances have not been delivered to the cockpit before push-back, and different procedures at different locations have caused some problems as well. Nonetheless, these are growing pains, and the potential benefits of this technology are very considerable once the "bugs" are worked out.

The routine use of data link for controller-pilot communications will change in fundamental ways the interaction processes between these two classes of human operators. Where they now work together in direct person-to-person conversational contact, these contacts will be by alphanumeric messages that must pass through two computers. Further, unlike voice messages today, which are primarily broadcast on a "party line", data link messages to aircraft will be selectively addressed; others in the air will not have access to them. The implementation schemes for data link all envision the availability of a voice communications channel for urgent messages, but the potential for decreased *team* (pilot-controller) involvement in problem-solving is worrisome.

Electronic library systems

An electronic library system (ELS) was planned for the 777, but most airplane customers did not feel it to be financially viable at this time. At least one airline and an avionics manufacturer have actively explored this concept, however. With today's computer technology, it would be possible to store virtually all of the information required by pilots (and now carried in their capacious flight bags) on CD ROM disks or other electronic medium, and to make it "instantly" available on a dedicated screen in the cockpit. Approach plates and enroute navigation charts as well as the flight and airplane operating manuals could be encoded in such a database.

I use quotes around "instantly" because instantly *available* and instantly *accessible* are not quite synonymous. Admittedly, pilots must now thumb through hard-copy manuals to find a desired bit of information. (Quick-reference handbooks assist in emergency and anomaly checklist retrieval.) With an electronic library system, they would have to navigate through numerous menus to find the same bit of information. With the electronic system, however, they would also have to learn the data architecture, preserve it in memory, associate the structure with the abbreviated identifiers on the screen, learn economical ways of accessing what they needed, and then perform the on-screen manipulation necessary to bring the desired data to hand.

Issues raised by electronic library systems

If pilots find it necessary to print material stored in an ELS (such as an approach chart) in order to scrutinize it more carefully or to move it to where they want it, little purpose will have been served by the provision of yet more expensive technology in the cockpit. Most of the material in the flight bag is alphanumeric, and simply transferring it to an electronic medium seems a clumsy way to use this technology. Since the ELS will be a single system, it is unlikely that certification authorities will permit it to be interconnected with flight-critical systems such as the FMS, and without such connectivity, more of its potential usefulness will be compromised. With connectivity, the automation becomes yet more complex and susceptible to unwanted surprises.

A capable expert system might be helpful to assist in navigating through ELS information, and some research has been done toward that end. Lacking such a system, one must consider whether a "paperless" cockpit represents a substantial improvement on what we now have. Things have improved since Ruffell Smith (1979) pointed out the 20 m^2 "blizzard of paper" required for a trans-Atlantic flight.

Much of the flight path navigational data that pilots need is now available in the large FMS database; few pilots using FMS find it necessary to refer more than occasionally to their navigation charts though all pilots still use approach plates, even for familiar airports, as memory aids. Charts are another area in which the printed page is a substantial improvement over electronic data. The best resolution available on monochrome CRTs (about 300 dpi) is substantially less than can be achieved on printed charts (1000 dpi); simple reproduction of such charts would not provide adequate spatial resolution of the data now provided, and navigation and approach charts would have to be reconstructed for effective electronic presentation.

Nevertheless, it is likely that at some time in the future, electronic libraries will become available in transport aircraft, especially if the computer equipment used to enable them is also found to have a commercially profitable purpose such as providing services for which passengers will pay.

Enhanced vision systems for pilots

Though air transportation is now highly reliable, visibility restrictions due to fog can still shut down airports completely for an indefinite period. If this occurs at a major airport such as Chicago's O'Hare, air traffic over a large part of the United States will be affected within a few hours. Though category 3 autoland can enable safe landings at suitably equipped airports in very bad visibility, taxiing may be impossible. To provide independent monitoring capability in the cockpit during such operations, the government, avionics firms and some air carriers have studied how pilot vision might be improved by sensors operating in portions of the electromagnetic (EM) spectrum less attenuated by these weather phenomena than the visible spectrum.

Two portions of the EM spectrum have been explored in depth. One is the infrared (IR) band, portions of which are relatively transparent to moisture in the air. The other is in the millimeter-wave (MMW) band of the microwave spectrum. In all cases, the studies have aimed at providing pilots with a synthetic visual image, either projected on a head-up display or on a head-down screen on the instrument panel, that would assure them of the location and orientation of a runway with respect to their airplane. Other studies have been carried out to determine whether images derived from more than one portion of the EM spectrum could be fused to provide such imagery (see Cooper, 1994b).

A computer technology that has been proposed for aviation applications is the architecture known as "neural networks". These networks of artificial neurons operate in analog fashion on inputs, usually in the form of perceptual fields, to yield an output in the form of a recognized object. Object recognition (particularly alphanumeric character recognition) has received a great deal of attention over two decades. A unique characteristic of such networks is that they have a limited capacity to "learn" and adapt their behavior over successive presentations of variations on a particular stimulus.

Neural nets have been proposed as an integrating element for multi-spectral imaging of objects in the environment. Coupled with an appropriate display medium, such networks might be able to accept and fuse microwave, infrared and visual imagery of a runway into a coherent representation which pilots could use for quasi-visual landings under conditions of limited visibility.

These programs have been variously called "synthetic vision", "enhanced vision" or "image fusion". Such technology could permit pilots to land without assistance from the ground on any appropriate surface anywhere if they were guided to the proximity of that surface by appropriate on-board navigation equipment. Thus one major benefit of such devices could be a decrease in the number, and therefore cost, of ground navigation aids, a major factor in less developed nations.

The technical difficulties lying in the way of such technology are formidable. Infrared images are substantially different from visible images in that they reflect temperature differences among objects in the environment rather than brightness or chromatic differences; while outlines may be clearly detected, they may not be the outlines expected. Also, while IR imagery can detect objects either colder or warmer than their surround, there are times of day when objects are at essentially the same temperature as their surround as they are being either heated by solar radiation or cooled in its absence. Runways or other paved surfaces that are clearly detectable under most conditions may be "invisible" when they have the same temperature as the surrounding earth. If a paved surface is covered by even a light coating of water, snow or ice, its apparent temperature will be that of the overlying contamination. Finally, nearly all infrared radiation is attenuated by airborne moisture, dust or smoke between the sensor and the objects of interest; for this reason, IR sensors may be useful only at fairly short ranges.

Millimeter wave radar relies on EM impulses generated in and propagated from the airplane toward the earth ahead. A fraction of this radiation is reflected from solid objects in the path of the radar beam, and a small fraction of the reflected radiation returns to the transmitting and receiving antenna. Since microwave frequencies are appreciably lower than the visible spectrum, resolution of objects is less than in visible light, though the temperature of such objects is not a factor. Metal objects are highly reflective, paved surfaces less reflective, and earth absorbs most microwave radiation impinging upon it. The reflectance of objects can be enhanced (or degraded) by surface treatment with various coatings, by variations in shape, surface roughness, and orientation. Metal passive corner reflectors can provide very bright returns. Large objects such as a runway can be visualized, though at the shallow angle from which an airplane approaches the runway, little of the transmitted radiation is reflected back to the transceiver antenna. Much smaller objects made of metal, such as surface vehicles, are easily detected: such obstructions on a runway can be detected easily. (Since vehicles have engines which emit heat, IR sensors also can usually detect such objects.)

Biological obstructions (animals, humans) do not reflect microwave radiation well; they will usually be invisible. Since they produce heat, they may be detected, though often not at a useful range, by IR sensors. Other obstructions (piles of dirt on a runway under construction, sawhorses or other markers) may or may not be differentiated from their surroundings. Despite these problems, MMW equipment has been demonstrated in aircraft and has been shown to provide sufficient information to permit an approach to be completed under at least test circumstances. Forward-looking (passive) infrared equipment (FLIR) is in wide use for target detection by the armed forces, often in combination with other sensors such as low-light level TV or synthetic aperture radar.

Finally, it has been proposed that enhanced terrain maps stored in aircraft and correlated with precise geographic position information from GNSS could be used to generate entirely synthetic imagery for pilots landing at airports. This technology could in theory free pilots entirely from environmental constraints to vision (but it would not be able to show runway obstacles unless it were augmented by forward-looking sensors of some type, operating in real time).

Issues raised by enhanced vision systems

The human factors issues associated with the use of this technology are likewise formidable. Since the images are qualitatively different from visual images, questions arise as to whether synthetic imagery should be transformed, and if so how, in order to make it more obvious what the pilot is seeing, or whether pilots should be taught the differences and required to use the processed imagery to decrease the likelihood that they will form a false or misleading impression of what the sensor "sees". Though much research has been done over many years (e.g., Kraft & Elworth, 1969; Stout & Stephens, 1975; Roscoe, 1979) to elucidate what visual cues pilots require for landing in impoverished visual environments, none of it has been able to specify an exact minimum set of required cues, and given the number of human variables, there may not be such a set.

If synthetic or enhanced imagery is projected on a wide-angle head-up display in the cockpit, questions arise as to whether pilots will be able to attend both to the display and to the external environment behind it. Most synthetic runway representations on head-up displays have been outline forms to make it less difficult for pilots to transition to outside visual cues during the landing maneuver,. The problem may be that the head-up display symbology which is used during the approach is more salient than the external scene, especially when viewed through fog by an inexperienced pilot (Lauber et al., 1982). It may be necessary to "declutter" the display during the final phases of the approach to avoid this problem, though this runs the risk of removing symbology that may be essential if the pilot has to execute a missed approach very near the runway.

Another problem is the relatively slow scan rate of radar. It is not possible to update radar imagery rapidly enough (roughly 30 Hz) so that a continuously changing picture is provided. Passive IR does not suffer from this handicap, though processing requires time if the images are transformed. Most jet aircraft are traveling over 200 ft/sec when they enter the landing flare; the environment is changing very rapidly and rapid updating of visual cues is necessary. We do not know exactly what image update rate is required for fully effective inner-loop control, though studies of this are underway.

Several air carriers have installed head-up displays to provide category II and III landing capability without the expense of triplex autopilots and other equipment. Many operate routinely in areas where the likelihood of fog and other restrictions to visibility is high, such as Alaska. Present head-up display equipment, however, interposes a device between the pilot and the windscreen, usually a large block of partially reflective plastic onto one of whose surfaces a flight guidance display is projected. These devices invariably attenuate the transmitted image of the outside environment by some amount; they also represent a hazard to the pilot's head in the event of a sudden deceleration of the airplane.

From a perceptual and cognitive viewpoint, the dangers of such devices are that pilots will be misled by what they think they see, or that they will not see correctly (through a head-up device) what they need to see to complete a safe landing. Some have proposed that synthetic or enhanced imagery should be provided on the instrument panel to obviate the latter problem, but this approach poses a new problem: the time required to transition from head-down to head-up visual orientation, a process that requires at least a few seconds and may take longer if external cues are minimal.

This has been handled in the past by a procedure called the monitored approach (Lauber et al., 1976), in which the pilot flying the approach remains oriented to the instruments (head-down) until reaching decision height, then executes a missed approach unless the other pilot, who is monitoring the external environment, announces that visual cues are sufficient to permit a landing to be made. In this case, the monitoring pilot, who is already oriented to the external view, takes over control and completes the landing. This procedure, pioneered by Aeropostale in France and adopted by British European Airways after the war, was highly successful, and variants are now used by many carriers.

The decision to land is one of relatively few in aviation which must be made very quickly (within very few seconds) under poor visibility conditions. It should also be kept in mind that if GNSS and enhanced vision technology are used to permit landings at airports without surface precision navigation aids (and this is an avowed objective), pilots will not have the assurance of their location which is provided by identifying such aids and "following" them to the airport. They may be more hesitant to make the decision to land under such circumstances, and this could negate some of the potential benefits of the technology. At such airports, pilots must be provided with unequivocal information as to their precise location and the suitability of the runway ahead before they can commit to landing, and throughout the landing process, including rollout and taxi.

Advanced integrated displays

Recognizing the extreme perceptual and cognitive demands placed upon military pilots during combat operations, the armed forces for many years have been investigating large flat-panel display technology in the hope of being able to provide pilots with highly integrated intuitive situation displays. These "big picture" displays, coupled with adaptive automation, would provide pictorial and analogical representations of terrain, threats, targets, predetermined course, and aircraft and weapons status. The technology is not yet available to provide displays of the size desired, let alone displays sufficiently robust to endure the combat environment, but in laboratory simulations, the representations appear to integrate much of the information required by pilots under such circumstances.

The U.S. Army has taken another approach in its Crew-Systems Research and Development Facility at its Aeroflight Dynamics Laboratory at Ames Research Center. This facility is a full-mission virtual helicopter simulator whose visual system presents a binocular helmet-mounted virtual environment display using synthetic but now quite realistic scene generation. This is another approach which can provide both terrain and target imagery, augmented by synthetic representation of relevant threats.

"Big picture" displays have been proposed for use in civil aircraft as well, though the costs have been perceived thus far to outweigh possible benefits. This situation may change, however, if a new high-speed (supersonic) transport reaches the development stage. NASA, in the United States, and government-backed consortia in Japan and Europe, are conducting generic high-speed research intended to enable such a development program by the end of this decade. One desired feature of such a transport is the ability to provide pilots with sufficient forward visibility without the considerable structural weight penalty associated with a movable visor and nose assembly which covers the windscreens during high-speed flight. Such a visor apparatus is used on the Concorde to permit a view over the nose of the aircraft during takeoff and approach when pitch angle is high compared with that of conventional aircraft.

A supersonic transport without a visor assembly would have cockpit side windows but none oriented directly forward, for aerodynamic reasons. Some sort of forward visual display would be necessary both for maneuvering at low altitude and for taxiing. It would probably be driven by a combination of television and other sensors, though some have proposed an entirely synthetic ("virtual") computer-generated display for this purpose.

An additional problem for ground maneuvering in a supersonic transport would be the position of the pilots, far forward of the steerable nose gear as well as the main landing gear position much further aft. Even if they had forward vision, additional views, perhaps from the nose gear position, might be necessary to enable them to remain within the confines of narrow taxiways and to negotiate turns with variable radii on airports. These technologies would qualitatively change the ways in which pilots maintain contact with their external environment. They pose both perceptual and cognitive questions related to reliability, trust, automation complexity and transparency (literally!) which will require much further research, not only on the technologies themselves but on the human's ability to remain in command in the range of situations in which he or she would be dependent upon them.

Issues related to information management

It is important to keep in mind the need for independent sources of data in a real-time, highly dynamic system. Though a pilot may have access to several apparently different types of information concerning a single topic in a highly automated airplane, he or she must always consider whether the redundant information was collected by independent systems, or whether it is merely two ways of representing data from the same source. If the former, it can be used for cross-checking; if the latter, a single sensor could corrupt both representations. In tightly-coupled systems, the difference may not always be obvious. To what extent does the pilot need to know the sources of the processed information that reaches him?

We have reached a point at which multiple sources of similar data are usually available to pilots and avionics with which to accomplish their functions. As noted immediately above, in the near future pilots may have access to representations of the airplane environment derived from the visual, infra-red and microwave portions of the electromagnetic spectrum.

In the enhanced or synthetic vision case, the answer is fairly obvious: these three electromagnetic bands, visual, IR and MMW do not provide the same data. Unless a way can be found to synthesize congruent imagery from each source, or to fuse disparate imagery into a consistent representation, it will be important that the pilot understand what data source is being used, and the limitations of the data. The training burden imposed by such technology will not be trivial unless these questions are either answered by image fusion and synthesis techniques, or unless pilots are given the opportunity through simulation and flight experience to become thoroughly familiar with what can be trusted and what cannot be under specific circumstances.

Another case in which disparate data sources are used is data from surface navigation aids and inertial sensors within the aircraft. In the past, the data derived from various sources has been presented in a common manner, or the data has been reconciled within the flight management computer prior to its presentation on the navigation display. Pilots can gain access to the sources of this data on their navigation displays (see figure 4-5 for an example).

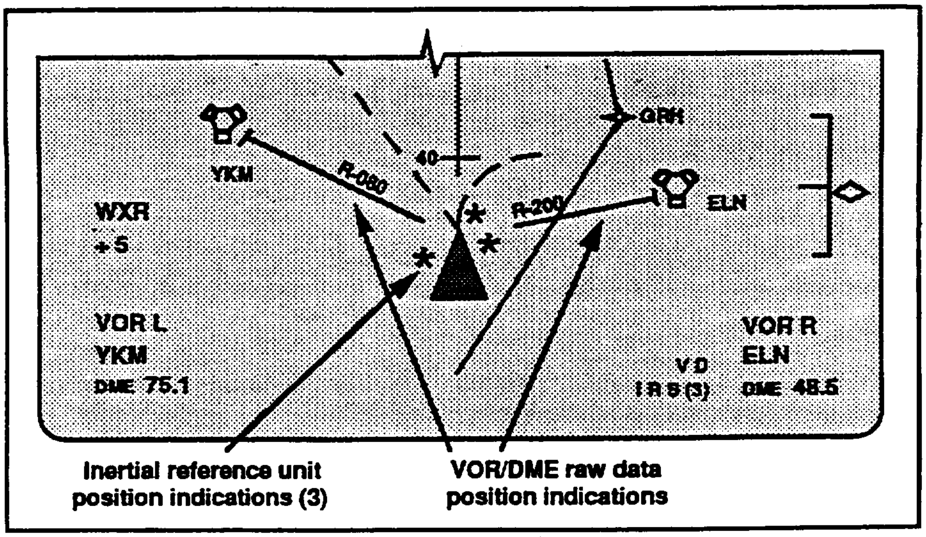

Fig. 4-5: Visualization of raw and processed navigation data on Navigation Display (Boeing 747-400)

Management automation in the future

Kelly et al. (1992, p. 2) indicated that "some improvements to flight management systems have been difficult to justify because they did not appear to provide new capabilities which would result in return on investment." It is probably fair to say that many pilots now flying FMS-equipped aircraft would welcome a simpler, more intuitive system with which they could interact more easily than is possible with today's CDUs. It is also likely that most designers and human factors specialists, given the knowledge of hindsight, would welcome the opportunity to redesign this interface, and that members of the avionics community have the knowledge necessary to do it better.

The fact remains, however, that today's flight management systems work. A very considerable investment in training has already been made, and the vast majority of pilots have found it possible to adapt successfully to present FMS idiosyncrasies. Many steps have been taken in newer systems to simplify reprogramming with the intent of reducing the inherent clumsiness of the system, to speed FMC response times (which were very slow in early devices), and to improve the legibility of the CDU screen. Any future attempt to revise the FMS interface radically will require extensive retraining of operators at considerable expense. Unless carefully done, a redesign may impose training transfer problems for pilots moving from the older to the new devices. These factors, leaving aside the return on investment issue, make it likely that flight management systems and their interfaces will continue to look and operate much as they now do for a considerable time to come.

Having said this, however, are no improvements possible without starting over with a clean sheet of paper? The answer to this question, if there is one, lies in looking carefully at problems known to be associated with FMS use in line service. Several investigators, prominent among them Sarter and Woods, have conducted such inquiries. Their data, gathered in flight observation and simulation experiments, indicate two principal sources of FMS interaction problems. The first class of problems involves mode errors or lack of mode awareness. As Sarter has pointed out (Sarter & Woods, 1994), today's flight management systems are "mode-rich" and it is often difficult for pilots to keep track of them (see figure 7-1). The second problem, which is related to the first, involves lack of understanding by pilots of the system's internal architecture and logic, and therefore a lack of understanding of what the machine is doing, and why, and of what it is going to do next.

Simply saying that improvement of the flight management system is not economically justifiable rationalizes away the many lessons learned from operational experience with these systems. If "the box" itself cannot be redesigned, it is possible and likely that redesign of some of the displays associated with it (the CDU format, the map display and particularly the mode annunciation panel) might accomplish some of the same purposes. There is, for instance, no true vertical navigation display at present, yet it is during climb and descent phases of operation that a majority of the problems in the interaction between operators and the automation arises. Reworking of mode annunciation panels to make mode data, and particularly mode changes, more salient could improve pilot understanding of what the automation is doing (Hutchins, cited in AWST, 1995b).

While modifying procedures is a poor substitute for fixing the basic problems that motivated the modifications, there are at least three possible approaches to these problems in addition to the display improvements mentioned immediately above, each of which has both advantages and drawbacks. Each, however, seems worthy of consideration by designers and operators.

- Without modifying the hardware, *system software revisions* could be made to simplify complex FMS functions with the intent of making them more understandable and/or transparent to operators (see previous paragraph).
- *Procedures* for the use of the FMS could be modified to simplify the use of the systems. Such modifications would involve the use of only a subset of FMS functions. Excluded functions could either be disabled or simply not used.
- *Pilot training* should be examined and revised with the intent of providing the operators with a better understanding of system logic and behavior under the range of conditions likely to be encountered in line operations.

Each of these alternatives will be examined briefly here.

- ***System software revisions* could be made to simplify complex FMS functions with the intent of making them more understandable and/or transparent to operators.**

In newer aircraft, Flight Management Systems are flight-essential equipment. This means that any changes in the systems or in how they function are subject to rigorous configuration management and certification criteria. Software changes, however small, are extremely expensive. Further, given the tight coupling among software modules, changes in one module may have cascading effects on other software elements. Any proposal for software modifications is subject to even greater cost constraints than are hardware modifications. Further, "cosmetic" software changes are unlikely to have appreciable effects on system complexity, the real issue underlying present problems with the FMS. A wholesale redesign of the system would probably be required to simplify it in a useful way.

Despite these negative comments, however, research should be undertaken to learn which of a large number of approaches to FMS architecture would convey the greatest benefits in terms of real system simplicity and transparency. I am unwilling to accept the thesis that advanced flight planning, management and guidance systems cannot be made easier for human operators to understand and to operate. Several research groups are now working on various aspects of this problem, though none, to my knowledge, has looked at the overarching question of FMS architecture and functionality.

- ***Procedural modifications* for the use of the FMS could simplify the use of the systems. Such modifications would involve the use of only a subset of FMS functions. Excluded functions could either be disabled or simply not used.**

Procedures have always been used to make up for deficiencies in equipment and technology, but it is also true that uses of technology are often sub-optimal because proper procedures for its utilization have not been developed and applied. We have FMS technology in being; it is unlikely to be fundamentally modified, and we know that human operators are having some difficulties in using it effectively. Here, I am not suggesting ways to get around specific problems; rather, I suggest that a systematic look should be taken at those FMS functions that are widely used, necessary for safe and effective mission accomplishment, and least likely to be misunderstood or misused. Functions that do not meet these criteria should be considered for abandonment. Is it really necessary to have four distinct descent modes, or would two suffice?

Is it really necessary that pilots be able to demonstrate their ability to use all FMS functions to be type-rated on a given piece of equipment, or is it necessary only that they be able to use a limited subset of the available modes to accomplish their mission under all foreseeable circumstances? Any reduction in FMS complexity would pay dividends during training, would decrease the cognitive burden imposed on pilots by the equipment, and would simplify flight procedures. Automation complexity is the fundamental problem in this domain; reducing that complexity offers the greatest hope of a successful resolution of that problem, even if system redesign is not possible.

Simplifying procedures for the use of the FMS would also permit us to avoid those corners of the FMS functional envelope that have posed the most serious problems in the past. The "open descent" issue in current Airbus airplanes is one example; climbs using vertical rate rather than speed modes is another. A third is operations that may cause pilots inadvertently to disable an airplane's "altitude capture" function. A fourth is restrictions on flight paths necessary to permit glide slope and localizer capture during approaches. The recent A300 accident at Nagoya (1994) suggests that mode interactions which permit simultaneous manual and automated control should be avoided. (This is not a new problem; it has been a source of incidents and accidents in general aviation for many years.) United Airlines is focusing its FMS training on "preferred modes" of operation of the FMS to simplify the pilot's tasks in managing the airplane.

These are only examples designed to provoke thinking about whether we can make the use of this very complex tool simpler by avoiding some of its less important capabilities. Pilots could point to several other possibilities, perhaps more important than some mentioned here, if they were asked to. Though a number of pilot opinion surveys has been conducted, to my knowledge none of them has asked, "What functions do you never use, and why?"

- ***Pilot training* should be examined and revised with the intent of providing operators with a better understanding of system logic and behavior under the full range of conditions likely to be encountered in line operations.**

To paraphrase Sarter and Woods (1994), "What is needed is better understanding of how the machine operates, not just of how to operate the machine." A more homely expression of this is, "If you can't see what you need to know, then you've got to *know* what you need to know" (to which Demosthenes (personal communication, 1994) added, "and if you don't know, you've got to be told!"). Given the flexibility and complexity of the current FMS, some of the mistakes pilots make in its operation suggest that they simply do not understand how it operates, and why it does things that way. There are good reasons in most cases, and they are known to the designers of the equipment (although the designers may not always have taken full account of the needs of the line pilot). Some are imposed by certification requirements, others by the system architecture and still others by the range of FMS interactions with the airplane and with other automation. But the problem of inadequate user understanding persists.

Explanations of these interacting requirements during training would be costly in terms of training time, without question. They would certainly be less expensive, however, than the loss of an aircraft and its passengers because of the lack of such knowledge. Accidents to date and growing experimental evidence (Sarter, 1994) do indicate inadequate understanding of FMS behavior and operating constraints, and pilots responding to surveys indicate that they have not been satisfied with the thoroughness of their computer-based training or with their ability to get answers to questions when they have asked them (Uchtdorf & Heldt, 1989).

An adequate internal model of an automated system is vital to a pilot's ability to predict how that system will function under novel circumstances. I believe that research in progress will point toward a better understanding of what pilots require to build correct and adequate models of the systems they operate. Hopefully, air carriers can find ways to assist them in forming such models during their training.

Management of human error

The alternatives presented above are not mutually exclusive. Experience with advanced automated systems indicates the need for simplicity, transparency and comprehensibility in the systems we use, as well as predictability in the behavior of those systems. Even though today's flight management systems fall short of human-centered principles in certain respects, it will be difficult, in today's economic climate, to generate much interest in radical re-work of any systems that are functional, let alone systems as capable as our present FMSs. Yet we must find ways to improve the error resistance and error tolerance of both our current systems and those of the future. I end this chapter with a short discussion of these all-important concepts.

The aviation system has been plagued by the problem of "human error" since it began. One of many reasons for this has been that our investigations of accidents has tended to focus rather narrowly on the specifics of individual cases, wherein a specific set of often unlikely circumstances, including erroneous actions by humans, has led to an undesired outcome. Points of commonality among accidents have been discerned and often corrected, but on the whole, our remedial measures have been specific and narrowly focused on the "sharp end" of the system.

In recent years, several investigators have looked farther in an attempt to discover more generic factors involved in accidents, among them Perrow (1984), Reason (1990), Lauber (1993), and Woods et al. (1994). Reason's "latent failure" model has been influential; in over-simplified form, it suggests that a variety of latent factors, or "pathogens", are present in most organizations and endeavors. Under certain usually uncommon circumstances, they may affect the course of an operation or production process in such a way that an untoward outcome ensues: an accident. Woods et al. have carried this construct further and have explored the variety of circumstances that can potentiate the effects on the operators at the "sharp end" of such enterprises. Lauber has stimulated systematic searches for such factors in the background of transportation accidents and has argued for their inclusion as probable or contributory cause factors in NTSB accident investigation reports.

The Dryden, Ontario (1989) accident briefly summarized in the Appendix is a classic example of such factors (Moshansky, 1992), but they have been major contributors to many mishaps. A full discussion is beyond the scope of this document, but it must be accepted that without full information concerning the context and environment(s) in which accidents occur, it is not possible to understand their genesis and how to take rational steps to prevent future accidents. Accidents are not only human failures; they are also failures of design, operation, management and often oversight. In short, they are *system* failures. They must be looked at as such if they are to be fully understood.

Error resistance

Ideally, aircraft automation should prevent the occurrence of all errors, both its own and those of its human operators. This is unrealistic, but it is necessary to design systems to be *relatively* error-resistant, both with respect to their own errors and those of the operator. *Resistance* is "an opposing or retarding force", a definition that recognizes the relative nature of the phenomenon. Resistance to error in automation itself involves internal testing to determine that the system is operating within its design and software guidelines. Resistance to human error is more subtle; it may involve comparison of human actions with a template of permitted actions ("reasonability" checks), a software proscription against certain forbidden actions under specified conditions (envelope limitation or protection is an example), or simply clear, intuitive displays and simple, uncomplicated procedures to minimize the likelihood of inadvertent human errors.

Automation of unavoidably complex procedures (such as fuel sequencing and transfer among a large number of widely-separated tanks to maintain an optimal center of gravity) is necessary and entirely appropriate provided the human is "kept in the loop" so he or she understands what is going on. The system must be able to be operated by the human if the automation fails; it must fail "safe" (in this case, it must be designed so a failure will not leave the airplane outside its operating limits) and it must provide unambiguous indication that it is (or is not) functioning properly. Guidance in performing complex tasks (and fuel balancing in some aircraft may be such a task) is helpful, whether it is in a quick reference handbook or in the form of an electronic checklist. Prompting has not been used as effectively as it could be in aircraft human-system interfaces, though the newest electronic checklists attempt to assist in this task.

Questioning of critical procedures or instructions to the automation (those that irreversibly alter aircraft capabilities), or requiring that critical orders be confirmed by pilots before they are executed, can be additional safeguards against errors. These queries can also be automated, either by themselves or as part of a procedures monitoring module which compares human actions with a model of predicted actions under various circumstances. Such models have been developed in research settings (Palmer, Mitchell & Govindaraj, 1990); some are now in use.

The human operator is known to commit apparently random, unpredictable errors with some frequency (Wiener, 1987; Norman, 1988); it is extremely unlikely that designers will ever be able to devise automation that will trap all of them. This being the case, it is essential to provide alternate means by which pilots can detect the fact that a human or an automation error has occurred. Such warnings must be provided in enough time to permit pilots to isolate the error, and a means must be provided by which to correct the error once it is detected. Where this is not possible, the consequences of an action should be queried before the action itself is allowed to proceed.

It must be noted here that automation also makes apparently random, unpredictable errors, and it is equally unlikely that designers will be able to devise the means to trap all of them. The human operator is the last (and best) line of defense against these failure, but that operator must be given the means to deal with such failures. Figure 4-6 shows some of these apparently random failures.

"As the nosewheel was about to touch down, the rudder moved, uncommanded, 16-17 degrees to the right. The airplane left the runway at about 130 knots..."

"As the aircraft banked, it encountered a wind shear...this buffeting triggered its automatic flap locking mechanism...the flaps locked at a full setting...the pilot aborted the landing. On the fourth try, he landed on runway 31...two passengers were slightly injured after the aircraft ran off the runway..."

"A V2500 engine 'shut itself down' during a descent...because of a fault in the automatic fuel flow logic which is being urgently investigated..."

"About half a mile from the runway threshold, the stick pusher activated while the airplane was slowing through 130 knots...the pilots estimated the pull required to overcome the forward yoke pressure at more than 250 pounds..."

"At the time, the airplane was operating at 31,000 ft, at night, with the autopilot engaged. The crew did not notice the initiation of the roll and first noted a problem when the INS warning lights illuminated. They then noted...a roll to the right with a bank angle in excess of 90 degrees."

"After touching down...the pilots selected spoilers and reverse thrust, but there was a delay of 9 seconds before they deployed..."

Fig. 4-6: Automation failures during aircraft operations.

Error tolerance

Since error resistance is relative rather than absolute, there needs to be a "layered defense" against human errors. Beside building systems to resist errors as much as possible, it is necessary and highly desirable to make systems tolerant of error. *Tolerance* means "the act of allowing something"; in this case, it covers the entire panoply of means that can be used to insure that when an error is committed, it is not allowed to jeopardize safety.

Nagel (1988) has pointed out that "it is explicitly accepted that errors will occur; automation is used to monitor the human crew and to detect errors as they are made." The aviation system is already highly tolerant of errors, largely by virtue of monitoring by other crew members and by air traffic control. But certain errors possible with automated equipment become obvious only long after they are committed, such as data entry errors during preflight FMS programming (or even errors in the construction of the FMS database, a factor in the Mt. Erebus DC-10 accident). New monitoring software, displays and devices may be required to trap these more covert errors.

As was suggested above, checks of actions against reasonableness criteria may be appropriate; for an aircraft in the eastern hemisphere, a west longitude waypoint between two east longitude entries is probably not appropriate. An attempted manual depressurization of an aircraft cabin could be an appropriate maneuver to rid the cabin of smoke, but it is more probably an error and should be confirmed before execution. Closing fuel valves on both engines of a twin-engine transport, an action that has occurred at least twice, is almost certainly an error if airborne (San Francisco, 1986; Los Angeles, 1987).

Given that it is impossible either to prevent or to trap all possible human errors, aircraft accident and especially incident data can be extremely useful in pointing out the kinds of errors that occur with some frequency. Formal system hazard analyses are appropriate to elucidate the most serious possible errors, those that could pose an imminent threat to safety. The latter should be guarded against regardless of their reported frequency (Hollnagel, 1993; see also Rouse, 1991).

Error management

An epidemiological model of, and approach to, the problem of human error in aviation was suggested over two decades ago (Barnhart et al., 1975; Cheaney & Billings, 1981). In a recent comprehensive review, Wiener (1993) has discussed intervention strategies for the management of human error. Wiener states that "The aim of intervention is to strengthen the lines of defense at any barrier, or any combination of barriers, and to insert additional lines of defense where possible" (p. 13). He also proposes, however, that "Each proposed method of intervention...should be examined with respect to its feasibility, applicability, costs, and possible shortcomings (e.g., creating a problem elsewhere in the system)". He offers guidelines for the design of error management strategies. This thoughtful study, and the others cited above, deserve careful scrutiny by operators and managers, as well as designers, of complex equipment.

Comment

In this chapter, I have presented a variety of automation innovations that I believe will be seen in, or at least proposed for application in, future aircraft. It is worth remembering again the criteria given by Kelly, Graeber and Fadden (1992): does a new system or function offer a reasonable likelihood of a return on investment? The return may be actual or potential, but it must be demonstrable in advance if the new system is to find its way onto a future airplane. It must be needed, not merely desired, in today's (and very probably tomorrow's) economic and competitive climate.

Nonetheless, while accidents prevented cannot be counted, it is clear that prevention is a great deal less expensive than accident costs. Two 737 accidents in recent years remain entirely unexplained at this time (Colorado Springs, 1992; Pittsburgh, 1994). Both had older digital flight data recorders which did not record control surface positions; that information might very well have led to an unambiguous finding of probable cause. A large part of the older fleet could probably have been equipped with advanced recorders for the cost of these two occurrences, and we would not continue to wonder whether there may be a latent defect waiting to cause another accident. In sharp contrast, the Aerospatiale ATR-72 which crashed after extended flight in icing conditions (Roselawn, IN, 1994), was equipped with a modern digital flight data recorder whose data enabled investigators to discover, literally within days of the accident, that icing had disturbed airflow over the ailerons beyond the pilots' ability to maintain control.

Some of the innovations discussed here are clearly needed if the industry is to continue to expand its horizons; some form of enhanced or synthetic vision is an example. Improved error tolerance is imperative. Capacity must be increased, by whatever means. Global satellite navigation and satellite data and voice communication are certainties. The need for some of the other innovations discussed here is less certain, though the technology for them exists. Many could have been implemented in the Boeing 777 had there been sufficient demand for them–but there was not.

Other innovations not yet thought of will be proposed for aircraft still in the future, though most will be introduced in civil aviation only if they can meet the test proposed by Kelly and his coworkers. Even an entirely new supersonic transport, if one is built, will be subject to the demands of the marketplace, and our manufacturers cannot afford to take chances, especially now. They will build even a radically new airplane with the caution they have displayed throughout history—and that airplane is more likely to be both safe and economically viable because of that caution.

It is the task of the human factors community to make that aircraft and any other new models easier to manage, more error tolerant, and thus safer, than those that have come before, despite the economic factors that militate against change if what we have is "good enough". Accidents, even the few we have, are sufficient evidence that "good enough" isn't—that as long as preventable accidents occur, our job is not finished.

5. Air traffic control and management automation

Introduction

Aircraft automation has a very long history (chapters 3-4). In contrast, air traffic control (ATC) automation is of relatively recent vintage, dating from the 1960s, when the potential advantages of computer management of flight plan data were first recognized by the FAA, which manages essentially all air traffic control in the United States. This discussion is focused on the United States system because it is a single integrated system free of the national boundary and political constraints that have hampered progress in air traffic control elsewhere, and because its operations have been a model for many other nations. This chapter discusses the evolution of air traffic control and management automation. The tasking of our complex ATC system is simple on its face: to provide safe separation among controlled aircraft and to expedite their passage to their destinations. Fulfilling the requirements of that tasking is less simple.

Background

The U.S. National Airspace System (NAS) utilizes computers for a great part of its data management and information transfer, but air traffic control itself is still an almost entirely human operation conducted by highly skilled air traffic controllers whose information is derived from radar data, voice communication with pilots and printed flight data strips. There are many sound reasons for this apparently primitive state of affairs, not the least being the necessity of a careful, evolutionary approach to modifications of the ATC system, a highly integrated complex of equipment ranging from elderly vacuum tube systems to modern digital devices.

Though ATC system automation is primitive compared to the advanced technology in the aircraft which it controls, the system is a truly remarkable, highly functional human-machine system which has accommodated itself to enormous demands upon it. In recent years, the system has been called upon to handle traffic volume well beyond what a few years ago was thought to be its capacity. It has done so because of the creativity and flexibility of its operators and managers, who have revamped the airspace and designed procedures to deal with constantly increasing demand due to increased competitive pressures on air carriers and other segments of the commercial aviation community.

During this same period, the air transport system itself been beset by constant change, totally unlike anything known during its 70-year history. In their former regulated (and stable) environment, air carriers were able to set operating standards at a level well above the minimums required by regulations. The same could be said of air traffic control. Safety and conservatism were the overriding factors in its design and implementation. This state of affairs changed dramatically during the 1980s for a number of reasons, including the air traffic controllers' strike in 1981 and an enormous increase in discretionary travel brought about by airline deregulation and the emergence of unfettered competition.

The aviation system worked well despite these perturbations, but carriers found it necessary to adopt radically different ways of doing business. A major change was the introduction of "hub-and-spoke" flying, in which carriers selected "hub" airports, flew long segments between them, then shunted passengers onto shorter "spoke" flights to get them to their destinations. This produced enormous concentrations of traffic that had formerly been more reasonably spaced, with consequent workload increases for controllers.

The air traffic control system found itself handling considerable increases in traffic with outdated equipment, chronic understaffing and less experienced controllers in many facilities. Since the early 1980s, the FAA has been working on plans for a radical upgrading of the ATC infrastructure involving major increases in automation to improve controller productivity, eliminate airspace bottlenecks and increase traffic throughput. The first of the new equipment was scheduled to be installed in the Seattle Air Route Traffic Control Center (ARTCC) in late 1994, but the implementation schedule has slipped considerably, and the costs have escalated by nearly three billion dollars.

Evolution of the Air Traffic Control System

Airport air traffic control

Air traffic control began at airports during the late 1920s. The first controllers used flags and stood outside; later, control towers were built and controllers used light guns to provide one-way communication with airplanes. Radios began to be used during the middle 1930s, though most smaller aircraft did not carry them until after world war II and light guns continued to be used well into the 1950s.

As all-weather transport flying increased and radar became available after the war, tower visual control of local air traffic was augmented by radar control of traffic in busier terminal areas. Terminal area controllers, attached to towers, were given separate radar facilities which permitted them to provide departing air traffic with a transition to the enroute environment and arrivals from that environment to a final approach to landing. Terminal radar approach control (TRACON) facilities were equipped with broadband radar, later augmented by data processing equipment and automated data communication with enroute Centers. Full performance level controllers functioned both as tower and TRACON controllers.

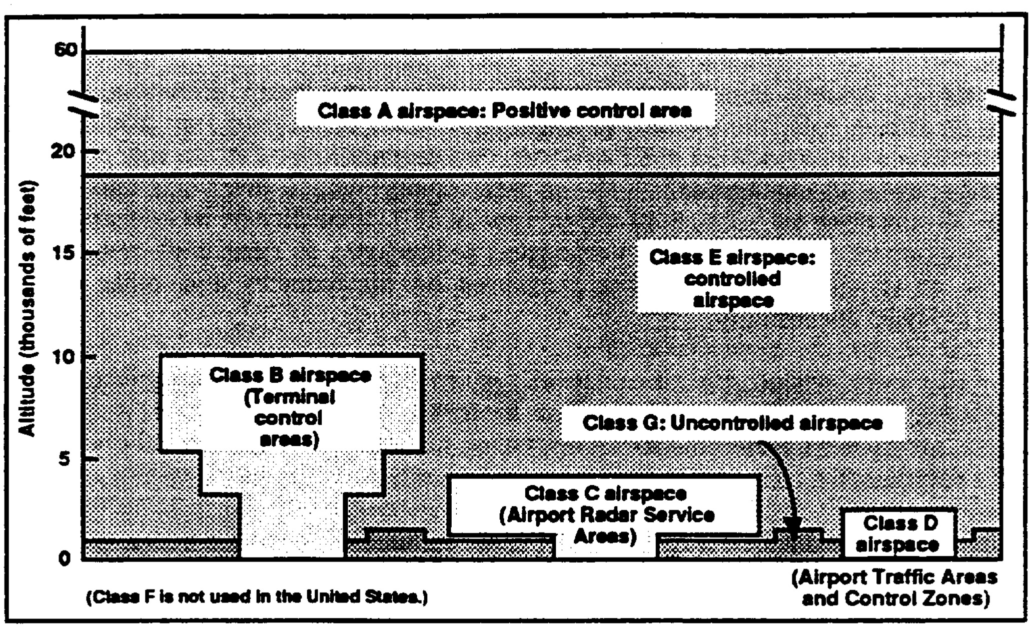

Fig. 5-1: U. S. Airspace Categories (FAA)

Continuing increases in air traffic motivated the FAA to establish new categories of terminal airspace, in part to separate fast jet traffic from slower, smaller (and harder to see) general aviation aircraft. Terminal Control Areas (TCAs) came into being; within these areas, generally shaped like an "inverted wedding cake", all traffic, whether flying under visual (VFR) or instrument (IFR) flight rules, was required to submit to positive control by terminal area controllers. Beacon transponders and radio transceivers were required in order either to land at the primary airport or simply to transit the area. Other airspace reservations with less stringent requirements but also involving increased surveillance and control were put in effect around less busy airports. Figure 5-1 shows the present (1994) categories of civil airspace over the United States. The increasing requirements in these categories of airspace imposed a heavier workload on air traffic controllers. In theory, they lessened surveillance workload for pilots, though high levels of vigilance were still required, particularly at the vertical and horizontal margins of terminal airspace where many light aircraft flying just outside the controlled areas could still be encountered.

Effects of increasing terminal airspace complexity

While these terminal areas unquestionably assisted in air traffic segregation, they imposed an increased procedural and information processing burden on pilots and controllers alike even with carefully-adjusted procedural separation requirements. When it became necessary to relax procedural separation standards and increase the use of visual separation procedures on approaches to accommodate continually increasing air traffic, the vigilance and information processing requirements, especially on pilots, increased further. The total dependence of the system on low bandwidth single-channel voice radio communications for real-time information transfer has increased workload still more. These problems will continue to require better solutions in the foreseeable future. They are made more pressing by the continuing demand upon air traffic control for still further increases in terminal area capacity, which has required innovative, complex procedures to stay ahead of (or even with) demand.

Enroute air traffic control

Enroute air traffic control began to be utilized in 1935 along airways marked by aeronautical beacon lights . Enroute Air Traffic Control Units (ATCU), (the first of which was established by TWA, United, Eastern and American Airlines at Newark because the government had no funds for it), communicated with air carrier dispatchers who forwarded the information by radio to aircraft. Flight plans were made mandatory in 1936; ATCUs were taken over by the CAA in 1937-38. In 1940, the CAA was reorganized to take account of its increasing responsibilities for air traffic control; thereafter, it acquired control over traffic at all municipal airports and established 23 Airway Traffic Control Centers. During world war II, approach control facilities began to be established at some of the busiest airports (see Nolan, 1994, for an excellent brief history of air traffic control).

Prior to the introduction of radar, enroute control facilities visualized traffic using flight progress strips (figure 5-2). All information input was by voice radio; controllers kept a mental three-dimensional picture of traffic under their control and annotated the strips to correspond with reported positions. Low-frequency radio navigation aids marked the various airway segments.

N186MC	3465	OKK	OKK FWA MOTER DTW			
BE20/R	P2040		~~140~~			
979	170		YIP 090			

Fig. 5-2: Flight progress strip, annotated.

In 1956, radar became available and controllers began to be provided with a visual representation of traffic within their sectors of control. Primary radar provided only a display of aircraft locations; altitudes were still reported by voice and procedural control was still required to insure vertical separation. When the radar failed, controllers had to revert quickly to "shrimp boats" (small annotated markers representing aircraft) and full procedural control based on flight strips and their mental picture of traffic, a function that required considerable skill. Communication was improved by the introduction of improved two-way VHF transceivers. Controllers still kept track of their traffic by using flight strips which they annotated as instructions were given to each airplane.

The introduction of interrogation devices, the Air Traffic Control Radar Beacon System (ATCRBS) at radar sites and transponders in aircraft which responded to queries from the interrogators, made possible secondary surveillance radar (SSR) systems (also referred to as "narrow-band" radar, as contrasted with primary or "broad-band" radar). The transponders provided coded identification of specific aircraft, eliminated ambiguity as to location, and improved returns from the responding aircraft. By the early 1960s, most enroute Centers were operating with SSR, to which was added over the next several years altitude reporting in the transponder replies. This information, along with aircraft identification codes, provided controllers with positive three-dimensional location information for aircraft being controlled.

A disadvantage of the beacon system was that primary radar targets were poorly visualized, and not all aircraft operating within the system had transponders. The controller had to provide separation to these aircraft as well if they were operating under instrument flight rules, and this task became much more demanding as enroute system controllers began to depend increasingly on direct representations of traffic. This is still a problem in many areas; although nearly all aircraft now carry transponders, some general aviation aircraft still do not have altitude-encoding ("mode C"), and radar images of these airplanes consequently may be ambiguous as to altitude. (This is also a problem for TCAS, which cannot provide conflict resolution advisories without altitude data.)

Air traffic management

The development of the Federal air traffic control system has often fallen seriously behind traffic demand. Even when Congress has recognized the problem and provided additional funding, usually following a major accident such as the midair collision of a TWA Constellation and a United Airlines DC-7 over the Grand Canyon (1956), it has been difficult to "get ahead" of the need for services. One result of this has been that controller morale has often been at a low ebb. This was evident following world war II, again during the Viet Nam war, and more recently, during the late 1970s.

Manifest and latent labor-management problems got out of control in 1981, culminating in a disastrous walkout of union controllers in August. The President of the United States acted decisively to end the strike and 10,000 controllers who did not return to work within a few days were summarily discharged. The national airspace system was placed under draconian capacity controls but continued to function at a fraction of its former capacity, manned by supervisors and the relatively few controllers who had not participated in the strike or who had returned to work within the permitted window for such action.

It was at this time that strategic air traffic management, the foundations for which had emerged during the Arab fuel embargo of 1975, assumed critical importance in airspace management. Working with air carriers and other airspace users, Flow Control allocated airspace capacity to operators in accordance with system resources, established throughput targets at tolerable levels, and literally managed the entire system. The facilities, staff and equipment available for this task were grossly inadequate, but the flow control system worked and provided ATC Centers and terminal area control facilities with the buffer they required to continue to provide traffic services with whatever personnel were available. Pilots and operators cooperated in every way possible, and the system never broke down completely.

The activities of Flow Control during this period made startlingly obvious the need for a continuing strategic management function, supported by a communications and information management infrastructure that would provide it with a "big picture" of U.S. air traffic. As the effects of the strike on tactical control were gradually ameliorated by time, new procedures and new trainee controllers, the FAA accelerated its efforts to provide its strategic traffic management function with the tools it needed.

After some years, the ATC System Command Center (SCC), located in Washington, finally received an automated system visualization device, the Aircraft Situation Display (ASD), which displays current aircraft positions and directions on a national scale, with superimposed maps of geographic and facility boundaries. The system incorporates selective digital filtering to permit controllers to visualize special categories of aircraft or situations of interest; system software also enables controllers to project and visualize the effects of intended strategies for management of air traffic in response to weather or other contingencies. It is thus a strategic planning tool as well as a representation of the current traffic situation. Weather displays are also available, and in the near future will be integrated with the ASD.

The Center's primary mission is to ensure that traffic demand does not exceed ATC system capacity. SCC personnel act mainly as coordinators between users of the airspace (largely air carrier dispatchers, with whom the Center has direct contact) and controllers in the various ATC facilities. During 1993, ASD displays also became available to air carrier System Operations Centers (SOCs), whose ability to manage their own traffic flow has been greatly enhanced by access to the larger picture of air traffic activity. The SCC performs an extremely important integrating function for aviation, though it does not direct individual aircraft. This integration is a key to the efficient utilization of finite airspace whose capacity is strained by the demands upon it.

Air traffic control automation

Radar itself may be considered a form of automation, in that it integrates and provides a visual representation of a geographic or spatial phenomenon, and thus constitutes "a system in which a production process is automatically performed by a self-operating electronic device" (chapter 1). Air traffic control radar facilities incorporate a great variety of electronic aids to reduce ground clutter, eliminate noise, overlay video maps on radar scopes, etc. In the early 1970s, the FAA began to install radar data processors (RDP) in enroute Centers, all of which make use of several remote radar sites to obtain full coverage of their airspace. Before radar data processing, sector controllers would utilize imagery from whatever individual radar provided acceptable coverage of their sector. RDP correlated the data from many radars to produce a composite synthetic image of all traffic using the best information available from its sensors. The result was a vastly improved visual representation of the best available data with less ambiguity and greater consistency, and thus decreased controller interpretive workload.

During the same time period, FAA installed flight data processors (FDP) that stored flight plan data, recognized the sectors through which flights would pass, and printed flight strips appropriate to each facility's responsibilities for flights. The FDPs were interconnected so that data on flights leaving a Center's area would be passed automatically to the next Center or terminal facility in line. FDPs also generated data for aircraft "tags" on controller plan view displays (PVD). Sector controllers continued to store the flight strips, annotate and move them to remind them of their flights' progress and requirements. Hopkin (1994b) has discussed the assistance that manual handling and marking of flight strips provides to controllers. He points out the information that adjacent sector controllers obtain simply by glancing at another sector's strip bay, the ability to re-sort the strips to take account of changes in traffic flow, etc. Controllers have shaped this tool, as humans always do, to serve their needs. Some authors believe that there is no longer a need for such tools (Vortac & Manning, 1994); others are less certain (Hughes, 1992; Hopkin, 1994a).

During the past decade, despite severe limitations on data processing capacity within aging ATC computers, several automated monitoring and alerting functions have been added to the ATC system. Conflict alert, designed to warn of a failure of separation minima, provides an audible alarm in the ATC facility if standards are transgressed. Unfortunately, violation of these separation minima subjects controllers to adverse action if they are found at fault. In response to controlled flight toward terrain incidents (and a small number of controlled flight into terrain accidents despite GPWS in aircraft), a minimum safe altitude warning (MSAW) module was developed. Later, an automated altitude monitoring function was added, which alerted controllers if pilots transgressed an altitude clearance limit (pilots violating their altitude clearances also face enforcement action by FAA).

Effects of air traffic control automation

As radar and ATC automation became more reliable in the 1970s, NASA Aviation Safety Reporting System reports began to contain comments from older controllers, trained and highly expert in the use of procedural control, worrying that their younger colleagues had become dependent on radar representations of traffic and thus were less skilled in constructing a three-dimensional mental image of the traffic under their control. Though some ASRS reports did indicate that sudden radar failures produced short-term disruption of traffic control, reports of serious incidents were uncommon. A few really dangerous losses of control did occur (e.g., Atlanta, 1981); these were usually ascribed to training or proficiency problems, though the investigations usually did not delve deeply into latent factors (Reason, 1990). Air traffic controllers (and ATC system managers) cultivated the image of great mental strength and individuality; this image did not willingly admit of personal or system weaknesses that could compromise the performance of their critical tasks (Rose, Jenkins, & Hurst, 1978; Flight Safety Foundation, 1982).

Nonetheless, the ATC system was under strain when its met its greatest challenge in 1981, the sudden departure of the great majority of its experienced operators. That it survived this challenge, even under severe constraints, reflects the capability and dedication of the humans who remained to operate it after the strike. The men and women who continued to control traffic were severely tested, but the basic structure of the system survived and remains in place today, awaiting advanced equipment which hopefully will enable the system to meet still greater challenges ahead. The plans for the new AAS were drawn to provide greater flexibility, productivity and capacity. Whether the system can meet its new demands will depend upon whether its design provides controllers with the flexibility to meet the challenges of an environment which is still not entirely under the control of the human operators in the system.

Comment

One of the continuing problems in the aviation system has been that its two principal components, the aircraft and the air traffic control infrastructure, have usually been considered in isolation. Aircraft designers have usually given only passing consideration to the system in which their machines must operate; ATC system designers have usually considered aircraft simply as point objects to be moved from place to place (a function often described as "moving tin"). Most controllers are not pilots, and virtually no pilots are, or have been, controllers. Designers in each sphere rarely have adequate knowledge of the other domain.

While this has not created insuperable handicaps in the past, evolving automation in aircraft, unaccompanied by similar development of the ATC system, has led to increasing disparities between aircraft and ATC capabilities. These, and increasing demands on the entire system, are now manifest as delays, which are expensive both to operators and to airline passengers. Though future ATC automation, the subject of the next chapter, may help resolve some of these discrepancies, it is critical that the future system's architecture recognize that the aviation system is a *single* system. Only with this recognition will the system be sufficiently functional to meet the demands upon it.

6. Future air traffic management automation

Introduction

The FAA is in the midst of the largest air traffic management system upgrade in its history. Its intended product is the Advanced Automation System (AAS). Europe is beginning the harmonization and integration of its multiple national air traffic control systems, and many members of the European Community are also undertaking massive equipment modernization programs. There is every reason to believe, therefore, that future air traffic control systems will look very different from the systems of today.

Two years ago (1992) the shape of the U.S. Advanced Automation System looked fairly clear, while that of Europe was very difficult to discern. Now, the outlines of the European system are beginning to reveal themselves while the shape of the future U.S. system is much less clear. "The cost of the (AAS) program, originally estimated at $4.3 billion, is now projected by the FAA at $7 billion...The system was to become operational in stages, beginning last year, but current estimates now project the earliest starting date as 1997" (Tolchin, 1994)[1]. Meanwhile, air traffic continues to increase.

Though discussion of future air traffic management systems is made much more difficult by the current unsettled state of affairs in the United States, it is plain what the future system is expected to accomplish. Further, we know in broad outline how the FAA wants to reach those objectives. From these facts, it is possible to suggest in some detail what the future system may look like and how it will function. What cannot be stated with any clarity at this time is what human and machine roles will be in that system, because its designers have not approached the question except in general terms. Joseph Del Balzo's (1992) forecast of "an era where air travel is unhampered by...the limitations of human decision-making..." suggests the depth of the concern about human reliability among senior system managers. If this concern is permitted to dominate the debate about the shape of the future aviation system, that system will *not* be a human-centered air traffic management system, and if ATC system automation is not human-centered, automation in the remainder of the system will not be either.

It is for these reasons that this document attempts to make the case for a human-centered automation system for air traffic control as well as for aircraft. There are not two systems (air and ground); there is one National Aviation System. Its elements must be designed and operated from a common philosophical base if the system is to be maximally effective. Forecasts of capacity demands indicate that even if the system operates optimally, its capacity will still be strained by early in the next century. We must, therefore, make the most of what we will have during that period.

Future air traffic control system characteristics

Assumptions

I shall assume that by the year 2000, most of the hardware and major software elements of a hypothetical advanced automated air traffic control system are in place. ATC computational resources will be adequate to process any system software that is likely to be devised. Interfaces between the human and machine components of the new system are in place. Most or all communication between ground and airborne components of the system is carried out by digital data link; voice is a secondary means of communication between ATC and aircraft under normal

---

1 It has since been decided to eliminate certain parts of the advanced automation system and to delay its implementation in facilities having less traffic, in order to lessen the overall cost. Cuts will also be made in the Initial Sector Suite development program.

circumstances. Finally, control of air traffic is still the responsibility of the ground ATC system (this assumption is being questioned; see discussion of "free flight" below).

The question, then, is what software will activate this system and how its components will work together to accomplish the mission. A range of hypothetical scenarios can be constructed. For reader convenience, I have named each using a scheme which will be discussed in detail in chapter 8 (see figure 8-2).

Scenario 1: Management by delegation

Scenario 1, the least radical, involves a system in which the controller manages by delegation, as do pilots of present-day aircraft. It is an outgrowth of today's system in many respects: the controller is given an enhanced multicolor plan view of traffic in a sector of airspace, a data display which presents flight strip analogues, rules governing the handling of that traffic, and a variety of automation tools which can be used to accomplish the task. Controllers have several such tools today; among them are predictors which show where traffic will be at a certain time in the future, history traces which show the immediate past trajectory of each aircraft, range settings with which they can set the area of coverage, variable polarization, declutter options, transponder code filtering, and others.

A larger area of coverage would be available, including other sector airspace. Short-term conflict prediction algorithms would suggest potential conflicts. A timeline might be available which would show traffic loading in the future. "What-if" gaming capability would assist the controller in examining decision options. Conflict alerting modules would warn the controller in advance of potential conflicts and would assist in evaluating the likelihood of conflicts given certain changes in trajectory. The computer would also monitor controller actions to insure that they comported with rules and procedures, and that limited-use airspace restrictions were observed.

Weather information would be shown; in low-altitude sectors, terrain and other obstacles would also be made visible as desired. The controller, within certain limits, would be able to select the strategy he wishes to utilize, and the computer would accept that strategy in its conflict predictions. More important, the controller could specify the level of assistance he wished the computer to provide; the automation could thus be adapted to a variety of cognitive styles and experience levels. Finally, memory aids would be provided which would enable a departing controller to brief a relieving controller quickly and comprehensively.

This scenario is roughly analogous to the environment of the pilot of a moderately automated future airplane; a variety of aids, developed in consultation with controllers of widely differing experience and expertise, would be available for use as needed. If a controller wished to control traffic without such assistance, the machine would let him do so while monitoring his actions for discrepancies (potential conflicts, actions not permitted by current procedures, potential incursions into special operations airspace, etc.). Most important, the computer would alert the controller to such anomalies before they resulted in transgression of permitted boundaries, to permit him to take corrective action early. In that sense, the computer would improve the error tolerance of the human-machine system.

Scenario 2: Management by consent

This scenario assumes a higher degree of machine intelligence somewhat like that projected for the Advanced Automation System's AERA 2 modules. In this scenario, the ATC computer accepts requests for flight plans or flight plan modifications. It examines the effects of these requested trajectories over a 20-30 minute period (and perhaps a longer period for initial requests), approves them if no conflict is detected, or suggests modifications to avoid a future conflict. (This may be done in automatic "negotiation" with the affected airplane's flight management computer.) The computer's output, when accepted by the controller, is an approved flight plan, either without or with modifications of the plan requested. This plan is shown (hopefully graphically, as on current aircraft navigation displays) to the controller. As in AERA 2, the controller may request another alternative or may input an alternative for evaluation. When a plan is acceptable to the controller, he or she gives consent, after which it is transmitted as data to the affected aircraft. Upon acceptance by the pilots, it is executed in the FMS.

Computer decision aids would be available to the controller to aid in visualizing the planned course of action (and changes from the present plan if one existed). Computer monitoring of controller actions would be performed throughout; as in the previous scenario, feedback to the controller would occur in time to develop a revised plan free of conflicts or transgression of rules and procedures.

This scenario differs from the previous one in that the machine takes initial and primary responsibility for development of plans, subject to consent by the controller. The level of automation is fixed, but the human can bypass machine decisions by making an alternative plan acceptable to the error monitor. As in today's aircraft, scenarios 1 and 2 are not mutually exclusive; it would be possible to embody both architectures in a single machine, giving the controller the ability to select which automation option he or she wished to utilize. This scenario would require somewhat more feedback from the computer to the human to permit the latter to monitor machine integrity on an ongoing basis, for the appropriateness of the computer's actions would be less obvious than in scenario 1, in which the human operator is more tightly coupled to system behavior.

Scenario 3: Management by exception

This scenario involves a somewhat higher degree of automation than has thus far been suggested by air traffic management for near-term implementation, either in the United States or Europe. In view of increasing demands on the ATC system, however, I think it likely that a more autonomous solution may be proposed as a "growth" version of the next-generation air traffic control system. During the last decade, there have been serious suggestions that high-altitude enroute traffic, given satellite navigation systems and automatic dependent surveillance, and backed by airborne collision avoidance systems, could function essentially autonomously without much, if any, ATC intervention (see discussion of "free flight", below). This scenario does not go that far; a measure of control remains with the ground infrastructure, but there are alternative ways of realizing a system in which management is by exception, and pilot-assisted ATC is one of them.

In this scenario, computers would perform all of the functions listed under scenario 2, but they would select and exercise decision options autonomously. The human air traffic monitor (he or she would no longer actually control traffic) would be informed by some means of the present and future (intended) traffic situation and would manage by exception. Compliance with machine-generated clearances would likewise be monitored by the computer, which would alert the human monitor to any undesired behavior of aircraft. The human could intervene by reverting to a lower level of automation, or could instruct the computer to resolve potential conflicts or problems. The human would also monitor machine function and would be aided in doing so by the machine's portrayal of the traffic situation and other data.

Here, the computer, and pilots in flight, are controlling air traffic. The controller's role is to insure that the machine is behaving in accordance with predetermined rules and that its actions are in conformance with directives and procedures. Though such a system initially would require controllers who could intervene as required, it might not require such backup after it had proved itself sufficiently expert and reliable. Instead, human monitors would be trained to evaluate and detect departures from permitted machine behavior and given means with which to limit machine authority as needed to maintain a safe operating environment.

Where would the responsibility lie in such a system? I believe it would have to vest in the operating organization and the system's designers. It could not remain with the system's operators; they would be too far removed from the details of system behavior to accept full responsibility for outcomes. This is a potentially troublesome problem, but a much more difficult problem would be to endow such an automated system with enough flexibility to encompass the range of environmental and other variables that can affect air traffic.

Having said this, however, I recognize the exponentially increasing capability of computers and I will readily admit that such a capable system is at least thinkable. It would be extremely expensive, but it could convey enormous return on investment if it worked, and its throughput under normal circumstances might be as good or better than that of other, less automated systems. It is important to remember that the newest aircraft flight control and guidance systems are essentially capable of being managed by exception; once programmed and off the ground, they will conduct a flight autonomously unless the pilots intervene. It is at least conceivable that at some point in the future, air traffic control automation will also be a highly intelligent machine agent, though it is far in the future.

Developments in progress

Flow control: strategic traffic management

Each of these three scenarios assumes the existence of a strategic management function. In the United States, the FAA's Enhanced Traffic Management System (ETMS) will improve the ability of the ATC System Command Center to manage traffic in cooperation with Traffic Management Units at each ARTCC and System Operations Centers at airlines. As mentioned earlier, SCC aircraft situation displays are already available to air carrier dispatchers, and this has laid the foundation for increased cooperation between SCC and its customers. Recall that the basic purpose of the SCC is to insure that air traffic demand does not exceed ATC facilities' ability to handle it. If a runway, or an airport, becomes unusable, the SCC commands and coordinates a reduction on traffic flow until the facility problem is resolved.

The ETMS will provide an enhanced aircraft situation display, a monitor-alert function, automated demand resolution, a strategy evaluation and recommendation module and other decision aids, and a directive distribution function, among other automated tools. Elements of these functions are already in use; the final product should provide personnel at the System Command Center with even more formidable strategic management capability.

A Central Flow Management Unit (CFMU) for western Europe came into operation in 1993. Located in Brussels, it is planned that there will be an equivalent facility in Moscow for eastern Europe. As in the United States, the CFMU will coordinate with Flow Management Positions at each Area Control Center.

Terminal area traffic management

These scenarios also assume the existence of software modules that will extend some type of automated air traffic control from takeoff to landing. Oddly enough, terminal control elements, which are substantially more difficult than enroute control, are also farther along, in large part because of a research and development effort called the Center-TRACON Automation System (CTAS). CTAS, undertaken by NASA's Ames Research Center in the mid-1980s, has developed as a decision aiding system; it does not operate autonomously. Rather, it provides displays and tools to help controllers secure maximum utilization of terminal airspace by flow planning and precise execution of descent and approach maneuvers (Erzberger and Nedell, 1989; Harwood and Sanford, 1993). Its functionality is generally similar to that proposed in scenario 2, above.

CTAS is a time-based system (Tobias & Scoggins, 1986) which when fully implemented contains three modules: a traffic management advisor (TMA), a descent advisor (DA) and a final approach spacing tool (FAST). The TMA has been developed for use by Traffic Management Units, which monitor the demand of arrival traffic and coordinate with ATC facilities to make decisions about balancing traffic flow so demand does not exceed capacity in Center and Terminal Areas (Sanford et al., 1993).

CTAS has undergone a great deal of simulation testing at NASA Ames, in cooperation with the FAA's Terminal Air Traffic Control Automation (TATCA) program. During the past year, elements of the system have been implemented at Denver for eventual testing with live traffic (Harwood & Sanford, 1993); tests at Dallas-Ft. Worth are also planned. The system offers considerable promise with regard to maximizing terminal area traffic throughput; it is an important element of NASA's Terminal Area Productivity program.

Enroute air traffic management: the AERA concept

Since the early 1980s, FAA and its contractors, notably the MITRE Corporation, have been developing an automated enroute air traffic control system (AERA). This proposed system has undergone many changes since it was initially proposed, but its outlines have remained. In brief, the AERA concept envisions automation similar to that described in scenario 2. Automation would maintain surveillance of air traffic movements, detect potential conflicts over a 20-30 minute window, and provide revised clearances to mitigate detected conflicts. Controllers could accept these machine decisions or could propose alternatives to deal with the detected problems. Data link would communicate clearances to aircraft (Kerns, 1994); voice communications would be available for emergencies.

The "Free Flight" concept

Prompted by the relative inflexibility of the present system of enroute control of air traffic and growing understanding of economic benefits if more flexible routes can be approved, airline managements and their representative organizations, ATA and IATA, have begun to consider seriously more radical innovations in air traffic management. They have recently proposed a "free flight" concept, in which operators would have the freedom to determine airplane paths and speeds in real time (IATA, 1994). Air traffic restrictions would only be imposed to ensure separation, to preclude exceedance of airport capacity, and to prevent unauthorized flight through special-use airspace. Such restrictions would be limited in extent and duration to correct identified problems. The radical nature of this proposal amounts, in essence, to a fourth scenario for future air traffic management. Relevant parts of the IATA document are therefore extracted here.

Scenario 4: Free flight

The "vision" of this concept (IATA, 1994) is "a global air traffic management system that allows airspace users maximum freedom of movement subject to the needs of safety, overall system efficiency, and the environment". "The following principles shall guide the development and operations of the future ATM system:

- "Safety must be maintained at its current level and enhanced where feasible.
- "The future system shall provide adequate capacity to meet demand at peak times and locations without imposing significant restrictions on traffic flow.
- "Aircraft operators shall have the flexibility to dynamically adjust flight trajectories and departure and arrival times to satisfy business operations.
- "ATM services will be provided in a cost-effective manner. Charges must be equitable, traceable, transparent and cost-related.

- "ATM services and procedures shall adhere to uniform principles world-wide. Requirements for airborne equipment capabilities must be internationally standardized.
- "The ATM system must be based on human-centered automation enabling high levels of performance.
- "ATM shall contribute to the protection of the environment by allowing flights to operate on optimum trajectories."

The IATA document states that its "vision can only be realized through the application of dynamic user-determined flight trajectories. The desired result is to operate in the airspace with the safety associated with instrument flight rules while simultaneously providing flexibility and capacity normally associated with visual operations" (p. 5). "Air traffic restrictions are only imposed to ensure separation, to preclude exceeding airport capacity and ensure safety of flight." (p. 5). "The air traffic manager intervenes on a 'by exception' basis to resolve any detected conflicts...In normal situations, aircraft maneuvering is unrestricted. Separation assurance may be enhanced by on-board systems."

(p. 6) "Over time, the (air traffic control) process has become increasingly more rigid and inefficient in order to cope with constantly increasing demand. Under the concept of free flight, the flight plan contract will *not* be needed to provide the air traffic manager with knowledge of intent for the separation of traffic. It is possible and necessary to shift from a process of clearance based separation to one of near-term position and velocity based separation. In the future system, each aircraft will be separated by two aircraft centred zones. The smallest zone...must remain sterile to assure separation...The outer zone...is used to indicate a condition where intervention may be necessary...An aircraft separated from other aircraft, so that its alert zone is clear, is free to change course, altitude or speed at will. *Subsequent* to any change, a revised plan will be data-linked to the ground system for planning purposes..." (emphasis supplied)

"Advanced automation is an essential element of the new air traffic management system. The purpose of this automation is to assist humans and not to replace human reasoning. Aircraft in potential conflict must be identified and appropriate advisories or resolution instructions will be suggested by automated systems. With timely and proper notification to controllers and pilots, near-term separation, within minutes of the point of closest approach, becomes feasible...

(p. 7) "The combination of GNSS, ATN and ADS will permit aircraft separation minima to be reduced significantly. The air traffic service provider will intervene only when there is a high probability of conflict. Intervention of (with?) an aircraft should be delayed until a conflict can be predicted accurately, but not so long as to require an unacceptable avoidance manoeuvre. The process of conflict detection and resolution must be automated, and after controller approval, resolution instructions can go directly to involved aircraft. Conflict resolution will involve a minimum disruption to the flight path of each aircraft, and following a resolution, aircraft will be released quickly to resume free flight."

While the AERA concept envisions a system that would be able to accommodate operator route preferences to a much greater extent than is presently possible, the "free flight" concept goes a step beyond this by limiting air traffic control authority to the resolution of short-term conflicts.

Issues raised by future air traffic management concepts

Both the AERA 2 and free flight concepts raise substantial issues with respect to human-machine cooperation in the aviation system. Both concepts envision radical changes in the architecture of airspace control, though the free flight concept is more revolutionary than the AERA concept.

Each concept implies major shifts in human and machine responsibilities, and each would involve major shifts in the locus of control of the aviation system. Some of the more important human-machine issues are discussed below.

Human and machine roles in the future system: AERA-2

As implied above, air traffic control automation can go in several directions: either toward a more autonomous machine system, or toward a system in which the human operator remains in command. Each direction presents different potential advantages and different potential problems.

There is substantial sentiment within FAA and Eurocontrol for a more automated system that reduces the probability of human error by reducing human control. Several studies of operational errors (defined as loss of prescribed separation between aircraft) have found a trend toward more errors under light or moderate, as opposed to heavy, workload (Kinney, Spahn, & Amato, 1977; Schroeder, 1982; Schroeder and Nye, 1993), though it has been hypothesized that more serious errors occur under heavy workload conditions (Rodgers and Nye, 1993). Deficient situation awareness has been implicated as a factor associated with the severity of operational errors. Not surprisingly, human operators are almost always found to be at fault (but see discussion of human error in chapter 4, page 66).

Though our understanding of latent factors in the causation of human errors has progressed considerably, there is no doubt that many in the air traffic control community look to automation as the principal way to improve ATC reliability. This being the case, it will be necessary to make a compelling case for keeping the human controller in effective command of the system once advanced ATC automation is available. I have said "effective command" because there seems little question about the controller's continuing *responsibility* for traffic separation regardless of the level of automation interposed between the controller and his or her traffic. It is encoded in high-level operating guidelines for the AERA 2 system when it becomes operational (Celio, 1990).

> "Responsibility for safe operation of aircraft remains with the pilot in command.
>
> "Responsibility for separation between controlled aircraft remains with the controller."

I argue in this document (see chapter 8) that if the human remains responsible for safety, that human must retain the authority with which to exercise that responsibility, by whatever means—automation must be a tool over which the human must have full authority. The operating guidelines offered by Celio do not give cause for comfort:

> "Since detecting conflicts for aircraft on random routes is more difficult than if the traffic were structured on airways, the controller *will have to rely* on the (automated) system to detect problems and to provide resolutions that solve the problem.
>
> "Alerts may be given in situations where later information reveals that separation standards would not be violated...This is due to uncertainty in trajectory estimation...Therefore, alerts must be given when there is the possibility that separation may be violated, and the controller *must consider all alerts as valid*."

In its Executive Summary, the report states,

> "Machine-generated resolutions offered to a controller that are free of automation-identified objections *are assumed feasible* and implementable as presented."
>
> "The controller *will use* automation to the maximum extent possible." (Emphasis supplied)

Note that if a controller accepts a computer decision and it turns out to be faulty, the controller is responsible. If the controller rejects a computer decision and substitutes one which is faulty, the controller is also responsible. This sort of dilemma represents a classic "double bind" (Woods et al., 1994). Note also that in this sort of system, de-skilling (Cooley, 1987) is very likely to occur over time. Finally, since the AAS computer will resolve conflicts over a relatively long time window (20 minutes or so), the controller who issues a machine-recommended clearance may not be able to assess retrospectively whether his choice was correct, for the outcome of that clearance will often occur in a sector not under his control and not visible to him. The alternative, of course, is to revert to short-term controller-initiated conflict avoidance, as occurs routinely in the present system.

Pilot, controller and machine roles in a "free flight" system

While the "free flight" proposal is new and has not yet undergone the intensive scrutiny it will certainly receive in the near future, it clearly represents a carefully studied proposal which expresses the frustration of operators with what is perceived as an increasingly outdated, cumbersome and inflexible ground-centered concept of aviation operational control. The first stage of a system precursor was implemented in January, 1995, however, for altitudes of 39,000 ft and above; lower altitudes will be included over the next year. Building on its previous experience with the aviation safety/automation program, CTAS and other control strategies, NASA is planning a new aeronautics initiative variously called "Air Traffic Management" or "Advanced Air Transportation Technology" and has established interdisciplinary teams to explore this concept and the technology needed to bring it to fruition.

The AERA concept poses major questions concerning the roles of the air traffic controller and the automation which would bring it to fruition. I believe that the free flight concept, as set forth above, poses more fundamental questions concerning human (both pilot and controller) and machine roles in the future air traffic management process. More important, it calls into question many of the fundamental assumptions on which the largely successful ATC system has been built. The architecture of a fully-developed air traffic management system designed around this concept would have to be radically different from that presently proposed for the AAS because of its emphasis on short-term tactical, rather than strategic, management and its implication that management should be almost entirely autonomous or by exception.

The design implications of a free flight system are beyond the scope of this document, but it is clear that such a system would involve a qualitative change in the roles of the humans and machines that operated it. Some of the issues raised by the concept are set forth below.

The free flight concept envisions that flight paths would be selected by pilots, or more likely dispatchers working in air carrier System Operations Centers, and implemented by the pilots *without* prior notification to the air traffic management system. This concept envisions the entry of a third, more-or-less co-equal, authority into the control process: the SOC, and it thus raises many questions about further distribution of authority and responsibility for air traffic movements (see chapter 8).

The air traffic management subsystem would be relegated to an oversight role unless a conflict were detected. It appears that the ATM system would function in somewhat the way that collision avoidance systems now function: by using aircraft data and extrapolated trajectories to develop separation zones around aircraft which would be used to determine a need for alerting or conflict resolution in real time. The concept implies the existence within the ATM system of computers that can accomplish the functions planned for the AERA-2 system, but with additional uncertainty posed by random variations in flight trajectories.

These uncertainties would pose problems for controllers (and for the ATM system) similar to but more acute than those they now face when TCAS issues a resolution advisory to pilots, who respond prior to notifying ATC that they are doing so. Yet "controllers" are expected to intervene, or supervise the computer that will intervene, "on a 'by exception' basis", "only when there is a high probability of conflict". The likelihood that controllers will be able to detect and diagnose probable conflicts under a high level of uncertainty is low, and the proposal recognizes this by stating that computers will accomplish this task and suggest appropriate resolution tactics. The computer, of course, will also have periods of uncertainty during aircraft maneuvers, before it is able to reestablish a stable trajectory projection and project it forward in time to evaluate whether the maneuver has created a potential conflict. Yet the proposal also states that the purpose of automation is to assist humans and not to replace human reasoning. The compressed times within which the humans would have to apply such reasoning and take action, given only retrospective notification of aircraft maneuvers, appear to have received somewhat less attention than they deserve in the development of the concept.

The IATA document clearly envisions TCAS, perhaps with lateral as well as vertical maneuver capability (the capability proposed for TCAS-3), as an additional means of conflict detection and resolution ("Separation assurance may be enhanced by appropriate on-board systems"). Yet TCAS resolution maneuvers are a prominent source of problems for controllers and the ATC system today and would almost surely present more difficult problems for them and for ATC computers in a less constrained free flight system.

The proposal does not explicitly mention significant additional requirements on pilots. Nonetheless, the lack of "assured separation" provided by the present, admittedly cumbersome system would actually require higher vigilance throughout flight operations, since maneuvers could be instituted without advance knowledge of the locations of other aircraft whose own trajectories might be affected by such maneuvers.

The requirement for knowledge of other aircraft positions and altitudes would require a cockpit display of traffic information. TCAS in its present form provides only an approximation of the information required for this task. As noted earlier, its representations of traffic are not entirely adequate even for its present tasks (and its software thus far has not been able to handle all of the situations in which it must provide traffic or resolution advisories). It appears that free flight would impose substantially greater requirements on airborne collision avoidance equipment, as well as considerably greater separation assurance requirements ("see and avoid (by whatever means)") and therefore workload on pilots. Pilots are not presently required, or trained, to think in terms of the four-dimensional resolution of traffic conflicts, yet this new task is what would be required of them during climbs and descents. This proposal would certainly increase the *involvement* of pilots in enroute operations, (see chapter 2), but it does not address how pilots would be kept adequately *informed* of the positions and paths of other aircraft which may become a problem for them.

It should also be noted that collision avoidance is a flight-critical function. TCAS at this time is a "single-thread" system; that is, only a single TCAS unit is installed in each airplane. A traffic management system that relied upon airborne collision avoidance systems to a greater extent would certainly require consideration of whether dual TCAS systems should be installed. Further, TCAS in all aircraft to date has been installed as a "stand-alone" system; its displays are integrated only partially with the remainder of the information management capability in the cockpit. Finally, TCAS was designed as a back-up system, like altitude alerters. It would surely become a "front-line" system if this proposal is implemented.

Perhaps the most worrisome aspect of the free flight proposal in its present form is its central assumption that automation can increase flight path flexibility without imposing greater order on the system it would control, and without providing human operators in the air and on the ground with the information they would require to maintain command over the system. Separation standards would no longer be constrained to provide time for prospective action to resolve potential conflicts; such conflicts would be resolved in real time as they occurred. *Intent* would no longer be required to be communicated.

It appears that little thought has been given to whether humans can operate and manage such a system. Rather, new technology will operate the system and humans will supervise its operation, but not necessarily with advance knowledge of how it is going to behave. As proposed, the airborne systems will not inform the ATM system of their intent in timely fashion; the ATM system and its supervisory controllers will not predictably be involved in air traffic movements, and will not have advance knowledge of any individual airplane's future trajectory. For these reasons among others, the likelihood that pilots and controllers will be able to remain in command of such a system is very low, for the system will not be predictable. The likelihood that those humans will not be held accountable for the results, however, is *negligible*.

Wiener (1993, p. 4) has pointed out (with respect to aircraft automation) that "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...suggests that this may be overly optimistic, and that automation merely changes the nature of error, and possibly increases the severity of its consequences." In an earlier paper (1987, p 179), he had said, "The experience from commercial aviation shows that it is unwise to dream of automating human fallibility out of a system. Automation essentially relocates and changes the nature and consequences of human error, rather than removing it, and, on balance, the human operator provides an irreplaceable check on the system. The search should be directed toward the management of human caprice, not the elimination of its source." *Human error is a symptom of a system problem.*

There is no reason to believe that automation in air traffic control and management will be a panacea, any more than it has been in the cockpit. As Woods has commented, *any* tool, including automation, shapes human behavior. The human errors expected in a highly automated system would be expected to be different, and indeed they are different. But automation does not, and can not, eliminate human error (though if properly designed, it can sometimes mitigate the consequences of human error).

Automation, of course, is not infallible either. The literature abounds with failures of automation to perform as expected; a few examples in aircraft are shown in figure 4-6. These failures are among the reasons why humans must be an *integral* part of the system—they are there to compensate for the imperfections of the automation. They are also there, as noted above, to accept responsibility for system safety. If they are to remain in command, they must be involved in system operation—not only when the automation fails, but during normal operations as well, in order to be in the loop when the inevitable failures occur. The human operator is the final line of defense in automated systems, and the new systems proposed for air traffic management are no exception.

Implications of future system design proposals

The complexity of any automated system for air traffic control will be far greater than the complexity of a flight management system, and pilots' problems in understanding that system's behavior have been discussed in chapters 3 and 4. It can be confidently predicted that similar problems will be encountered in the air traffic management domain if controllers are unable to form adequate mental models of the system's processes. Those processes must be comprehensible and predictable, both so the controller can predict them and so that failures of the automation can be detected. Consciously *reducing* the predictability of a highly integrated, cooperative human-machine system seems a strange way to achieve greater system safety.

A summary of comments regarding the human's role in air traffic management made during a recent conference on European ATM is instructive but unsettling:

"'The present system of air traffic control has been in existence with few fundamental changes for 40 years. Even with technological improvements, the present system is likely to reach capacity limits by 2005,' says Peter Whicher of Logica. The provision of automatic aids to assist the controller is only marginally likely to defer the problem, and the deadline (Whicher) sets for getting a new concept installed and running successfully, with a potential capacity of at least five times 1992 traffic, is 2010.

"The basic requirement *is to minimise human control involvement in routine events* and concentrate skills on system and safety management, and on the resolution of exceptional situations.

"'To permit unrestricted ATC growth we should first determine how to eliminate one-to-one coupling between a proactive sector controller and every aircraft in flight—and so avoid him becoming reminiscent of the man with a red flag in front of early motor vehicles. With improved area navigation and flight management systems, pilots can and are willing to take direct responsibility for routine enroute track-keeping functions,' Peter Whicher explains, 'freeing controllers to concentrate on the key areas where human skills have most to offer—traffic management, system safety assurance, and dealing with the exceptional occurrence.'

"Mr. Whicher foresees two possible concepts of control for the next century: one is *full aircraft autonomy*, the other is its opposite—*full ground control automation*." (Cooper, 1994a, emphasis supplied)

The role of the future controller proposed here is that of a monitor, not a manager, except when exceptional situations are detected. If an automated ATC system works well, such situations should arise relatively rarely—and the human controller is back to the situation Mackworth (1950) investigated so effectively, searching over long periods of time for rare events that may not be particularly obvious when they arise. As with pilots of long-haul aircraft, some form of active involvement is required if controllers are to remain in command of the traffic situation. Further, active involvement in air traffic control is necessary to prevent skill degradation (Cooley, 1987; Rauner, Rasmussen, & Corbett, 1988).

If the controller is to remain in command, and if automation is responsible for conflict detection and resolution, it must inform the controller of what it is doing and how. We know from previous studies in aircraft, nuclear power plants and elsewhere that complex automation tends to be opaque to its observers. Controllers must be informed, not only of the traffic situation, but of the processes that are being invoked to modify that situation, if they are to remain controllers rather than simply machine monitors. If the controller is *not* to remain in command, then system architects must state more clearly who is to replace him, and how. Responsibility for an adverse outcome *will* be placed at some human's door (see chapter 14, liability issues).

Whicher's concept of the future ATC system might be economical, but field observations and empirical research suggest that it is unlikely to be effective. Are there alternatives that will still accomplish the objective of increased throughput? I believe that management by consent, as exemplified in scenario 2 above, offers at least a greater likelihood of preserving controller involvement in the tactical management of air traffic. There is a problem with such an approach; it may be difficult to prevent situations in which consent is perfunctory rather than thoughtful, if a controller is tired or distracted. Nonetheless, it is preferable to management by exception (scenarios 3 or 4), in which the "controller" is not intimately involved in the control process.

Given that a majority of controller operational errors occurs during periods of light rather than heavy traffic, I would prefer from a human factors viewpoint to see a work environment in which the controller could adjust his or her workload as required by invoking automation to offload some of the routine tasks while preserving authority over the more complex and challenging tasks such as planning and management of exceptional situations. This approach to ATC automation resembles that available today in advanced aircraft, where the pilot is able to preserve control skills by exercising them, but is also able to lighten routine workload when desired.

Cooperative human-machine air traffic management systems

As Benjamin Franklin observed at the signing of the Declaration of Independence, "We must all hang together or we shall assuredly hang separately." Much the same can be said of human operators and automation in complex systems. What is required is a *cooperative* relationship between humans and machines, in which each intelligent agent augments the strengths and compensates for the deficiencies of the others. Can the basis for such a relationship be established in future automated ATC systems? I believe it can be, but that it must be a part of the *fundamental architecture* of such a system, which means the basis must be established very early in the design process.

Ongoing attempts to make air traffic management more effective can, and should, point the way to the shape of the future tactical air traffic control system. But we must not lose sight of the strengths of the current system, and of why it works as well as it does. Before new technology is designed for a future system, ATM concepts should be brought under intensive scrutiny to determine the ingredients of success in a complex, distributed human-machine system whose performance can be evaluated and measured quantitatively. The cognitive factors that make for success or failure in this team enterprise are beginning to be understood and can serve as a model for the design of the future tactical ATM system. Without this model to drive the architecture of the system, the technology will fail.

Comment

The fundamental question raised by present proposals for the architecture of the future air traffic management system is simply whether future ATC automation should be designed to assist human controllers or to supplant them. As I have said above, a fully automatic ATC system may be thinkable, and might have important economic benefits. I do not believe its productivity would be appreciably higher than a cooperative human-machine system; it would be less flexible than a cooperative system by virtue of being unable to call upon human creativity in dealing with unplanned contingencies, and there will always be such contingencies. Further, the difficulties that have already arisen in connection with the development of system software for AAS will be magnified many times by the enormous cost of developing a more fully autonomous system even if it is possible in theory.

While the "free flight" concept envisions very important economic benefits for air carriers, and perhaps increased ATM system productivity (if fewer controllers were needed), it would require that a full ATM infrastructure remain in place to deal with "exceptions". Much new ATM automation would be required to deal with conflict prediction in a less orderly system involving random, unpredictable flight paths. This factor would also decrease the amount of time available to human managers who would be expected to exercise flexibility in the resolution of conflicts. The new automation will bring with it more of the problems to be discussed in chapters 7 and 8.

Dr. Hugh Patrick Ruffell Smith, a very wise human factors expert, observed in 1949 that, "Man is not as good as a black box for certain specific things; however, he is more flexible and reliable. He is easily maintained and can be manufactured by relatively unskilled labour." We should think carefully about this observation as we contemplate the shape of the future ATC system.

Part 2: The Roles of Human Operators in the Aviation System

In part 1, I have discussed the developmental history of automation in aviation. In part 2, I will try to encapsulate some of the benefits, and some of the costs, of aviation automation in terms of the human operator's ability to work cooperatively with highly automated systems. Not all of these costs, by any means, are inherent in the automation; many have resulted from humans' deficient mental models of that automation. Other problems result from cumbersome interfaces between the humans and their automated tools. Whatever the reasons for these problems, they tend to make the human-machine system less effective, less reliable or less safe. As noted in the foreword, this document is not a study only of humans who use automation, nor of the automation itself, but of the *system* in which both attempt to work cooperatively to accomplish social objectives.

In chapter 7, I summarize and generalize some of the problems introduced in part 1 to remind the reader of what they are, where they are seen, and why they occur. Chapter 8 discusses in more detail a central question in human-machine system design and operation: the respective roles of the human and machine, and how responsibility and authority are apportioned in such systems. Chapter 9 discusses an important issue with regard to aviation system design: whether the future aviation system should be more tightly coupled, or whether it should remain integrated but uncoupled, as at present. The points made in these chapters are the basis for the human-centered automation concepts previously presented in chapter 2, and for the guidelines presented in part 3.

7. Benefits and costs of aviation automation

Introduction

The NASA Aviation Safety/Automation program (NASA, 1990), the work of Wiener and Curry which preceded it (Wiener and Curry, 1980; Curry, 1985; Wiener, 1985; 1989; 1993; studies by Rouse and colleagues (1980; 1983; 1987; 1988), research by Sarter and Woods (1991; 1992; 1994), and contributions by Rasmussen (1988), Reason (1990) and many others, are the theoretical and empirical foundations for these comments on humans and automation. There is now a great deal of data concerning human cognitive function in complex, dynamic environments. This chapter will hopefully demonstrate to designers and operators working in the aviation domain that there is a considerable body of knowledge that can help them to do their respective jobs more effectively.

I do not apologize for dwelling upon the unwanted behavior both of automation and people, because it is only through such study that we can minimize the costs while increasing the already considerable benefits of this technology. It is important that we not lose sight of the benefits (see immediately below), for aviation cannot advance without automation if we are to meet future challenges which will tax our ingenuity to the utmost. We must not "throw the baby out with the bath water".

But it is equally important that we not ignore the potential costs of yet more sophisticated automation, for if it is not designed and used properly it can make the future aviation system less flexible, less effective and less able to meet those challenges. In recent years, it has become evident that our operators do not always understand or properly manage the automation they now have at their disposal. It is essential that we make every effort to understand why this is true, if we are to design future automation so that it will be more effective and error tolerant than what we now have.

Benefits of aviation automation

I have referred in several places to the benefits derived from aviation automation to date. Let me summarize explicitly what these benefits are, to keep this discussion of problems in context. Wiener and Curry (1980) discussed system goals. Paraphrased, they are:

- **Safety**
- **Reliability**
- **Economy**
- **Comfort**

I will briefly cite demonstrated benefits with respect to each of these system goals. This list is not inclusive, but it will provide some insights into the extent to which we rely upon automation to accomplish our objectives.

Safety has always been proclaimed by the aviation industry as its primary objective. An examination of air carrier accidents by Lautmann and colleagues (1987) suggests that more highly automated aircraft have had substantially less accidents than earlier aircraft. Ten years after their introduction, the Boeing 757/767 types have been involved in only one fatal mishap (Thailand, 1991), a remarkable record. Other new types have been involved in more mishaps, but the record is still generally good. (For a balanced discussion of this question, see AWST 1995a,b)

Reliability has been improved; autoland-capable automation and other innovations have increased the number of flights able to operate at destinations obscured by very low visibility. Newer systems (GNSS, enhanced vision) have the potential to improve approach and landing safety worldwide. Improvements in Air Traffic Control also have the potential to increase reliability in the future system.

Economy has been improved by flight management systems that can take costs into account in constructing flight plans, though the benefits possible from such computations have been diluted by the inability of the present ATC system to permit aircraft to operate routinely on most cost-efficient profiles. Despite this limitation, significant economies are being achieved in the United States by more extensive coordination of non-preferred and direct routes between air carrier Systems Operations Centers and the FAA's System Command Center.

Comfort has been improved by gust alleviation algorithms in the newest aircraft, as well as by the ability of newer aircraft to fly at higher altitudes, above most weather. Greater flexibility enabled by ATC automation will permit pilots to utilize a wider range of options to achieve more comfortable flight paths.

In what respects are we still deficient with respect to these system goals? Most of our accidents can be traced to the human operators of the system, and increasing numbers can be traced to the interactions of humans with automated systems. More can be done to make aircraft automation more human-centered, but perhaps even more important, advanced automation can be used to make the system as a whole more resistant to and tolerant of human errors, be they in the implementation or the operation of these systems.

Costs of aviation automation

The 1989 ATA Human Factors Task Force report stated that "During the 1970s and early 1980s, the concept of automating as much as possible was considered appropriate. The expected benefits were a reduction in pilot workload and increased safety...Although many of these benefits have been realized, serious questions have arisen and incidents/accidents have occurred which question the underlying assumption that the maximum available automation is always appropriate, or that we understand how to design automated systems so that they are fully compatible with the capabilities and limitations of the humans in the system" (pp. 4-5). Let us examine this statement, which was largely responsible for the inquiry described in this book and its predecessor (Billings, 1991).

At the time the ATA report was prepared, the outlines of the A320 and B-747-400 automation suites were just becoming visible to the knowledgeable observers on the Task Force. The MD-11 was at an early stage of development and its cockpit design was not yet firm. It is clear that in the A320 and MD-11, the "concept of automating as much as possible", with the intent of reducing flight crew workload and minimizing human errors, was in fact considered appropriate, though the two design teams took different approaches. The 747-400 was much more conservative in its automation philosophy and more evolutionary than revolutionary in its application.

It is clear, with the hindsight afforded by five years of operational experience, that at least some pilots have found certain of the automation features in this new generation of aircraft difficult to understand and to manage. The difficulties that have been experienced appear to me to have been due in large part to five factors. Four are design factors: complexity, brittleness, opacity and literalism. A fifth related factor is training, which in turn is related to understanding. Each is considered in more detail here. A discussion of other relevant factors follows.

Complexity

As indicated in chapters 3 and 4, today's aircraft automation suites are very capable, increasingly flexible and very complex. Tactical control automation (enabled through a mode control panel, as in figure 3-9) is tightly coupled to strategic flight management (the FMS, with its CDU interface) in ways that are not always obvious. The FMS itself is capable of autonomous operation through several phases of flight. Both parts of the system are "mode-rich", (Sarter and Woods, 1994); default and reversion options vary among modes.

When these interactions cause unwanted behavior (from the pilot's viewpoint), the pilot has no mental model that allows him or her to correct the situation short of reverting to a lower level of management (see chapter 8) or turning the automation off, which is not always desirable and may not be possible in some circumstances. "Turning it off" (Curry, 1985), for instance, may disable certain protective features such as FMS knowledge of altitude restrictions during a descent into a terminal area, or the automation's intent to level the aircraft at a given altitude during a climb. Pilots of recent, very powerful aircraft have become concerned about the rate at which the airplane was approaching a level-off altitude and have reverted to autopilot vertical speed mode to slow the climb as they approached the new altitude, unaware that this reversion also cancelled the altitude capture mode. The result has often been a deviation above assigned altitude.

Another aspect of automation complexity is the great flexibility found in the modern flight management and autoflight system. Modern systems have many modes for each of several control elements (figure 7-1). These modes interact in ways not always obvious to pilots. Operators must learn about, remember and be able to access information concerning each mode in order to use it effectively; this imposes a considerable cognitive burden, makes it less likely that the operator will have an appropriate mental model of the automation, and increases the likelihood that modes may be used improperly. In addition, the capability of the modern FMS means that the system may direct the airplane through several modes of operation autonomously, in ways which may leave the pilots uncertain of exactly why the automation is behaving in a certain manner at a particular point in time.

Aircraft Flight Modes		
Autothrust Modes	Vertical Modes	Lateral Modes
TOGA FLX 42 MCT CLB IDLE THR SPD/MACH ALPHA FLOOR TOGA LK	SRS CLB DES OPEN CLB OPEN DES EXPEDITE ALT V/S-FPA G/S-FINAL FLARE	RWY NAV HDG/TRK LOC* LOC/APP NAV LAND ROLLOUT

Fig. 7-1: FMS and autoflight modes in the Airbus A320 (after Sarter and Woods, 1994)

Sarter and Woods (1994) and Sarter (1994) have discussed mode errors and mode awareness. Figure 7-1 is adapted from their paper. It illustrates the mode flexibility (and complexity) in a modern transport aircraft. Compare this with the relatively small number of flight modes in the Lockheed L-1011 automation shown in figure 3-10.

Each of the modes listed represents a different set of operating instructions for the automation. The mode in use (or armed, ready for use) is displayed in an alphanumeric legend on a flight mode annunciator panel at the top of the primary flight display. In their conclusions, the authors of this very useful paper state that, "As technology allows for the proliferation of more automated modes of operation...human supervisory control faces new challenges. The flexibility achieved through these mode-rich systems has a price: it increases the need for mode awareness—human supervisory controllers tracking what their machine counterparts are doing, what they will do next, and why they are doing it...While we understand a great deal about mode problems, the research to examine specific classes of countermeasures in more detail and to determine what is required to use them effectively, singly or in combination, is just beginning."

Hollnagel (1993) suggests that increasing system complexity leads to increasing task complexity. This leads to an increasing opportunity for malfunctions, which leads to an increasing number of unwanted consequences, which in turn leads to solutions that ultimately increase system complexity still further. He notes that this is sometimes humorously referred to as the "law of unintended consequences". The "law" states that the effort to fix things sometimes worsens the damage. While we are perhaps not there yet in this domain, the quantum increase in complexity of aircraft automation has unquestionably created new opportunities for human errors, both those that are inadvertent and those that result from deficient or "buggy" knowledge of the system being utilized.

I believe that automation complexity has been at least part of the problem in several incidents and accidents involving this new generation of aircraft (see Mulhouse-Habsheim, 1988; Bangalore, 1990; Strasbourg, 1992; Manchester, 1994; Paris, 1994; Toulouse, 1994). This is not to say that the automation has not functioned as it was intended to function; it has usually done exactly what its designers and programmers told it to do. The problem has been rather that the human operators have not understood its intended functioning and consequently have used it either beyond its capabilities or without regard to its constraints or rules. In another recent example of this problem, an A300-600 crashed at Nagoya, Japan, (1994) after the pilot flying inadvertently engaged an autopilot mode (TOGA), then provided opposing inputs to the airplane's autoflight systems which were counteracted by the autopilot when it was engaged to stabilize the flight path (Mecham, 1994).

The likelihood that all of the subtleties of such complex systems will be fully comprehended by pilots, even after considerable line experience with the systems, is not high (Wiener, 1989; Sarter and Woods, 1992); the likelihood that they will be understood after a few weeks of training is very small indeed. Uchtdorf and Heldt (1989), studying pilot understanding of the A310, indicated that a year or so of line experience may be required before pilots feel fully comfortable with the automation features—and this does not guarantee that they understand the entire system, only that they feel comfortable with enough of its modes to operate it effectively.

Brittleness

As software becomes more and more complex, it becomes more and more difficult to verify that it will always function as desired throughout the full operating range of the aircraft in which it will be placed. The reason for this is that there is an almost infinite variety of circumstances that can affect its operation, only a subset of which can be evaluated prior to certification even if they are known to the evaluators. Even then, there will be conditions, not thought of by the designers, which will inevitably arise at some point in the course of the airplane's operation. Brittleness is an attribute of a system which works well under normal or usual conditions, but which does not have desired behavior at or close to some margin of its operating envelope.

An example might be a pitch control system that was selected, reverted or defaulted to "vertical speed" mode while an airplane was climbing. The autoflight system would attempt to maintain constant vertical speed by gradually increasing pitch angle at the expense of airspeed, which would gradually decay to unsafe levels. One of several examples was an Aeromexico DC-10 (Luxembourg, 1979) whose autoflight system maintained a climb at constant vertical speed until the airplane stalled; the pilots were thought to have improperly programmed the autopilot for constant vertical speed instead of constant airspeed and subsequently failed to notice the decaying airspeed until too late to maintain control (Luxembourg, 1979). Another example would be a descent mode that involved idle power without safeguards to insure that such a descent could not continue all the way to the ground (see Bangalore, 1990), or an autothrust system that permitted power to remain at idle after descending onto the glide slope followed by a decrease in descent rate and a consequent decrease in airspeed to unsafe levels.

An example of brittle automation was present in the TCAS software when it was first implemented in civil transports. Under certain circumstances, the TCAS logic was able to recognize a hazard but was unable to advise a safe maneuver to resolve the conflict. When this occurred, the system simply "threw up its hands" and indicated to the pilot that there was a conflict but the system could not resolve it. FAA certification pilots raised serious objections to such a mode and the software was modified to exclude this problem, though at the expense of commanding much more drastic avoidance actions under such circumstances, which has caused greater altitude excursions. This problem has still not been fully resolved, though the TCAS system is no longer able to "walk away" from a conflict that requires a resolution advisory.

Yet another example of brittleness was seen, I believe, in the crash of a third-generation aircraft at Mulhouse-Habsheim after an experienced A320 pilot made a low pass over the airfield at minimum airspeed during an air show (1988). During his low pass, he descended below 100 feet above ground level and was unable to obtain enough power quickly enough to avoid trees at the far end of the runway. The automation prevented the airplane from stalling, but when the pilot descended below 100 feet, the automation disabled the angle of attack protection also built into the airplane's flight control system. This feature, which under any other circumstances would have applied full power and rotated the airplane into a climb, must be disabled to permit the machine to land.

Opacity

Three questions with which Wiener (1989) paraphrased the frequent responses of pilots to automation surprises, "What is it doing?", "Why's it doing that?", and "What's it going to do next?", may be indicative of either or both of two problems. One is a deficient mental model of the automation—a lack of understanding of how and why it functions as it does. This can be due to automation complexity, or to inadequate training, or both.

Another problem, however, is not that the operators do not understand the behavior being observed, but rather that the automation does not help them to understand by telling them what it's doing (and if necessary, why). Sarter & Woods (1994, p. 24) have observed that "The interpretation of data on the automation as process is apparently a cognitively demanding one rather than a mentally economical one given the 'strong and silent' character of the machine agent."

This problem represents a failure in communication or coordination between the machine and human elements of the system. It may occur because of inadequate displays, or because of deficient mental models, or because one or more human and/or machine components of the system do not understand the intent of another component at a particular point in time (See chapter 2). Regardless of the cause, the net effect is diminished awareness of the situation, a serious problem in a dynamic environment.

In earlier times, automation with less capability simply controlled the airplane's attitude and path; pilots could usually understand exactly what it was doing and how by observing the same instruments they used when they were controlling the airplane manually. Today's automation may use any combination of several modes to accomplish the objectives it has been ordered to reach. The information about what it is doing is almost always available somewhere in some form, though not necessarily in terms that the pilot can easily decipher. Why it is behaving in that manner is often not available except in the source code which controls it. What it is going to do next is often, though not always, unavailable on the instrument panel.

In short, as automation complexity increases, it becomes more difficult for the designer to provide obvious, unambiguous information about its processes to the monitoring pilot (even if the designer believes that the pilot needs this information and therefore tries to provide it). I call this "opacity". Others have referred to it as a lack of transparency; the two terms are synonymous in this context. Still others have used the term "lack of feedback" to refer to automation's failure to communicate effectively with the human operator (Norman (1989) has argued that the problem is not automation complexity, but lack of feedback to its operators).

As noted earlier, automation opacity may be deliberate: one sure way to keep the operator from intervening in a process is to deny him or her the information necessary to permit intervention in that process. Much more commonly, I think, it is the desire, and need, to avoid overburdening the operator with information that is not essential to the performance of his or her necessary functions (as those functions are understood by the designer). The capabilities of the computer and its screens have made it possible for designers to overwhelm pilots with information and data. Opacity at some level is required to avoid overwhelming the pilot with data. We know that the ability of pilots to assimilate information is context-dependent, and that when we provide more data without adequate consideration of context we simply make it less certain that they will attend to that which they really need to know. (Woods, 1993c).

The mode awareness problems cited by Sarter and Woods (1992) are in part due to opacity, though modes are always announced on mode annunciator panels. In part, the problem is one of salience: alphanumeric symbols must not only be attended to, but must be read, to convey information. Hutchins (1993) has attempted to ease this problem by using iconic representations, with some experimental success (see AWST, 1995b, for an illustration of this approach). Woods

(1994) speaks of "apparent simplicity, real complexity" as one of our more serious problems with advanced automation.

There have been some notable examples of the effects of opacity on advanced flight decks, though it must be noted that in most of the cases, the information could have been found had there been time to look for it. This tends to reinforce the notion that drowning the operator in information isn't a wise way to design a system. Perhaps the most notable recent example is an accident that occurred during an approach to Strasbourg (1992), when the flight crew inadvertently commanded the autopilot to descend at a 3300 ft/min vertical speed rather than at a 3.3° flight path angle (figure 7-2). The FCU display read "-33" instead of "-3.3", though smaller letters on the LCD display also read "HDG/VS" instead of "T/FPA" and the symbology on the primary flight display was also different in the two modes.

The fact remains that the pilots, already heavily loaded because of late ATC instructions and inexperience in the airplane, missed these discrepancies and descended into the ground several miles from their destination (Strasbourg, 1992). Changes have been made in later cockpits of this type to show "-3300" *vs.* "-3.3" in the hope of eliminating this possible source of confusion. Another example is the "TOGA" (takeoff/go-around) indication in the A300 at Nagoya (1994), which was initially missed by the pilot flying. It is worth noting that in both these cases, the flight crew provided the autoflight system with an incorrect indication of their intent (see chapter 2). The automation was performing in accordance with an acceptable, but inappropriate, instruction.

Literalism

A fourth attribute of automation (and of computers in general) could be described as its literalism or "narrow-mindedness" (Dekker, personal communication, 1994). Automation is able only to do exactly what it is programmed to do, as it did in the two cases cited immediately above. Human problem solvers are *creative* in their reasoning and their search for solutions to a problem. They can and will draw knowledge or evidence from any available source (either in memory or external to themselves: reference books, manuals, contact with others by radio, etc.), as long as that knowledge is relevant to the problem to be solved. Automation, on the other hand, is constrained by its instructions and as such is insensitive to unanticipated changes in goals and world states that may fall well within its usual operating range but were unanticipated by the designers of its software. It is in this sense that computer literality contrasts with brittleness; the latter term refers to undesired automation behavior at the margins of the operating envelope.

As an example of this, some flight management systems with vertical navigation capability will calculate an optimal descent point, based on cost factors, that is closer to a destination airport than pilots may wish for a smooth, gradual descent. The pilots may be unaware of the logic that drives this decision and action, but they learn through experience that they can "trick" the automation by programming a higher tailwind than is actually present. This false information causes the automation to begin the airplane's descent at an earlier point in time, thus achieving the pilots' desired ends. Human operators have always shaped the tools at hand to assist in accomplishing their objectives, but this shaping also increases task demand and cognitive workload.

Training

I indicated above that a fifth relevant factor is training. Let me preface this discussion by saying that if we cannot *show* the pilot what he or she needs to know in a given situation, then the pilot needs to *know* what (s)he needs to know. The only way this knowledge can be acquired is through education and training.

In the early 1960s, Trans World Airlines ordered its first DC-9 aircraft, also its first jets with a two-person crew complement. For a number of reasons, the airline decided to undertake a major revision of its training philosophy for the new airplane; its new, and highly successful, training program emphasized the specific behavioral objectives (SBOs) required of pilots, rather than the older (and until then universal) approach of "teaching the pilot how to build the airplane". Previous training programs had emphasized detailed knowledge of how airplane systems were constructed, how the various parts contributed to the whole, and based on this knowledge, how to operate them. The new approach provided significant economies in training time, which is expensive, and appeared to be fully as successful in teaching pilots how to operate the new airplanes without burdening them with more systems knowledge than they "needed to know". United Airlines later adopted a similar training philosophy, with similar success, and a training revolution was underway.

There has been continual pressure to minimize training time for the last 30 years. Pilots are paid virtually the same amount for training as for line flying, and when they are in training they are not flying trips that produce revenue for their company. There is no question that the SBO concept has been effective and efficient. Until recently, there has been no reason to question the concept.

The complexity of advanced automation, however, gives rise to questions about this approach to training. As indicated above, pilots must have an adequate mental model of the behavior of the equipment they are flying. I believe that our experience to date with advanced automated aircraft suggests that the training we now provide does not always give them a sufficient basis for forming such models. One example of this, in the MD-11, was that takeoff speeds could be incorrectly calculated by the FMS if engine anti-ice significantly warmed certain sensors. An error message was generated, but this message was inhibited by flap extension. If flaps were lowered at the beginning of taxi, before airflow over the sensors had time to cool them, the erroneous speeds were "locked in" and takeoff speeds were incorrectly displayed on the speed tape of the PFD.

There is no question about the growing complexity, and opacity, of automated systems in these aircraft. I believe that questions must be raised about whether training in *how to operate* these more complex and less transparent systems, as opposed to *how they operate,* is sufficient to provide pilots with the information they need when the systems reach their limits or behave unpredictably. One of the few disadvantages of digital computers as compared with their analog forebears is that analog devices usually degrade gradually and in a predictable manner, while digital computers usually fail abruptly and in an unpredictable way. If a pilot does not have an adequate internal model about how the computer works when it is functioning properly, it will be far more difficult for him or her to detect a subtle failure. We cannot always predict failure modes in these more complex digital systems, so we must provide pilots with adequate understanding of how and why aircraft automation functions as it does.

Comments about automation (Rudisill, 1994) make it plain that many pilots do not understand the reasons *why* aircraft and avionics manufacturers have built their automation as they have—and there are usually very good reasons, though they may not be known to the users of the automation. This, again, is a failure of training to explain how the system operates and why, rather than simply how to operate the system.

Other observed problems with aviation automation

Reliance on automation

Several examples have shown that pilots given highly reliable automated devices (and most are) will come, over time, to rely upon the assistance they provide. They rely upon the correct function of configuration warning systems, altitude alerters and other information automation to which they have become accustomed. When GPWS was first introduced, the nuisance warnings to which it was prone caused pilots to distrust it; conformance with its warnings had to be mandated by company standard operating procedures. Later models have proved themselves more trustworthy, and they are relied upon. Pilots have long been served reliably by autopilots and are sometimes less alert in monitoring their behavior than they should be, as evidenced by the failure to detect uncommanded roll inputs in a few early 747s (e.g., Nakina, 1991). Controllers likewise rely upon the data presented to them on their CRTs, even though much automation is required to present the synthetic images with which they work. They are surprised by occasional tag swaps and other misrepresentations of the data when they occur.

It does little good to remind human operators that automation is not always reliable or trustworthy when their own experience tells them it can be trusted to perform correctly over long periods of time. Many pilots have never seen these automation elements fail, just as many of them have never had to shut down a malfunctioning engine except in a simulator, and in any case, humans are not good monitors of infrequent events. The solutions to the "human failings" of trust, and of inattentiveness, must be found elsewhere. If we are to continue to provide operators with automation aids, we must make the system in which they are embedded more error tolerant so that such "failings" will not compromise safety of flight. In this area, there is much more we can do, even though much has been accomplished in the past.

Clumsy automation

Wiener (1989) coined this descriptor to denote automation that lightens crew workload when it is already low, but requires more attention and manipulation at times when workload is already high. He and others have cited today's flight management systems as having this characteristic, as I have noted in chapter 3. In the aviation context (though clumsy automation is by no means limited to aviation), it is in locations where traffic density is highest that ATC will most often have to change clearances to adjust to unexpected problems. It is also in these areas that aircraft are climbing or descending and preparing to land, maneuvers that also impose a higher task demand than does cruising flight at high altitude.

These are the phases of flight that involve the highest likelihood of conflicts with other aircraft and that therefore demand that as much attention as possible be devoted to scanning for such traffic. Programming a flight management computer requires that the non-flying pilot's attention be inside the cockpit and focused on the CDU for some period of time, an attentional requirement that directly competes with outside scanning and monitoring the activities of the flying pilot. It is for this reason that some captains do not permit reprogramming of the FMS when they are below 10,000 feet. They simply disengage the automation if necessary. This, however, removes many useful functions that the FMS can provide in this flight regime, and also makes unavailable machine knowledge regarding routes and altitude restrictions.

Though efforts have been made in the newest FMSs to lighten this burden, the FMS CDU is still a complex interface requiring both visual and cognitive attention; reprogramming, often required to meet ATC requirements during flight into terminal areas, can still be cumbersome. Flights into Los Angeles are often cited by pilots as perhaps the most taxing example. ATC often finds it necessary to reassign aircraft to a runway different from that originally intended, and a second reassignment is not uncommon later in the descent. Since these runways differ in position and are served by different navigation fixes and ILS transmitters, it is necessary to re-tune radios in older aircraft, and to reinstruct the FMS in newer machines. These tasks require appreciable "head-down" time, which prevents the non-flying pilot from maintaining a traffic watch and monitoring the flying pilot's actions while descending into what may well be the world's most heavily-traveled terminal airspace.

Digital *vs.* analog control

I have mentioned earlier the criticism by pilots of automation that makes it necessary for them to enter new navigation radio frequencies through alphanumeric keystrokes on the CDU rather than by turning rotary selectors as they did on older radio control units. Whether digital frequency entry actually takes longer has not been studied, to my knowledge, but I must confess that I share the bias of these pilots. At this time, new communications frequencies are still accessed through the older types of control heads, most of which also show and make available both the old and new frequencies. This is a help to pilots if they are unable to establish radio contact on a new channel, but communication frequencies also may be accessed in future through the FMS.

In the autoflight control wheel steering (CWS) mode, pilots manipulate their control columns to instruct the automation what rates of change are desired for a maneuver. Once placed in a certain attitude, the autopilot will hold that attitude until other control instructions are received. This "rate command" function is all accomplished digitally in newer aircraft, but the pilot perceives a graded input which produces a continuous response. In contrast, the "command mode" of the autopilot is controlled by providing it with digital numeric targets representing airspeed, desired altitude and heading, and sometimes desired vertical rate. In today's aircraft, these digital values can either be specified through rotary switches on the mode control panel in a manner quite similar to the selection of new radio frequencies in older aircraft, or by digital numeric input to the FMS.

The control wheel steering mode can be a trap, as was evidenced in a DC-10 incident in which, after a close-in turn to final approach, the flying pilot, who was heavily loaded, forgot that he was in that mode and incurred a tail strike during the subsequent landing (NASA ASRS, 1976a). Some carriers disable the control wheel steering mode, and some airframe manufacturers believe it to be an unnecessary function in most of their aircraft. It is the normal mode of autopilot control in Boeing 737-200 series aircraft, however; it permits quick tactical changes to flight path, and it therefore represents a potentially useful intermediate between fully manual and fully automatic flight. It is shown as "assisted control" in my control and management continuum (see chapter 8). In at least one new airplane, the MD-11, all longitudinal control is carried out through the CWS function of the autoflight system, and full-time CWS for lateral (roll) control is also available as a customer-specified option.

Fully autonomous automation

Some automation elements have been essentially autonomous for a long time. No pilot would think of hand-flying a jet throughout cruise, as one instance. Many airlines require the use of the autobraking function for all landings, and autospoilers are also used routinely. Several other automatic functions that are used at all times have been mentioned in chapters 3 and 4. Despite this, concern has been expressed in various quarters about more complex functions that are now essentially autonomous, several of which can be "turned off" only with difficulty or not at all.

Among these functions are the full-time "envelope protection" system in the A320, which in effect prevents pilots from exceeding certain flight parameters under any circumstances. This could more accurately be called an "envelope limiting" system. Several current and planned aircraft have systems that fulfill similar functions, though in a somewhat different manner. The MD-11's automatic systems control computers, as noted above, will reconfigure aircraft subsystems autonomously if they sense specific malfunctions in those systems. Systems such as these give rise to questions concerning pilot authority and responsibility. These questions are discussed in more detail in chapter 8.

Skill degradation

One potentially serious problem in human-machine systems with highly capable automation is a loss of certain skills by the human when the automation routinely performs tasks that require such skills. This effect has been observed in numerous contexts. It may be due largely to lack of practice of the particular skill by the human operator, though in certain contexts, other factors may play a part.

Psychomotor skill decrements were observed by pilots transitioning from copilot positions in the DC-10, a fairly automated airplane, to command positions in less automated aircraft such as the

727. After some failures to complete this transition, air carrier training personnel suggested to pilots approaching transition that they should forego the use of the automation for a couple of months prior to transition, in order to obtain more practice in manual control. The pilots took this advice and were able thereafter to complete transition training without difficulty. Note, in this example, that the pilots coming to transition all had extensive flying experience in older, relatively unautomated, aircraft. Their problem was to reacquire skills which they had already possessed in adequate measure before their transition to the more automated DC-10.

The advent of the new generation of highly automated aircraft, and the replacement of the older machines by such airplanes, implies that at some point in the future, some pilots may begin their airline careers flying as first officers on advanced aircraft that incorporate envelope protection and a variety of other control automation. Such automation may include limits on rate of roll, bank angle, pitch rate as a function of speed, gust alleviation and other functions.

Will pilots who have never had to acquire the finely-tuned manual skills which older pilots take for granted be able to demonstrate such skills at an acceptable level if they must transition to another aircraft that lacks these advanced features? Similarly, will they have learned the cognitive skills necessary for unassisted navigation if the flight management software fails? Finally, and perhaps most important given the high reliability of today's aircraft, will they acquire the judgmental skills and experience that alone can enable them to make wise decisions in the face of uncertainty or serious mechanical or environmental problems? At this point, no one knows the answers to such questions, but we do know that it is these skills, collectively called "airmanship", that provide the last line of defense against catastrophes in aviation operations.

Similar questions can be asked about some air carriers which effectively require their pilots of advanced aircraft to utilize the automation on a full-time basis. *Flight International,* in its Letters columns, carried a brisk debate on this topic early in 1993; "Excessive reliance on equipment to help pilots fly 'smarter and safer' has become institutionalized to the point of becoming dangerous." (Hopkins, 1993, p. 40) "... I remember being admonished by the chief pilot for daring to hand-fly a raw-data standard instrument departure, and, worse still, for practising enroute VOR tracking by hand flying for 10 min in the cruise." (Laming, 1993, p. 140).

Some operators suggest to their pilots that they should exercise as many options as possible, and that they should fly at each level of automation on a periodic basis, to remain familiar with the systems and to maintain proficiency. Delta Airlines has stated these goals formally in its statement of automation philosophy: "Pilots must be proficient in operating their airplanes at 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" (Byrnes and Black, 1993). Many airline pilots make it a point to fly at least part of each flight segment manually to maintain their skills, regardless of the policies and preferences of their carriers.

Recall that similar questions were raised with respect to the ability of air traffic controllers, trained only in a full radar environment, to transition to procedural control of air traffic in the event of a massive radar failure. The ability of the FAA System Command Center to offload controllers during such failures has lessened this concern to some extent, but it is still possible for controllers to be grossly overloaded by system contingencies such as occurred after ATC communications and data transfer were suddenly shut down by a massive failure of communications facilities in New York (Lee, 1992).

Crew coordination

Wiener (1993) has discussed crew coordination and resource management in the context of automated aircraft. In his extensive cockpit observations in advanced aircraft (Wiener, 1989), he noted several crew coordination issues (pp. 177-178):

- "Compared to traditional models, it is physically difficult for one pilot to see what the other is doing (on the CDU)...Though some carriers have a procedure that requires the captain (or pilot flying) to approve any changes entered into the CDU before they are executed, this is seldom done; often he or she is working on the CDU on another page at the same time...

- "It is more difficult for the captain to monitor the work of the first officer and to understand what he is doing, and vice versa.

- "Automation tends to induce a breakdown of the traditional (and stated) roles and duties of the pilot-flying versus pilot-not-flying and a less clear demarcation of 'who does what' than in traditional cockpits. In aircraft in the past, the standardization of allocation of duties and functions has been one of the foundations of cockpit safety...

- "There is a tendency for the crew to 'help' each other with programming duties when workload increases. This may or may not be a good thing...but it clearly tends to dissolve the clear demarcation of duties..."

Costley, Johnson and Lawson (1989) found in flight observations in 737 and 757 aircraft that less communication occurred in more advanced cockpits. Wiener interprets these findings in terms of extremely low workload during cruise in advanced automated aircraft, and expresses concern "because of the presumed vulnerability of crews to boredom and complacency". He concludes that "Field studies of the introduction of the new-technology aircraft lead me to believe that the demands on the pilot in the new aircraft are qualitatively different from those in the traditional models..." His findings agree with others reported here: that our traditional models of the behavior of competent air transport pilots may be insufficient guides to behavior in newer aircraft, because the machines themselves are, in certain respects, qualitatively different from older aircraft. New models that emphasize the increased cognitive loading on pilots are needed to guide our designs and implementation in the future.

We may have been shielded to some extent from problems in this realm by the very high experience levels of many first officers, as well as captains, in today's system. Many former captains with extensive command experience are now flying as copilots after having been laid off by defunct or bankrupt carriers. This will lessen during coming years, however.

Monitoring requirements

Leaving aside issues of transparency or opacity, pilots (and in the near future, air traffic controllers as well) must monitor flight progress closely, for others, human and machine, are monitoring as well, to an extent unprecedented in the history of the industry. One problem inherent in automation is that pilots cannot usually detect that it not going to do what they expected it to do until after it has failed to do it. It is only after automation has "misbehaved" that operators can detect its "misbehavior" and correct it. Unfortunately, when this occurs in aviation, the aircraft may already be in a position from which rapid reactions may be necessary to return it to nominal conditions.

During an idle power descent, an airplane may descend 50 feet during each second it takes the crew to recognize an anomaly, decide to take action, make a control input and wait for an appropriate response. Aircraft are separated by only 1000 feet vertically below 29,000 feet; deviations of 500 or more feet are not uncommon after an autopilot has failed to capture an altitude. Such a deviation can be easily observed by air traffic control personnel and, if there is a conflict, by ATC automated conflict alert software. If the deviation is reported, pilots may face disciplinary or enforcement action from FAA.

For these reasons as well as others, pilots must closely monitor the behavior of their automated systems, but if an anomaly occurs, they must sometimes take very prompt action.

Present automation (except the ubiquitous altitude alerting system) provides no predictive or premonitory warning that a failure is likely to occur in the immediate future; such information would give pilots time to prevent, rather than correct, the problem. Fortunately or unfortunately, flight path automation is reliable enough so that pilots may be tempted to relax their guard on the (justified) assumption that it will almost always behave correctly. Moray, Lee and Hiskes (1994) have even suggested that this is the logical and appropriate strategy for pilots to adopt, since it is rare for such malfunctions to occur; thus, pilots are better advised to spend more time monitoring aspects of their flight that involve more uncontrolled variability.

Without question, the most effective monitoring of pilots flying is by a non-flying pilot in the same cockpit. This redundancy is absolutely critical. The vast majority of errors in the cockpit are detected, announced and corrected without adverse consequences, often before any sort of anomaly can occur. When this fails, air traffic controllers often detect and warn of small anomalies, permitting the pilot to correct them at an early stage. All of this cross-monitoring assumes that the monitoring agents understand the intent of the monitored agents, as they usually do (see chapter 2). Newer automation could do more than it has thus far been called upon to do to strengthen still further the error tolerance of the aviation system (chapter 4).

Automated system "navigation" problems

Though manufacturers of the latest flight management systems have gone to considerable effort to simplify the operation of these systems, they are still exceedingly complex and all interaction with them must be through several displays brought up sequentially on a single small screen containing a large amount of alphanumeric information. As more functions have been implemented, more and more screens have been designed, each requiring serial access by the operator (see figure 3-29). In today's system, a great deal of information must be accessed through a very small "keyhole". As a consequence, "navigating" among the many screens has become complicated. This requirement imposes yet another cognitive burden on operators, who must remember enough of the FMS architecture to recall how to get to specific information when it is needed.

One method that designers have utilized to lessen the memory burden is to increase the number of modes in the FMS itself. This simplifies the navigation problem within the FMS but increases the requirement to remember the various modes and what each is used for. As these remarkable devices become still more capable, this cognitive burden imposed by the need for mode awareness can be expected to increase, unless a different approach is taken to their design (Woods et al., 1994).

Data overload

Automation and the glass cockpit have increased considerably the amount of information available to pilots. The information is of much higher quality than was available in the past, a true blessing for it decreases ambiguity and uncertainty, but the quantity imposes much higher attentional demands than in the past. The flight navigation displays on today's panels integrate a great deal of data into an integrated, clear and intuitive representation of the aircraft's location, directional trend and chosen course—but this screen may also contain data regarding severe weather, wind shears, waypoints, airfields, obstructions and other traffic, almost none of which was explicit in earlier aircraft. Depending on the circumstances of the flight, any part or all of this information may be relevant. Much of it, fortunately, can be turned off when it is not needed. Nonetheless, the pilot must now manage a potential glut of information, where in the past, he simply had to wonder about it.

Pilots have often demonstrated that they want access to *all* information that may be relevant to their decision processes in flight, and that they are willing to accept a higher workload to deal with it. Unfortunately, as Fadden has noted, if they have too much information, it become less certain that they will be able to prioritize and integrate the data in time to address the problem which is most important. Particularly when virtually all information is visual in form, this is a serious potential problem for designers. Some have suggested adaptive displays which can be automatically decluttered as the pilot becomes more heavily loaded, but this poses other problems relating to operator authority (chapters 8 and 13).

Comment

I have tried here to summarize some of the attributes of contemporary aircraft automation that appear to have been associated with problems in pilot cognitive behavior. Few of these problems represent failures of the automation as such; most represent either conceptual failures at the design or operator level, or problems in the implementation of these concepts. As machines grow more complex and difficult to understand, operators are more likely to err in their operation, so the net effect of these problems is often seen as human error at the sharp end. As Reason (1990) and Woods et al. (1994) have pointed out so clearly, to say this and stop is simply to *insure* that the serious latent factors that lie behind human error will go unnoticed, and that attempts to insulate the system against such errors in the future will not get at the systemic and conceptual problems which cause most errors.

It is for this reason that I have tried, in this chapter, to generalize from the particular problems cited in earlier chapters to the conceptual issues that appear to me to underlie many or most of those problems. These issues, I believe, are the "latent factors" which we must attack if we are to make aviation automation more human-centered.

As I said in the foreword, it is necessary that we look not only at the human or at the machine, but at the *system,* if we are to correct system faults or to design and implement more effective systems in the future. If we do not take this approach, our present systems, as tightly integrated as they are, will simply acquire more layers of "band-aids" as we attempt to solve specific problems one by one, without considering the effects of those solutions on the system as a whole, or on the competing demands upon both pilots and controllers. I am frankly worried that this may be what we are doing in our present attempts to improve TCAS, a very tightly coupled system, by adding more and more software to lessen nuisance warnings while trying to maintain and extend the basic usefulness of the deviceby placing new requirements on it.

8. Human and machine roles: responsibility and authority

Introduction

Much industrial automation has been implemented on the implicit assumption that machines could be substituted for humans in the workplace. The Fitts (1951) list of functions that are best performed by humans and those best performed by machines exemplifies this concept. Jordan (1963), among others, has proposed that humans and machines should be considered as *complementary*, rather than competitive. The design and operation of the modern transport airplane exemplifies the concept of complementarity, but in certain respects its automation very much exemplifies the principle of the interchangability of parts. There are good reasons for this based on the historical precedents that have come down to us from earlier attempts to assist the pilot, but we must question whether we should still be designing and operating machines in that manner and whether a somewhat different approach could solve some of the problems we now perceive in aviation systems.

Today's aircraft automation controls an airplane more or less as the pilot does (though most automation has less control authority in order to provide the pilot with time to overpower or disable it should that become necessary; this is a certification requirement). It navigates as the pilot does, or would if pilots could carry out in real time the complex calculations now performed by the computer. It operates the systems as the pilots do, or would do if they do not forget or overlook any of the procedural steps. In the near future, it will communicate with ATC, accept and execute ATC clearances, and report its location when not under radar coverage, just as pilots do now. Some have noted that automation usually performs all of these functions correctly, that it does not become tired or distracted or bored or irritable, that it often "speaks" more clearly and succinctly than pilots do, that its data stream is easily comprehended by ATC computers in any nation, and that it does all these things without complaints. They have concluded that automation is as capable as the human for these functions, and some air carriers have mandated that it be used whenever possible. Are these "parts" interchangeable? That is the subject of this chapter.

The pilot as controller and manager

It should be clear from chapters 3 and 4 that pilots may play any of a variety of roles in the control and management of a highly automated airplane. These roles range from direct manual control of flight path and aircraft systems to a largely autonomous operation in which the pilot's active role is minimal. This range of allocation of functions between human and machine can be expressed as a control-management continuum, as shown in figure 8-1.

None of today's aircraft can be operated entirely at either end of this spectrum of control and management. Indeed, an airplane operated even by *direct manual control* may incorporate several kinds of control automation such as yaw dampers, a Mach trim compensator, automated configuration warning systems, etc. Conversely, even remotely piloted vehicles are not fully autonomous; the locus of control of these aircraft has simply been moved to another location.

Most transport flying today is *assisted* to a greater or lesser extent, by hydraulic amplification of control inputs and often by computer-implemented flight control laws. Flight directors, stability augmentation systems, enhanced displays, and in newer aircraft various degrees of envelope protection, assist the pilot in his or her manual control tasks. To some extent, pilots can specify the degree of assistance desired, but much of it operates full-time and some of it is not intended to be by-passed. The pilot remains in the control loop, though it is an intermediate rather than the inner loop (chapter 3, figure 3-12).

VERY HIGH ← LEVEL OF AUTOMATION → VERY LOW

MANAGEMENT MODE	AUTOMATION FUNCTIONS	HUMAN FUNCTIONS
AUTONOMOUS OPERATION	Fully autonomous operation Pilot not usually informed System may or may not be capable of being disabled	Pilot generally has no role in operation Monitoring is limited to fault detection Goals are self-defined; pilot normally has no reason to intervene
MANAGEMENT BY EXCEPTION	Essentially autonomous operation Automatic reconfiguration System informs pilot and monitors responses	Pilot informed of system intent; Must consent to critical decisions; May intervene by reverting to lower level of management
MANAGEMENT BY CONSENT	Full automatic control of aircraft and flight Intent, diagnostic and prompting functions provided	Pilot must consent to state changes, checklist execution, anomaly resolution; Manual execution of critical actions
MANAGEMENT BY DELEGATION	Autopilot & autothrottle control of flight path Automatic communications and nav following	Pilot commands hdg, alt, speed; Manual or coupled navigation; Commands system operations, checklists, communications
SHARED CONTROL	Enhanced control and guidance; Smart advisory systems; Potential flight path and other predictor displays	Pilot in control through CWS or envelope-protected system; May utilize advisory systems; System management manual
ASSISTED MANUAL CONTROL	Flight director, FMS, nav modules; Data link with manual messages; Monitoring of flight path control and aircraft systems	Direct authority over all systems; Manual control, aided by F/D and enhanced navigation displays; FMS is available; trend info on request
DIRECT MANUAL CONTROL	Normal warnings and alerts; Voice communication with ATC; Routine ACARS communications performed automatically	Direct authority over all systems; Manual control utilizing raw data; Unaided decision-making; Manual communications

VERY LOW ← LEVEL OF INVOLVEMENT → VERY HIGH

Fig. 8-1: The control/management continuum for pilots

Whether pilots of limited experience should be required by to have and demonstrate direct manual control ability in today's airplanes, which incorporate highly redundant automated control assistance, is a reasonable question, but beyond the scope of this document. Airbus has rendered this issue moot to some extent by providing *shared control* as the A320's basic control mode. Pilots' control inputs are considerably modified and shaped by the flight control computers; envelope limitations prevent them from exceeding pre-determined parameters. In this airplane, pilots are provided with considerable assistance even during control failure modes; true manual flight capability is limited to rudder control and stabilizer trim and is designed only to maintain controlled flight while the automated systems are restored to operation. Under all normal circumstances, the aircraft automation is responsible for much of the inner loop control, though control laws are tailored to respond in ways that seem natural to the pilot. In the MD-11, a combination of longitudinal stability augmentation and control wheel steering is in operation at all times; roll control wheel steering is available as an option.

When an autopilot is used to perform the flight path (and/or power) control tasks, the pilot becomes a manager rather than a controller (this is also true to some extent of the shared control option). The pilot may elect to have the autopilot perform only the most basic functions: pitch, roll and yaw control (this basic autoflight level is no longer available in all systems); he or she may command the automation to maintain or alter heading, altitude or speed, or may direct the autopilot to capture and follow navigation paths, either horizontal or vertical. This is *management by delegation,* though at differing levels of management, from fairly immediate to fairly remote. In all cases, however, the aircraft is carrying out a set of tactical directions supplied by the pilot. It will not deviate from these directions unless it is incapable of executing them.

As always, there are exceptions to the generalizations. The 757/767 will not initiate a programmed descent from cruise altitude without an enabling action by the pilot. Other modern flight management systems require that the pilots provide certain inputs before they will accept certain conditional instructions. *Management by consent* describes a mode of operation in which automation, once provided with goals to be achieved, operates autonomously, but requires consent from its supervisor before instituting successive phases of flight, or certain critical procedures. The consent principle has important theoretical advantages, in that it keeps pilots involved and aware of system intent, and provides them the opportunity to intervene if they believe the intended action is inappropriate at that point in time.

This management mode may become more important as "smart" decision-aiding or decision-making systems come into use (see chapter 13). A protracted period of close monitoring of these systems will be necessary; requiring consent is one way to monitor and moderate the potential influence of these systems. While management by consent is an attractive option worthy of further exploration, it must be *informed* consent. More fundamental human factors research is needed to identify how to implement it without the consent becoming perfunctory.

Management by exception refers to a management-control situation in which the automation possesses the capability to perform all actions required for mission completion and performs them unless the pilot takes exception. Today's very capable flight management systems will conduct an operation in accordance with pre-programmed instructions unless a change in goals is provided to the flight management system and is enabled by the pilots. Such revisions occur relatively frequently when air traffic control requires changes in the previously-cleared flight path, most often during descent into a terminal area. Some FMS lateral and waypoint management tasks now operate by exception.

The desire to lighten the pilot's workload and decrease the required bandwidth of pilot actions led to much of the control automation now installed in transport aircraft. The more capable control and management automation now in service has certainly achieved this objective. It also has the capacity, however, to decrease markedly the pilot's involvement with the flying task and even with the mission. Today's aircraft can be operated for long periods of time with very little pilot activity. Flight path control, navigation, and in some aircraft subsystems management are almost entirely automatic. The capable, alert pilot will remain conversant with flight progress despite the low level of required activity, but even capable, motivated pilots get tired, lose their concentration and become diverted, or worry about personal problems unrelated to the flight. A critical task of the designer is to find ways to maintain and enhance pilot involvement during operation at higher levels of automation.

This is less simple than it sounds, for pilots will both resent and find ways to bypass tasks that are imposed merely for the purpose of ascertaining that they are still present in the cockpit. Tasks to maintain involvement must be flight-relevant or even flight-critical, and equally important, must be perceived by pilots to be relevant. Designing pilot involvement into highly automated systems will not be easy but must be accomplished to minimize boredom and complacency, particularly in very long range aircraft which spend many hours in overwater cruise. The progress of avionics, satellite navigation and communications, and data link will very likely have an opposite effect unless this uniquely human factor receives more consideration than it has to date.

Fully autonomous operation denotes operation in accordance with instructions provided by system designers; no attention or management is required of the pilots. Until recently, relatively few complex systems operated fully autonomously. With the introduction of the A320 and MD-11, however, major systems operate in this way.

A fundamental question is how wide a range of control and management options should be provided. This may well vary across functions; indeed, pilots often prefer to operate using a mix of levels, for example controlling thrust manually while managing the autopilot and using the flight director to monitor navigation. Pilot cognitive styles vary; their skill levels also vary somewhat as a function of the amount of recent flying they have done, how tired they are, etc. These factors lead me to argue that a reasonable range of options must be provided, but widening that range is expensive in terms of training time and time required to maintain familiarity with a broader spectrum of automation capabilities as well as in terms of equipment costs.

One possible way to keep pilots involved in the operation of an aircraft is to limit their ability to withdraw from it by invoking very high levels of management. Another, perhaps preferable way is to structure those higher levels of management so that they still require planning, decision-making and procedural tasks. The use of a management by consent approach, rather than management by exception, could be structured to insure that pilots must enable each successive flight phase or aircraft change of status, as an instance. It has been suggested by one air carrier that long-haul pilots should be given the tools with which to become involved in flight planning for maximum economy on an ongoing basis; this is another approach to maintaining higher levels of involvement, but it is presently being implemented as a dispatcher function.

The role of the air traffic controller

When a more highly automated ATC system is implemented, its computers will be able to search for traffic conflicts and to provide at least decision support in resolving them. This is the foundation of the FAA's automated en route air traffic control system (formerly referred to as AERA), and it is a key feature of the "free flight" proposal (chapter 6). Direct ATC computer-to-flight management computer data transfers, and probably direct "negotiations" between these computers, will likewise be a part of such a system, which opens the possibility of direct control of air traffic by ATC automation without involvement of either controllers or pilots.

I have discussed a control/management continuum in terms of pilot roles in an automated system. A similar construct can be proposed for air traffic controllers and their automation (figure 8-2), though it should be kept in mind that air traffic controllers actually *direct* and *coordinate* the movements of aircraft; only pilots control them. In this respect, the controller's task is fundamentally different from that of the pilot.

As in the case of pilots, a very broad range of roles is theoretically possible, ranging from unassisted procedural control without visualization aids such as radar all the way to autonomous machine control of air traffic. Indeed, the former option will probably continue in some parts of the world, even while other areas adopt advanced automation. The important point is that the role of the controller, and probably the involvement of the controller in the details of the operation, can vary greatly, from absolute direct authority over the entire operation to a relatively passive oversight function in which air traffic control tactics are purely the computer's task.

Whether such a broad range of roles is desirable is another matter entirely. The first principles of human-centered automation indicate that involvement is necessary if the human operator is to remain in command of the operation. I question the controller's ability to remain actively involved for very long if he or she has no active role in the conduct of an almost entirely automated process. On the other hand, *some* range of options should be permitted, to account for differences in cognitive style, variations in workload, and a wide range of controller experience levels.

VERY LOW ← LEVEL OF AUTOMATION → VERY HIGH

VERY LOW ← LEVEL OF INVOLVEMENT → VERY HIGH

MANAGEMENT MODE	AUTOMATION FUNCTIONS	HUMAN FUNCTIONS
AUTONOMOUS OPERATION	Fully autonomous operation Controller not usually informed System may or may not be capable of being bypassed	Controller has no active role in operation Monitoring is limited to fault detection Goals are self-defined; controller normally has no reason to intervene
MANAGEMENT BY EXCEPTION	Essentially autonomous operation Automatic decision selection System informs controller and monitors responses	Controller is informed of system intent May intervene by reverting to lower level
MANAGEMENT BY CONSENT	Decisions are made by automation Controller must assent to decisions before implementation	Controller must consent to decisions Controller may select alternative decision options
MANAGEMENT BY DELEGATION	Automation takes action only as directed by controller Level of assistance is selectable	Controller specifies strategy and may specify level of computer authority
ASSISTED CONTROL	Control automation is not available Processed radar imagery is available Backup computer data is available	Direct authority over all decisions Voice control and coordination
UNASSISTED CONTROL	Complete computer failure No assistance is available	Procedural control of all traffic Unaided decision-making; Voice communications

Fig. 8-2: A control/management continuum for air traffic controllers

Human and machine roles

Present aircraft automation does not plan flights, though it is able to execute them and to assist in replanning (e.g., after an engine failure). It cannot configure an airplane for flight or start the engines. It knows with great precision where runways are, but not how to get to them from a gate, nor from a runway turnoff to a gate after landing. Flight control automation is locked out during the takeoff sequence, though thrust is under automatic control from early in the process in some aircraft. Automation controls neither the landing gear nor the flaps during takeoff and approach. From shortly after takeoff until the airplane touches down at a destination, however, automation is fully capable of executing all the required elements of a flight, though it does not, at this time, accomplish the checklists required during the process.

There is, of course, no reason why automation could not perform taxi maneuvers, though implementing this function would be extremely costly. There is absolutely no reason why landing gear and flap actuation could not be automatic. The few aspects of subsystem management that are still manual in some of the newer aircraft (e.g., the MD-11) could certainly be automated as well. Why, then, have they not been? The answer does not lie in the inadequacies of technology, but in the intricate domains of sociology, psychology and politics.

Pilots are perceived to be essential because passengers are not willing to fly in an autonomous, unmanned airplane—though millions entrust themselves every day to the Bay Area Rapid Transit, the Washington Metro, and other mass transit systems in which the locus of control has shifted from the operator station to a central control room. The trains on these systems do carry a human operator, but under normal circumstances, the operator does not operate the vehicles and is proscribed from doing so. Airport "people-movers", some of which travel over several miles of dedicated track or roadway, do not have an on-board operator; the voice announcements are recorded or synthetic. Note that these systems are *not* fully autonomous; humans control them, as they always did, but the control is supervisory and remote (Sheridan, 1984).

The flight environment, however, is far more complex than that of a modern light-rail system, and many of the variables are not under the control of system managers. Pilots are essential because they are trained to compensate for unexpected variability. Automation does fail, and unlike surface vehicles, airplanes cannot simply come to a stop while the automation is fixed. Once in flight, they must be guided to a landing. In other words, pilots and air traffic controllers are essential because they are able to make good decisions in difficult situations. We have not yet devised a computer that can cope with the variability inherent in the flight and air traffic environment.

The human role, then, is to do what the automation cannot do: to plan, to oversee, to reflect and make intelligent decisions in the face of uncertainty, and to make passengers (and air carrier management, and the FAA) feel comfortable about air transportation.

Responsibility and authority

If a controller fails to maintain separation because of a tag swap or a radar outage, is the computer "grounded"? No; the controller remains responsible for traffic separation regardless of the circumstances. There may be mitigating circumstances, but this responsibility cannot be delegated.

If an automated airplane gets lost and lands at the wrong airport, or encounters severe turbulence and incurs structural damage, or runs out of fuel and crash lands, or violates regulations for whatever reason, is the flight management computer held to account? Not to my knowledge. The pilot, not the autopilot, is in command of the flight and is responsible for its safe conduct.

Does the pilot have the authority required to fulfill this responsibility? What responsibility, and what authority, does the pilot have in today's system and today's airplanes? It is a maxim of military command that authority can be delegated by a commander. Responsibility for the outcome cannot be delegated to others. It remains with the commander.

These precepts are extremely important in aviation. Though aviation involves a widely distributed system in which no individual can get the job done by himself, the roles of all the humans in the system come together in the process of flight. In that process, the pilot and dispatcher share responsibility for the plan which guides the flight. The pilot is solely responsible for its safe execution, and the air traffic controller is solely responsible for keeping the flight safely separated from other air traffic.

Part 91.3 of the Federal Aviation Regulations describes the "responsibility and authority of the pilot in command". It is brief and succinct:

(a) The pilot in command of an aircraft is directly responsible for, and is the final authority as to, the operation of that aircraft.
(b) In an in-flight emergency requiring immediate action, the pilot in command may deviate from any rule of this part to the extent required to meet that emergency.
(c) Each pilot in command who deviates from a rule under paragraph (b) of this section shall, upon the request of the Administrator, send a written report of that deviation to the Administrator.

This regulation confers upon the pilot essentially unlimited authority to depart from the accepted rules for the conduct of flights if that pilot believes that an emergency situation exists. Under his emergency authority, the pilot is permitted to request whatever assistance is necessary, to declare for his flight absolute priority for any maneuver, flight path or action, and to take whatever steps are necessary, in his view, to protect his passengers. His or her decisions may be questioned afterward, but the authority remains and is recognized without question at the time.

It is a matter of record that pilots have sometimes not used their emergency authority when hindsight says they should have done so. Some situations, like the fuel emergency that led to the loss of Avianca flight 107 (Cove Neck, NY, 1990), seem obvious to anyone, though the Board raised the question of whether the pilot's very limited English competency may have permitted him to think that he had made such a declaration when the proper enabling words ("Mayday" or "Emergency") had not been used. In other cases, pilots have been inhibited by fear of the paperwork and questions that inevitably follow such a declaration (though onerous questions after a safe landing are a great deal easier to walk away from than an aircraft accident).

Pilots, then, have as much authority as they need to permit them to fulfill their responsibility for flight safety—or do they? Does a pilot whose control authority is limited by software encoded in the flight control computer have full authority to do whatever is necessary to avoid an imminent collision, or ground contact? U.S. transport aviation involving jet aircraft was scarcely 4 months old in 1959 when a Boeing 707 entered a vertical dive over the North Atlantic Ocean. The pilots recovered from the dive and landed the airplane safely at Gander, Newfoundland. Post-flight inspections revealed severe structural damage of the wing and horizontal stabilizer, but all the passengers survived and the airplane flew again after major repairs (NTSB, 1960). Would this have been possible if flight control software had limited the forces that could be applied to levels within the normal flight envelope of the airplane?

Limitations on pilot authority

In the A320/330/340 series aircraft, the flight control system incorporates envelope limitation. Certain parameters (bank angle, pitch or angle of attack) cannot be exceeded by the pilot except by turning off portions of the flight control computer systems or flying outside their cutoff values, as was done during the low-altitude flyover prior to the Mulhouse-Habsheim accident (1988). Predetermined thrust parameters also cannot be exceeded.

Systems designed for autonomous operation pose serious philosophical questions with respect to pilot authority as well as pilot involvement. These questions arose first in the design of fighter aircraft and were discussed succinctly in an unsigned editorial in *Flight International* (1990). The American F-16 fighter's fly by wire control system incorporates "hard" limits which "preserve the aircraft's flying qualities right to the limit of its closely defined envelope" but do not permit the pilot to maneuver beyond those limits. The *Flight* editorial pointed out that "There is, however, another approach available: to develop a 'softer' fly-by-wire system which allows the aircraft to go to higher limits than before but with a progressive degradation of flying qualities as those higher limits are approached. It is this latter philosophy which was adopted by the Soviets with fighters like the MiG-29 and Sukhoi Su-27. It is not, as Mikoyan's chief test pilot...admits, necessarily a philosophy which an air force will prefer." (He) says, however: "Although this...approach requires greater efforts...it guarantees a significant increase in the overall quality of the aircraft-pilot combination. This method also allows a pilot to use his intellect and initiative to their fullest extent." (Farley, 1990) The "softer" approach has been taken in the MD-11 and Boeing 777, which permit pilots to override automatic protection mechanisms by application of additional control forces. The flying qualities are degraded in this mode, but the pilot retains control authority. (The MD-11 also has "soft" power control limits, while the 777 incorporates "hard" limits on engine power, for reasons I do not understand.)

Though civil aircraft do not face the threat posed to a fighter under attack whose maneuverability is limited, their pilots do on occasion have to take violent evasive or corrective action, and they may on rare occasions need control or power authority up to (or even beyond) normal structural and engine limits to cope with very serious problems. The issue is whether the pilot, who is ultimately responsible for safe mission completion, should be permitted to operate to or even beyond airplane limits when he or she determines that a dire emergency requires such operation. The issue will not be simply resolved, and the rarity of such emergencies makes it difficult to obtain empirical support for one or the other philosophy. Nonetheless, the issue is a fundamental one.

The MD-11 incorporates angle of attack protection, but its limits can be overridden by the pilot, as can the limits of the autothrust system. In the MD-11, however, aircraft systems operate autonomously to a considerable degree. Failure detection and subsystem reconfiguration are also autonomous if the aircraft system controllers (ASC) are enabled (the normal condition). Any system may be operated manually, though the protections provided by the ASC systems are not available during manual operation.

Comment

The increasing capabilities of advanced automation pose a severe temptation to new aircraft design teams. They can decide that the safety of the airplane makes it important that they limit the authority of the pilots, and they can implement that limitation very easily in airplane software. Or they can match the software limits to the structural parameters of the airplane insofar as possible, though this is an approach that has not yet been implemented. Whether they have considered all of the circumstances that may confront a pilot in line operations is a question that may only be answered when totally unforeseen circumstances arise, perhaps years after the airplane has left the factory.

Given that pilots bear the ultimate responsibility for the outcome, it would seem that their authority to do whatever is necessary to insure that the outcome is favorable should be foreclosed only with extreme reluctance. The concept of "soft limits" on control authority may represent one useful and constructive approach to this dilemma. What is important is to realize how easily the pilot's authority can be compromised, given the technologies that are now available. It may take only a line or two of software and may or may not be known or obvious to the pilot.

The same dilemma will face us in the near future with respect to air traffic controllers, as the tools they use are automated in the AAS. This question has not received the attention it deserves, and the rarity of situations that force the issue makes it very difficult to provide good data in support of any extreme position. It is necessary that we realize, however, that issues involving such rare events must sometimes be handled on the basis of the best available *a priori* reasoning. The views of pilots and controllers on this issue are clear: if they have the responsibility, they want the authority necessary to exercise it.

9. Integration and coupling in the future aviation system

Introduction

The technical challenge of developing advanced automated aircraft pales in the face of the challenge posed by the need for a highly integrated air traffic management system. Simply developing a set of agreed-upon standards for such a system has already taken five years, and the task is far from finished. FAA, ICAO and other organizations must produce standards and requirements for data link technologies, the aeronautical telecommunications network, automatic dependent surveillance, future ATC procedures, satellite surveillance, navigation and communications, ground communication links, integration of satellite and radar surveillance, the necessary airborne equipment, and assessment of the problems posed by a mix of airborne capabilities (Paulson, 1994). Integrating all of the pieces needed for a truly integrated aviation system will be a staggering task.

The U.K. National Air Traffic Service (NATS) has supported studies to insure that a variety of technologies can "play together" in a future environment. In October 1991 Eurocontrol and the U.K. CAA demonstrated the automatic delivery of clearance data, weather interrogation by pilots, and the transmission of ATC instructions and pilot acknowledgements using a BAC 1-11 airplane belonging to the Royal Aircraft Establishment. "Downlinked autopilot settings were automatically checked against the controllers' original instructions, enhancing safety, while the downlinking of other avionics data (such as true airspeed, heading and vertical rates) reduced voice traffic and the controller's workload. The Volmet (weather) messages were printed in the cockpit, reducing the pilots' workload, and the downlinking of ATC messages and pilot acknowledgements gave the controllers assurance that the message had reached the correct recipient and was unlikely to be misinterpreted.

"Studies suggest that aircraft-derived data could provide additional inputs to ground-based trackers, reducing position uncertainty and enabling improved conflict alert algorithms to reduce the number of nuisance alerts while giving earlier warning of potential conflicts" (Paulson, 1994). Earlier in 1991, I proposed that ATC clearances transmitted to aircraft by datalink be downlinked to ATC computers as they were executed, to provide confirmation of FMS and presumably pilot intentions and to provide positive confirmation that the aircraft would proceed in accordance with ATC intentions (Billings, 1991).

However limited, the U.K. experiments represent an encouraging start on the task of integrating the ground and airborne components of the aviation system. Since 1991, a number of other demonstrations have been conducted to examine other elements of an integrated system. In this chapter, I examine the implications of creating such a system for the humans who must operate within it. In accordance with Perrow's (1984) cautions, I shall also examine issues related to coupling and complexity in such systems.

Elements of an integrated aviation system

A very large number of functional capabilities must be in place in a future aviation system if it is to accomplish the tasks assigned to it. Briefly, these functions are to facilitate the movement and tracking of large numbers of variably equipped aircraft on or over any part of the earth's surface, to assist them in landing and taking off from airports, and to provide all assistance necessary during contingency operations. These tasks must be accomplished in all extremes of weather, across national boundaries, with limited resources. The aviation system is information-bound, and the complexity of the system results largely from the complexity of moving all necessary information in real time to all system participants who have a need for it.

Avionics data have been downlinked and processed automatically during the UK NATS mode S trials. Some air carriers have achieved a 96% success rate in delivery of oceanic clearances by

VHF ACARS, and at certain airports, predeparture clearance delivery is now routinely accomplished by this route. Two carriers have successfully tested ADS over the Pacific, transmitting data through satellites to air traffic control facilities on land. Other elements of the system have also been tested in simulation; some have had flight trials. Large-scale GPS testing has been performed, and A330 and A340 aircraft have been certificated for satellite navigation by the JAA in Europe.

There appear to be no technological barriers to the implementation of the technologies required for a more highly integrated system. The barriers that remain are in the areas of standards, procedures, software, and harmonization across nations. The knotty issue of how ATC will cope with a broad mix of aircraft capabilities is more difficult in a constrained economic climate. ICAO's Required Navigation Performance concept may help to some extent, though retrofit of advanced equipment in a large number of regional and commuter aircraft may not be economically possible in the near term.

The software issue is critical; the elements of this system must be able to communicate, and the design and verification of software to make this happen throughout the system will be immensely difficult tasks. Nordwall (1993, p. 30) points out that when air traffic controllers began to work with prototype AAS software, 500-700 change orders were generated. The AAS system will incorporate over two million lines of code; a system for the ground support of free flight is likely to be substantially more complex. A long period of debugging will be required, and some verification work may not be able to be performed until the system is on line with live traffic, for the present system may not be fully integrated with the new one. The overall system will be extremely complex, distributed across a great many nodes. Integration of such a system is far different from integration of the many control and display modules in even as complicated a system as a nuclear power plant.

Coupling and complexity

In our present aviation system, the various automation elements are not necessarily coupled except by information. That is to say that the various elements operate *independently*. The "coupling" among them is procedural: it is agreed among the various system participants that upon receipt of a given instruction or request, a system component will take certain actions. The results of those actions may be visible in many parts of the system, but they are not predetermined. Though the various system components may be very complex in and of themselves, they are not physically or virtually linked.

Most officials in the air traffic system and an increasing number in the air carrier technical community envision direct communications between ATC computers (and perhaps, in the future, airline SOC computers as well) and aircraft flight management computers, though it is generally accepted at this time that when clearance modifications are uplinked to an aircraft, they will be subject to consent by the pilots. Direct negotiation of such clearance modifications between computers is also envisioned by FAA, however, and forms a part of the free flight concept (IATA, 1994). Such a process could confront both controllers and pilots with a result arrived at by processes that were opaque to them. It is also planned to require acceptance of datalinked messages within a certain short time interval (40 seconds has been mentioned), though presumably execution of an uplinked clearance could be delayed for some further period of time to permit more review by the pilots. Nonetheless, the clearance execution process can be time-critical under some conditions.

These proposals present potentially serious problems for human operators. It is not always easy to understand a complicated clearance, particularly if it involves waypoints or instructions that depart from expectations. The process may require, for instance, that the pilots consult navigation charts, their dispatchers, or the FMS map display, even though the FMC may have sufficient information to comply with the clearance. A new clearance may not comport with the pilot's view of the environment; it may require the expenditure of extra fuel or may take the airplane too close to the limits of an operating envelope. These factors will sometimes require deliberation and decision-making by the flight crew, all of which will take time.

Executing an uplinked flight plan is simple, requiring only a single keystroke on the FMS CDU. If procedures for voice or ACARS negotiations with ATC to secure a revision are difficult or time-consuming, a flight crew already busy with another problem may not have the time and may accept an undesirable clearance rather than argue about it. The controller may also need time to understand a complex recommended clearance revision and may not have the time at that moment due to the pressure of other tasks. These are problems that occur now; they can be dealt with by the methods used in the present system, but *only if provision is made for them* in the design of the future system.

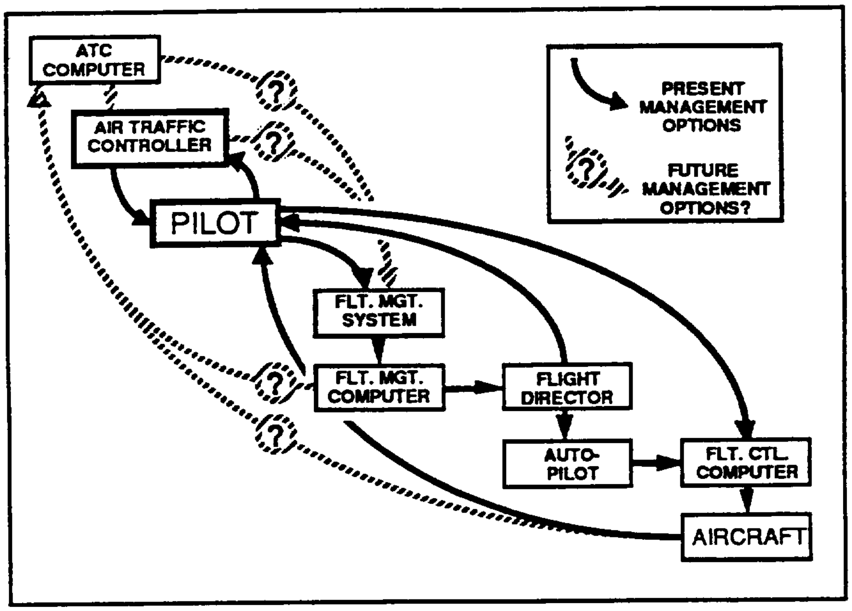

Fig. 9-1: Some options for the future management of air traffic.

A more important issue is the hypothetical (at this time) situation that would arise if it were to be decided that clearances arrived at by computer-to-computer negotiation need not require pilot or controller consent (figure 9-1). The future system will make this entirely feasible, and automatic execution of such clearances might assist ATC by insuring prompt responses to ATC commands. In this case, the ATC and airborne components of the system would be *coupled* as well as integrated.

The airplane flight path would be managed by exception rather than consent (pilots would presumably still be able to countermand the actions of the FMS, though they would not necessarily be given advance notice of its intent). This hypothetical situation begins to resemble the position of the air traffic manager under the free flight concept.

The Automated Air Traffic Management System concept

As noted in chapter 6, NASA is presently considering the elements of a new research and development program devoted to advanced air traffic management (now called Advanced Air Transportation Technology). The objective of the program is to develop advanced "conflict-free, knowledge-based automated systems for real-time adaptive scheduling and sequencing, for global flow control of large numbers and varieties of aircraft, and for terminal area and ground operations that are compatible with 'free flight' enroute operations" (Lebacqz, personal communication, 1994). This system will involve much tighter coupling, not merely integration, of the ground and airborne elements of the aviation system. These concepts run a very real (and very high) risk of infringing significantly on the authority of both air traffic controllers and pilots, despite their proponents' claims that the new automation will be human-centered.

Issues raised by tightly coupled systems concepts

In a much more tightly coupled hypothetical system involving automatic clearance execution, it would unquestionably be more difficult for pilots to understand how a clearance was arrived at and why it was given, since they would not have access to the ATC computer's reasoning. Similarly, it would be much more difficult for a responsible controller to understand the rules by which the clearance was derived, since he or she would not have access to the FMS data. This is the complexity-coupling problem discussed by Perrow (1984). It would certainly result in more surprises for the human operators, and would seriously diminish their ability to develop mental models of the ATC automation.

Though cruise flight is a comparative low workload period for pilots of advanced aircraft, it is quite certain that the cognitive burdens, and workload, now placed upon enroute controllers will be transferred to pilots, not mitigated, if such a concept comes to fruition. This has happened before, when "profile descents" were imposed in busy terminal areas. Controllers found their workloads lightened by the new procedures, but pilots found their task demands to be considerably increased.

At this time, pilots *do not* have in their cockpits the information necessary to permit them to accomplish "air traffic control" other than short-range conflict avoidance using TCAS, which provides far less than a fully adequate presentation even of immediate potential threats. Despite their limitations, which are considerable, TCAS displays are now being used on a test basis for in-trail climb separation over the Pacific Ocean. Other uses, to include lateral separation during closely-spaced (1700 ft) parallel approaches to landing, are being actively considered, and displays for this function are in development. Note that none of this new functionality has been integrated into the cockpit task flow, nor have the displays been looked at in the larger context of cockpit and flight management, as so often happens when new functions are considered for retrofit in present flight decks.

Comment

Removing pilots or controllers from the command loop, even under constrained conditions, would be a comparatively small step from a technical viewpoint. It would represent, however, an enormous, *qualitative* change in the rules by which the aviation system has been governed throughout its history. It would diminish the authority of the human operators appreciably, and it would change the dominant mode of system management as much as would the free flight concept. It would, however, be technologically feasible and implementable, perhaps at relatively low cost, and it could result in decreased workload for either pilots or controllers or possibly both—for which reasons, it will probably be seriously considered at some point in the future. This is the reason I have chosen to raise the specter here.

The differences between *integration* of independent systems and *coupling* of interdependent systems need to be clearly understood. The disadvantage of an uncoupled system is that its elements may, or may not, always behave predictably when certain instructions are issued. A pilot may turn too slowly after receiving a controller's request for an immediate maneuver (and this is probably more likely when a data linked instruction is received than when a controller issues an urgent voice instruction), as an instance. The most significant *advantage* of an integrated but uncoupled system is that the operators are much more likely to understand it, and therefore less likely to be surprised by its behavior.

Given a system as complex as the future aviation system will be, however, attempts to couple its ground and airborne elements will inevitably make it more difficult for operators to predict its behavior, particularly under other than nominal conditions. I believe that this would be likely to result in less safe rather than more safe operations.

Part 3: Requirements and Guidelines for Aviation Automation

In part 3, suggested requirements and guidelines for the design and application of future automation in aviation are presented. It is suggested that detailed "how to do it" guidelines can only be discussed in the context of a specific design philosophy and constraints for a specific system. For that reason, the guidelines proposed here are written from a system viewpoint and are designed to be used as input to the development of requirements for such specific systems.

Chapter 10 is concerned with requirements and generic guidelines for aircraft automation. Chapter 11 deals with future air traffic management automation, and chapter 12 discusses guidelines for aircraft certification.

10: Requirements and guidelines for aircraft automation

Introduction

The predecessor to this document (Billings, 1991) was successful in stimulating a dialogue between knowledgeable people in the aviation community concerning the roles and functions of human operators in the system. The guidelines it presented were less useful to designers, however, because of their generality. Since that time, however, I have become steadily more convinced that specific design guidelines can only be proposed in the context of a particular system being designed with specific goals and subject to specific constraints. That being the case, can a document such as this offer any useful guidance to those who must design future aviation automation? I am not sure of the answer to this question, but I am indebted to those reviewers who have tried to guide me in proposing such guidance. The entire document to this point is in reality an attempt to provide that guidance in narrative form.

Fadden (personal communication, 1994) has suggested that, "While there are people in aviation who do not understand some very basic facts about human beings, the design, operations and regulatory climate have improved to the point where the conflict between principles is the primary area of interest....Getting (the value of individual guidelines) into the airplane is tied to resolving the conflicts (between principles) in the most effective way possible. I would suggest that the majority of automation issues in the second, and certainly the third, generation jets are tied to the balance between competing (human) objectives, not to ignorance of those objectives."

In accordance with these comments, I have attempted in part 3 to reorder my statements of requirements to emphasize priorities and conflicts among the problems discussed in chapters 2 and 7. First, however, we should remind ourselves of what this part of the document is all about. The reader will recall that I have suggested in chapter 2 some "common factors" I believe are found in automation-associated incidents and mishaps:

- *Loss of state awareness, associated with automation:*
    - *Complexity*
    - *Coupling*
    - *Autonomy*
    - *Inadequate feedback*

In chapter 7, I elaborated on these and other automation characteristics that appear to have been associated with problems in the operation of highly automated systems:

- *Automation characteristics*
  - *Brittleness*
  - *Opacity*
  - *Literalism*
  - *Clumsiness*
  - *Monitoring requirements*
  - *Data overload*

To generalize still further, the *fundamental problem* in this human-machine system seems to me to be that ***human operators sometimes do not understand what their automated tools are doing, and why.*** For that reason, they have difficulty in using automation effectively to serve their objectives. There are many reasons for inadequate understanding; some are related to design deficiencies, some to inadequate training, and some to characteristics of the humans, including their tendency to rely uncritically on these normally reliable tools.

I have said in chapter 2 that I believe a philosophy of human-centered automation can help to lessen these aviation system problems. These requirements and guidelines are aimed at the conceptual issues underlying the (largely cognitive) problems listed here. The guidelines are necessarily presented sequentially; they are like FMS screens which can only be accessed one at a time. They are not independent, however, and many or most of them have implications for at least several others. *These guidelines must be considered as a whole, not only as "stand-alone" statements, and the designer must achieve whatever balance is possible among them, keeping in mind the problems that have been observed and their implications.*

In a landmark paper in 1980, Earl Wiener and Renwick Curry discussed "Flight-Deck Automation: Promises and Problems" (see Appendix 2). Their contribution has been the stimulus for a great deal of research during the 15 years since it was published. After presenting candidate guidelines for control and information automation, the authors concluded that "the rapid pace of automation is outstripping one's ability to comprehend all the implications for crew performance. It is unrealistic to call for a halt to cockpit automation until the manifestations are completely understood. We do, however, call for those designing, analyzing, and installing automatic systems in the cockpit to do so carefully; *to recognize the behavioral effects of automation;* to avail themselves of present and future guidelines; and to be watchful for symptoms that might appear in training and operational settings..." (emphasis supplied) Their statement is true today and their call is as appropriate as when it was written. The remainder of this section is devoted to expanding on their guidelines with the benefit of an additional 15 years of experience and hindsight.

Requirements for human-centered aircraft automation

There are innumerable guides for aerospace system designers. All present more or less specific prescriptive guidance, often context-free, which may or may not meet the particular requirements of a design engineer working under specific constraints on a specific system. Many are not indexed in a way that makes the material immediately accessible to those who need it. Design engineers frequently complain that most do not provide the guidance required in the design process, nor sufficiently firm reasons for taking a certain path in preference to others that may be easier or less expensive in a given project.

Let me reiterate that I do not believe that specific "how to" guidance is appropriate or particularly useful except in the context of a particular system, within which there may be many perhaps equally effective ways to implement a particular function. In this section, I have tried to provide guidance with respect to "what to do" rather than "how to do it", for I believe that our knowledge of cognition and behavior is sufficient to provide some general outlines of what needs to be present in a human-centered aviation system. It is probably more appropriate to call these "requirements for human-centered automation", or guidelines for the development of requirements.

Principles of human-centered automation—general guidelines

I return to the first principles of human-centered automation set forth in chapter 2, and repeat them here as general guidelines, with some further discussion of each of them. These principles deal at a fundamental level with the relationship between human operators and the machines which assist them in carrying out their mission. (For information on the mishaps cited here, see the Appendix.)

1. *The human operator must be in command.*

Fully autonomous transport aircraft are probably technically feasible, but are not politically possible at this time, in my view, because social factors would prevent them from being accepted by those who wished to utilize the services they offered. On the other hand, we accept and utilize the products made available by unmanned satellites without question, and their reliability at this time is of a high order. Were fully autonomous vehicles to become the dominant mode of transportation, this document would not be necessary, though a different document devoted to the human factors of ground control systems might be useful. I have assumed, for purposes of argument, that human "commanders" will continue to be responsible for the safety of air transport, and these guidelines are based on that premise. To the extent that it is true, I believe that the human operator must be given authority commensurate with that responsibility.

There are three ways that command authority can be compromised. A pilot in command can effectively relinquish that role, either to other humans or to the automation, by indecisiveness when a decision is required. This is fortunately rare, though it has been observed both in simulation (Ruffell Smith, 1979) and in flight (Portland, OR, 1978) when the captain delayed making the decision to land until his fuel supply was insufficient to permit a controlled landing. Operators can provide command and CRM training to reduce the likelihood of such behavior, but it can still occur, especially if the first officer is a strong-willed, dominant person and the captain is relatively passive.

A second way in which command authority can be degraded is by overly restrictive operator policies and procedures which "hamstring" the commander's authority, or by operator failure to back its commanders when disputes arise with company, government or other ground support personnel. The Air Ontario F-28 accident (1989)grew out of a situation in which the captain was required by his company to off-load fuel to permit a full passenger load in an airplane whose APU was inoperative. This combination placed him in a classic "double bind" when he landed at Dryden to refuel (Moshansky, 1992).

A third way in which command authority can be degraded is by an airplane's designers. "Hard" airplane or engine operating limitations encoded in automation software can preclude a pilot from making full-capability maneuvers if they are required in an emergency. Inadequate feedback on cockpit displays can deny a pilot the information he or she needs to recognize, evaluate and respond to a developing aircraft or automation problem, as may have occurred prior to the A330 accident at Toulouse, France (1994), when the pilots' mode annunciator panels "decluttered" after the airplane exceeded 25° of pitch during a test flight.

It is a fundamental tenet of this concept of human-centered automation that aircraft and ATC automation exists to *assist* pilots and controllers in carrying out their responsibilities as stated above. The reasoning is simple. Apart from the statutory responsibility of the human operators of the system, automation is not infallible. Like any other machine, it is subject to failure. The human's responsibilities include detecting such failures, correcting their manifestations, and continuing the operation safely to a conclusion or until the automated systems can resume their normal functions.

2. ***To command effectively, the human operator must be involved.***

To exercise effective command of a vehicle or operation, the commander must be involved in the operation. *Involved* is "to be drawn in"; the commander must have an active role, whether that role is to control the aircraft (or traffic) directly, or to manage the human and/or machine resources through which control is being exercised. The pilot's involvement, however, must be consistent with his or her command responsibilities; the priorities of the piloting or "aviating" tasks remain inflexible. The pilot flying must not be helped to become preoccupied by a welter of detail.

As we have implemented more capable and independent automation, particularly in long-haul aircraft, we have not made it appreciably harder for an alert, competent pilot to maintain situation awareness. What we have done, however, is to make it easier for a tired, bored, complacent or distracted pilot to distance him or herself from the situation. This is not new; Korean Air Lines flight 007 (Sakhalin Island, 1983) was probably flying in heading rather than INS mode for some considerable time before the first of its two incursions into Soviet airspace. What is important is that none of three crewmembers detected the mode error. They were not adequately involved.

Ways must be found to keep pilots involved in their operations by requiring of them meaningful (*not* "make-work") tasks at intervals during a long flight. Ideally, these tasks should have perceptual, cognitive and psychomotor components so that the pilots must perceive or detect, think about, and respond actively to some stimulus. This may require that designers "un-automate" some tasks or functions now performed by the automation. Such a step involves the risk that the tasks may be missed or performed wrong, but if we know enough about the task to have automated it, we also know enough to implement an error-detection module which will alert the pilot if the task is not performed or is performed incorrectly.

Modern aircraft automation is extremely capable; it has made it possible for the aircraft commander to delegate nearly all tactical control of an operation to the machine. Human-centered aircraft automation must be designed, and operated, in such a way that it does not permit the human operator to become too remote from operational details. We know how to automate, and we know ways of keeping pilots involved. The goal here must be to do both simultaneously, a less easy task but an essential one.

3. ***To remain involved, the human operator must be appropriately informed.***

Without appropriate information concerning the conduct of an operation, involvement becomes less immediate and decisions, if they are made, become unpredictable. The level of detail provided to the pilot may vary, but certain information elements cannot be absent if the pilot is to remain involved, and more important, is to remain able to resume direct control of the aircraft and operation in the event of automation failures.

Both the content of the information made available and the ways in which it is presented must reinforce the essential priorities of the piloting task; in particular, state and situation awareness must be supported and reinforced at all times. A quantity of data which could overwhelm the pilot if presented poorly can be easily assimilated if displayed in a representation that requires less cognitive effort to understand. The navigation display is a good example of this.

In highly automated aircraft, one essential information element is information concerning the activity and capability of the automation. Just as the pilot must be alert for performance decrements or incapacity in other human crew members, he or she must be alert for such decrements in automated systems that are assisting in the conduct of the operation. This leads to the requirement that:

4. ***The human operator must be informed about automated systems behavior.***

The essence of command of automated systems is the selection and use of appropriate means to accomplish an objective. Pilots must be able, from information about the aircraft subsystems, to determine that total system capability is, and will continue to be, appropriate to the flight situation and their selected strategies for its conduct.

In most aircraft systems to date, the human operator is informed only if there is a discrepancy between or among the units responsible for a particular function, or a failure of those units sufficient to disrupt or disable the performance of the function. In those cases, the operator is usually instructed to take over control of that function. To be able to do so without delay, it is necessary that the human operator have access to historical information concerning the operations to date if these are not evident from the behavior of the airplane or system controlled.

It is therefore necessary that the pilot be aware both of the function (or malfunction) of the automated system, and of the results of its processes, if the pilot is to understand why complex automated systems are doing what they are doing. Wiener and Curry (1980) argued for displays of trend information to provide pilots with advance information concerning potential failures. They noted that the provision of such information would also increase pilots' trust of their automation. Fuel usage greater than nominal (as determined by the FMS knowledge of flight plan) might be a candidate; engine parameters that might later require shutdown may be another.

5. ***Automated systems must be predictable.***

To know what automation to use (or not to use), the pilot as manager must be able to predict how the airplane will be affected by that automation, not only at the time of selection but throughout the flight. It is important that not only the nominal behavior, but also the full range of allowable behaviors, be understood; all unpredicted system behavior must be treated as possibly anomalous behavior. This was less difficult when automation only performed continuous flight control tasks; it becomes far more difficult when automation performs many discrete tasks. Its inability to perform those tasks may become evident only after it has failed to do so, and pilots are less likely to detect a failure to perform than aberrant performance.

If pilots are to monitor automation against the likelihood of failures, they must be able to recognize such failures, either by means of specific warnings or by observation of aberrant behavior by the automated systems. Both are probably desirable for critical systems, to improve detection probability. To recognize aberrant behavior, the pilot must know exactly what to expect of the automation when it is performing correctly. This requires that the normal behavior of automated systems be predictable and that the pilot be able to observe the results of their operation. It also argues strongly for *simplicity* in the design and behavior of such systems.

6. ***Automated systems must also monitor the human operators.***

Because human operators are prone to make errors, it is necessary that error detection, diagnosis, management (Wiener, 1993) and correction be integral parts of automated systems. Much effort has gone into making critical elements of the aviation system redundant. Pilots monitor the behavior of air traffic controllers, who in turn monitor the performance of pilots, as an important instance.

Automated devices already perform a variety of monitoring tasks in aircraft, as indicated throughout this document. It is indisputable, however, that failures of an automated warning system have enabled serious mishaps when the automation did not warn that it was disabled and pilots, perhaps made complacent by its effective functioning over a long period, failed to notice the conditions it was designed to detect. Designing warning systems to detect failures of warning systems can be an endless task, but it is necessary to recognize the human tendency to rely upon reliable assistants and to consider whether additional redundancy may be required in safety-critical alerting systems in today's operating environment.

Data now resident in flight management and other aircraft computers can be used to monitor pilots more comprehensively and effectively, if specific attention is given to the monitoring function. I have mentioned the substantial number of non-obvious navigation data entry errors, some of which have had serious effects long after they were committed. Research should be conducted using the growing body of accident and incident data to determine other areas in which errors are common or have particularly hazardous implications, and ways should be devised to detect such errors and alert pilots to their presence. Both Langley and Ames Research Centers have experimented with procedures monitors; some new electronic checklists alert pilots to items not performed.

The most difficult task, of course, is to monitor pilot decision making. When a pilot consciously decides to do nothing, his or her decision cannot be differentiated by any algorithm from a failure to do something. Further, advanced automation has made the need for decisions and actions infrequent during cruising flight (too infrequent, perhaps: see guideline 2). The advent of extremely long haul aircraft has emphasized the problem of monitoring human alertness and functionality.

There is no way to make the system totally error proof, and each additional piece of hardware or software has a potential decremental effect on system reliability, but as Wiener (1993) put it, multiple "lines of defense" against errors is essential if we are to make the system as foolproof as possible.

7. ***Each agent in an intelligent human-machine system must have knowledge of the intent of the other agents.***

Cross-monitoring (of machine by human, of human by machine and of human by human) can only be effective if the agent monitoring understands what the monitored agent is trying to accomplish, and in some cases, why. The intentions of both the automated systems and the human operators must be known *and communicated;* this applies equally to the monitoring of automated systems by pilots, of aircraft by human controllers on the ground, and of air traffic control by human pilots in flight.

Under normal circumstances, pilots communicate their intent to ATC by filing a flight plan, and to their FMS by inserting it into the computer or calling it up from the navigation data base. ATC, in turn, communicates its intent to pilots by granting a clearance to proceed; data link in the near future will make this information directly available to the FMS as well.

It is when circumstances become abnormal that communication of intent among the various human and machine agents may break down, as occurred in the Avianca accident at New York. The communication of intent makes it possible for all involved parties to work cooperatively to solve problems. Cooperation among intelligent agents is the cornerstone of human-centered automation. Many controller problems occur simply because pilots do not understand what the controller is trying to accomplish, and the converse is also true. Finally, neither automation nor ATC can monitor pilot performance effectively unless it understands the pilot's intent, and this is most important when the operation departs from normality (e.g., during an unannounced airplane response to a TCAS resolution advisory).

In at least two recent accidents at Strasbourg (1992) and Nagoya (1994), the automation did not warn in unmistakable terms that it was behaving in a manner contrary to pilot intentions. It *could not* do so, because the pilots had inadvertently signalled contrary intentions to the automation. We must ease the task of communicating intent to the machine component of the system, but we must also find better ways to protect the human-machine system against *mis*-communication of intent, which appears to have occurred in both mishaps.

To the "first principles" set forth above, I will add two others of a general nature which have emerged from this review of aviation automation.

8. ***Functions should be automated only if there is a good reason for doing so.***

In the past, to quote a Douglas (1990) briefing, the dominant design philosophy has been, "If it is technically and economically feasible to automate a function, automate it." The effects of this philosophy were warned against by the ATA Human Factors Task Force report (1989) and are manifest throughout this document. There are, however, tasks that pilots cannot accomplish by themselves (usually because of their complexity or because there is not time to do them), and other tasks that we know they do poorly, such as monotonous repetitive work or monitoring for rare events. Better criteria are needed to motivate the automation of functions on a human-centered flight deck. Among criteria that might be applied are the following:

- If the time within which action is required following a signal or stimulus is less than will normally be required for detection, diagnosis and decision to act (less than perhaps 3-5 sec), the task should be considered for automation.
- If a task is very complex, requiring many rote steps, or if the task is very difficult to perform correctly, the task should be redesigned or considered for automation.
- If a complex task, improperly performed, will lead to a high probability of an adverse outcome, or if an adverse outcome will threaten the safety of the mission, that task should be redesigned or considered for automation.
- If a task is boring, repetitive or distracting, especially if it must be performed frequently, that task should be considered for automation.

To quote from Wiener and Curry (1980), "Any task can be automated. The question is whether it should be..." Why is this function being automated? Will automating the new function improve system capabilities or flight crew awareness? Would *not* doing so improve the pilot's involvement, information, or ability to remain in command? Each of these questions should be asked and answered prior to the implementation of any new element of automation in the cockpit.

9. ***Automation should be designed to be simple to train, to learn, and to operate.***

I believe that aircraft automation to date has not always been designed to be operated under difficult conditions in an unfavorable environment by tired and distracted pilots of below-average ability. Yet these are precisely the conditions where its assistance may be most needed. Simplicity, transparency and intuitiveness should be among the cornerstones of automation design.

Training must be considered during the design of *all* cockpit systems and should reflect that design in practice. Particular care should be given to documenting automated systems in such a way that pilots will be able to understand clearly *how they operate* and how they can best be exploited, as well as how to operate them.

These "first principles" are not absolutes; they are but one approach, intended to promote a more cooperative relationship between pilots and automation that allows the humans in command of the system to utilize automated assistance to its fullest potential. It is vital that humans understand and be able to communicate with these tools; it is equally vital that the tools understand what the humans want and communicate with them as they are performing their tasks.

Specific requirements and guidelines

Some more specific guidelines for human-centered automation follow from the principles above. These are the most important:

10. *Automated systems must be comprehensible to pilots.*

As automation becomes more complex and coupled, with more potential interactions among modes, pilots must be helped to understand the implications of those interactions, and especially to understand interactions which can be potentially hazardous at a critical point in flight. Automated systems need to be as error resistant as possible in this respect, for the likelihood that pilots will remember all such potential interactions is low if they are not encountered frequently. The memory burden imposed by complex automation is considerable; infrequently-used knowledge may not be immediately available when it is needed. "Prompting" or brief explanations should be considered with regard to such knowledge items.

The ultimate solution to this problem lies in keeping the operation of the airplane, and of its automation, simple and predictable. If it is simple enough, it may not need to be automated at all. If it is predictable and reasonably intuitive, it may not need to be particularly simple, for the pilot will understand and remember it. Complexity is the enemy of comprehensibility.

11. *Automation must insure that the pilot is not removed from the command role.*

Increasing automation of aircraft and of the ATC system, and increasing integration and coupling of the ground and airborne elements of that system have the potential to bypass the humans who operate and manage the system. One way to guard against this is to design future flight management systems so that the pilot is shown the consequences of any clearance before accepting it; another is to insure that the pilot must actively consent to any requested modification of a flight plan before it is executed. A third, more difficult way is to make it possible for pilots to negotiate easily with ATC on specific elements of a clearance, such as altitude changes, rather than having to accept or reject an entire clearance or modification. All three, and possibly other ways as well, may be required to keep pilots firmly in command of their operations in a future, more automated system.

These steps will require more than simply software changes. They will require detailed negotiations between the operating community and air traffic management system designers. In view of the rapidity with which the enabling technology is being pursued, *the long-term goals and objectives of system designers and planners with respect to future human and machine roles in the system need to be known with precision.* I do not believe that they have been set forth with sufficient clarity thus far, and I believe also that the potential consequences of fundamental changes in the locus of command of the system are so major as to require informed consensus before proceeding farther with system redesign.

12. *A primary objective of automation is to maintain and enhance situation awareness. All automation elements and displays must contribute to this objective.*

The minimum elements of information required by pilots at all times are a knowledge of the airplane's position, velocity, attitude, error rate, status, threats, the status of the aircraft control automation and other aids, what must be done next, and when it must occur (figure 10-1). These are the elements of situation awareness. Many other information elements will be required in some form at specific times, however. The question is not whether these are needed, but in what form they will best reinforce the pilot's awareness of his or her situation and state.

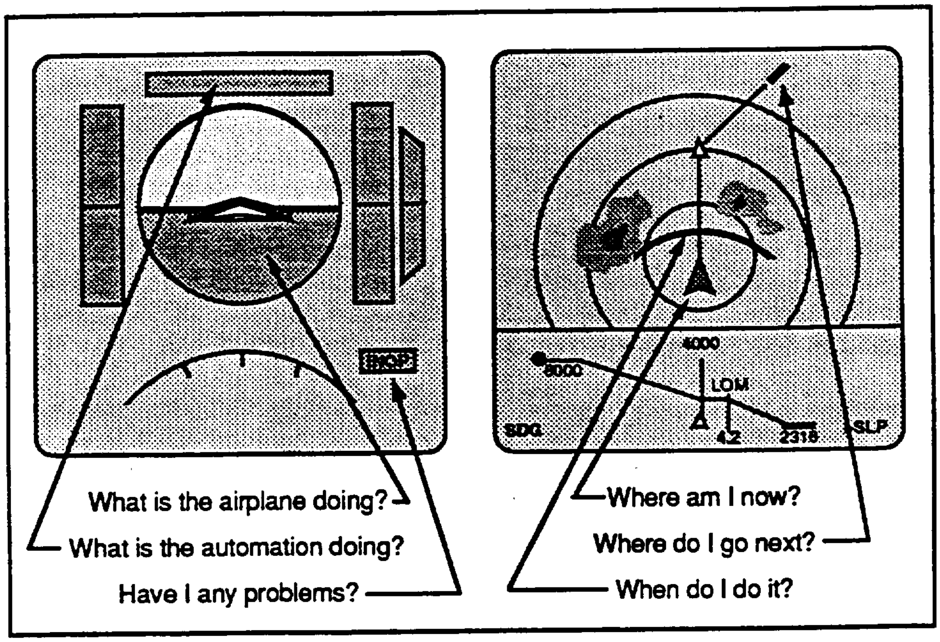

Fig. 10-1: Required elements of information for pilots

13. *Management automation should make airplanes easier to manage.*

A major problem with flight management systems is that they are often cumbersome to operate. Under some circumstances, it is easier to operate without them than to use them, with the predictable result that they are apt to be bypassed under these circumstances. This is a pity, for the error resistance that they bring to flight path management is also bypassed.

One partial solution to this problem is to improve the interfaces between system and pilot so that they can be manipulated more easily. This will not be a trivial task, for it may require establishing a different level of interface between the pilot and the system, one which involves a high-level interaction rather than the present point-by-point description of desired ends. On the other hand, data link may enable a higher-level interaction and may even require it for effective interaction with ATC, most of which may be through the FMS.

Within the constraints of present-generation systems, continued efforts to improve the ease of system programming and operation in high workload segments of flight would be most helpful to pilots, and would improve system safety. Much progress has been made in easing the task of modifying approach tasks to accommodate revised ATC instructions. The problem of manually tuning navigation and communications radio aids rapidly has been mentioned by pilots; providing alternate interfaces (similar to those available in older aircraft) through which these and other cumbersome tasks could be accomplished more readily is worthy of consideration.

The proliferation of modes in newer flight management systems has imposed an increasing cognitive burden on pilots. Both the modes themselves, and their inadequate feedback, have induced erroneous actions in flight crews not entirely familiar with them. Operators should determine whether all modes are required and should consider simplifying training and operational workload by eliminating those not entirely necessary, or by making their use optional.

14. ***Designers must assume that human operators will rely on reliable automation, because they will.***

Once pilots have flown an automated airplane long enough to become comfortable with it, they will come to "know" which control, information and management elements can be trusted. Thereafter, many (though not all) pilots will become increasingly reliant upon the continued functionality of those elements and therefore less liable to be suspicious of them if they become unreliable.

If information is derived or processed, the designer must insure that the data from which it is derived are also either visible or accessible for verification. If it is not critical information for a particular flight phase, make it available only on request, but insure that it remains accessible, as has been done with raw navigation data (figure 4-5).

Future automated decision support systems may pose a serious problem in this regard if pilots come over time to rely on the quality of the machine decisions. A poor machine decision may be much more difficult to detect than an aberrant subsystem operation. It may also be much more difficult to determine whether a machine decision is correct, because of the complexity of the process that motivates it.

It is not enough simply to warn pilots in training that their automation is not infallible. They will rely on their own experience to assign subjective probabilities of failure. If a machine has "always worked well" in their experience, they will assume that it will continue to work well, and they will usually be correct—but not always, which motivates the need for error (and failure) tolerant automation.

Guidelines for aircraft control automation

Several guidelines relate specifically to requirements for control automation. Among them are the following:

15. ***Control automation should be limited in its authority. It must not be permitted to become "insubordinate".***

Control automation should not be able to endanger an aircraft or to make a difficult situation worse. It should not be able to assume a state that could cause an overspeed, a stall, or contact with the ground without explicit instructions from the pilot, and possibly not then. If either the pilot or the automation approaches safe operating limits, the automation should alert the pilot, giving him or her time to recognize the problem and take corrective action.

The pilot should not be permitted to select a potentially unsafe automatic operating mode without being challenged; automation should either foreclose the use of such modes or should alert the pilot that they may be hazardous. Many useful modes are "open-ended"; in these cases, continued pilot involvement is especially important. Alternatively, the designer should consider whether there is really a need for such a mode, or whether another way to accomplish the same function would be a safer, more error resistant approach.

The edges of the operating envelope are a particular problem. Some accidents involving automation have occurred at, or outside, the normal range of operating conditions. Since designers can never guarantee that aircraft will never reach these conditions, automation must be designed so that it is tolerant of such conditions, or in any event, does not worsen them. The phenomenon of "brittleness" is difficult to predict, but very serious when it occurs, usually during an emergency when there may not be time to compensate for it.

16. ***Control automation must never be permitted to perform, or fail, silently.***

This is a corollary of principle 3. "Fail-passive" control automation represents a potential hazard in that its failure may not and usually does not change aircraft performance at the time if the airplane is in a stable condition. Such failures must be announced unambiguously to insure that the pilots immediately resume active control of the machine. Automation must never encourage a situation in which "no one is in charge", for pilots must always "aviate" even if they have delegated control to the autopilot. The Everglades accident was a good example of what can happen if this tenet is violated (Miami, 1972).

A particular case of this is uncoupled sidestick controllers, both of which can be operated simultaneously (the inputs are summed) without tactile or other feedback to either pilot. Consideration should be given to indicating to both pilots any situation in which commands are being input from both controllers.

17. ***Designers should not foreclose pilot authority to override normal aircraft operating limits when required for safe mission completion without compelling reasons for doing so.***

In a recent review of aircraft automation, Hughes and Dornheim (AWST, 1995a,b) reported that "Airbus Industrie officials believe that if the technology exists to automate a function that would prevent a pilot from inadvertently exceeding safety limits, this should be done." This statement does not consider that pilots may find it necessary to *deliberately* exceed safe operating limits, but the same automated protection would apply in such a case.

Limitations on pilot authority may leave the pilot unable to fulfill his or her responsibility for safety of flight. An ASRS incident report, one of many, underscores the need to preserve pilot capability to do what is necessary; an abrupt 50° banked turn was required for collision avoidance in a wide-body airplane (NASA ASRS, 1986). There have been several cases in which pilots have violated aircraft structural limits in an acute emergency; in nearly all of these, the aircraft have been recovered, though with damage (Atlantic Ocean, 1959; Luxembourg, 1979; Pacific Ocean, 1985). These maneuvers would not have been possible had hard envelope limits been incorporated.

I believe that the "soft envelope limits" approach represents one way to avoid limiting pilot authority while enhancing flight safety. Other automated modules that "lock out" flight-critical functions should also be capable of being overridden in an emergency. The implementation of "hard" limiting functions should be undertaken only after extensive consultation with both test and line pilots.

18. ***Control automation should provide the human operator with an appropriate range of control and management options.***

The control and management of an airplane must be safely accomplished by pilots whose abilities and experience vary, under circumstances that vary widely. To provide effective assistance to whomever is flying, under whatever conditions, a degree of flexibility is required in aircraft automation. The aircraft control-management continuum has been discussed;

problems at the extremes of this continuum have been indicated (very high workload at the low end of the spectrum, decreased involvement at the high end of the spectrum).

The range of control and management options appropriate to a given airplane must be wide enough to encompass the full range of pilots who may operate it, under the full range of operating conditions for which it is certificated. It should not be wider than is needed to provide an appropriate range of workloads, however, to avoid unnecessary complexity. I have attempted in chapter 8 to suggest how wide a range of options may be sufficient.

19. ***Designers should keep the flight crew involved in the operation by requiring of them meaningful and relevant tasks, regardless of the level of management being utilized by them.***

As indicated in principle 2, high levels of strategic management have the potential to decrease pilot involvement beyond desirable limits. Automation should be designed to minimize this detachment, so that pilots are ready to reenter the loop in the event of its failure. Keeping pilots meaningfully involved may require less automation rather than more, but it is critical to their ability to remain in command of an operation.

I have suggested that requiring management by consent rather than management by exception may be one way to maintain involvement, though it has also been pointed out that we do not yet know how to keep consent from becoming perfunctory, and this must also be avoided. One way to assist may be to give more attention to workload management, as is suggested in guideline 20.

20. ***Control automation should be designed to be of most help during times of highest workload, and somewhat less help during times of lowest workload.***

Some field studies of aircraft automation have suggested that it may appreciably lighten workload at times when it is already low, yet impose additional workload during times when it is already high, during climbs and particularly descents. While much of the additional burden relates to problems in interacting with the flight management system itself, the end product of that interaction is the control and guidance of the airplane as it moves toward its destination.

Avionics manufacturers have made appreciable strides in easing this workload by providing lists of departure, arrival and runway options at particular destinations. Air traffic control authorities pressed to increase capacity at busy terminals, however, may develop and utilize procedures that differ from those anticipated by the designers. In particular, "sidestep" maneuvers to alternate parallel or converging runways are a problem in this regard, especially if clearances are altered late in a descent. Easing such problems may require a better understanding by ATC of what is, and is not, reasonable to ask of the pilots of a highly automated airplane. Given the congestion at our busiest terminals, however, ATC is likely to continue to seek more, rather than less, flexibility from pilots and any short-term improvements will have to be in the cockpit (see also management automation guidelines below).

21. ***Control automation should be designed both for maximum error resistance and maximum error tolerance.***

Both automated control systems and their associated displays should be designed to be as error resistant as is feasible by incorporating the simplest possible architecture, clear, intuitive displays and unambiguous responses to commands. Designers should also incorporate clear, unambiguous statements for the design use of each control mode in their software documentation.

The designs should incorporate the highest reasonable degree of error tolerance as well. Consideration should be given to embedding monitoring and error-trapping software in the systems. Accident and incident data should be reviewed on an ongoing basis to identify likely human and machine deficiencies and these deficiencies should receive special attention in this process.

Human errors, some enabled by equipment design, bring more aircraft to grief than any other factor. Error resistant systems can protect against many of these errors, but it is necessary to give pilots authority to act contrary to normal operating practices when necessary and this requires that designs also incorporate error tolerance. Automation should be used wherever possible to monitor pilot actions and warn of mistakes, slips and lapses (Norman, 1981).

Guidelines for aircraft information automation

It will have been noted that some of the guidelines above relate to information provided to the pilots as well as to the control of the airplane and its subsystems. It is not always possible to draw a clear distinction between control and information automation, for all automation involves the requirement to keep pilots informed. The following are suggested guidelines specifically for information automation.

22. *Emphasize information in accordance with its importance.*

The most important information should be most obvious and most centrally-located. Information relevant to aircraft control deviations, power loss or impending collisions with obstacles is always more important than information concerning other facets of the operation. Changes in state or status are more important than information concerning static states. Symbolic information should be redundantly coded (shape, size, color, use of two or more sensory modalities) to insure that it is detected. Auditory (sounds) or tactile information displays can be used to reinforce, or in some cases to substitute for, visual information; this can be particularly useful during periods of high visual workload.

A strenuous and largely successful attempt has been made to decrease the large number of discrete auditory warnings that were present in older cockpits. The use of discrete voice warnings is increasing, however; GPWS, TCAS and windshear alerts all incorporate voice signals, and an increasing number of aircraft also incorporate synthetic voice altitude callouts on final approach. This may be less of a potential problem when data link replaces some of the voice communications now required, but there remains the potential for interference among voice messages, as well as the potential for overuse of voice signals leading to diminished attentiveness to voice emergency messages.

23. *Alerting and warning systems should be as simple and foolproof as possible.*

Warning systems for discrete failures do not present a particular problem as long as they are annunciated in such a way that the pilot can determine the root cause. This has not always been the case. Whether reconfiguration of aircraft systems following such a failure should be autonomous remains an open question awaiting more experience with the MD-11 systems. The problem of quantitative warning system sensitivity and specificity has been discussed: false or nuisance warnings must be kept to minimum levels to avoid the unwanted behavioral effects of excessive alarms.

At the risk of providing pilots with more information than they need to know, I believe (as did Wiener and Curry) that it is often appropriate to provide pilots with trend information before a parameter reaches a level requiring immediate action, to improve their awareness of a potentially serious situation. As they pointed out, this serves the added purpose of increasing pilots' trust of the automated monitoring systems. When alerts are provided and response time is not critical, many pilots will attempt to evaluate the validity of the information. Means should be provided for them to do so quickly and accurately.

Warnings and alerts must be unambiguous. When common signals are used to denote more than one condition (e.g., the master caution and master warning signals), there must be a clear indication of the specific condition which is responsible for the alert. This is not a problem in most newer aircraft, though large numbers of discrete messages may occur during emergencies (see incident report at beginning of chapter 13).

24. ***Integration of information does not mean simply adding more elements to a single display.***

Integration in psychology means "the organization of various traits into one harmonious personality". An integrated display combines disparate information elements into a single representation that renders unnecessary many cognitive steps the pilot would otherwise have to perform to develop a concept. It thus relieves the pilot of mental workload. Glass cockpit navigation displays are very effectively integrated. Electronic primary flight displays are not integrated; rather, they combine a great deal of information, previously shown on many instruments, on a single screen. The elements, however, are still discrete and the mental workload of inferring aircraft state is still required. The same is true of most power displays in today's cockpits.

Clutter in displays is undesirable, for pilots may fail to notice the most important information or may focus on less important data. Pilots are able to add or remove display elements from navigation displays. Fairly radical (pilot-selectable) decluttering of the PFD would still provide the pilot flying at cruise on autopilot with all information required to monitor the autopilot and return to the control loop rapidly if required.

Many subsystem displays can also be made more simple and intuitive. Again, the controlling variable should be what the pilot needs to know under normal and abnormal circumstances. As long as all information necessary to take over manual control of these systems is available when required, it is not necessary that other data be visible in circumstances in which they are not central to the pilot's tasks.

25. ***Automation poses additional monitoring requirements; pilots must be able to monitor both the status of the automation and the status of the functions controlled by that automation.***

Should automation status be announced, as well as the status of the functions being controlled? One can argue that it should be, by some means (perhaps a selectable synoptic display). *No* information can mean either that everything is normal or that a sensor or annunciator has failed. Particularly in the case of subsystems, where nothing important happens for long periods of time, pilots need some type of reassurance that the automation is still monitoring the systems. The "need to know" concept assumes different dimensions in aircraft that are usually managed rather than directly controlled.

Automation can fail covertly as well as overtly, and in either case, the pilot must become, or be ready to become, a controller rather than a manager. To do so, he or she must know by some means that the automation has failed, and the condition of the controlled elements or functions.

26. ***Design system automation to insure that critical functions are monitored as well as executed.***

The safety benefits of independent monitoring are indisputable. ATC radar permits controllers to monitor flight path control; TCAS permits pilots to monitor controller actions. Some aircraft functions are not independently monitored at this time; airplane acceleration with respect to runway remaining during takeoff is one, ILS guidance during instrument approaches is another. A third is aircraft position on the airport surface, at many facilities. Monitoring of input to aircraft systems, especially the FMS, remains a problem despite the partial monitoring capability provided by map displays.

In the first two cases mentioned, new technology will be required. In the latter case, FMS software should be provided to monitor, as well as assist in, pilot interactions with the system. Where critical errors could compromise safety, independent monitoring of inputs by downlinking of FMS data for comparison by ATC computers with uplinked clearance data should be enabled. It is not clear at this point in time that airplane-to-ATC digital data link will be used to confirm that clearance data has been received and entered into the FMC correctly. This link could also confirm that manually-entered flight path data such as revised altitude clearances conforms to ATC intentions. Such a monitoring link could add an important element of redundancy and error-tolerance to operations within the system.

Guidelines for aircraft management automation

Management automation has been a remarkably successful tool in the cockpit; the development of air traffic automation will further improve its utility and effectiveness. It has made the aviation system more error resistant, though it has also enabled new errors in the cockpit, as does any new equipment that must be operated by humans. It is recognized that there are substantial economic disincentives to making qualitative changes in flight management systems, given the investments in hardware, software and training that have already been made. Nonetheless, it is necessary that research and development efforts, at least, continue with the aim of making future flight management system interface designs more human-centered and more error tolerant.

The following guidelines are suggested for future flight management systems and other management automation.

27. ***Flight management system interfaces must be as error tolerant as possible.***

In view of the known problems in data entry, FMS software should accomplish as much error trapping as is possible. A few ways of doing this have been suggested above. When data link is available, the data entry process may be simplified, but that does not necessarily imply that data entry errors will be eliminated. Many intermediate altitude restrictions will still have to be entered manually (usually into the MCP). This task is known to be error-prone; the downlinking of such data when they are executed would trap many such errors, if ATC software were provided to verify the correctness of the entries.

As noted earlier, CDUs refuse to accept incorrectly-formatted entries, but they do not provide feedback as to why an entry was rejected. If the computer knows, why doesn't it tell the pilot? Some data entry errors are obvious, but others may be less obvious and pilots may be tired or distracted by other problems. In general, the less often a pilot is required to perform a particular programming task, the more likely it is that the details of accomplishing that task will be forgotten. Infrequently-performed tasks, therefore, should be the ones on which pilots receive the most help. Prompting could be very useful under these circumstances.

28. ***Insure that flight operations remain within the capacities of the human operator.***

There are very few flight maneuvers that require such precision that they have been entrusted only to automation. Pilots generally have not been asked to engage in operations unless they can demonstrate their ability to perform them without machine aid. The limited capacity of the airspace system, however, has motivated intensive efforts to increase system throughput by making better use of presently-available runways and terminal airspace. As noted earlier, this includes studies of "free flight", closely-spaced parallel approaches, the use of more complex approach paths, closer spacing in the terminal area, and other initiatives. At least some of these maneuvers will require extreme precision in flight path control. It is likely that automation will be called upon to perform them, and possible that it will be required.

This will be a safe approach if, and only if, pilots are provided with the monitoring capability required to maintain full situation awareness throughout the performance of the maneuvers, *and with ways of escaping from the maneuvers safely and expeditiously in the event of a contingency either within the airplane or the system.* New monitoring automation and displays may well be necessary in the cockpit if pilots are to remain in command during such maneuvers, just as higher scan-rate radar and enhanced displays will be necessary for the controllers who will monitor such operations.

Guidelines for error management

In his recent document, "Intervention Strategies for the Management of Human Error", Wiener (1993) has provided an excellent review of the literature and a number of guidelines for the management of human error, to which modern transport aircraft are still highly vulnerable. He provides an approach to error management involving intervention strategies at all levels. His report should be read by all designers and operators of these aircraft. Many of the guidelines above involve error management at one or another level. I will add only one further guideline for consideration, motivated by my increasing concern about the disparities among new equipment from various manufacturers.

29. ***Standardize critical interfaces across fleets and manufacturers wherever possible to prevent flight crew errors in operation.***

During and after world war II, Ruffell Smith in the Royal Air Force and teams of human factors investigators at the USAF Aeromedical Laboratory attempted to improve the standardization of controls and displays in military aircraft. Their attempts were not entirely successful, but over time, a considerable degree of commonality in conventional controls and displays has become the consensus among designers, certification authorities, operators and pilots. This commonality, unfortunately, has not yet been extended to flight deck automation.

The differences among these systems should be evaluated in the light of the tasks that must be performed by pilots using them. Manufacturers have adopted quite different philosophies for the operation of their airplanes, and it is this fact, more than superficial differences among the systems, that may cause difficulties for pilots moving from one to another. Air carriers operating mixed fleets need to insure that a single operating philosophy and consistent operating policies can be applied in all of their aircraft. In the long run, it is they, the customers, who can do the most to increase standardization in automation, as in other aspects of their aircraft. To a considerable extent, manufacturers produce what they are told to produce by customers.

Nomenclature:

MD-11	Flight control panel	FCP
747-400	Mode control panel	MCP
777	Mode control panel	MCP
A320	Flight control unit	FCU
F-100	Flight mode panel	FMP

Arrangement and spacing of data displays on panel:

MD-11	SPEED		HEADING		ALTITUDE		VS/FPA
747-400	SPEED	(Break)	HEADING		VERT SPD		ALTITUDE
777	SPEED	(Break)	HEADING		VS/FPA		ALTITUDE
A320	SPEED	HEADING	(Break)		ALTITUDE		VS/FPA
F-100	SPEED	(Break)	HEADING	(Break)	ALTITUDE		VERT SPD

Input actions on panel:

Knob action:	PUSH	TURN	PULL
MD-11	Hold	Preselect	Select
747-400	Various	Select	None
777	None(?)	Select	None
A320	—>FMGS	Preselect	Select
F-100	Hold	Preselect	Select

Fig. 10-2: Mode control panels in current aircraft

Fig. 10-2 shows elements of a number of mode control panels. It indicates some of the differences among these interfaces with respect to nomenclature, positions of data elements and input actions. With mixed fleets being the rule in larger carriers, these design disparities have caused and will continue to cause errors in operation by pilots who have transitioned from one to another of these aircraft.

In addition, some FMS modes operate differently in different aircraft types, another source of potential difficulties in the operational use of the equipment. Industry efforts should be instituted to move toward greater standardization of automation elements, to prevent reversion errors which are most likely to occur under stressful emergency conditions.

Comment

These guidelines have implications for controllers, airspace planners and others in the system as well as for pilots and flight deck designers. They should be read as requirements guidelines for the airborne component of the aviation system, not only as guidelines simply for cockpit design, because changes anywhere in a coupled system can produce changes elsewhere as well.

Workload removed from one element of the system will often be reflected in additional workload elsewhere. This was the case when profile descents were implemented, and it has occurred again with the implementation of pre-departure clearances delivered through airline system operations centers rather than directly from air traffic control facilities. It may occur yet again if pilots are given more responsibility for traffic separation during the enroute phase of flight, a concept that has been seriously considered by FAA in its airspace redesign efforts. During the past year, as an example, tests have been conducted to evaluate the use of TCAS as a separation aid for aircraft climbing through an altitude occupied by another aircraft on oceanic routes not under radar surveillance. The "free flight" concept is under active consideration.

The standardization issue raised in the last guideline will become a matter of urgency as more air carriers move toward mixed fleets. Chapter 14 discusses the increasing tendency among carriers to standardize their fleets; as noted there, some carriers have refused to select EDUs rather than electromechanical instruments in new aircraft, to maintain commonality across a range of aircraft of a common type. Whether this is justified, as opposed to the alternative of maintaining commonality in EDU *displays* within the cockpit, has not been evaluated.

During the period before the emergence of advanced automation, most large airlines enforced rigid standards across their fleets in cockpit design, placement of switches and other controls, and procedures. This was not a problem until aircraft from some of these carriers were sold to others, and pilots from failed carriers began to work for other airlines having disparate standards. Some smaller fleets today, however, have marked differences within the cockpits of even a single type and variant. This lack of standardization extends to automation and will cause serious errors. The solution adopted thus far is to provide "differences training" to insure that pilots are aware of the differences they will encounter, but this cannot be a fully effective way of dealing with the problem.

A recurrent theme running through these suggested guidelines (and through this entire document) is that "simpler is often better". The overriding human factors problems in today's aircraft are the complexity of the tools provided to help pilots do their job, and deficient understanding of how the tools work. More efforts devoted to simplifying the design and operation of these essential tools will decrease required training and cross-training, improve the error resistance and error tolerance of the systems, ameliorate the increasing cognitive burdens placed on pilots of these aircraft, and ultimately increase system safety.

11. Guidelines for air traffic control and management automation

Introduction

It is necessary to remember the important distinctions between pilot and air traffic controller tasks in the aviation system. The pilot receives essentially instantaneous feedback from an airplane and its displays once he makes a control input. The "controller", on the other hand, *directs* traffic by giving voice instructions to an intermediary (the pilot); he or she must then wait an indeterminate period of time to observe whether the airplane appears to be executing the requested action. The difference in required lead time may be considerable and it can have major consequences for controller planning, as can the fact that controllers must often manipulate several aircraft rather than only one. In these respects, the controller's tasks are conceptually more difficult than those of the pilot.

Also more difficult for the controller is the fact that he or she must ordinarily work entirely through representations of the monitored system rather than being able to observe its behavior directly. (Tower controllers in VMC are an exception.) Unlike controllers, pilots receive not only visual, but also tactile, proprioceptive and sometimes auditory feedback from their airplane and environment. Woods and Holloway (in Woods, 1994a) illustrate the problem in this manner (figure 11-1). The controller is handicapped by having to view the monitored system entirely through a representation rather than being able to view its behavior directly.

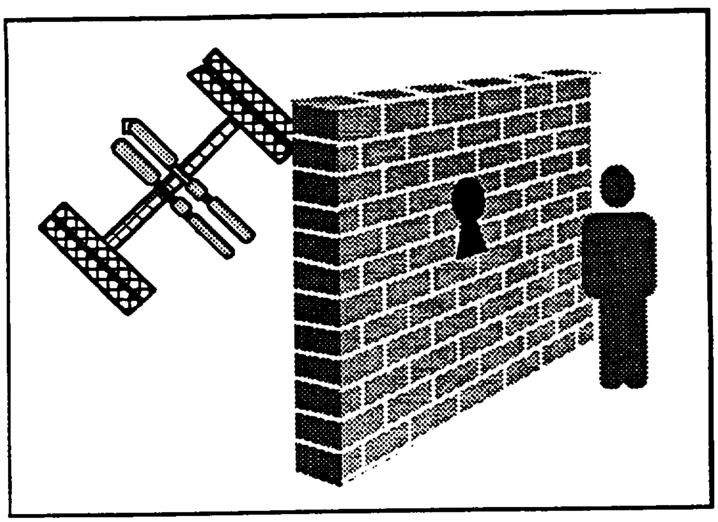

Fig. 11-1: The keyhole property (redrawn from Woods, 1994)

"The viewport size is very small relative to the large size of the artificial data space...that could potentially be examined. This property is often referred to as the keyhole effect (Woods, 1984). Given this property, shifting one's 'gaze' within the virtual perceptual field is carried out by selecting another part of the artificial data space and moving it into the limited viewport."

The controller sees only a plan view of the traffic space; the third dimension must be provided by alphanumeric data and by symbols on another screen. To assess traffic not yet visible, a second screen which portrays flight data must be examined.

(The "keyhole" problem afflicts pilots as well; their view of the traffic situation is incomplete, and TCAS as implemented today is not an efficient means of providing them with information concerning other traffic not yet in conflict. The "party line" is of help, but much of the information conveyed to other aircraft may be ambiguous.)

Controllers become adept at constructing a mental model of the traffic under their direction from this imperfect view, but under the stress of heavy traffic, they are in danger of losing their internal model, a serious problem because "once the picture has been lost, the controller can seldom recall it in its entirety again but has to rebuild it painstakingly aircraft by aircraft. . ." (Hopkin, 1994, p. 173).

For all these reasons, the controller requires different tools to perform different tasks from those of the pilot. It is easy to argue that controllers need more help from automation than do pilots, but this neglects the obvious fact that they are now performing very well indeed without many of the aids that pilots take for granted. *Any attempt to produce guidance for ATC automation must take account of what controllers now do so effectively without such aiding, and why they are able to perform successfully in a largely "manual", or unaided, work environment.*

Human-centered automation for air traffic control

I hope it is obvious from chapter 2 that I believe in the importance of human-centered automation for air traffic controllers as well as for pilots. In fact, I believe this approach to automation may be more important in the ATC domain because of the factors mentioned above. The opportunities for proper design are very great, because major elements of the automation system for ATC are not yet in place. The need is equally great, because ATC will be the instrumentality through which the required gains in traffic capacity will have to be realized. Pilots can help, but they can only control one airplane at a time. Controllers will bear the brunt of the additional traffic. They will need effective and highly efficient tools to help them manage the additional loads.

The first principles of human-centered automation have been discussed at some length in chapter 2, and again in chapter 10. I will not repeat them here except to say that I am convinced that human air traffic controllers must remain in firm command of the future ATC system if it is to meet the challenges that will be imposed upon it. They must retain authority commensurate with their great responsibilities. If future ATC automation is *not* human-centered, the entire system will lose this focus and the flexibility that goes with it. That flexibility, both on the ground and in the air, is what has enabled the current system to cope with traffic demands to date. It will be even more necessary in the more crowded system of the future.

How can flexibility be maintained in the face of a need to move more aircraft, spaced more closely, with less room for error? I believe this can be accomplished by providing human controllers with decision and monitoring aids that will enhance their considerable cognitive capabilities while maintaining surveillance of traffic to insure that it is moving in accordance with their requirements. Controllers do *not*, in general, need to be told how to move airplanes; that is what they do best. What they do need, at a minimum, is confirmation that their plans are appropriate and assistance in keeping track of whether airplanes are moving in accordance with those plans. These are types of assistance that computers are quite capable of providing even without major advances in computational capability.

The NASA/FAA CTAS program (Tobias & Scoggins, 1986; Erzberger & Nedell, 1988; 1989) has demonstrated that properly designed decision *aids*, which take account of aircraft dynamic capabilities, can help arrival controllers to decrease traffic dispersions considerably, thereby increasing terminal area throughput. It has also demonstrated that properly designed management and spacing aids can assist materially in the controller's planning processes, while leaving the human able to exercise his or her expertise and judgment as the traffic situation unfolds.

As noted previously, many system designers believe that only a truly radical reshaping of the traffic management architecture and infrastructure will be able to accommodate traffic expansion beyond perhaps 2010 (Whicher, quoted by Cooper, 1994a). I am not convinced that the future ATC system must be radically restructured to meet the demands that will be placed upon it. On the contrary, I believe that the new system should perhaps rely more upon controller expertise than is envisioned in present proposals for its architecture. I am more optimistic that a human-centered ATC system, *complemented by the proper intelligent tools*, can get the job done well beyond that time. What are the proper tools, and what must they be able to do to help the human operator do his or her job? That is the question that must be examined.

Guidelines for human-centered air traffic control automation

Assumptions

The following guidelines are designed to help in the definition of requirements for future air traffic control system automation. They assume that adequate computing capacity will be available to accomplish whatever functions and provide whatever tools will best serve the controller in the future system. They also assume that sensor capacity of some sort (whether radar located on the ground or GNSS and ADS in aircraft, or both) will be able to provide precise, nearly real-time, data concerning aircraft positions, states and environmental conditions. Finally, they assume that both broadcast voice and selective data communications will be enabled in the new system, and that most routine ATC message traffic will be by means of digital data link, whether through mode S transponders, ACARS or some new communications functionality.

As in the previous chapter, I have not attempted to set forth detailed human factors engineering guidelines for air traffic control automation. To do so when the shape and content of the future system is not yet defined would be pointless. These guidelines, like those proposed previously, provide general guidance which hopefully can contribute to requirements definition for the future system.

First principles of human-centered air traffic control automation

To recapitulate briefly the first principles, as applied to air traffic control (see chapters 2 and 10 for discussion of these general guidelines or principles):

1. ***The human operator must remain in command of the air traffic control and management system.***

2. ***The controller must remain actively involved in the direction of air traffic.***

3. ***The controller must be informed of relevant traffic and of the results of his/her actions with respect to its movement.***

4. ***The controller must be able to monitor the automation assisting him/her.***

5. ***That automation must behave predictably.***

6. ***ATC automation must also monitor the controller's decisions and actions.***

7. ***All system elements must understand the controller's intentions, and the controller must understand their intentions.***

The ability to monitor the automation, and thus the need for automation predictability, is perhaps even more important in the ATC domain than in flight, because the controller has less comprehensive feedback than the pilot with respect to the behavior of the controlled system. As Norman has observed, "The problem is that the operations under normal operating conditions are performed appropriately, but there is inadequate feedback and interaction with the humans who must control the overall conduct of the task. When the situations exceed the capabilities of the automatic equipment, then the inadequate feedback leads to difficulties for the human controllers" (Norman, 1989, p. 1).

The two additional general guidelines proposed in chapter 10 are also appropriate here:

8. ***Functions should be automated only if there is a good reason for doing so.***

The questions asked with regard to aircraft automation must also be answered by the designer of air traffic control automation: Why is this function being considered for automation? Will automating this function improve the controller's capabilities or awareness? Would *not* doing so improve the controller's involvement, information, or ability to remain in command?

9. ***Automation should be designed to be simple to train, to learn, and to operate.***

Training must be considered at each step in the design of any automated system and should reflect that design in practice. This will be particularly important in ATC automation because controllers, unlike many pilots, have not had experience with advanced automation and will have to learn to operate within, and develop confidence in, a new and very different system. The propensity of designers to rely upon keyboard entry (with its attendant visual and psychomotor workload) may be a particular problem in the advanced automation system; controllers rely to a great extent on their vision for real-time information transfer. Their present information management systems do not require a great deal of visual attention; it is important that their future system controls also be easy to operate.

Guidelines for human-centered air traffic control automation

Based on the foregoing, I offer the following guidelines for air traffic control automation. As in the previous chapter, the guidelines are loosely ordered in terms of their importance.

10. ***Future ATC automation must insure that the controller is not removed from the command role.***

I have indicated my serious concern with regard to the level of authority which will be reserved to the controller in the advanced automated system. While it may not always be appropriate for the controller to have to work one-on-one with aircraft under his or her control, it is vital that the controller remain in command of all air traffic and able to modify its behavior as required to perform the mission.

The temptation to build more autonomous automation is pervasive, particularly when an express purpose of that automation is to "improve human productivity" (which in the past has usually meant to accomplish the same or greater throughput with less human involvement). But the losses in system productivity which will result if controllers are unable to remain "in the picture" are likely to negate any gains achieved by more autonomous machine systems. The air traffic management system, like the aircraft it directs, is not at this time planned as a fully autonomous system. If that is true, then the controller must play a central role, not only when automation fails but when it is functioning normally.

11. ***ATC control automation should be explicitly limited in its authority, and its limits must be explicitly understood by human controllers.***

The authority of control automation must be explicitly limited so that there is never a question about its operating boundaries. Human controllers must understand these limits and their implications, and that they will be responsible for all decisions and actions that lie outside machine authority. This is analogous to the role of the military commander, whose subordinates may proceed independently within specific doctrinal and operating guidelines but who may not transgress those guidelines without authorization. While the authority may vary as a function of the level of management invoked by the human controller, the rules must be simple enough to be fully understood.

12. ***Future ATC automation should not make air traffic management more difficult for controllers.***

Examples of "clumsy" automation making the pilot's task more difficult have been cited. The controller will be subjected to the same problem unless care is taken to make new representations at least as informative as the present ones, new functions as simple to invoke, and new capabilities as intuitive as possible so that the controller is not required to perform additional cognitive tasks to understand them. It is recognized that the enroute controller, at least, may be utilized somewhat differently in the advanced system. Designers must be certain that new tools and representations support the different tasks controllers will be expected to perform, while maintaining and if possible enhancing their situation awareness (see below).

13. ***The primary objective of information automation is to maintain and enhance situation awareness. All display modes must contribute to this objective.***

The radar controller's video display units or radar scope are the sole means by which he or she can maintain cognizance of the system being controlled or monitored. Much progress has been made over the years in reducing ambiguity, clarifying presentations, providing aiding features and improving the quality of the input data which is processed for use on this display. Ordinarily, these representations of system activity are sufficient to keep controllers "in the picture" by providing them with information they use to update their mental models of the traffic under their control.

Efforts have been made over the years to improve these representations. In particular, attempts have been made to provide three-dimensional representations of air traffic, thus far without notable success. A planform display remains the standard in air traffic management, as it does in most military command and control systems. The fact remains, however, that a good deal of cognitive activity is required to construct and maintain a three-dimensional mental model from the available imagery. Not all controllers accepted for training ever develop the ability, and this is one reason for high attrition rates in controller training.

The advent of advanced display media incorporating color and improved imagery offers the opportunity to examine again various aspects of ATC displays, with the aim of decreasing the mental effort involved in their interpretation. Among the features that have been proposed is more effective highlighting of significant events and new alerting techniques. Care must be taken, however, to insure that controllers can transition easily from the old to newer displays. Equally important, attempts should be made to assist the controller unfortunate enough to lose his mental model of traffic to regain it more easily and quickly, by systematic analyses of the cognitive processes now used by expert controllers and the provision of visual aids keyed to flight progress data.

14. ***ATC automation interfaces should be as simple and intuitive as possible.***

Digital cockpit interfaces (the CDU), with which pilots must interact by entering alphanumeric strings, are a major source of distraction from outside scanning by the non-flying pilot. The controller often will not have a data person assisting him or her, and will have to divide his/her attention between the primary display and the electronic flight data displays. If data entry in the AAS is made as cumbersome as it sometimes is in aircraft, another major distraction from the primary task of maintaining traffic surveillance will have been introduced.

It has been pointed out that invoking display aiding functions may require significantly more manual effort in prototype advanced sector suites than in the older display units. This situation is analogous to the clumsiness of certain FMS functions in the cockpit. It will assuredly lead to less use of these functions during periods of high workload, when they may be most needed (see also guideline 9, above). Every effort must be made to assist controllers in calling up the functions most used as quickly and easily as possible, with the least diversion of visual and cognitive attention from traffic. Controllers in the future will be required to interact more with their computers rather than less; the lessons learned from clumsy avionics automation should be applied here.

15. ***Future ATC automation must insure that traffic control remains within the capabilities of the human operator who must accomplish the task if the automation fails.***

Today's air traffic control system, particularly in crowded terminal areas, is operating to tighter tolerances than have ever before been permitted. The trend toward decreasing tolerances still further will continue, not only around airports but in continental and oceanic enroute airspace as well. The FAA has specified extremely high reliability for critical elements of the future automated system (some hardware elements can be off-line for only four seconds per year!), but it can be predicted with utter confidence that functional failures will continue to occur, whether due to software bugs, communications system failures, environmental contingencies, human errors or acts of God. In those cases, human controllers will be required to "make do" safely despite degraded machine capabilities, as they have always had to.

The problem with this is that new automation may well enable the system, when it is functioning normally, to operate at higher capacities and to tighter tolerances than are possible when the human controller is operating without the automated tools. If higher throughput is possible with new technology, it will become, over time, the normal and expected throughput. Hollnagel's concept of risk homeostasis (1993) applies here, as elsewhere. Procedures must be devised to permit the human-machine system to operate safely under *all* contingencies which may arise. Among the conditions that *will* arise is machine failure, and the reversion procedures must take account of human capabilities and limitations.

The system software will be subjected to exhaustive testing before it is placed on line. Care must be taken to explore the margins of its operational envelopes, however, to insure (insofar as is possible) that it is not brittle—that there are not conditions under which it begins to behave in ways that makes the controller's task more difficult.

16. ***ATC automation must be comprehensible to controllers.***

This guideline is a general caution which is applicable to control, information and management automation. The increased amount and sophistication of future ATC automation will inevitably be accompanied by greater complexity and less transparency as more functions are automated and coupled. Particular care should be taken to constrain the number of new modes in which the automation can operate. Sarter and Woods (1994) have talked of "mode-rich" automation in aircraft; Woods (personal communication, 1994) has made plain his belief that ideal automation should be "modeless". Simpler automation will both speed the transition to the new system and increase its acceptance. More important, it will decrease the likelihood of human errors in its use, both initially and throughout its lifetime. Controllers must be helped to understand not only how to operate the new devices, but how the new devices operate and their limits, if they are to remain in command of the system.

17. ***ATC automation should perform tasks in a manner understood by controllers.***

It is accepted that future control automation will have a longer predictive threshold, or "window", than do human controllers, and that this ability to resolve conflicts over a longer time and a wider space will be important when more aircraft are on random tracks. Nonetheless, decisions made or offered by the automation will be more likely to be understood and accepted by human controllers if those decisions incorporate conflict resolution strategies similar to, or at least understood by, those controllers. The automation must be able to explain its decisions if requested, preferably by graphic representations that can be assimilated quickly and easily (see guideline 18).

18. ***The controller must be able to visualize the consequences of a decision, whether made by him/her or by the automation.***

I have mentioned my concern that an automated air traffic control function which can resolve potential conflicts over a longer time period may place human controllers in the position of being unable to visualize the likely consequences of their decisions (when the conflict resolution occurs in a downstream sector), and unable after the fact to determine whether their decision was in fact appropriate. This undesirable state of affairs puts the controller in the unpleasant position of being unable to select knowledgeably among machine-offered decision options, and unable to learn from subsequent experience whether the options selected were the right ones.

I believe, therefore, that it is important that human controllers be able to visualize, by viewing predictive displays, the likely consequences of a conflict resolution decision, whether that decision is made by them or by the automation. It is also important that controllers be able to visualize a wider field of view on request in order to view the resolved situation later, to obtain feedback concerning their earlier actions.

19. ***ATC automation should be designed to assist the human controller to manage workload.***

Several studies of controller operational errors have indicated that larger numbers of errors tend to occur during periods of low or moderate, as opposed to high, controller workload (usually measured as number of aircraft being controlled) (Rodgers & Nye, 1993). If this is the case, then future automation that relieves the human controller of most routine workload may tend to *increase* the likelihood of human error, even though the automation may assume a portion of the tasks in which errors might be committed.

There is an urgent need for further studies of the relationship between level of automation and the probability of errors in human tasks. Some laboratory work has been done, but before automation design is predicated on the results it is necessary that studies in more naturalistic settings be performed. It is possible that the CTAS evaluations planned at Denver and Dallas-Fort Worth in the immediate future may yield new insights into the relationships between workload and error in more automated environments, but it is also quite possible that CTAS, which maintains a high level of human involvement by design, may not be an appropriate analog of a future enroute system in which the controller is less actively involved in routine operations. (See also the following guideline.)

20. ***The human controller must be kept involved in the operation by being required to perform meaningful and relevant tasks, regardless of the level of management automation being utilized.***

One of the stated objectives of the AAS is to improve controller, and therefore system, productivity. Whicher (in Cooper, 1994a) suggested that "To permit unrestricted ATC growth we should first determine how to eliminate one-to-one coupling between a proactive sector controller and every aircraft in flight—and so avoid him becoming reminiscent of the man with a red flag in front of early motor vehicles...Pilots can and are willing to take direct responsibility for...track-keeping functions, freeing controllers to concentrate on the key areas where human skills have most to offer—traffic management, system safety assurance and dealing with the exceptional occurrence" (p. 8).

I would argue that the degree to which the controller becomes involved with individual aircraft should, within reasonable bounds, be his or her choice: in other words, that the controller should have the freedom to select the level of control and management to be exercised under particular circumstances, just as pilots now may select the level of automation assistance they wish to invoke. There should certainly be levels which provide considerable assistance, to permit the controller to focus on specific problems. There should also be levels which permit the controller to direct traffic, in order to retain the skills necessary for minimally aided control. But at each level, the controller must have meaningful tasks to perform. As noted above, each level of management must be a *cooperative* endeavor between the human and the machine, requiring active participation by both components of the human-machine system.

21. ***Automation must never be permitted to perform, or fail, silently.***

Much of the activity of future ATC automation will be transparent to human operators. In particular, its ongoing or periodic monitoring of trajectories and its continuous searching for potential conflicts will not (and should not) be visible. The operator, however, must be informed that these activities are ongoing, for the absence of such information can mean either that the machine has not located any potential events of interest, or that it is not performing correctly. Ways must be found to keep controllers informed of these processes, and of their failure if the automation becomes degraded in any respect.

22. ***ATC automation should be designed for maximum error resistance and error tolerance.***

The future AAS will be designed with improved error resistance, in that automated conflict prediction will be an essential element. Controllers will remain responsible for insuring that conflicts do not occur, but computers will augment their watch over traffic and will probably provide decision options to assist them in resolving conflicts when they are detected. These automated functions will thus increase the redundancy of the ATC system. The automated safety functions in use today: conflict alert, minimum safe altitude warnings, etc., will still be there performing their vital monitoring functions and acting to improve the error tolerance of the system. Can more than this be done? I believe it can.

As indicated previously, data link architecture should be designed to insure that ATC computers receive confirmation of flight path changes when they are executed in flight management computers or through mode control panel entries. These data, indicative of aircraft intent, should be automatically compared with previously-issued ATC instructions to insure conformity with planned trajectories. If there is a conflict, a controller should be notified so that he or she can determine where the difference lies and resolve the problem. In today's system, detection of an incorrect or undesired flight path can only occur after the airplane has already strayed appreciably from the desired path. *Prospective* monitoring of airplane intent would make it possible, in many instances, to detect and correct these problems before they happen. This functionality could prevent a substantial fraction of the altitude deviations that plague today's system. The UK CAA flight demonstration in early 1991 indicated the feasibility of such an approach, using currently available equipment. Note, however, that proposals for free flight do not make use of a "flight plan contract" that would facilitate prospective monitoring.

23. ***Emphasize information in accordance with its importance.***

More information displayed on VDUs will increase controller workload. Consideration should be given to the use of a limited number of auditory signals to denote information of particular importance. One promising way to direct attention to an event of interest, for instance, is to use synthesized directional auditory signals to indicate the approximate azimuthal location of the event. The technology has been evaluated in flight simulations as a way of drawing attention to potential conflicts detected by TCAS (Begault, 1992); it has proved quite effective in that application. This approach may likewise offer potential benefits in air traffic control.

The use of color to increase the salience of displayed signals can be effective in attracting attention, but redundant coding of such signals should be implemented wherever possible. Size, shape and brightness cues in addition to color will make it more likely that important information will be attended to.

24. *Alerting and warning displays should be as simple and foolproof as possible.*

Alerting and warning systems in current ATC suites are fairly simple, in part because the monochrome displays permit only the use of blinking symbols and auditory warning tones as information transfer devices. The use of advanced color displays will permit the use of colors, new icons and other symbols as alerting devices. It will be important to keep alerts to a minimum, in order that their meanings remain simple and universally understood. Wherever possible, the exact nature of the alert, and the aircraft involved, should be specified in a way that immediately makes the nature of the problem obvious to the responsible controller.

Consideration should be given, as noted earlier, to providing alerting trend information to the appropriate controller before mandated boundaries are encroached upon. There is a danger that this will lead to an increased number of nuisance alerts under some circumstances; that danger should be balanced against the problem of not warning until a violation has occurred. Certainly the prevailing practice of broadcasting audible conflict alerts is undesirable from a psychological viewpoint; it holds an "offending" controller up to ridicule, and it distracts others who may be busy solving their own problems.

25. *Less information is generally better than more information, if it is the right information for a particular circumstance.*

The increased functionality of the advanced automation system will provide more information that may be useful to controllers. It will also bring the temptation to add that information to controller displays, as the implementation of advanced automation has added complexity to aircraft displays. New display elements should be considered for display only if consultation with active controllers reveals that it will add significantly to their capability. If a consensus is in favor of adding elements, it must be realized that the additions will tend to distract from attention to existing elements; every effort should be made to simplify, rather than make more complex, the information extraction task. The addition of the color modality can help direct attention, but the temptation to add color for color's sake or to make a more visually appealing picture must be resisted. It is quite likely that a simple, largely monochrome representation, with color used only sparingly for very specific purposes, will be most effective.

26. *Integration of information does not mean simply adding more elements to a single display.*

If displays are to be redesigned in any major way, consideration should be given to a higher degree of integration of the existing displays if this can be accomplished without compromising the integrity of the critical information. Data from on-the-job training with regard to task elements that are difficult for trainees to assimilate would be helpful to the designers of these displays. In order to effect maximum transfer of training from the present to the new controller suites, it is quite possible that essential elements of the old displays should be retained unchanged or only minimally modified.

New features should be displayed analogically or by means of icons where appropriate. Wherever possible, displays should focus attention on changes in the data and on events of potential interest, leaving static or less interesting data in the background.

Comment

The Wiener (1993) and Woods et al. (1994) discussions of error management should receive careful attention from ATC system designers as well as the operators of the system (see chapter 10, guidelines for error management). The future AAS has been widely espoused as a system that will minimize human errors; it is more likely that it will transform them as automation has done in aircraft, foreclosing some while enabling others. What is critical is that the future system also be effective at detecting, trapping and mitigating the effects of those errors that will still occur.

It is worth pointing out once again that enroute and approach/departure controllers, unlike pilots, cannot "see out the window"—that their *only* contact with the real world is through the representations provided by their traffic and other displays. Woods (1994a) has discussed the heavy obligation this places on the designer, who must create virtual representations that provide all needed information under all circumstances. Human operators can visualize the processes they are controlling *only* through such representations—the "keyholes" provided by the computer.

I believe that to keep controllers actively involved in their task, it is necessary as well as desirable to provide them with a moderate degree of management flexibility, by permitting them to take a more, or less, direct role in controlling traffic. They should be able to be supervisory controllers when they wish, or to be more active in the process. This alone will maintain their skills if there are circumstances under which they may have to revert to a direct controlling role.

Given the limited reliability of automation to date, I think it very unlikely that the AAS will be infallible; no other advanced automated system has ever been, regardless of its specifications. Further, if controllers are to continue to be considered professionals, it is vital that they be given a measure of authority over their own working conditions, which includes (as with pilots) a degree of choice as to the means by which they wish to accomplish the job. With adequate computer monitoring, this should not lead to increased numbers of critical errors. Rather, it is more likely that it will permit controllers to make best use of their automation at some level even when its full capabilities are not available.

12. Guidelines for certification of aviation automation

Introduction

A criticism of the earlier NASA Technical Memorandum on Human-Centered Automation (Billings, 1991) was that it made almost no mention of certification and included no guidance with respect to that process. I am indebted to the FAA Air Transport Certification personnel who drew my attention to this oversight. This chapter is accordingly devoted to a brief consideration of aircraft certification from the human factors viewpoint, and to some suggested guidelines for certification personnel. I acknowledge here the help and support provided by the late Berk Greene, and the guidance so kindly made available by Donald Armstrong and Guy Thiel, all FAA certification pilots, in the preparation of this chapter.

In the United States, the FAA is solely responsible for certifying new aircraft and avionics equipment. Recognizing the extreme problems that would result were an uncertifiable aircraft to be presented for approval at the end of its development cycle, certification people, all of them highly experienced engineers and pilots, are deeply involved in discussions with aircraft manufacturers throughout the design process. In this consultative process, which goes on for several years, they become intimately aware of novel or different features that may be incorporated into a new design. Their advice is sought on issues that may be problematical or that may raise concerns later in the certification process. (Unfortunately, this is less likely to be true for new functions when they are proposed for aircraft already in service. Such modifications would benefit from the input of certification personnel, but they often are not consulted.)

The certification role is a difficult one. Title 14, Code of Federal Regulations (CFR), Part 25, Airworthiness Standards: Transport Category Airplanes, governs the certification process. § 25.1, **Applicability**, says only the following:

(a) This part prescribes airworthiness standards for the issue of type certificates, and changes to those certificates, for transport category airplanes.
(b) Each person who applies under Part 21, for such a certificate or change, must show compliance with the applicable requirements in this part.

A manufacturer may choose to satisfy the requirements set forth in part 25 in any of a considerable number of ways. If compliance can be demonstrated, the airplane must be certified, even if the certifying authorities are less than comfortable with the approach that has been taken. While common sense usually prevails, certification staff cannot demand more than the regulation requires. Their decisions are constrained by the Administrative Procedure Act, which forbids arbitrary or capricious actions by the Administrator; a finding of non-compliance can be grounds for an appeal under this Act.

The only other regulation bearing directly on the type certification process is Part 21; §21.21 describes the conditions under which an applicant is entitled to a type certificate:

(2) For an aircraft, that no feature or characteristic makes it unsafe for the category in which certification is requested.

This requirement is powerful but little used, because it switches the burden of proof from the manufacturer to the certifying authorities to show how a design feature or characteristic is both unsafe and not otherwise addressed in the basic regulation. More often, new technology is handled by the development of special conditions: rulemaking for particular novel or unusual design features that were not envisioned when the appropriate sections of Part 25 were adopted. Here, the Administrative Procedure Act applies; special conditions must be handled like any other rulemaking, with publication in the Federal Register, the seeking of public comments, and the addressing of those comments before the special condition can be made effective. This time-consuming process, unique to the United States, makes establishment of the complete body of airworthiness requirements for a new or highly-modified aircraft occur much later in the design process than the manufacturer would prefer—akin to starting the ball game without knowing where the goal posts are.

Further, certification is usually the final step in a new airplane's development process. Given the schedule slips that invariably occur in the course of a complex airplane's years-long development and the financial burden on the manufacturer if initial deliveries of a new airplane are delayed, the FAA certification staff is routinely under enormous pressure throughout the latter phases of the certification process, especially if all does not go as planned or if some areas require further study or flight test. The certification process itself is extremely expensive because of the substantial amount of flying required, and this is another factor that places pressure on FAA personnel.

Finally, today's airplanes are software-intensive; the Boeing 777 incorporates some 5 million lines of source code in its various computers. Software verification is extremely difficult, and "bugs" are bound to occur as the airplane goes through its flight testing, including certification. These can also complicate and delay the certification process.

At present, the handling of software revisions deemed to be hazardous should erroneous information result requires extensive software verification and validation before approval. Because so many of the "bugs" are discovered late in the certification program, flight crew "workarounds" are often resorted to in order to obtain certification on schedule. The result is a succession of program upgrades, typically about a year apart; in the meantime, the burden of remembering to use the "workarounds" falls upon line pilots. This certification process lacks a method of "beta testing" because the total product must be fully approved before delivery. The only control device available to certification authorities is a limitation against use of the deficient modes, or reliance on workarounds.

Regulatory basis for considering human factors in certification

Some sections of Part 25 cover various aspects of the standards in exquisite detail, with precise quantification of the required performance. Other parts, however, go into much less detail and require highly subjective judgments on the part of the certifying authorities. Nowhere is this more obvious than in the section that discusses crew complement. § 25.1523, **Minimum flight crew**, is quoted in its entirety:

> The minimum flight crew must be established so that it is sufficient for safe operation, considering—
>
> (a) The workload on individual crewmembers;
>
> (b) The accessibility and ease of operation of necessary controls by the appropriate crewmember, and
>
> (c) The kind of operation authorized under § 25.1525.
>
> The criteria used in making the determinations required by this section are set forth in Appendix D.

Extracts from Appendix D are shown here:

> *Criteria for determining minimum flight crew.* The following are considered by the Agency in determining the minimum flight crew under § 25.1523:
>
> (a) *Basic workload functions.* The following basic workload functions are considered:
>
> (1) Flight path control.
> (2) Collision avoidance.
> (3) Navigation.
> (4) Communications.

(5) Operation and monitoring of aircraft engines and systems.
(6) Command decisions.
(b) *Workload factors*. The following workload factors are considered significant...:
(1) The accessibility, ease, and simplicity of operation of all necessary...controls...
(2) The accessibility and conspicuity of all necessary instruments and failure warning devices...The extent to which such instruments or devices direct the proper action is also considered.
(3) The number, urgency, and complexity of operating procedures...
(4) The degree and duration of concentrated mental and physical effort involved in normal operation and in diagnosing and coping with malfunctions and emergencies.
(5) The extent of required monitoring of (aircraft systems) while enroute.
(6) The actions requiring a crewmember to be unavailable at his assigned duty station...
(7) The degree of automation provided in the aircraft systems to afford (after failures or malfunctions) automatic crossover or isolation of difficulties to minimize the need for flight crew action to guard against loss of hydraulic or electric power to flight controls or to other essential systems.
(8) The communications and navigation workload.
(9) The possibility of increased workload associated with any emergency that may lead to other emergencies.
(10) Incapacitation of a flight crewmember whenever the applicable operating rule requires a minimum flight crew of at least two pilots.

This guidance was last amended in 1965, at about the time the first model of the Boeing 737 was in its development process. In 1986, the FAA issued an Advisory Circular, AC 25-1523, Minimum Flightcrew, in which it provided expanded guidance based on its earlier Engineering Flight Test Guide for Transport Category Airplanes (FAA Order 8110.8). The regulation itself takes no account of the radical changes that have occurred on the flight deck since that time, nor of the revolution caused by digital computational capability, as discussed in chapter 4, but the revised guidance is considerably more specific and discusses acceptable methods for determination of flight crew workload.

In all transport aircraft, the minimum flight crew is fixed by design at the beginning of development. The FAA's role is to evaluate the design as operated by the minimum crew using the manufacturer's proposed procedures. If problems are encountered, they are inevitably resolved by rebalancing workload and revising procedures, not by increasing the minimum flight crew.

The overarching issues

Certification personnel are not evaluating simply aircraft components. They are given *an airplane*, which must operate as an internally-consistent entity. The machine is very complex, yet all of its functions must operate together harmoniously. As certification pilots examine all of these many functions, they must always consider how an average pilot operating under difficult circumstances might misunderstand, misread or misinterpret what he or she sees; how such a pilot might be led to inappropriate decisions by the information provided by the machine; how he or she might make errors of omission or commission in executing those decisions; how line pilots might find it difficult to recover from failures or their own errors, and how tolerant the airplane will be of such mismanagement when it is in line service. They must do all of this in a comparatively short time, always under pressure, and they must then accept the responsibility of approving the airplane. This is not a job for the faint-hearted.

The certification process

Faced with this mandate and these constraints, certification authorities have attempted to evaluate flight deck workload in comparative terms, measuring the difficulty of the flight crew's tasks in each new airplane against workload in earlier, "benchmark" airplanes certified for and successfully operated by a crew of two persons. As noted in chapter 1, the findings of the Presidential Task Force on Crew Complement (1981) effectively permitted the FAA to certify aircraft of any size for a two-person crew, provided that sufficient aids were provided to keep workload within tolerable limits.

This comparative evaluation is carried out by FAA certification pilots and other highly experienced air carrier inspectors. It necessarily yields subjective estimates of workload, though attempts have been made in recent years to utilize quantitative measures derived from empirical research. Aircraft are evaluated in operational scenarios which simulate air carrier operations as much as possible. A variety of malfunctions is simulated in the course of the workload certification flights, including the incapacitation of one crewmember as required by Appendix D. Among the simulated malfunctions are failures and degraded operation of many elements of the automation.

It should be noted that aircraft are certified under Part 25 of the FAR. After certification, however, they are operated under Part 121 of the regulations. Part 25 says little about either the range of conditions encountered in line flying, or about the capabilities of the range of air carrier pilots who will operate the new airplane. Though an attempt is made in certification to examine the widest range of environmental conditions and malfunctions possible, only a very limited subset of these conditions can be evaluated. Likewise, only a very limited number of Agency pilots, all highly experienced, can take part in the certification process, which means in effect that until the first airplane is delivered, it will have been flown extensively only by company and FAA pilots of above-average experience and ability.

Transport aircraft are among our nation's most important exports. The United States has led the world in the design and production of aircraft throughout most of the history of aviation. The FAA is widely regarded as the model for aircraft certification, and those involved in the process must continually be aware that they are certifying machines that will be operated throughout the world. Though certification is carried out solely under U.S. regulations, the difference between our rules and those of other nations imposes yet another source of implicit pressure on certification staff. A major effort is underway at this time to reconcile, or "harmonize", our regulations and those of the European Union Joint Airworthiness Authority, which will regulate the certification process in Europe. Since the fall of the Soviet Union, airworthiness considerations applied in the Commonwealth of Independent States have also had to be considered, as U.S. aircraft begin to penetrate the market in the newly independent states of northern Asia. It should be mentioned also that the issue of cultural differences, and their impact on flight crew operations, is another aspect of the problems faced by certification personnel, who know that the aircraft will be used in different ways by operators worldwide.

I have pointed out previously that operations well within the envelope may not show evidence of brittle automation (see chapter 7), nor for that matter of organizational latent factors which may come to light only when a line crew is fatigued or distracted by other operational anomalies. All of these factors are considered by certification pilots, themselves operating under a different sort of pressure, but it is not surprising that operational problems with new aircraft sometimes are not recognized until they are operating in line service.

Other relevant sections of FAR Part 25

Several other sections of Part 25 contain material which, taken together, are relevant to discussion of human factors requirements for certification. They are abstracted here:

§ 25.143: **Controllability and Maneuverability**

(a) The airplane must be safely controllable and maneuverable during—

(1) Takeoff;

(2) Climb;

(3) Level flight;
(4) Descent; and
(5) Landing.

(b) It must be possible to make a smooth transition from one flight condition to any other flight condition without exceptional piloting skill, alertness, or strength, and without danger of exceeding the airplane limit-load factor under any probable conditions...

§ 25.171: **Stability**

The airplane must be longitudinally, directionally, and laterally stable...In addition, suitable stability and control feel (static stability) is required in any condition normally encountered in service, if flight tests show it is necessary for safe operation.

§ 25.671: **Control Systems**

(c) The airplane must be shown...to be capable of continued safe flight and landing after any of the following failures or jamming in the flight control system and surfaces...within the normal flight envelope, without requiring exceptional piloting skill or strength. Probable malfunctions must have only minor effects on control system operation and must be capable of being readily counteracted by the pilot...

(d) The airplane must be designed so that it is controllable if all engines fail...

§ 25.672: **Stability augmentation and automatic and power-operated systems**

If the functioning of stability augmentation or other automatic or power-operated systems is necessary to show compliance with the flight characteristics requirements of this part, such systems must comply with § 25.671 and the following:

(a) A warning which is clearly distinguishable to the pilot under expected flight conditions without requiring his attention (sic.) must be provided for any failure in the stability augmentation system or in any other automatic or power-operated system which could result in an unsafe condition if the pilot were not aware of the failure. Warning systems must not activate the control systems.

(b) The design of the stability augmentation system or of any other automatic or power-operated system must permit initial counteraction of failures...without requiring exceptional pilot skill or strength, by either the deactivation of the system, or a failed portion thereof, or by overriding the failure by movement of the flight controls in the normal sense.

(c) It must be shown that after any single failure of the stability augmentation system or any other automatic or power-operated system—

(1) The airplane is safely controllable when the failure or malfunction occurs at any speed or altitude within the approved operating limitations...

(3) The trim, stability, and stall characteristics are not impaired below a level needed to permit continued safe flight and landing.

§ 25.771: **Pilot compartment**

(a) Each pilot compartment and its equipment must allow the minimum flight crew...to perform their duties without unreasonable concentration or fatigue.

(c) If provision is made for a second pilot, the airplane must be controllable with equal safety from either pilot seat.

§ 25.1309: **Equipment, systems, and installations**

(c) Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards.

§ 25.1329: **Automatic pilot system**

(a) Each automatic pilot system...must be designed so that the automatic pilot can be quickly and positively disengaged by the pilots to prevent it from interfering with their control of the airplane...

(f) The system must be designed and adjusted so that...it cannot produce hazardous loads on the airplane, or create hazardous deviations in the flight path, under any condition of flight appropriate to its use, either during normal operation or in event of a malfunction, assuming that corrective action begins within a reasonable period of time.

(h) If the automatic pilot system can be coupled to airborne navigation equipment, means must be provided to indicate to the flight crew the current mode of operation. Selector switch position is not acceptable as a means of indication.

§ 25.1335: **Flight director systems**

If a flight director system is installed, means must be provided to indicate to the flight crew its current mode of operation. Selector switch position is not acceptable as a means of indication.

In addition to this regulatory guidance, a number of Advisory Circulars apply to specific facets of certification where no other guidance is available.

Guidelines for human factors certification

Recognizing that FAA can legally impose only a *minimum* standard as codified in regulations that in many respects do not incorporate the lessons learned during a period of exceedingly rapid technological advances, can any generic guidelines be offered that can help certification authorities? They, after all, are the experts, and it is presumptuous to assume that this very difficult and exacting job can be thoroughly understood by anyone who has not "been there". Nonetheless, a careful examination of Appendix D and the remainder of Part 25 suggests certain areas in which requirements can be suggested, if only to provoke argument.

I shall incorporate here the thoughts set forth in chapter 2, *A concept of human-centered automation,* as the overarching philosophy which should be applied. I believe this is justified by a careful reading of the regulation, which states repeatedly that flight must be possible under a great variety of conditions without exceptional skill or strength, and that it must be possible for the pilot to remain in command of the airplane under all but extremely improbable failures. The pilot must be warned of potentially unsafe conditions; the airplane's design must minimize crew errors. The crew must be able to perform their duties without unreasonable concentration or fatigue.

The regulation discusses workload and discusses factors that may increase it, but does not consider the possibility of workload being too low, a factor not thought about very much prior to the introduction of advanced automation. It has become clear in the last decade or so that either overload or underload can pose hazards; both are considered here.

Principles for certification of human-centered aircraft automation

With regard to the "first principles" of human-centered automation (chapter 2), the following general guidelines or requirements are suggested. They are also summarized at the end of this chapter.

1. ***Automation should not be able to remove the pilots from effective command of their aircraft.***

   It has been indicated elsewhere that sophisticated automation can decrease pilot authority in ways that may not be immediately evident. I believe that pilots must be made aware of any modes or features that may act in this way, and that provisions should be incorporated to permit them to "quickly and positively" override these functions when an emergency requires it.

2. ***Automation should not remove the pilots from direct involvement in the operation.***

In 1965, when the present Part 25 was implemented, "underload" was not a serious problem. The term "automation complacency" had not yet been invented, and such automation as was available accomplished only tactical functions under direct instruction from pilots. The regulation did take note of the ease with which pilots could mistake and misuse navigation modes and required that these modes be annunciated (and errors in selection of these modes continue to occur today). New automation should keep pilots meaningfully involved in the operation, by whatever means. I also believe ways should be found to increase that involvement to minimize the likelihood that they will accept and tolerate inappropriate mode selections, especially in long-range aircraft in which workload is likely to be very low.

3. ***Automation must keep the pilots informed of its actions.***

Recognizing that automation now performs a great number of discrete functions as well as the continuous task of flight path control, it is increasingly necessary that the automation inform the human operators of what it is doing. This guideline is intended to suggest that pilots must remain involved with, by being informed of, the actions of the automation that conducts the flights that they manage, as well as of failures in that automation. In the Nagoya accident (1994), autotrim was being applied, but there was no audible or other signal to indicate this activity. When the pilot regained control, the pitch trim was in an extreme nose-up condition.

4. ***Automation failures or malfunctions must be clearly annunciated to the pilots.***

Because automation performs discrete as well as continuous functions, its failure to continue performing these functions may not be obvious. This guideline is intended to suggest that such failures must be positively annunciated to the crew.

5. ***Automation must behave predictably under all circumstances.***

Much of this book deals with the importance of predictability in the behavior of automated systems, so that pilots can form a "correct" mental model of their functions. Very complex functions are especially likely to be misunderstood by pilots. It is important that they be able to follow, whether by dedicated displays or by the behavior of the airplane and its systems, the behavior of the automation. Means must be made available by which they can accomplish this critical monitoring task without undue attention. Equally important, the automation must behave predictably, in a manner that facilitates monitoring by its human operators.

6. ***Automation should monitor the actions of pilots and should warn them when their actions pose a potential threat to safe continuation of the flight.***

We know that humans err with some frequency, and a great deal is known from operational experience about serious and potentially dangerous mistakes in the operation of highly automated aircraft. Automation should monitor human behavior with respect to known or likely sources of error, and should alert pilots when their behavior does not comport with appropriate operating procedures. A deliberate attempt should be made during certification trials to make such errors and to insure that automation either proscribes them without specific consent, or warns against them. Humans are not very good monitors; computers are excellent monitors, but they have not been given this task to nearly the extent that they should have been. Increased error resistance and error tolerance should be primary aims of advanced automation in new aircraft.

7. ***Automation should inform pilots of its intentions and should request consent for actions that may critically affect the conduct of the flight.***

An essential ingredient of what Endsley (1994) calls "deep" situation awareness is an understanding of the near-term future situation. Just as I believe that humans must be given the means by which to indicate their intent to the automation assisting them, I believe it is essential that automation indicate its near-term intent to the humans on the team, especially when mode changes, major changes in state or changes that could compromise the ability of the airplane to complete its mission are contemplated. This occurs today under some circumstances (the "flare" annunciation during coupled approaches, the green arc on the navigation display), but it should be applied as a general rule in complex systems.

Guidelines for the certification of control automation

8. ***Automation involving modes of control known to be potentially hazardous should contain safeguards to guard against its use under inappropriate conditions.***

Experience has shown that under certain circumstances, the "open descent" mode of operation can present predictable hazards. If such a mode is provided, should it be allowed to operate without restrictions to prevent it being used below a safe altitude? Similarly, it is known that the "vertical speed" mode can result in a critical decrease in airspeed during climbs at higher altitudes. The possibility of this misuse of the VS mode should be guarded against when the mode is implemented.

Other automated modes may have to be used under circumstances which could present potential hazards. They should be identified and appropriate cautionary information should be provided to pilots under those circumstances, as occurs when alpha floor protection is removed during landing (see accident at Mulhouse-Habsheim, 1989). Design features that experience has shown to be hazardous should not be utilized without such safeguards against misuse or inadvertent use in the stress of line operations.

9. ***Automation design must permit its use at some lower level of authority if stability augmentation systems have failed.***

Fly-by-wire technology has made direct manual control of aircraft impossible under most circumstances. Even "manual" flying is accomplished through computer assistance in these aircraft, and the normal mode of operation is the fully assisted mode. In the A320/330/340 series, a "direct" mode of control is available if the normal mode fails. In this mode, many of the protections built into the flight control system are bypassed, and the airplane flies as though directly controlled by the pilot through the proportional sidestick controller. The automation has less authority, but the pilot's authority is unchanged.

An analogous reversion mode should be available in any aircraft having highly augmented controls, but it must be capable of being used under normal conditions as well so that pilots may remain proficient in its use through regular practice. Ideally, it should "feel" as much like the normal control modes as possible, so that the pilot is able to accomplish the control task without significant diversion of attention from other tasks.

10. ***Marginally stable aircraft should be required to have full-time automation assistance, even in reversion control modes.***

Some newer aircraft have deliberately been designed to be neutrally stable or marginally unstable in the pitch axis. Any tendency to instability is compensated for by automated stability augmentation systems. Such aircraft can be difficult to fly if the augmentation fails. (The Space Shuttle is an extreme example of this problem.) Such aircraft should incorporate back-up augmentation to alleviate pilot workload in event of a failure of the primary systems. Again, the less difference in control feel between the primary and backup systems, the less will be the added workload for the pilots following such a failure.

This may also be a problem in aircraft (such as a future high-speed civil transport, HSCT) that incorporate automatic center of gravity trimming for high-speed flight. Either a means to return the center of gravity to an appropriate range automatically, or assistance in flying the airplane following an automation failure, should be incorporated in such aircraft, to keep pilot workload within reasonable limits. With regard to the HSCT, the same can be said regarding flight on the "back side of the power curve", which will be required during low-speed flying during the approach to landing. To quote from Part 25, "The trim, stability, and stall characteristics are not impaired below a level needed to permit continued safe flight and landing"; this should also be true in any reversion mode.

Guidelines for the certification of information automation

11. ***Primary flight displays have become extremely complex. Certification pilots must decide how much information is too much.***

Though navigation displays in newer aircraft have been integrated and, in the process, have become easier to read, primary flight displays have become more cluttered through the addition of a considerable amount of additional information. Mandatory TCAS and wind shear advisory systems have added still more information to this display. Certification personnel should give consideration to whether this much information on the primary flight display is likely to distract, rather than inform, pilots when they are heavily task-loaded.

The PFD is critical for situation awareness, but the amount of information presented on this screen may be reaching limits using the conventional format. An increasing amount of data on this display is presented as alphanumerics, which must be read serially to be comprehended. This is also true of the mode annunciation panel which appears on this screen. Certification authorities should consider whether pilot duties can be performed "without unreasonable concentration or fatigue" using these displays.

Woods (1994a) has pointed out that how information is represented is absolutely critical. The combination of discrete and continuous data into a more integrated display (such as the symbolic combination of velocity and acceleration data on some tape airspeed displays) can enable considerably easier and more precise speed control, particularly during turbulence. The use of flight path vector symbols is another example long advocated by Bray and others as an information management and integration tool.

12. ***Do the most important information elements stand out in complex displays? Has proper use been made of order, form, thickness of line segments, size and font of type and use of empty space, as well as color, to highlight particularly salient information?***

Appendix D of Part 25 also emphasizes "the...conspicuity of...failure warning devices" as a workload factor. Though the number of discrete warning and alerting devices has been decreased considerably in glass cockpit aircraft, the number of discrete messages that can occur is still large and these alerts are almost invariably alphanumeric: they must be read to be comprehended. All are usually in the same size print; more important items may be boxed and shown in a different color.

On busy displays, however, this may not be sufficient to draw attention to the most important items in what can sometimes be a lengthy list (see incident report that begins chapter 13). Is the most critical information always obvious? Is the busy pilot's attention drawn to the items requiring action?

13. ***The status of flight-critical automation should be obvious at all times, not only when some element has failed.***

This is a corollary of the first principles. It is an appropriate guideline in view of Part 25, Appendix D, which states that "the degree and duration of concentrated mental...effort involved in normal operation" is to be considered as a workload factor. Affirmative information concerning automation activity, modes and especially mode changes is much more easily monitored than the lack of such information. It is possible that an automation synoptic could be of help in view of the complexity and depth of the automated systems in advanced airplanes.

Guidelines for the certification of management automation

Management automation was in its infancy when Part 25 was rewritten in 1965. It is not surprising that it was not considered in the regulation. Nonetheless, Appendix D cited "the degree of automation provided in the aircraft systems" as a workload factor, and coupled navigation systems were discussed. The certification staff over time has developed precedents and an Advisory Circular which deals with flight management systems and there is little question that they are of great value in today's system.

Bearing in mind that these management aids do relatively little that pilots cannot do without them aside from over-water navigation (though at the cost of much higher workload), what guidelines are appropriate in this area? Those which I offer here have more to do with present systems than with those that may be implemented in the future, for the reasons stated elsewhere in the document about the direct and indirect costs of moving to a radically redesigned flight management system in a future aircraft.

14. ***Flight management systems and their associated control-display units should assist pilots in programming, particularly for seldom-performed functions.***

As pilots gain experience with the FMS, they become facile in performing those tasks that they are required to perform frequently. Errors in programming these functions are usually slips or lapses rather than mistakes. Where possible, the CDU should indicate the error when it rejects an entry.

Rarely-performed programming tasks are less likely to be recalled when needed. Cueing should be available in the software to assist pilots to perform such tasks rapidly and correctly. Contemporary CDUs rarely provide such assistance, which means that pilots must sometimes spend much longer than should be necessary in performing even relatively simple, but unfamiliar, tasks using the CDU. This can be an important workload factor.

15. ***Reprogramming tasks which must be performed at busy times in flight should be simplified wherever possible to minimize the amount of "head-down" time during flight at low altitudes.***

In the newest flight management systems, avionics manufacturers have gone to considerable effort to simplify reprogramming in and approaching terminal areas. Certification staff should be on the alert for functions that are still cumbersome if they must be performed at the expense of other monitoring functions important to safe flight at low altitudes. Pilots still "turn it off" rather than permit themselves to be distracted during the busiest periods of a flight, and thereby deprive themselves of the protective features in the systems.

16. ***Flight management systems should incorporate the maximum practicable amount of internal error-checking to improve the error resistance of the entire system.***

As has been noted elsewhere, computers are tireless and patient monitors. More use can and should be made of automation to monitor human performance. As the aviation system becomes more tightly coupled, the costs of even minor human errors will rise and system tolerance of such errors will decrease. The flight management system "knows" a great deal about the aircraft and about navigation. It should be used to the maximum extent possible to increase error resistance and error tolerance. I have mentioned that "reasonableness checks" could catch some programming errors; non-sequential altitudes programmed into climb and descent profiles could also be questioned. A study of machine monitoring of human entry procedures and common errors would be useful as a basis for incorporating more systematic error trapping within the FMS.

17. ***Management automation should be standardized across fleets to the extent possible, to minimize the likelihood of errors by pilots transitioning from other aircraft.***

While flight management systems tend to operate in a somewhat standard fashion (though much more could be done by air carriers to improve such standardization across fleets), mode control panels may look and operate quite differently in different aircraft (see chapter 10, guideline 29). Error tolerance and safety would be improved if more effort were devoted to making the tools themselves, and the tasks performed using these tools, more standard across fleets. Certification staff, who work with many aircraft, are uniquely positioned to advocate such standardization, as they have done with respect to primary flight and other displays in the past, using both persuasion and FAR Part 25, though it is air carriers that will be most effective in enforcing standardization across their fleets, by requiring it when they purchase new aircraft.

Summary

To summarize these guidelines briefly, I have restated them as questions to be considered during the certification process. I recognize the lack of specificity and the tradeoffs that are always necessary during design, but it seems to me that these questions still need to be near the forefront of the certification pilot's mind as he or she examines a particular automation suite in a new airplane.

1. Is the pilot truly *in command* under all circumstances?
2. Is the pilot actively *involved* at all times?
3. Does the automation always keep pilots *informed* of its actions?
4. Are failures or malfunctions clearly *announced*?
5. Is the automation always understandable and *predictable*?
6. Does automation *search for pilot errors* and warn pilots about them?
7. Does automation inform pilots of its *intentions*? Is it easy for pilots to inform automation about their intentions?
8. Are there potentially hazardous modes? If so, are there *safeguards* against inappropriate use of such modes?

9. Are all backup control modes *usable without undue effort*?
10. Do such control modes provide adequate assistance to pilots under all conditions?
11. Are flight and systems displays easy to understand, or cluttered?
12. Is the most important information always obvious?
13. Is the status of control automation, and its mode changes, always obvious?
14. Does the FMS and its CDU assist pilots in programming?
15. Are tasks which must be performed at busy times simple to execute?
16. Does the FMS incorporate checks to guard against input errors?
17. Is this FMS unique? Will it require extensive relearning to be used effectively?

Comment

It is worth stating again that safety is relative rather than absolute. Accidents are usually a conjunction of many factors operating together. Most of the latent factors (Reason's "resident pathogens") are beyond the control of the manufacturers and those who certify their airplanes. All that builders and certification authorities can do is to produce (and authorize the use of) an airplane that is as resistant to, and tolerant of, both human errors and machine failures as is feasible given the state of the art. Nonetheless, attention to first principles *can* be of help in these processes.

I believe the central problems for the human operators who work with today's aircraft automation are the complexity and opacity of these tools. Put in terms of the "first principles", the human operator must be able to *understand* the automation, and must be *informed* about its activities. To simplify the tools will require time and a better understanding of the facets of the machine that are difficult to understand; in the meantime, more and better training in how and why they operate as they do offers the best likelihood of ameliorating many of the problems outlined in this book. The opacity issue is also difficult and will ultimately require definitive solutions, but this is an area in which certification experts can be of real help by demanding that new automation keep the pilot informed of its activities and intentions.

Sarter and Woods have had little difficulty in demonstrating deficient mode awareness and understanding in pilots in simulation studies in the Boeing 737-300 and Airbus A320, simply by using probes that require more than superficial understanding of how the flight management system and mode control panel actually function (Sarter and Woods, 1992b, Sarter, 1994). Their work shows that even pilots experienced in these aircraft can get into trouble during non-routine operations because of shallow knowledge of these systems. Certification pilots can do much to improve these automation deficiencies by utilizing such probes in their certification scenarios, and almost as much by simply being aware of the sorts of problems that line pilots are likely to have in handling their automation during routine operations.

Part 4: Issues for Future Aviation Automation

The last part of the document deals with some issues facing system designers and operators. Chapter 13 contains a brief overview of newer computational concepts and techniques, including artificial intelligence (AI) and expert systems (ES, RBES), which have been proposed for use in future system automation. Chapter 14 contains some general comments and a brief conclusion.

13. Advanced and novel automation concepts in the future system

Charles E. Billings and Sidney W. A. Dekker

Introduction

As has been noted, today's tightly-coupled automation systems have become extremely complex and in many cases, relatively opaque to their operators. At the same time, these systems have limits which may or may not be clear to their operators. An example of the problems that can be created is seen in this information, extracted from a 1991 incident report:

"Flight XXX departed on schedule; heavy rain and gusty winds were experienced on takeoff and during the departure. The climbout was normal until approximately FL 240 when numerous caution/warning messages began to appear, indicating a deteriorating mechanical condition. The first...was OVHT ENG 1 NAC, closely followed by BLEED DUCT LEAK L, ENG 1 OIL PRESSURE, FLAPS PRIMARY, FMC L, STARTER CUTOUT 1, and others. No. 1 generator tripped off line and the #1 engine amber "REV" indication appeared. However, no yaw control problems were noted. The maximum and minimum speed references on the airspeed (tape) came together, followed by stick shaker activation.

At approximately FL 260, the cabin was climbing rapidly and could not be controlled. The Captain initiated an emergency descent and turned back to the departure airport. The crew began to perform emergency procedures and declared an emergency. During the descent, the stick shaker activated several times but ceased below FL 200. Due to the abnormal flap indication and the #1 engine reverse, airspeed during the descent was limited to 260-270 knots.

The Captain called upon the two augmented crew pilots to assist during the remainder of the flight. While maintaining control of the aircraft, he directed the first officer to handle ATC communications and to accomplish multiple abnormal procedures with the help of the additional first officer. The additional captain maintained communications with the lead flight attendant and company operations as the emergency progressed and later assisted in the passenger evacuation.

Fuel dumping began on descent below 10,000 feet. The fuel jettison procedure was complicated as the left dump nozzle appeared inoperative. The crew dumped 160,000 lb of fuel; this action took about 40 minutes. When the fuel dumping was completed, the captain requested vectors for a 20 mile final for runway XX.

The crew extended flaps early using alternate procedures due to an abnormal leading edge indication and the FLAPS PRIMARY message...a final approach speed of V_{ref} + 20 and 25° of trailing edge flaps was planned. They selected auto brakes number 4. The weather was still bad with strong, gusty winds and heavy rain causing moderate turbulence during the approach.

The ILS approach and landing were normal. At touchdown, maximum reverse was selected on #2 and #3 engines and about half reverse on #4 engine... As the aircraft passed a taxiway turnoff, the tower advised that they saw fire on the left side of the aircraft...this was the first time crew members were aware of any fire...a runway turnoff was used, and the aircraft stopped on a taxiway...(a difficult but successful evacuation followed).

This incident is an example of an electronic system "nightmare". The crew received and had to sort out 42 EICAS messages, 12 caution/warning indications, repeated stick shaker activation and abnormal speed reference information on the primary flight display. Many of these indications were conflicting, leading the crew to suspect number one engine problems when that engine was actually functioning normally. There was no indication of fire presented to the crew when a fire actually existed...

Aviation automation to this time has been accomplished with conventional numerical computational methods and conventional software architectures. These have yielded remarkable capabilities, but numerical methods have inherent limits. It has been difficult to provide decision support using numerical techniques, and many human factors researchers have argued that in cases like this, decision support technology is needed by pilots to avoid serious overload. Note, incidentally, in the above occurrence, that four pilots were fully occupied in dealing with this emergency; one can only ponder how the outcome might have been affected had only the normal crew complement of two persons been in the cockpit.

Such concerns have motivated the application of a number of novel computational concepts and techniques to aircraft automation. These approaches, generally speaking, are designed to enable machines to carry out reasoning tasks we normally ascribe to human intelligence. During the past 30 years, newer classes of computational technology have been developed, using symbolic rather than numerical manipulation of the behavior of objects. Their purpose is to free computation from the narrow, inflexible bounds of numerical and arithmatic deduction and permit a broader, inferential approach to computer reasoning.

Cognitive assistance (the ability to reason, plan and allocate resources) has been accepted in several domains; these computational methods have been successful in a variety of applications. They are often resource-intensive; complex programs may run slowly because of the large knowledge bases that must be searched. They are imperfect and limited, but many have believed them to be the wave of the future. Their more enthusiastic advocates have suggested that they have clear advantages for certain aviation applications, and for that reason they are considered here.

Diagnosis of aircraft system faults

The management of disturbances, and the presentation to pilots of information concerning them, is a function that appears to be well-suited to artificial intelligence (AI) approaches. It has been examined in depth by several researchers, stimulated in large part by leadership at NASA's Langley Research Center. Before considering this work, a word should be said about the constraints that a dynamic problem-solving environment imposes on any diagnostic process.

The diagnosis of faults on a flight deck differs fundamentally from static systems in which a malfunctioning device can be taken off-line for trouble-shooting. In a dynamic system, the process must go on while the fault is handled; an aircraft cannot be "parked at a waypoint" while the trouble is dealt with. Fault scenarios are event-driven; symptoms emerge over time in a fluid, sometimes cascading fashion (Woods, 1993c). In some cases, "disturbance management" requires that faults be ignored temporarily while the process is kept under control. In others, the true nature of the fault is not known and cannot be discerned until some outcome has ensued (as in the case cited above).

The challenges associated with the nature of dynamic faults are legion, as indicated above. I shall review various AI proposals set forth to address some of these challenges. It should be remarked that an evaluation much longer than the one that follows would not do justice to the complexity of the work that has been done in this area of AI. Further, it must always be kept in mind that in the cockpit or an ATC facility, the issue is not just a single human working with a computer, but rather multiple humans and often multiple tools working cooperatively to supervise and maintain the operation of a complex system. In such settings, each human must evaluate what others are doing, as well as what the total system is doing.

Rule-based diagnostic systems

The first general AI proposal for aiding diagnosis in real-time systems was the use of rule-based expert systems (RBES). Machine expert systems are designed to support trouble-shooting by human problem solvers (Clancey, 1983). Their strength is a large knowledge base, built up from domain information and experience provided to it by many domain experts. All the known faults in the domain, and all their associated symptoms and root causes, are enumerated and encoded in a knowledge database. The reasoning performed on the knowledge base during diagnosis by an "inference engine" is typically rule-based. This means, in simple terms, that rules guide the machine problem solver from symptom to symptom until a root cause for the observed fault has been found. The human may have to function as a data-gatherer for the machine, and is the critic of its results.

The locus of control in this type of diagnostic reasoning resides with the machine, not with the human. Such a constellation has been called the paradigm of the "intelligent system as prosthesis" (Roth, Bennett, & Woods, 1987), where the RBES functions as a replacement or remedy for a presumed deficiency in the human reasoner. Experience with such systems has indicated that, as might be expected, the human and the expert system typically proceed in parallel to try to diagnose and solve the problem using whatever data is available. Intelligent agents do not typically work as "team players" with humans.

The degradation of joint human-machine performance in such a system has been well-documented (e.g. Roth et al., 1987). However, this is not the only reason why an ES as aid in the diagnosis of in-flight faults is ineffective. The time needed to accumulate experience and gather knowledge on all of the subsystems that make up a commercial aircraft is prohibitive. Pre-enumeration of all possible faults and all of their symptoms is simply not possible for any but the most simple or longest-serving airframes still flying. ESs cannot deal with novel faults at all. The models that motivate the machine's decisions are implicit rather than explicit, which renders the machine's results both brittle and difficult for the human to understand.

In dynamic situations, the computer's progression through many low-level symptoms, and the conversation-style interface with most ESs, is unsuitable for time-pressured situations in which symptoms can emerge in a cascading and seemingly unconnected fashion. Although various expert systems have been and are being developed for aerospace applications (see for instance Pilot's Associate below), none is in use today nor is likely to be in the near future (see Malin et al. (1991) for an extensive evaluation of fault management systems in primarily space applications).

Model-based diagnostic systems

Contrasting sharply with rule-based diagnosis is model-based diagnosis. This AI approach has also been called "reasoning from first principles", or "deep reasoning" as it relies on only a limited number of basic assumptions or principles about causality in the underlying system. Central to model-based diagnosis is the ability to view malfunctioning as anything other than what the system is supposed to do (Davis & Hamscher, 1988). The behavior of the system is observed (with appropriate sensors) on the one hand, while it is predicted on the basis of a model of the system on the other. Discrepancies between observations and predictions are called symptoms. The fundamental assumption is that if the model of the system is indeed correct, then all symptoms arise from actual malfunctions in the system.

Model-based diagnosis is much more robust than rule-based reasoning. Among the aviation studies done in this domain (see for instance: Rogers, 1990; Ovenden, 1991 and also Malin et al., 1991), Kathy Abbott (1990) has studied and described a model-based diagnostician for aircraft systems: DRAPHYS (Diagnostic Reasoning About Physical Systems). DRAPHYS is part of a larger fault management research program supported by NASA Langley Research Center. Some of the modules developed under the NASA Faultfinder program have been taken up by others and restructured and enhanced (e.g., the Boeing effort on the Flight Deck Engine Advisor using elaborations of DRAPHYS and its monitoring cousin MONITAUR). The goal is to develop a system which advises the crew of inconsistencies, adverse performance trends or non-normal situations before the conditions become critical and then to assist the crew in system diagnosis while recommending applicable procedures in response to the situation (Shontz, Records, & Antonelli, 1992). DRAPHYS is discussed below in more detail in order to contrast the model-based approach (including its promises and problems) with rule-based expert systems.

DRAPHYS generates candidate hypotheses about the root causes of faults in an incremental, constructive approach, following the cascading emergence of symptoms. In that respect, DRAPHYS has the capability of degrading gracefully, just as human problem solvers would. If it decides it can no longer generate useful hypotheses at a more detailed level of system description, it confines its troubleshooting to a higher level of system description.

DRAPHYS knows that not all faults should be approached using the same underlying model as its criterion of "right behavior". Faults can propagate through a system functionally (due to functional connections) as well as physically (due to physical proximity of affected components, for example a fractured fan blade severing a hydraulic line), and DRAPHYS has different underlying models to aid in the succesful diagnosis of both classes of problems.

More exotic symptom scenarios are presented by faults that propagate and interact physically as well as functionally. DRAPHYS is able to utilize these classes of models in such a way that (hybrid) interactions between the various types of progressions (i.e. functional and physical) can be captured and reasoned upon. Another proposal for how to deal with this (Bylander, 1988) goes back to the use of knowledge bases: though model-based diagnosis is suitable to determine which hypotheses explain which symptoms, many model-based systems cannot reason with uncertainty. That is, they cannot order or rank their hypotheses according to their plausibility relative to each other. The interaction with a knowledge base may be able to suggest which of several hypotheses is more likely than others relative to what is known about the domain.

Another problem with model-based diagnosis is the grain of analysis of the reasoning. Information about an underlying fault may very well reside in the rate at which a symptom changes its behavior. In DRAPHYS, there is no difference between a slowly decreasing and a rapidly oscillating fan speed; both are called "abnormal". Yet diagnosis of an underlying fault can be different on the basis of the behavior of the symptom at a finer grain of analysis. The tradeoff here, of course, is the increasing complexity of the model with the incorporation of more detailed system behavior. This can have negative consequences in terms of longer search times and the need to deal with more failure hypotheses.

Ultimately, the need for a finer grain of reasoning depends entirely on the context in which diagnosis takes place. It may matter for diagnosis of an engine malfunction, while it may not matter in case of a malfunctioning air conditioning pack. Indeed, the need for deep assessment of symptoms may vary as a function of context: in cases where full, consistent engine performance is absolutely critical (such as takeoff), the difference between rapidly fluctuating and steadily decreasing N1 speed does not matter. These issues, together with intermittent faults and faulty sensors (a serious problem in these systems), are further challenges to and future research targets for model-based diagnosis methods.

Finally, AI systems of these types need a monitoring "front end" which can decide which of the system's findings are to be pursued further, and which are trivial or redundant. The introduction of faults into a complex, tightly-coupled system such as an aircraft can lead to symptoms in many parts of the system, and thus to an "explosion" of hypotheses regarding the root causes of the disturbance. Such a "front end" is extremely sensitive to how the system's hypotheses are represented. For example, under acute time pressure, pilots typically read the first line of computer output and begin looking for a prescribed procedure with which to solve the problem represented. If the AI system presents no procedural solution, it cannot work cooperatively with the humans to solve the problem.

Autonomous intelligence

Whether such systems simply perform their assigned functions autonomously or are able to work as "team players" is often less related to their inherent capabilities than to the design of the interface between the systems and the humans responsible for management of the overall process. A conversational representation of AI behavior is a grossly inadequate communications tool for a pilot or controller under time pressure. Human operators cannot sort out the multiple symptoms in tightly-coupled systems and are unlikely to have time to decide which of ten or more possible faults is the culprit in a particular anomaly. Here, as elsewhere, "representations are never neutral" (Woods, 1994a); if they do not help solve the problem, they are perceived as part of the problem.

"The electronic crew member"

In the early 1970s, investigators became interested in the interaction process between humans and AI systems. Rouse (1988, p. 432) describes the criteria for what are now called "adaptive aiding" systems: "...the level of aiding, as well as the ways in which human and aid interact, should change as task demands vary. More specifically, the level of aiding should increase as task demands become such that human performance will unacceptably degrade without aiding. Further, the ways in which human and aid interact should become increasingly streamlined as task demands increase. Finally, it is quite likely that variations in level of aiding and modes of interaction will have to be initiated by the aid rather than by the human whose excess task demands have created a situation requiring aiding. The term *adaptive aiding* is used to denote aiding concepts that meet (these) requirements." (*Author's note:* It is implied here that the pilot who needs such assistance will usually be too busy to ask for it, a premise that needs careful examination.)

Following development of the concept and modeling studies of human performance (Rouse, 1980), several empirical studies were performed to evaluate and expand the concept and its potential applications. These led to the elaboration of a comprehensive "framework for adaptive aiding" (Rouse and Rouse, 1983). This work, in turn, was embodied in the Pilot's Associate program, carried out by the Lockheed-Georgia Company under sponsorship of the Defense Advanced Research Projects Agency.

In this application, adaptive aiding "is an element of an overall intelligent interface, which includes AI modules for display management, error monitoring, and adaptive aiding...One particularly interesting aspect of this effort is the nature of the expertise embedded in the many expert systems that make up the Pilot's Associate. There are suites of expert systems for mission planning, tactics planning, situation assessment, and systems status monitoring that include expertise on aircraft, flying, military doctrine, and so on. In contrast, the primary expertise within the six expert systems that make up the pilot-vehicle interface is expertise on human information processing and performance, with special emphasis on how situational characteristics and information presentation affect the formulation of intentions and subsequent plans. Thus, to an extent, the pilot-vehicle interface is a highly specialized human factors expert." (p. 433)

Rouse (1988, p. 441) concludes that, "In retrospect, the notion of adaptive aiding is much more evolutionary than revolutionary. User-initiated adaptation has long been the norm in aerospace system (e.g., autopilots). The are also many everyday examples of humans adapting their automobiles and appliances. Thus the primary innovation of adaptive aiding is not adaptation *per se* but the possibility of aid-initiated adaptation." (*Author's note:* There is a fundamental difference, however, between *user*-initiated adaptation and *machine*-initiated adaptation. The user almost always has more knowledge of the world state and its implications than the machine.)

Building on its Pilot Associate program, Lockheed has continued its interest in this class of computer aids. Work is in process on new "associate" technologies for dispatchers, air traffic controllers and others. The Air Force's Armstrong Laboratory has continued to study adaptive aiding systems for pilots, and there is a "surface movements advisor" element in NASA's Terminal Area Productivity research program.

Issues raised by advanced computational concepts

Human and machine roles

Let me first return to the paradigm of the human or machine as prostheses of one another. In chapter 2, and repeated in chapter 9 and implicitly elsewhere in this document, the prosthesis paradigm is contrasted with what could be called the paradigm of "the cognitive instrument" (Roth et al., 1987). In the cognitive instrument paradigm, automation is not in place to supplant human functions. Rather, automation consists of tools to assist human beings in their problem solving tasks. Machines should be considered as complementary, instead of competitive. We should ask ourselves again: is the effort of AI in diagnosis directed towards supplanting the human diagnostician? Or is it aimed at aiding the human problem solver?

In most relevant AI research, great emphasis is placed on how to conduct automated diagnosis and less attention is paid to how the information from such automated diagnostic processes could benefit flight crew in various contexts. Such issues as the flight crew information requirements for fault management on the commercial flight deck are addressed within the NASA Faultfinder program (Rogers, 1990; Abbott & Rogers, 1992). The study of information presentation in this program is focused on understanding the cognitive activities associated with fault management, so that needed support of human information processing and decision-making can be offered.

Note that such issues are embedded in the question in chapter 2 about whether crews in newer aircraft are sufficiently "drawn in" to their operations. Following the cognitive instrument paradigm, the aim of automated fault diagnosis should *not* be to interpose more automated processes between pilot and aircraft. Instead, diagnostic systems should bring pilots closer to what is going on within a subsystem, rather than alienating them from the process.

Adaptability *vs.* adaptation

Adaptability (the ability to adapt autonomously given certain input conditions) is a characteristic of some of these computational concepts. (An example was the mode annunciator panel decluttering in the A330 accident at Toulouse in 1994.) It is this characteristic that gives rise to certain concerns about their use in a high-risk, dynamic environment such as aviation.

Many machine systems are designed to adapt autonomously: In the A330, autospoiler extension occurs slowly upon landing until reverse thrust is selected, and rapidly thereafter. In many aircraft, trailing-edge wing flaps will not extend (or will retract) above a certain airspeed to avoid excessive airloads. Warning systems are inhibited in most newer aircraft during takeoff; some function only during cruise flight. The brightness of newer cockpit displays is controlled as a function of ambient light in the cockpit. These systems, however, adapt in known ways to known stimuli; they remain predictable, and if they do not behave in the expected way, the pilot is alerted to the presence of a malfunction and can compensate for it.

I have suggested throughout that the machine component of this human-machine system must be predictable, so that the human can understand and form a clear mental model of the machine's present and expected behavior. There is a good deal of difference between a machine system that can be adapted—that is adaptable—and a system that can adapt autonomously in perhaps unpredictable ways. In the former case, the human operator is at the locus of control; in the latter case, the machine is at the locus of control. With regard to maintaining command of the process, the difference is crucial. Note that machines that behave in unexpected ways produce surprises for their operators. In the systems under discussion, surprises can also occur because it is not possible to fully characterize the ways in which complex AI systems may behave when confronted with novel circumstances.

Roth et al. (1987) discussed this in the context of intelligent decision systems: "Psychologists are fond of discovering biases in human decision making. One judgmental bias is the overconfidence bias where people at all levels of expertise overestimate how much they know. However, we sometimes forget that these biases can apply to the designers of machines as well as to the users of machines. This means that the designer of an intelligent decision support system is likely to overestimate his/her ability to capture all relevant aspects of the actual problem solving situation in the behavior of the machine expert." (p. 502) Aid-initiated adaptation was a factor in the Charlotte wind shear accident (1994); it also posed problems in the Tarom Airlines A310 incident at Orly Airport (Paris, 1994).

Comment

These factors have led me over the past decade to a position of possibly extreme conservatism with regard to the potential of AI systems as autonomous agents, and particularly self-adapting systems, for flight-critical applications. I recognize that these newer computational architectures have considerable promise for defined tasks that can be bounded (such as some of the diagnostic tasks discussed above). I also realize that object-oriented programming may significantly decrease the enormous software development cost involved in the development of some of today's very complex, integrated systems. To the extent that these software technologies can ease the large and growing development burden without making verification of software even more difficult than it is today, they should be adopted.

But at its present state of development, "In high-risk, dynamic environments, we believe that technology-centered automation has tended to decrease human involvement in system tasks, and has thus impaired human situation awareness; both are unwanted consequences of today's system designs, but both are dangerous in high-risk systems. Adaptive ("self-adapting") automation represents a potentially serious threat...to the authority that the human pilot must have to fulfill his or her responsibility for flight safety" (Billings and Woods, 1994).

In civil aviation, at least, it is unlikely that AI concepts will find their way into flight-critical automation systems until they have been thoroughly proven in less critical applications. One that has been looked at is the use of an AI system to assist pilots to navigate through the large volume of data in an electronic library system. Another is the use of AI to assist airline systems operation centers and dispatchers in resolving flight replanning problems (Smith, McCoy, Layton, & Bihari, 1993; Layton, Smith, & McCoy, 1994). A third, and possibly the one most likely to be adopted in the near future, is the use of AI to create more adaptive and individualized computer-assisted training modules. This application would also give airlines and manufacturers the opportunity to evaluate these technologies and to gain confidence regarding their usefulness and limitations.

14. Comments and conclusion

Introduction

In this chapter, I have appended some topics that need to be mentioned but do not fit well elsewhere. The comments are personal and represent my concerns regarding some issues that face us now, or are likely to in the near future. They are followed by a brief conclusion.

Is cockpit commonality an opportunity, or an issue?

An anonymous Associated Press report dated August 22, 1994, discusses fleet cockpit commonality and its economic implications for air carriers. It describes an Air Canada decision to order 25 new Airbus aircraft rather than refurbish its DC-9s despite an increased cost of $20 million per aircraft, which Air Canada estimates will save $3.5M per year due to decreases in spares inventory and the ease with which pilots can be exchanged with its 34 A320s already in service. Julius Maldutis, of Salomon Brothers, is quoted as saying that "Increasingly, you'll see airlines being supplied by a single manufacturer...the battle between manufacturers is increasingly not for the next 20 airplane deals, but for the next 200 airplane deals to convert airlines entirely to your product."

The AP report continues, "Some analysts say the common features among different models give a strong selling advantage to Airbus, (which) intentionally designed five models (the A319, A320, A321, A330 and A340) to have similar cockpits, handling characteristics and common spare parts. Airbus says the airlines can get about 20% more flying out of a pilot because less training is required...Airbus estimates that the similarities between its A319/A320/A321 aircraft can save an airline $1.3M per year for each jet. The common features of the A330/A340 are worth $1.8M per year per jet."

(The report might also have noted that Lufthansa has developed a carefully-structured program of dual qualification in which its Airbus pilots fly both the very long-range A340 and the A320 so that they can keep their proficiency high on shorter trips. Given that other international air carriers have felt it necessary to provide additional simulator flying to maintain the skills of pilots who fly only extremely long routes, this approach has considerable appeal. Of course, the report might also have mentioned that in the same week, Northwest Airlines, another A320 operator, announced *its* intention to refurbish, modernize and add "hush kits" to its sizeable DC-9 fleet, from which it estimated it could get perhaps two decades of additional service at much lower cost!)

The report continues, "Boeing has not been left out...by flying only Boeing 737s, Southwest (Airlines) has been able to keep costs low by stocking only one type of (everything). Southwest pilots only need to know their ways around one cockpit layout" (because Southwest has also limited the authority of the flight management systems installed in its -300 aircraft and has specified electromechanical rather than CRT displays in its newer aircraft).

"When Boeing set out to update the 737, a major customer told Boeing to change whatever it wants, 'but put a padlock on the cockpit door' to keep the designers out. The different models of the 737 have identical cockpits and pilots can move between the longer-range 757 and 767 with only an additional hour of training."

While these statements are not entirely correct, the article makes an important point which has major implications both for operators and for the human factors community. I have tried to indicate in this document that current automation suites are not free of human-machine interface problems, some of which have become more serious as more and more capable automation has been implemented. Are we, for economic reasons, at the point where air carriers would rather live with "the devil they know" than move toward correction of some of the acknowledged human factors problems on their flight decks?

I believe that at this point in time the answer to this question is probably "Yes". United Airlines many years ago estimated that each pilot retirement forced the movement (either upgrading or transition to another airplane), training and qualification of some 13 other pilots. The expense was enormous, even at a time when air carriers were making money. Air carriers have spent years trying to minimize training costs; commonality among cockpits will certainly be of assistance.

Is this truly a "no-cost" benefit? Possibly, though that has not been our experience in the past. As indicated above, Southwest has chosen to limit sharply the utility of its newer aircraft automation by limiting their flight management systems' functionality. The systems have to be initialized to set their inertial reference systems, but they are not used for direct navigation. The carrier has also stayed with electromechanical instruments to insure commonality between its 737-200s and the -300 series aircraft, which has precluded it from installing the more integrated navigation displays normally available in the later 737s.

While Airbus cockpits do have a very high degree of commonality, the computer architecture and FMS functionality across types are not really identical (though the differences are *normally* transparent to pilots). I am concerned, however, about the behavior of the different software in these types at the margins, and the potential for surprises under difficult circumstances. In the initial report of the investigation of the A330 accident at Toulouse (1994), it was stated by Airbus that the combination of problems that occurred during that flight was unlikely or impossible in other Airbus models, for a variety of aerodynamic and other reasons. Further, the software involved in implementation of the altitude acquisition mode differed across types.

I doubt that line pilots are made aware of such differences during training, and many may not be of concern to them. On the other hand, this mishap need not have happened, and I am impelled to wonder what other occult problems may be lurking at the margins of operating envelopes, waiting to snare pilots who have operated successfully in another type and who may therefore have been led to believe that they can operate in the same ways in this aircraft.

The liability issue in aviation operations

In recent years, we have seen an increasing number of criminal prosecutions of flight crew, and even air carrier managers, after aircraft accidents and even incidents in which they were alleged to have been negligent in the performance of their express or implied duties. The manager was charged after the A320 Strasbourg accident (1992) for his failure to require ground proximity warning systems in Air Inter aircraft.

This trend has begun to appear in the United States as well, with the successful prosecution of three pilots for having detectable levels of blood alcohol in their bodies while engaged in flight duties. In the United States, the Federal Aviation Regulations (with one exception, interference with a flight member in the performance of duty) are not criminal law, and their violation is almost always a civil rather than a criminal matter. The pilots mentioned were tried under a law prohibiting operation of a commercial motor vehicle under the influence of alcohol. Obviously, such issues are a matter of serious concern to pilots and can affect their behavior and decision-making processes.

In nations which govern under the Napoleonic code, and even in some common law jurisdictions, violation of Air Navigation Orders is potentially a criminal offense. "Two Korean pilots were jailed in Libya in 1990 after landing short at Tripoli, killing 72 passengers and at least five others. In 1983, a Swissair crew was convicted and fined in Greece after skidding off the end of a wet runway in Athens; 14 passengers died." (Wilkinson, 1994).

In a celebrated case in the United Kingdom in 1989, the pilot in command of a Boeing 747 was convicted of negligent endangerment of his passengers after an unstable autocoupled approach at London's Heathrow Airport during which the aircraft came within 70 feet of the ground outside the airport boundary. The airplane was landed safely from a second approach. The pilot in command was demoted to first officer by his company. After revoking his pilot in command license, the UK Civil Aviation Authority brought criminal charges, one of which was sustained in a split jury decision. The pilot was fined; his appeal was rejected. He subsequently committed suicide (Wilkinson, 1994). The two pilots involved in a recent A-300 accident in Korea are under criminal investigation concerning their conduct of the flight and landing.

Air traffic controllers have not been immune. A Yugoslav controller was jailed following a midair collision over that nation, and others have also been prosecuted, though I do not have details concerning specific cases.

I have indicated elsewhere my concern that holding pilots or air traffic controllers criminally liable for negligence is likely to inhibit seriously our ability to investigate air accidents. Regardless of what may be said about the duty of a professional person to disclose information that may compromise him or her but may save others, the fact is that many otherwise honest and upright people find it difficult or impossible to do so. When aviation professionals know that their statements following an accident may cause them lasting harm, they are unlikely in many cases to be forthright with accident investigators. Today's legal climate insists that blame be apportioned, but the *only* way we are likely to continue to be able to learn lessons from accidents is to insure that the principals in such accidents can talk freely about what happened and why.

How do you punish a computer?

Who is liable for the behavior of a highly automated system? If automation continues to become more pervasive and authoritative, who will be responsible for its actions? At this time, we simply say that the pilot and controller remain responsible, but if a more autonomous air traffic control system is put in place, can this *a priori* assignment of responsibility continue?

The Eurocontrol Experimental Center is France is pursuing long-term research into future air traffic management systems. One approach being explored is "complete air-ground automation of the separation assurance function"; the other is aircraft autonomy in an "open sky", using "electronic visual flight rules" (Maignan, in Cooper, 1994a). Our present concepts of responsibility and authority are silent on the implications of such automation, but I cannot imagine how a controller could be held responsible for a loss of separation in a fully autonomous air traffic management system, nor even in a system such as I posited in scenario 3 in chapter 6 (page 79).

Nonetheless, it is unlikely that those inclined toward the assignment of blame will take much pleasure in suspending or fining a computer after an aviation incident. Given that our tort system requires the apportionment of liability, how will this be done? Is anyone in our legal establishment considering these implications of increased automation of the air traffic management system?

Conclusion

David Woods (1994b) has described automation problems succinctly: "Automated systems that are strong, silent, clumsy, and difficult to direct are not team players." He goes on, "Automated systems are

- *strong* when they act autonomously;
- *silent* when they provide poor feedback about their activities and intentions;
- *clumsy* when they interrupt their human partners during high workload, high criticality periods or add new mental burdens during these high tempo periods;
- *difficult to direct* when it is difficult and costly for the human supervisor to instruct the automation about how to change as circumstances change."

I believe the central problems for the human operators who work with today's aircraft automation are the complexity and opacity of these tools. Put in terms of the "first principles", the human operator must be able to understand the automation, and must be informed about its activities. As indicated in chapters 7 and 10, this understanding by human operators of the capabilities, limitations, and possible problems with their tools is the conceptual problem that must be attacked if humans and machines are to be able to work more cooperatively, as a team, in pursuit of system goals.

This document is by no means a complete chronology of automation. It suggests requirements for new automation designs, but it does not specify how to implement those requirements in a particular setting. What I have tried to do is to suggest characteristics of automation that cause problems for at least some of its operators, the types of problems that these characteristics cause, and means of bypassing some of the problems without compromising the effectiveness of automated tools.

In a future system in which the human does not play such a central and critical role, these human-automation interactions might be less of a problem. On the other hand, any such system is likely to remain under the control of humans at some level, and the problems posed by clumsy, brittle or uninformative automation will still need to be solved at that level.

Though aviation is a remarkably safe way to move people and goods, preventable accidents continue to occur. To an increasing extent, these accidents involve both human operators and their machines. They represent *system* failures, and they will only be prevented by a systematic approach to *all* components of the aviation system. Automation is now a central element in that system. It has been extremely successful in improving the reliability and productivity of the system. Like all technology, its successes have brought with them new problems to solve.

I hope that this document will improve the quality and depth of the dialogue about these problems and their solutions between system architects and the manufacturers who must realize their designs, between manufacturers and the customers who purchase their products, between the customers and the operators who manage and direct the systems, and between all of them and the government officers who must certify the system and maintain oversight of its safety and effectiveness. That was the primary purpose of the predecessor document, and that remains the purpose of this revision. All these people, and many others in the aviation community, are critical to the continued success of the aviation system, upon which so many millions of our citizens rely for safe transportation.

Appendix 1: Aircraft accidents and incidents

This appendix contains brief descriptions of some salient aspects of aircraft mishaps cited in the text. The occurrences are listed chronologically; each summary is followed by a reference.

6/30/1956: TWA L1049A and United Air Lines DC-7, Grand Canyon, AZ

At approximately 1031 hrs PST, a TWA L-1049A and a United Air Lines DC-7 collided at about 21000 ft over Grand Canyon, AZ. Both aircraft fell into the Canyon; there were no survivors among the 128 persons aboard the two flights. There were no witnesses to the disaster.

The Civil Aeronautics Board determined that the flights were properly dispatched. In flight, the TWA crew requested 21000 ft, or 1000 ft on top (above cloud tops). 21000 ft was denied by ATC because of UAL 718. TW then climbed to and flew at 21000 ft above clouds. The last position report from each aircraft indicated that both were at 21000 ft, estimating their next fix at 1031. The aircraft were in uncontrolled airspace and were not receiving traffic control services at the time of the collision.

The Board determined that the probable cause of the collision was that the pilots did not see each other in time to avoid the collision. The Board could not determine why the pilots did not see each other but suggested the following factors: intervening clouds, visual limitations due to cockpit visibility, preoccupation with matters unrelated to cockpit duties such as attempting to provide the passengers with a more scenic view of the Grand Canyon, physiological limits to human vision, or insufficiency of enroute air traffic advisory information due to inadequacy of facilities and lack of personnel. (CAB, 1957)

2/3/1959 Pan American World Airways B-707 over the Atlantic Ocean

Pan American flight 115 was enroute from London, England to New York when it entered an uncontrolled descent of approximately 29000 feet. Following recovery from the manuever, the airplane was flown to Gander, Newfoundland, where a safe landing was made. A few of the 129 persons on board suffered minor injuries; the aircraft incurred extensive structural damage.

The aircraft was at 35000 ft in smooth air with the autopilot engaged when the captain left the cockpit and entered the main cabin During his absence the autopilot disengaged and the aircraft smoothly and slowly entered a steep descending spiral. The copilot was not properly monitoring the aircraft instruments and was unaware of the airplane's attitude until considerable speed had been gained and altitude lost. During the rapid descent the copilot was unable to affect recovery. When the captain became aware of the unusual attitude he returned to the cockpit with considerable difficulty. With the aid of the other crew members, he was finally able to regain control of the aircraft at an altitude of about 6000 feet.

The Civil Aeronautics Board determined that the accident resulted from the inattention of the copilot to the flight instruments during the captain's absence from the cockpit, and the involuntary disengagement of the autopilot. Contributing factors were the autopilot disengage warning light in the dim position and the Mach trim switch in the "off" position. During analysis, which was hindered by the flight data recorder having exhausted its supply of metal recording foil, it was indicated that the airplane had reached Mach 0.95 in its abrupt descent. Very high G forces were indicated by the recorder and had been reported by the pilots during their attempts to recover from the spiral dive. After landing at Gander, the lower surface skin of the horizontal stabilizers was found to be buckled; both wing panels and both outboard ailerons were damaged; the wing-to-fuselage fairings were damaged and a three-foot section of the right fairing had separated in flight. Both wing panels suffered a small amount of permanent set. All four wing-to-strut fairing sections of the engine nacelle struts were buckled and other damage was also evident. (CAB, 1959)

6/18/1972: British European Airways Trident, Heathrow Airport, London, England

This aircraft commenced its operation under the command of a very senior BEA captain. The first officer was relatively inexperienced and the second officer was a recent graduate of the airline's training school. The airline was undergoing a difficult labor-management conflict, and the captain had been involved in a heated altercation in the crew room before departure.

Shortly after takeoff, when the first reduction of flaps occurred, it is thought that the first officer inadvertently actuated the wing leading edge slat handle as well, raising the slats at a speed too low to sustain flight. Based on post-mortem evidence, it is believed that the captain had a severe cardiac event at about the same time. Many warning lights and aural signals were actuated by the premature retraction of the slats. The inexperienced first officer was unable to diagnose the problem or to regain control of the airplane, which crashed into a reservoir just west of the airport. There were no survivors. (Department of Trade and Industry, 1973)

12/29/1972: Eastern Air Lines L-1011, Miami, FL

The airplane crashed in the Everglades at night after an undetected autopilot disconnect. The airplane was flying at 2000 ft after declaring and executing a missed approach at Miami because of a suspected landing gear malfunction. Three flight crewmembers and a jumpseat occupant became immersed in diagnosing the malfunction. The accident caused 99 fatalities among the 176 persons on board.

The NTSB believed that the airplane was being flown on manual throttle with the autopilot in control wheel steering mode, and that the altitude hold function was disengaged by light force on the yoke. The crew did not hear the altitude alert departing 2000 ft and did not monitor the flight instruments until the final seconds before impact. The Board found the probable cause to be the crew's failure to monitor the flight instruments for the final 4 minutes of the flight and to detect an unexpected descent soon enough to prevent impact with the ground. The Captain failed to assure that a pilot was monitoring the progress of the aircraft at all times. The Board discussed overreliance on automatic equipment in its report and pointed out the need for procedures to offset the effect of distractions such as the malfunction during this flight (p. 21). (NTSB, 1974a)

7/31/1973: Delta Air Lines DC9-31, Boston, MA

This airplane struck a seawall bounding Boston's Logan Airport during an approach for landing after a flight from Burlington, VT to Boston, killing all 89 persons on board. The point of impact was 165 ft right of the runway 4R centerline and 3000 ft short of the displaced runway threshold. The weather was sky obscured, 400 ft ceiling, visibility 1 1/2 miles in fog.

The CVR showed that 25 sec before impact, a crewmember had stated, "You better go to raw data; I don't trust that thing." The next airplane on the approach, 4 minutes later, made a missed approach due to visibility below minimums. The accident airplane had been converted from a Northeast Airlines to a Delta Air Lines configuration in April, 1973, at which time the Collins flight director had been replaced with a Sperry device; there had been numerous writeups for mechanical deficiencies since that time. The flight director command bars were different (see fig. 11, page 20 for the two presentations), as were the rotary switches controlling the flight director. The crew were former Northeast Airlines pilots. If the crew had been operating in the go-around mode, which required only a slight extra motion of the replacement rotary switch, the crew would have received steering and wing-leveling guidance only, instead of ILS guidance. Required altitude callouts were not made during the approach.

The NTSB found the probable cause to be the failure of the crew to monitor altitude and their passage through decision height during an unstabilized approach in rapidly changing meteorological conditions. The unstabilized approach was due to passage of the outer marker above the glide slope, fast, in part due to nonstandard ATC procedures. This was compounded by the flight crew's preoccupation with questionable information presented by the flight director system.

The Board commented that, "An accumulation of discrepancies, none critical (in themselves), can rapidly deteriorate, without positive flight management, into a high-risk situation...the first officer, who was flying, was preoccupied with the information presented by his flight director system, to the detriment of his attention to altitude, heading and airspeed control..." (NTSB, 1974b)

4/12/77: Delta Air Lines L-1011, Los Angeles, CA

This airplane landed safely at Los Angeles after its left elevator jammed in the full up position shortly after takeoff from San Diego. The flight crew found themselves unable to control the airplane by any normal or standard procedural means. They were able, after considerable difficulty, to restore a limited degree of pitch and roll control by using differential power on the three engines. Using power from the tail-mounted center engine to adjust pitch and wing engines differentially to maintain directional control, and verifying airplane performance at each successive configuration change during an emergency approach to Los Angeles, the crew succeeded in landing the airplane safely and without damage to the aircraft or injury to its occupants. (McMahon, 1978)

12/181977: United Airlines DC-8, near Kaysville, UT

A cargo aircraft encountered electrical problems during its approach to the Salt Lake City Airport. The flight requested and accepted a holding clearance from the approach controller. The flight then requested and received clearance to leave the approach control frequency in order to communicate with Company maintenance (one of the two communications radios had failed due to the electrical problem). Flight 2860 was absent from the approach control frequency for over 7 minutes, during which time the flight entered an area near hazardous terrain. The approach controller recognized the crew's predicament but was unable to contact the flight.

When the crew returned to his frequency, the controller told the flight that it was too close to terrain on its right and to make an immediate left turn. After the controller repeated the instructions, the flight began a left turn. About 15 seconds later, the controller told the flight to climb immediately to 8000 ft. Eleven seconds later, the flight reported that it was climbing from 6000 to 8000 ft. The airplane crashed into a 7665 ft mountain near the 7200 ft level.

The NTSB determined that the probable cause of the accident was the approach controller's issuance and the flight crew's acceptance of an incomplete and ambiguous holding clearance, in combination with the flight crew's failure to adhere to prescribed impairment-of-communications procedures and prescribed holding procedures. The controller's and flight crew's actions were attributed to probable habits of imprecise communication and of imprecise adherence to procedures, developed through years of exposure to operations in a radar environment. A contributing factor was failure of the airplane's no. 1 electrical system for unknown reasons. The Board noted that the GPWS would not have provided a warning until 7.7 to 10.2 sec before impact, which was too late because of the rapidly rising terrain. (NTSB, 1978a)

5/8/1978: National Airlines B727-235, Escambia Bay, Pensacola, FL

Flight 193 crashed into Escambia Bay about 3 miles short of the runway while executing a surveillance radar approach to Pensacola Airport runway 25 at night in limited visibility. The aircraft came to rest in about 12 ft of water. Of 58 persons on board, 3 passengers drowned.

The NTSB determined that the probable cause of the accident was the flight crew's unprofessionally conducted nonprecision instrument approach, in that the captain and crew failed to monitor the descent rate and altitude and the first officer failed to provide the captain with required altitude and approach performance callouts. The crew failed to check and utilize all instruments available for altitude awareness, turned off the ground proximity warning system, and failed to configure the aircraft properly and in a timely manner for the approach. Contributing to the accident were the radar controller's failure to provide advance notice of the start-descent point, which accelerated the pace of the crew's cockpit activities after the passage of the final approach fix.

The Board noted that the approach was rushed, that final flaps were never extended and that the captain was unable to establish a stable descent rate after descending below 1300 ft. The captain either misread or did not read his altimeters during the latter stages of the approach; the first officer did not make any of the required altitude callouts. The flight engineer's inhibition of the GPWS coincided with the captain's raising the nose and decreasing the descent rate. The pilots were misled into believing the problem was solved. (NTSB, 1978b)

12/28/1978: United Airlines DC-8-61, Portland, OR

This airplane crashed into a wooded area during an approach to Portland International Airport. The airplane had delayed southeast of the airport for about an hour while the flight crew coped with a landing gear malfunction and prepared its passengers for a possible emergency landing. After failure of all four engines due to fuel exhaustion, the airplane crashed about 6 miles southeast of the airport, with a loss of 10 persons and injuries to 23.

The NTSB found the probable cause to be the failure of the Captain to monitor the fuel state and to respond properly to a low fuel state and to crewmember advisories regarding the fuel state. His inattention resulted from preoccupation with the landing gear malfunction and preparations for the possible emergency landing. Contributing to the accident was the failure of the other two crew members to fully comprehend the criticality of the fuel state or to successfully communicate their concern to the Captain. The Board discussed crew coordination, management and teamwork in its report. (NTSB, 1979a)

3/10/1979: Swift Aire Aerospatiale Nord 262, Marina Del Rey, CA

This commuter aircraft was taking off at dusk from Los Angeles enroute to Santa Maria, CA, when a crewmember transmitted "Emergency, going down" on tower frequency. Witnesses stated that the right propellor was slowing as the airplane passed the far end of the runway; popping sounds were heard as it passed the shoreline. The airplane turned north parallel to the shoreline, descended, ditched smoothly in shallow water, and sank immediately. The cockpit partially separated from the fuselage at impact. The accident was fatal to the two crewmembers and one passenger.

The flaps were set at 35°, the right propellor was fully feathered and the left propellor was in flight fine position. It was found that the right propellor pitot pressure line had failed; the line was deteriorated and would have been susceptible to spontaneous rupture or a leak. The left engine fuel valve was closed (it is throttle-actuated). Once the fuel valve has been closed, the engine's propellor must be feathered and a normal engine start initiated to reopen the valve. The aircraft operating manual did not state this and the pilots did not know it.

The NTSB found that the right engine had autofeathered when the pitot pressure line had failed; the pilots shut down the left engine shortly thereafter, probably due to improper identification of the engine that had failed. Their attempts to restart the good engine were unsuccessful because of their unawareness of the proper starting sequence after a fuel valve has been closed. Engine failure procedures were revised following this accident. (NTSB, 1979b)

11/11/1979: Aeromexico DC-10-30 over Luxembourg

During an evening climb in good weather to 31,000 ft enroute to Miami from Frankfurt, flight 945 entered pre-stall buffet and a sustained stall at 29,800 ft. Stall recovery was affected at 18,900 ft. The crew performed a functional check of the airplane and after finding that it operated properly they continued to its intended destination. After arrival, it was discovered that parts of both outboard elevators and the lower fuselage tail maintenance access door were missing.

The flight data recorder showed that the airplane slowed to 226 kt during a climb on autopilot, quite possibly in vertical speed mode rather than indicated airspeed mode. Buffet speed was calculated to be 241 kt. After initial buffet, the #3 engine was shut down and the airplane slowed to below stall speed.

The NTSB found the probable cause to be failure of the flight crew to follow standard climb procedures and to adequately monitor the airplane's flight instruments. This resulted in the aircraft entering into prolonged stall buffet which placed it outside the design envelope. (NTSB, 1980)

10/7/1970: Aircraft Separation Incidents at Hartsfield Airport, Atlanta, GA

This episode involved several conflicts among aircraft operating under the direction of air traffic control in the Atlanta terminal area. In at least two cases, evasive action was required to avoid collisions. The conflicts were caused by multiple failures of coordination and execution by several controllers during a very busy period.

The NTSB found that the near collisions were the result of inept traffic handling by control personnel. This ineptness was due in part to inadequacies in training, procedural deficiencies, and some difficulties imposed by the physical layout of the control room. The Board also found that the design of the low altitude/conflict alert system contributed to the controller's not recognizing the conflicts. The report stated that, "The flashing visual conflict alert is not conspicuous when the data tag is also flashing in the handoff status. The low altitude warning and conflict alerts utilize the same audio signal which is audible to all control room personnel rather than being restricted to only those immediately concerned with the aircraft. This results in a 'cry wolf' syndrome in which controllers are psychologically conditioned to disregard the alarms." (NTSB, 1981)

1/13/1982: Air Florida B-737, Washington National Airport, DC

This airplane crashed into the 14th Street bridge over the Potomac River shortly after takeoff from Washington National Airport in snow conditions, killing 74 of 79 persons on board. The airplane had been de-iced 1 hour before departure, but a substantial period of time had elapsed since that operation before it reached takeoff position. The engines developed substantially less than takeoff power during the takeoff and thereafter due to incorrect setting of takeoff power by the pilots. It was believed that the differential pressure probes in both engines were iced over, providing incorrect (too high) EGT indications in the cockpit. This should have been detected by examination of the other engine instruments, but was not.

The NTSB found that the probable cause of the accident was the flight crew's failure to use engine anti-ice during ground operation and takeoff, their decision to take off with snow/ice on the airfoils, and the captain's failure to reject the takeoff at an early stage when his attention was called to anomalous engine instrument readings. Contributing factors included the prolonged ground delay after deicing, the known inherent pitching characteristics of the B-737 when the wing leading edges are contaminated, and the limited experience of the flight crew in jet transport winter operations. (NTSB, 1982)

9/3/1983: Korean Air Lines B-747 over Sakhalin Island, USSR

The airplane was destroyed in cruise flight by air-to-air missiles fired from a Soviet fighter after it strayed into a forbidden area enroute from Anchorage, AK to Soeul, Korea. The airplane had twice violated Soviet airspace during its flight. The flight data and cockpit voice recorders were not recovered from the sea. After extensive investigation by the International Civil Aviation Organization, it was believed that its aberrant flight path had been the result of one or more incorrect sets of waypoints loaded into the INS systems prior to departure from Anchorage.

Many years later, the Russian government made available further information on the flight which supported a finding that the crew had inadvertently left the airplane's autopilot in heading mode rather than INS mode for an extended period of time. As a result, the flight path took the airplane over Soviet territory, where it was destroyed by a Soviet fighter. (Stein, 1985; see also incident of 2/13/90.)

2/28/1984: Scandinavian Airlines DC-10-30, J. F. Kennedy Airport, NY

After crossing the runway threshold at proper height but 50 kt above reference speed, the airplane touched down 4700 ft beyond the threshold of an 8400 ft runway and could not be stopped on the runway. It was steered to the right and came to rest in water 600 ft from the runway end. A few passengers sustained minor injuries during evacuation. The weather was very poor and the runway was wet.

The airplane's autothrottle system had been unreliable for approximately one month and had not reduced speed when commanded during the first (Stockholm-Oslo) leg of this flight. The Captain had deliberately selected 168 kt to compensate for a threatened wind shear. The throttles did not retard passing 50 ft and did not respond to the autothrottle speed control system commands (the flight crew was not required to use the autothrottle speed control system for this approach).

The NTSB cited as the probable cause the flight crew's disregard for prescribed procedures for monitoring and controlling airspeed during the final stages of the approach, its decision to continue the landing rather than to execute a missed approach, and overreliance on the autothrottle speed control system which had a history of recent malfunctions. It noted that "performance was either aberrant or represents a tendency for the crew to be complacent and over-rely on automated systems". It also noted that there were three speed indications available to the crew: its airspeed indications, the fast-slow indicators on the attitude director, and an indicated vertical speed of 1840 ft per minute on glide slope. In its report, the Board discussed the issue of overreliance on automated systems at length (report pp. 37-39) and cited several other examples of the phenomenon. (NTSB, 1984)

2/19/1985: China Airlines B747-SP, 300 miles northwest of San Francisco

The airplane, flying at 41,000 ft enroute to Los Angeles from Taipei, suffered an inflight upset after an uneventful flight. The airplane was on autopilot when the #4 engine lost power. During attempts to relight the engine, the airplane rolled to the right, nosed over and began an uncontrollable descent. The Captain was unable to restore the airplane to stable flight until it had descended to 9500 ft.

The autopilot was operating in the performance management system (PMS) mode for pitch guidance and altitude hold. Roll commands were provided by the INS; in this mode, the autopilot uses only the ailerons and spoilers for lateral control; rudder and rudder trim are not used. In light turbulence, that airspeed began to fluctuate; the PMS followed the fluctuations and retarded the throttles when airspeed increased. As the airplane slowed, the PMS moved the throttles forward; engines 1, 2 and 3 accelerated but #4 did not. The flight engineer moved the #4 throttle forward but without effect. The INS caused the autopilot to hold the left wing down since it could not correct with rudder. The airplane decelerated due to the lack of power. After attempting to correct the situation with autopilot, the Captain disengaged the autopilot at which time the airplane rolled to the right, yawed, then entered a steep descent in cloud, during which it exceeded maximum operating speed. It was extensively damaged during the descent and recovery; the landing gear deployed, 10-11 ft of the left horizontal stabilizer was torn off and the no. 1 hydraulic system lines were severed. The right stabilizer and 3/4 of the right outboard elevator were missing when the airplane landed; the wings were also bent upward.

The NTSB determined that the probable cause was the Captain's preoccupation with an inflight malfunction and his failure to monitor properly the airplane's flight instruments which resulted in his losing control of the airplane. Contributing to the accident was the Captain's overreliance on the autopilot after a loss of thrust on #4 engine. The Board noted that the autopilot effectively masked the approaching onset of loss of control of the airplane. (NTSB, 1986)

3/31/1986: United Airlines B-767, San Francisco, CA

This airplane was passing through 3100 ft on its climb from San Francisco when both engines lost power abruptly. The engines were restarted and the airplane returned to San Francisco, where it landed without incident. The crew reported that engine power was lost when the flight crew attempted to switch from manual operation to the engine electronic control system, a procedure which prior to that time was normally carried out at 3000 ft during the climb. The EEC switches are guarded. It is believed that the crew may have inadvertently shut off fuel to the engines when they intended to engage the EEC, as in the incident cited immediately below. (AWST, 1986)

6/30/1987: Delta Air Lines B-767, Los Angeles, CA

Over water, shortly after takeoff from Los Angeles, this twin-engine airplane suffered a double-engine failure when the captain, attempting to deactivate an electronic engine controller in response to an EEC caution light, shut off the fuel valves instead. The crew was able to restart the engines within one minute after an altitude loss of several hundred feet. The fuel valves were located immediately above the electronic engine control switches on the airplane center console, though the switches were dissimilar in shape.

The FAA thereafter issued an emergency airworthiness directive requiring installation of a guard device between the cockpit fuel control switches. (AWST, 1987)

7/8/1987: Delta Air Lines L-1011/Continental Airlines B-747 over Atlantic Ocean

These two airplanes experienced a near midair collision over the north Atlantic ocean after the Delta airplane strayed 60 miles off its assigned oceanic route. The incident, which was observed by other aircraft in the area but not, apparently, by the Delta crew, was believed to have been caused by an incorrectly inserted waypoint in the Delta airplane's INS prior to departure. (Preble, 1987)

8/16/1987: Northwest Airlines DC9-82, Detroit Metro Airport, Romulus, MI

The airplane crashed almost immediately after takeoff from runway 3C[1] enroute to Phoenix. The airplane began its rotation about 1200-1500 feet from the end of the 8500 ft runway and lifted

1 Runways are numbered to indicate their magnetic heading to the nearest 10°; 3=30° (actually from 26-34°). Parallel runways also have letter designators: L=left, C=center, R=right.

off near the end. After liftoff, the wings rolled to the left and right; it then collided with a light pole located 1/2 mile beyond the end of the runway. 154 persons were killed; one survived.

During the investigation, it was found that the trailing edge flaps and leading edge slats were fully retracted. Cockpit voice recorder (CVR) readout indicated that the takeoff warning system did not function and thus did not warn the flight crew that the airplane was improperly configured for takeoff.

The NTSB attributed the accident to the flight crew's failure to use the taxi checklist to insure that the flaps and slats were extended. The failure of the takeoff warning system was a contributing factor. This airplane has a stall protection system which announces a stall and incorporates a stick pusher, but autoslat extension and post-stall recovery is disabled if the slats are retracted. Its caution and warning system also provides tone and voice warning of a stall, but this is disabled in flight by nose gear extension. (NTSB, 1988b)

6/26/1988: Air France Airbus A320, Mulhouse-Habsheim, France

This airplane crashed into tall trees following a very slow, very low altitude flyover at a general aviation airfield during an air show. Three of 136 persons aboard the aircraft were killed; 36 were injured. The Captain, an experienced A320 check pilot, was demonstrating the slow-speed maneuverability of the then-new airplane.

The French Commission of Inquiry found that the flyover was conducted at an altitude lower than the minimum of 170 ft specified by regulations and considerably lower than the intended 100 ft altitude level pass briefed to the crew by the captain prior to flight. It stated that, "The training given to the pilots emphasized all the protections from which the A320 benefits with respect to its lift which could have given them the feeling, which indeed is justified, of increased safety...*However, emphasis was perhaps not sufficiently placed on the fact that, if the (angle of attack) limit cannot be exceeded, it nevertheless exists and still affects the performance.*" (emphasis supplied) The Commission noted that automatic go-around protection had been inhibited and that this decision was compatible with the Captain's objective of maintaining 100 ft. In effect, below 100 ft, this protection was not active.

The Commission attributed the cause of the accident to the very low flyover height, very slow and reducing speed, engine power at flight idle, and a late application of go-around power. It commented on insufficient flight preparation, inadequate task sharing in the cockpit, and possible overconfidence because of the envelope protection features of the A320. (Ministry of Planning, Housing, Transport and Maritime Affairs, 1989)

8/31/1988: Delta Airlines B727-232, Dallas-Fort Worth Airport, TX

The airplane, flight 1141, crashed shortly after takeoff from runway 18L enroute to Salt Lake City. The takeoff roll was normal but as the main gear left the ground the crew heard two explosions and the airplane began to roll violently; it struck an ILS antenna 1000 ft past the runway end after being airborne for about 22 sec. 14 persons were killed, 26 injured, 68 uninjured.

The investigation showed that the flaps and slats were fully retracted. Evidence suggested that there was an intermittent fault in the takeoff warning system that was not detected and corrected during the last maintenance action. This problem could have manifested itself during the takeoff.

The NTSB found the probable cause to be the Captain's and first officer's inadequate cockpit discipline and failure of the takeoff configuration warning system to alert the crew that the airplane was not properly configured for takeoff. It found as contributing factors certain management and procedural deficiencies and lack of sufficiently aggressive action by FAA to correct known deficiencies in the air carrier. The Board took note of extensive non-duty related conversations and the lengthy presence in the cockpit of a flight attendant which reduced the flight crew's vigilance in insuring that the airplane was properly prepared for flight. (NTSB, 1988a)

3/10/1989: Air Ontario Fokker F-28, Dryden, Ontario, Canada

This airplane was dispatched from Winnipeg, Man. to Thunder Bay, Ont., thence via Dryden, Ont. back to Winnipeg, with an inoperative auxiliary power unit. While preparing for the return trip at Thunder Bay, the crew found more passengers than had been planned for or could be accommodated if enough fuel for the entire flight to Winnipeg was boarded, as it had been. The captain preferred to offload passengers rather than fuel; he was overruled by the company. This action required a delay for defueling at Thunder Bay and a landing at Dryden to take on additional fuel. The company's system operations center did not inform the captain of freezing rain forecast for Dryden.

Upon arriving at Dryden, which had no ground power units with which to start the airplane's engines, the captain was required to take on fuel with one engine running. This was a permitted action, though it was performed with passengers on board, which was not permitted. The airplane could not be de-iced with engines running, however, and freezing rain was falling prior to his takeoff, which was also delayed by a lost aircraft trying to land. The airplane crashed immediately after takeoff; ice was noted on the wings by surviving passengers and cabin crew.

The captain in this accident was placed in a "triple bind". He could not uplift sufficient fuel to fly to Winnipeg with the full passenger load. If he landed at Dryden, he could refuel but could not de-ice if required. The defueling at Thunder Bay had already made his flight over one hour late. He received inadequate information and no guidance from his company.

The subsequent Commission of Inquiry found a large number of latent factors at many levels within the company, its parent, Air Canada, and Transport Canada, the regulatory authority. (Moshansky, 1992)

11/21/1989 British Airways B747, Heathrow Airport, London, England

The aircraft approached London in very bad weather after a flight from Bahrain. Fuel was low due to headwinds; the copilot had been incapacitated for part of the flight due to gastroenteritis and diarrhea. The copilot was not certified for category II or III landings. BA flight operations authorized the approach despite the copilot's lack of qualifications. The approach, to runway 27 instead of 9 as briefed, was hurried. When the aircraft captured the localizer and glide slope, the autopilots failed to stabilize the aircraft, possibly due to late capture of the radio beams. 125 feet above ground, the runway was not in sight and the captain gently began a missed approach. The aircraft sank to 75 feet above ground before gaining altitude. After a second, successful approach, the aircraft landed safely.

An investigation by British Airways disclosed that during the first approach, the aircraft had been seriously to the right of the localizer course and had overflown a hotel to the north of the airport only a few feet above the highest obstacle on its course. The pilot and crew were suspended; legal action was later taken against the captain for endangering the passengers and persons on the ground. (Wilkinson, 1994)

1/25/1990: Avianca B-707-321, Cove Neck, New York

Avianca flight 052 crashed in a wooded residential area during an approach to Kennedy International Airport after all engines failed due to fuel exhaustion. The flight from Medellin, Colombia had been placed in holding patterns three times for a total of about 1.3 hours. During the third period of holding, the crew reported that the airplane could not hold longer than 5 minutes, that it was running out of fuel, and that it could not reach its alternate airport in Boston.

Subsequently, the flight executed a missed approach at Kennedy. While trying to return to the airport, the airplane lost power in all four engines and crashed 16 miles from the runway.

The NTSB determined that the probable cause of the accident was the failure of the flightcrew to adequately manage the airplane's fuel load, and their failure to communicate an emergency fuel situation to air traffic control before fuel exhaustion occurred. Contributing to the accident was the flightcrew's failure to use an airline operational control dispatch system to assist them during the international flight into a high-density airport in poor weather. Also contributing was inadequate traffic flow management by the FAA and the lack of standardized understandable terminology for pilots and controllers for minimum and emergency fuel states. Windshear, crew fatigue and stress were other factors that led to the unsuccessful completion of the first approach and thus contributed to the accident. (NTSB, 1991a)

2/13/1990 El Al B747 and British Airways B747 over the Atlantic Ocean

An El Al B-747 enroute from Tel Aviv to New York almost collided with a British Airways 747 in the Reykjavik Flight Information Region after its crew failed to switch back from heading mode to INS mode after being cleared by Shanwick control to a new oceanic track. The crew deviated 110 nm north of the new track before realizing their error. Upon recognizing the error, the flightcrew notified ATC but provided no information on the magnitude of their deviation. ATC cleared them to turn left to reintercept their cleared track, which they did.

The near collision occurred while the crew were navigating back to the correct track without descending 1000 ft below the prevailing traffic flow, as prescribed by North Atlantic Special Procedures for In-flight Contingencies. The El Al 747 passed right-to-left ahead of a westbound British Airways 747 which took evasive action, missing El Al by approximately 600 ft. (Pan American World Airways, 1990)

2/14/1990: Indian Airlines Airbus A320, Bangalore, India

(Official report not available) This airplane crashed short of the runway during an approach to land in good weather, killing 94 of 146 persons aboard including the pilots. The best available data indicates that the airplane had descended at idle power in the "idle open descent" mode until shortly before the accident, when an attempt was made to recover by adding power but too late to permit engine spool-up prior to impact. The airplane was being flown by a Captain undergoing a route check by a check airman.

The crew allowed the speed to decrease to 25 kt below the nominal approach speed late in the descent. The recovery from this condition was started at an altitude of only 140 ft, while flying at minimum speed and maximum angle of attack. The check captain noted that the flight director should be off, and the trainee responded that it was off. The check captain corrected him by stating, "But you did not put off mine". If either flight director is engaged, the selected autothrust mode will remain operative, in this case, the idle open descent mode. The alpha floor mode was automatically activated by the declining speed and increasing angle of attack; it caused the autothrust system to advance the power, but this occurred too late for recovery to be affected before the airplane impacted the ground. (Lenorovitz, 1990)

12/3/1990: Northwest Airlines B-727 and DC-9, Detroit Metro Airport, MI

These two aircraft collided while the 727 was taking off and the DC-9 had just inadvertently taxiied onto the active runway. The DC-9 was lost on the airport in severely restricted visibility. Both aircraft were on the ground. The accident site was not visible from the tower due to fog; ASDE was not available.

The Board determined that the probable cause of the accident was a lack of proper crew coordination, including a reversal of roles, on the part of the DC-9 pilots. This led to their failure to stop taxiing and alert the ground controller of their positional uncertainty in a timely manner before and after intruding onto the active runway. A number of contributing factors were also cited. (NTSB, 1991b)

2/1/1991: US Air B-737 and Skywest Fairchild Metro, Los Angeles, CA

This accident occurred after the US Air airplane was cleared to land on runway 24L at Los Angeles while the Skywest Metro was positioned on the runway at an intersection awaiting takeoff clearance. There were 34 fatalities and 67 survivors. The Metro may not have been easily visible from the control tower; airport surface detection radar equipment (ASDE) was available but was being used for surveillance of the south side of the airport. The controller was very busy just prior to the time of the accident.

The NTSB investigation indicated that the controller cleared the Metro into position at an intersection on runway 24L, 2400 ft from the threshold, two minutes before the accident. One minute later, the 737 was given a clearance to land on runway 24L. The Board determined that the probable cause of the accident was the failure of Los Angeles Air Traffic Facility management to implement procedures that provided adequate redundancy and the failure of FAA's Air Traffic Management to provide adequate policy direction and oversight. These failures ultimately led to the failure of the local controller to maintain awareness of the traffic situation. (NTSB, 1991c)

5/26/1991 Lauda Air (Austria) B767-300ER over Thailand

This airplane was climbing to altitude on a flight between Bangkok and Vienna when its right engine reverser actuated because of a mechanical failure. The flight crew was unable to control the airplane due to the high level of reverse thrust coming from the right engine. The airplane crashed after an uncontrolled descent. Simulation studies indicated that recovery from such an event was not possible for pilots without advance knowledge of the event. (Ministry of Transport and Communications, Thailand, 1993)

8/12/1991: Ansett Australia A320 and Thai Airways DC-10: Sydney, Australia

During simultaneous crossing runway operations at Kingsford Smith Airport, a Thai DC-10 was landing on runway 34 and an Ansett A320 was on short final approach for intersecting runway 25. Landing instructions for the DC-10 included a requirement for the aircraft to hold short of the runway 25 intersection. While observing the DC-10's landing roll during his landing, the A320 captain judged that the DC-10 might not stop before the runway intersection. He elected to initiate a missed approach from a low height above the runway. The go-around was successful; the A320 passed the centerline of runway 34 at a radio altitude of 52 ft. Under heavy braking, the DC-10 slowed to about 2 kts ground speed when it reached the edge of runway 25.

During the A320 go-around, differing attitude command inputs were recorded from the left and right sidesticks for a period of 12 seconds. Neither the captain, who had taken over control, or the copilot, was aware of control stick inputs from the copilot during this period. Activation of the "takeover button" on the control stick was not a part of Ansett's standard operating procedures. The incident analysis noted that "Although the A320 successfully avoided the DC-10, under different circumstances the cross controlling between the pilots could have jeopardized a safe go-around...This simultaneous input situation would almost certainly have been immediately apparent, and corrected rapidly had there been a sense of movement between the two sidesticks." (Bureau of Air Safety Investigation, 1993)

12/12/1991: Evergreen International Airways B-747, Nakina, Ontario, Canada

While in cruise flight at 31000 ft, a cargo aircraft entered a steep right bank (greater than 90°) and descended more than 10000 feet at speeds approaching Mach 1. During the recovery, with vertical accelerations greater than 3g, the right wing was damaged. About 20 feet of honeycomb structure from the underside of the wing was missing; a small honeycomb panel on the upper portion of the wing was damaged and some structure was protruding into the airstream. Upon recovery from the dive, the aircraft was experiencing control difficulties; the crew successfully diverted to Duluth, MN. During the approach and landing, the left and right flaps, as well as the right horizontal stabilizer, were damaged by debris from the damaged right wing. There were no injuries.

The Transportation Safety Board of Canada determined that the flight upset was caused by an uncommanded, insidious roll input by the channel A autopilot roll computer; the roll went undetected by the crew until the aircraft had reached an excessive bank angle and consequential high rate of descent. The recovery action was delayed slightly because of the time required by the crew to determine the aircraft attitude. (NTSB, 1992a)

1/??/1992: Air Inter Airbus A320 on approach to Strasbourg, France

The airplane was being given radar vectors to a non-precision (VOR-DME) approach to the airport at Strasbourg. It was given vectors that left little time for cockpit setup prior to intercepting the final approach course. It is believed that the pilots intended to make an automatic approach using a flight path angle of -3.3° from the final approach fix; this maneuver would have placed them at approximately the correct point for visual descent when they reached minimum descent altitude.

The pilots, however, appear to have executed the approach in heading/vertical speed mode instead of track/flight path angle mode. The Flight Control Unit setting of "-33" yields a vertical descent rate of -3300 ft/min in this mode, and this is almost precisely the rate of descent the airplane realized until it crashed into mountainous terrain several miles short of the airport. A push button on the FCU panel cycles the automation between H/VSI and T/FPA mode.

Modifications to A320 vertical speed/flightpath angle displays (in vertical speed mode, four digits are shown; in flight path angle mode, only two digits are visible) were subsequently made available by the manufacturer to avoid this error. New production A320s have been modified in this manner since November, 1993 (Aerospace, 1994a).

12/8/1992: United Airlines B737-291, Colorado Springs, CO

United Airlines flight 585 was on final approach course following a flight from Denver, CO to Colorado Springs, CO under visual meteorological conditions when it was observed by numerous eyewitnesses to roll steadily to the right and pitch nose down, reaching a nearly vertical attitude when it impacted the ground, killing all 25 occupants.

Despite an exhaustive investigation which is continuing, the NTSB has thus far been unable to identify conclusive evidence to explain the loss of this aircraft. It is surmised by the Board that either a rudder control anomaly, or a "rotor", a horizontal axis wind vortex, may have precipitated the loss of control, but this is not certain. (NTSB, 1992b)

9/14/1993: Lufthansa A320, Warsaw, Poland

The aircraft, carrying 70 persons, landed at Warsaw in a downpour with strong, gusty winds. The pilot carried extra airspeed because of the wind conditions; a probable wind shear late in the approach made its ground speed still faster at touchdown. The airplane landed gently despite the gusts. It continued for approximately 8 sec after touchdown before being able to activate ground spoilers and reverse thrust. The airplane overran the runway end, traversed an embankment beyond the departure end and caught fire. Two persons, including the copilot, were killed; 55 were injured.

"Preliminary findings of the Polish inquiry...suggest that the crew, having been advised of wind shear and a wet runway, correctly added 20 kt to the approach speed. When the forecast crosswind unexpectedly became a tailwind, making ground speed about 170 kt, the wheel spinup and oleo squat switches did not (activate). For a critical 9 sec (during which the aircraft may have been aquaplaning) thrust reverse, wheelbraking and lift dumping (full spoiler deployment) remained disarmed...Although the A320 was...still to have the softer landing double-oleo modification, which might have 'made' the switches, the priority question raised by the accident is whether pilots should have manual override of safety locks..." (Aerospace, 1994b; AWST, 1994a)

4/26/1994: China Airlines A-300-600R, Nagoya, Japan

During a normal approach to landing at Nagoya runway 34 in visual meteorological conditions, the captain indicated he was going around but did not indicate why. Within the next 30 seconds, witnesses saw the aircraft in a nose-up attitude, rolling to its right before crashing tail-first 300 ft to the right of the approach end of the runway.

During the approach, the copilot flying apparently triggered the autopilot TOGA (takeoff-go-around) switch, whereupon the automation added power and commanded a pitch-up. The captain warned the copilot of the mode change, but the copilot continued to attempt to guide the aircraft down the glide slope while the automation countered his inputs with nose-up elevator trim. Ultimately, with stabilizer trim in an extreme nose-up position, the copilot was unable to counteract the trim with nose-down elevator. The aircraft nosed up to an attitude in excess of 50°, stalled, and slid backwards to the ground. 264 people were killed in the crash.

This accident is still under civil and criminal investigation. It is presently thought that the pilots failed "to realize that their decision (to continue the approach) contradicted the logic of the airplane's automated safety systems. In February, 1991, an Interflug A310 at Moscow experienced a sudden, steep pitch-up similar to the one observed in this accident." (*Aviation Week & Space Technology*, 5/2/94, p. 26; 5/9/94, pp. 31-32; 12/5/94, p. 29)

On 8/31/94, The NTSB issued Safety Recommendations A-94-164 through -166 to the FAA. Its Recommendation stated, "the Safety Board is concerned that the possibility still exists for a pilot-induced 'runaway trim' situation at low altitude and that...such a situation could result in a stall or the airplane landing in a nose-down attitude..." Referring to other transport category aircraft autopilot systems, the Board said, "It is noted that the (autopilot) disconnect and warning systems are fully functional, regardless of altitude, and with or without the autopilot in the land or go-around modes. The Safety Board believes that the autopilot disconnect systems in the Airbus A-300 and A-310 are significantly different...additionally, the lack of a stabilizer-in-motion warning appears to be unique to (these aircraft). The accident in Nagoya and the incident in Moscow indicate that pilots may not be aware that under some circumstances the autopilot will work against them if they try to manually control the airplane."

The Board recommended that these autopilot systems be modified to ensure that the autopilot would disconnect if the pilot applies a specified input to the flight controls or trim system, regardless of the altitude or operating mode of the autopilot, and also to provide a sufficient perceptual alert when the trimmable horizontal stabilizer is in motion, irrespective of the source of the trim command. (NTSB, 1994)

6/6/1994: Dragonair A-320, Kai Tak Airport, Hong Kong

The airplane was attempting a landing at Kai Tak Airport during a severe storm. As the aircraft banked at about 1000 feet, it encountered a wind shear that registered -1.6g. It lost 12 kt of airspeed in 1 second. The buffeting triggered its automatic flap locking safety mechanism, which is set if there is more than a 40 mm difference between the positions of the flaps to prevent them from becoming asymmetrical. The flaps locked at a full setting of 40°, or "flaps 4" (the landing position). The airplane's (leading edge) slats were in the no. 3 position of 22°. Sensing an anomaly, the electronic centralized aircraft monitoring system (ECAM) flashed a warning message for the pilot to correct it by moving the flaps lever to Flaps 3.

Unable to do so, the pilot aborted the landing. On the fourth try, he landed on runway 31, which allowed an approach without a banking maneuver. Two passengers were slightly injured after the aircraft ran off the runway. The incident is still under investigation. The article notes that a similar incident apparently occurred to an Indian Airlines A320 in November, 1993. Airbus Industrie has recommended since this incident that pilots disregard the ECAM warning message. The software is being rewritten to eliminate the message; changes are also to be made in the flight control computers to prevent discrepancies between the flap lever position and the position of the flaps. (AWST, 1994)

6/21/1994: Brittania Airways B757-200, Manchester, United Kingdom

The aircraft was at light weight and was conducting a full-power takeoff. An altitude of 5000 ft had been selected. The autopilot went to altitude acquisition mode passing 2200 ft because of the rapid climb speed. Power was reduced by the autothrust system and the airplane's speed began to drop rapidly toward takeoff safety speed because of the high pitch angle. Flight director bars continued to command pitch up, then disappeared from view. The pilot reduced the pitch attitude to 10° nose-up and normal acceleration resumed. This incident resembles in many respects the more serious occurrence of the A330 at Toulouse (6/30/94, below), which also involved a rapid switch to altitude acquisition mode after takeoff. (Civil Aviation Authority, UK, 1994)

6/30/1994: Airbus A330-322 test flight, Toulouse Blagnac Airport, France:

This airplane was on a Category III certification test flight to study various pitch transition control laws in the autopilot Speed Reference System mode during engine failure at low altitude, rearward center of gravity and light aircraft weight. The flight crew included an experienced test pilot flying as captain, a copilot from a customer company, a flight test engineer, and three passengers. The copilot was handling the aircraft.

During the takeoff, the copilot rotated the airplane slightly rapidly; the landing gear was retracted. The autopilot was engaged 6 sec after takeoff at a speed of 150 kt and a pitch angle of almost 25° nose up. Immediately thereafter, the left engine was brought to idle power and one hydraulic system was shut down, as planned for the test.

When the airplane reached 25° pitch angle, autopilot and flight director mode information were automatically removed from the PFD. A maximum pitch angle of 29° was reached 8 sec after takeoff; the airplane was decelerating. The angle of attack reached 14°, which activated the alpha protection mode of the flight controls. The captain disconnected the autopilot 19 sec after takeoff. Subsequent control actions by the captain, which included reducing power on the right engine to regain control, deactivated alpha floor protection on the left engine. The airplane slowed to 100 kt, appreciably below minimum single-engine control speed of 118 kt, and yawed to the left. The left wing then stalled; speed reached 77 kt with an increasing left bank. Pitch angle reached 43° nose down and the airplane crashed 36 sec after takeoff.

During investigation, it was found that the aircraft autopilot had gone into altitude acquisition (ALT*) mode. In this mode, there was no maximum pitch limitation in the autoflight system software. As a consequence, at low speed, if a major thrust change occurs (as it did here), the autopilot can induce irrelevant pitch attitudes since it is still trying to follow an altitude acquisition path which it cannot achieve.

The investigating committee believed that the accident was caused by the conjunction of several factors, none of which taken separately would have produced the accident. The committee cited the planned and inadvertent conditions under which the flight test was undertaken (high thrust, very aft center of gravity, trim within limits but nose-up, a selected altitude of 2000 feet, late and imprecise definition of respective tasks between the pilot and copilot regarding the test to be performed, firm and quick rotation by the copilot, captain busy with the test actions, taking him out of the piloting loop). They also noted that the lack of pitch protection in the ALT* mode of the autopilot played a key role. Contributing factors included the inability of the flight crew to identify the active autopilot mode (due to the FMA declutter action at 25° nose-up), crew confidence in the anticipated aircraft reactions, late reaction of the flight test engineer to the rapid evolution of flight parameters (particularly the airspeed), and a late captain reaction to an abnormal situation.

A subsequent published article noted that "Contradictory autopilot requirements appear as a key factor that contributed to the loss of control: the 2,000 ft altitude was selected while the autopilot also had to simultaneously manage the combination of very low speed, an extremely high angle of attack, and asymmetrical engine thrust." (Director General of Armaments (France), 1994)

7/2/1994: US Air DC-9-31, Charlotte, NC

The airplane was returning from Columbia, SC to Charlotte, NC, when it encountered a wind shear during a very heavy rainstorm while on final approach to the Charlotte-Douglas Airport. A wind shear alert had been received and the crew had briefed a missed approach if necessary. The captain flying ordered a missed approach at 200 feet because of poor visibility and strong, gusty winds. The first officer initiated the missed approach; the landing gear was retracted and flaps reduced from 40° (landing position) to 15°. At 350 ft the crew felt a severe sink developing; full throttles were applied, but full thrust occurred only about 3 sec before impact, too late to arrest the descent and impact about 0.2 nm to the right of runway 18R. 37 occupants were killed.

The crewmembers were unable to recall whether they had heard an aural warning from the wind shear detection system; investigation later revealed that the system's sensitivity is sharply reduced while wing flaps are in transit, to minimize the likelihood of false or nuisance warnings when airflow over the wing is disturbed during the change of configuration. Data provided to the NTSB by the system's manufacturer indicated that an alert would have been furnished 12 sec after a wind shear was detected if flaps were in transit, whereas an alert would have been generated in the presence of a severe shear within 5 sec under other circumstances. As a result, the time lag "rendered the system useless" because the warning "would have occurred too late" for the pilots to perform a successful escape maneuver, according to the NTSB. It is not known whether the pilots were aware of this automatic reduction in sensitivity during flap transit.

The NTSB recommended that the FAA issue a flight standards bulletin informing pilots that wind shear warnings will be unavailable when flaps are in transit, and require modifications in the standard wind shear alert system to delete the delay feature, thereby ensuring "prompt warning activation" when flaps are transitioning between settings. The Board did not speak to the fact that this delay was incorporated in the system's software specifically to avoid nuisance warnings caused by temporary airflow disturbances. Honeywell had stated that such false alarms could cause pilots to "overreact or lost confidence" in the system's detection capabilities. (Phillips, 1994c)

9/8/1994: US Air B737-300, Pittsburgh, PA

During a routine approach to Great Pittsburgh International Airport, US Air flight 427 was cleared to turn left to a heading of 100°, reduce speed to 190 kt and descend to 6000 ft in preparation for a right downwind on a visual approach to runway 28R. The pilots extended their slats and flaps to the "Flaps 1" position. As the airplane began its turn, it rolled left, then decreased its bank angle, then increased it again to at least 100° as the nose pitched downward. The airplane struck the ground 23 sec later at an angle of about 80° and an airspeed in excess of 260 kt. The accident was not survivable.

The NTSB has undertaken extensive investigations of this accident, which thus far remains unexplained. Data collection is continuing. The similarity between certain aspects of this accident and a B737-291 accident at Colorado Springs, CO on 12/8/92, also unexplained, has prompted intensive studies of rudder control and other aircraft mechanisms by the Board, the Boeing Company and component manufacturers. In both cases, the Board has been hampered by the availability of only limited data from the flight data recorders, which were older models with limited parameter recording capability. (Phillips, 1994b; see also page 69)

9/24/1994: Tarom (Romanian) Airlines A310-300, Orly Airport, Paris, France

The airplane, carrying 182 persons on a flight from Bucharest to Paris, was on final approach to Orly Airport under visual meteorological conditions when it suddenly assumed a steep, nose-high attitude, then rolled into a dive before the pilots regained control at 800 feet above ground. No one was seriously injured and the airplane landed safely. A videotape taken by a witness showed the airplane in a steep nose-up attitude, then rolling off on one wing and descending in a nose-down attitude for several seconds before recovery. The digital flight data recorder was apparently inoperative during the incident, but data were obtained from the cockpit voice recorder and a direct access recorder used for maintenance purposes.

It is believed that the autopilot "suddenly went into the 'level change' mode" because flap limit speed was exceeded by 2 knots during the approach; this resulted in the pitch-up. "According to one report, the electric trim countered the pilot's action" during the attempt to recover from the pitch-up. (AWST, 1994b; Aerospace, 1994c; see also AWST, 1995b)

10/31/1994: American Eagle Airlines ATR72, Roselawn, IN

The airplane went out of control and crashed after flying at 10,000 ft at relatively low airspeed in a holding pattern for an extended period under icing conditions. The airplane carried a highly capable digital flight data recorder, whose data indicated that severe lateral control instability occurred, due, it is presently thought, to an accretion of ice ahead of the ailerons but aft of the wing leading edge de-icer boots. The airplane was being flown on autopilot when control was first lost.

The accident is still under investigation, but the NTSB has issued urgent safety recommendations. The FAA has warned ATR42/72 pilots to avoid prolonged flight under icing conditions and to avoid high angles of attack if lateral instability occurs. Autopilot use under such conditions is proscribed, because autopilot corrective actions can mask the onset of the controllability problem. NTSB was aware of "similar, uncommanded autopilot disengagements and uncommanded lateral excursions" that have occurred on ATR42 aircraft in the past six years. (Phillips, 1994a)

Appendix 2: Wiener and Curry guidelines for aircraft automation

In a landmark paper in 1980, Earl Wiener and Renwick Curry discussed "Flight-Deck Automation: Promises and Problems". Their contribution has been the stimulus for a great deal of research during the 15 years since it was published. This chapter begins with a discussion of these authors' thoughts on this subject.

Wiener and Curry pointed out that even in 1980, the question was "no longer whether one or another function can be automated, but, rather, whether it should be" (p. 2). They questioned the assumption that automation can eliminate human error. They pointed out failures in the interaction of humans with automation and in automation itself.

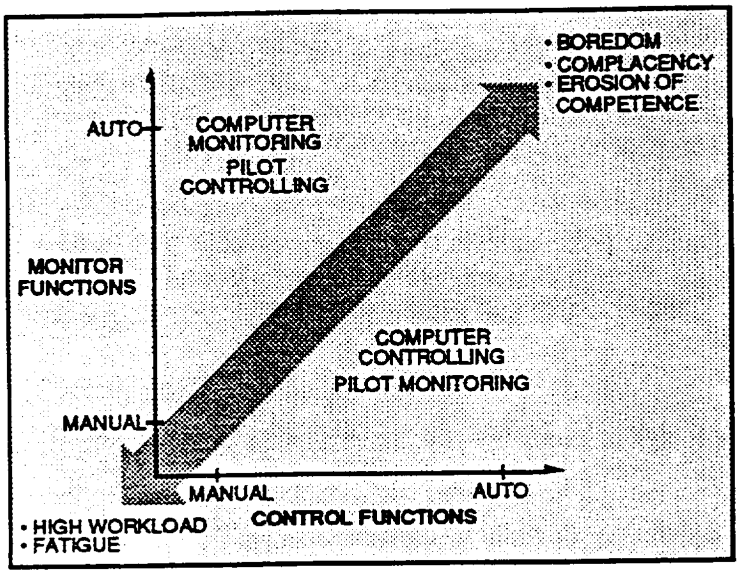

Fig. A2-1: Monitoring and control functions (redrawn from Wiener and Curry, 1980).

They discussed control and monitoring automation and emphasized the independence of these two forms of automation (figure A2-1); "it is possible to have various levels of automation in one dimension independent of the other".

The authors then discussed system goals and design philosophies for control and monitoring automation. They offered some generalizations about advantages and disadvantages of automating human-machine systems and went on to propose some guidelines for the design and use of automated systems in aircraft.

It is worth reviewing Wiener and Curry's guidelines because they foresaw many of the advantages and disadvantages of automation as it is used today. The following are abstracted from their guideline statements.

Control tasks

1. System operation should be easily interpretable 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...this may require user control of certain parameters, such as system gains (see guideline 7). 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...

3. Design the automation to prevent peak levels of task demand from becoming excessive...keeping task demand at reasonable levels will insure available time for monitoring.

4. ...The operator must be trained and motivated to use automation as an additional resource (i.e., as a helper).

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

6. If automation reduces task demands to low levels, provide meaningful duties to maintain operator involvement and resistance to distraction...it is extremely important that any additional duties be meaningful (not "make-work")...

7. Allow for different operator "styles" (choice of automation) when feasible.

8. Insure that overall system performance will be insensitive to different options, or styles of operation...

9. Provide a means for checking the setup and information input to automatic systems. Many automatic system failures have been and will continue to be due to setup error, rather than hardware failures. The automatic system itself can check some of the setup, but independent error-checking equipment and procedures should be provided when appropriate.

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

Monitoring tasks

11. Keep false alarm rates within acceptable limits (recognize the behavioral effect 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 the proper format so that this validity check can be made quickly and accurately...Also, provide the operator with information and controls to diagnose the automatic system and warning system operation.

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 possibly training hardware...to insure that flightcrews are exposed to all forms of alerts and to many of the possible combinations of alerts, and that they understand how to deal with them.

The authors concluded that "the rapid pace of automation is outstripping one's ability to comprehend all the implications for crew performance. It is unrealistic to call for a halt to cockpit automation until the manifestations are completely understood. We do, however, call for those designing, analyzing, and installing automatic systems in the cockpit to do so carefully; *to recognize the behavioral effects of automation;* to avail themselves of present and future guidelines; and to be watchful for symptoms that might appear in training and operational settings..." (emphasis supplied) Their comments are as appropriate as when they were written.

References

Abbott, K. H. (1990). *Robust fault diagnosis of physical systems in operation.* Unpublished doctoral dissertation, Rutgers University, New Brunswick, NJ.

Abbott, K. H., & Rogers, W. H. (1992). *Presenting Information for Fault Management.* NASA Langley Research Center publication.

Abbott, T. S. (1989). *Task-oriented display design: Concept and example* (NASA Technical Memorandum 101685). Hampton, VA: NASA Langley Research Center.

Abbott, T. S. (1990). *A simulation evaluation of the engine monitoring and control system display* (NASA Technical Paper 2960). Washington, D.C.: NASA.

Advanced Qualification Program. Amendment 14 CFR 121-219, Oct. 2, 1990.

Aerospace (1994a): Unattributed current news item concerning Air Inter A320 accident at Strasbourg, France. *Aerospace*, February, 1994, p. 5.

Aerospace (1994b): Unattributed current news item concerning Lufthansa A320 accident on landing at Warsaw, Poland. *Aerospace*, February, 1994, p. 6. See also *United Press International*, articles of 9/15/93 and 9/17/93 concerning Lufthansa Airbus A320 accident at Warsaw, Poland.

Aerospace (1994c): News item concerning excursion of Romanian Airlines A310 while on final approach to landing at Orly Airport, Paris. *Aerospace*, November, 1994, p. 5.

Air Safety Regulation (1994, January). Carrier mismanagement, deliberate aerobatics cited in crash. *Air Safety Week*, 8(4), pp. 1-2.

ATA (1989, April): Air Transport Association of America: *National plan to enhance aviation safety through human factors improvements.* Washington,, D. C.

Aviation Occurrence Report (1991): *Flight Control System Malfunction, Evergreen International Airlines, Inc. Boeing 747-121 N475EV, Nakina, Ontario, 12 December 1991.* Report no. A91H0014, Transportation Safety Board of Canada. Also see: National Transportation Safety Board Safety Recommendations A-92-31 through -35, May 14, 1992. Washington, D.C.: NTSB.

AWST (1986): NTSB impounds United 767 after engine power loss. (1986, April 7) *Aviation Week & Space Technology*, p. 36.

AWST (1987): Engine shutdown prompts FAA directive. (1987, July 6). *Aviation Week & Space Technology*, p. 36.

AWST (1994a, 6/27): A320 Flap Advisory. *Aviation Week and Space Technology* 140(26), p. 32.

AWST (1994b, 10/3): Comments on Romanian Airlines A310 excursion on approach to Orly Airport, Paris. *Aviation Week & Space Technology*, 10/3/94, p. 37.

AWST (1995a, 1/30): Automated Cockpits Special Report, part 1. *Aviation Week and Space Technology* 142(5): 52-65.

AWST (1995b, 2/6): Automated Cockpits Special Report, part 2. *Aviation Week and Space Technology* 142(6): 48-57.

Barnhart, W., C. E. Billings, G. E. Cooper, R. Gilstrap, J. K. Lauber, H. W. Orlady, B. Puskas and Stephens, W. (1975): *A Method for the Study of Human Factors in Aircraft Operations.* Moffett Field, CA: Ames Research Center. NASA TM X-62,472, September, 1975.

Begault, D.R. (1993): Head-Up Auditory Displays for Traffic Collision Avoidance System Advisories: A Preliminary Investigation. *Human Factors,* 35(4):707-717.

Begault, D.R., & Wenzel, E.M. (1992): Techniques and applications for binaural sound manipulation in human-machine interfaces. *International Journal of Aviation Psychology* 2(1), pp. 1-22.

Billings, C. E. (1991). *Human-centered aircraft automation: A concept and guidelines* (NASA Technical Memorandum 103885). Moffett Field, CA: NASA- Ames Research Center.

Billings, C. E., & O'Hara, D. B. (1978). *Human factors associated with runway incursions* (ASRS Eighth quarterly report, NASA Technical Memorandum 78540). Moffett Field, CA: NASA-Ames Research Center.

Billings, C. E., & Woods, D. D. (1994, April). *Concerns about adaptive automation in aviation systems.* Paper presented at the First Automation Technology and Human Performance Conference, Washington, D.C.

Boeing Commercial Airplane Group (1993). *Accident prevention strategies: Removing links in the accident chain: Commercial Jet Aircraft Accidents world wide operations 1982-1991* (Boeing Airplane Safety Engineering B-210B). Seattle, WA.

Boeing Commercial Airplane Group (1994). *Statistical summary of commercial jet aircraft accidents: Worldwide operations 1959-1993* (Boeing Airplane Safety Engineering B-210B). Seattle, WA.

Braune, R., & Fadden, D. M. (1987, October). *Flight deck automation today: Where do we go from here?* Paper presented at SAE Aerotech '87. Long Beach, CA.

Broadbent, D. E. (1971). *Decision and Stress.* London: Academic Press.

Bureau of Air Safety Investigation. (1993). *Near Collision at Sydney (Kingsford Smith) Airport, 12 August 1991* (BASI report B/916/3032). Civic Square, ACT, Australia: Transport and Communications.

Bylander, T. (1988). Diagnosis by integrating Model-Based reasoning with Knowledge-based reasoning. *OSU LAIR report 88-TB-DIAG.* Columbus, OH: The Ohio State University.

Byrnes, R. E., & Black, R. (1993). Developing and implementing CRM programs: The Delta experience. In: E. L. Wiener, B. G. Kanki, & R. L. Helmreich (Eds.), Cockpit *Resource Management.* San Diego, CA: Academic Press.

Caracena, R. L., Holle, R. L., & Doswell, C, III. (1989). *Microbursts: A handbook for visual identification.* Washington, DC.: National Oceanic and Atmospheric Administration.

Celio, J. C. (1990). *Controller perspective of AERA 2* (MITRE Corp. Report MP-88W00015, Rev. 1). McLean, VA.: MITRE Corporation.

Chappell, S. L., Billings, C. E., Scott, B. C., Tuttell, R. J., & Olson, M. C., & Kozon, T. E. (1988). *Pilot's use of a traffic-alert and collision avoidance system (T/CAS II) in simulated air carrier operations* (NASA Technical Memorandum 100094 (2 volumes)). Moffett Field, CA: NASA-Ames Research Center.

Cheaney, E. S., and C. E. Billings (1981): *Application of the Epidemiological Model in Studying Human Error in Aviation.* 1980 Aircraft Safety and Operating Problems Conference, NASA CP 2170.

Civil Aeronautics Board (1957). *Trans World Airlines Lockheed 1049A and United Air Lines Douglas DC-7, Grand Canyon, AZ, June 30, 1956.* (CAB Report no. SA-320). CAB, Washington, DC.

Civil Aeronautics Board (1959). *Pan American World Airways Boeing 707 over the Atlantic between London, England, and Gander, Newfoundland, February 3, 1959.* CAB, Washington, DC.

Civil Aviation Authority (UK) (1994): *Narrative report on B 757-200 incident at Manchester, England.* Occurrence no. 9402551G.

Clancey, W. J. (1983). The epistemology of a rule-based expert system—a framework for explanation. *Artificial Intelligence,* 20, 215-251.

Cooley, M. (1987). Human centred systems: An urgent problem for systems designers. *AI & Society,* 1, 37-46.

Cooper, G. (1994a, March). Euro Flow Control. *Aerospace,* 21(3), pp. 8- 11.

Cooper, G. (1994b, September): Seeing through the fog. *Aerospace* 21(9), pp 16-18.

Corker, K. M., & Reinhardt, T. (1990). *Procedural representation techniques applied to flight management computer systems: A software representation system* (BBN contract no. W288-386; BBN report ref. 5653). Cambridge, MA.: BBN Systems and Technologies, Inc.

Costley, J., Johnson, D., & Lawson, D. (1989, April). A comparison of cockpit communication B737-B757. *Proceedings of the Fifth International Symposium on Aviation Psychology* (pp. 413-418). Columbus, OH: The Ohio State University.

Curran, J. A. (1992). *Trends in Advanced Avionics.* Ames, IA: Iowa State University Press.

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.

Davis, R., & Hamscher, W. (1988). Model-based reasoning: Troubleshooting. In: H. E. Shrobe (Ed.) *Exploring Artificial Intelligence.* San Mateo, CA: Morgan Kaufman.

Del Balzo, J. M. (1992). Worldwide aviation after the year 2000: A new era begins. In G. M. Crook (Ed.), *Airports and Automation.* London: Thomas Telford..

Department of Trade and Industry (1973): *Trident G-ARPI. Report of the Public Inquiry into the Causes and Circumstances of the Accident near Staines on 18 June, 1972.* London: Her Majesty's Stationery Office, Civil Aviation Accident Report, April, 1973.

Director General of Armaments (France) (1994): Investigation Committee report on *A330 Accident in Toulouse on 30 June 1994*. Unpublished report. See also Sparaco, P., in *Aviation Week & Space Technology*, 7/11/94, pp. 26-27)

Dornheim, M. A. (1991, February 11). 737-Metro crash raises controller workload issues. *Aviation Week & Space Technology*, 134, p. 27. See also: L.A. Tower tapes show controller unaware of aircraft holding on runway. (1991, April 8) *Aviation Week & Space Technology*, 134, p. 61.

Douglas Aircraft Co. (1990). *Functional decomposition of the commercial flight domain for function allocation*. Final report to NASA-Langley Research Center, contract no. NAS1-18028.

Endsley, M. R. (1994). Situation awareness in dynamic human decision-making: Theory. In: R. D. Gilson, D. J. Garland, & J. M. Koonce (Eds.), *Situational awareness in complex systems*. Daytona Beach, FL: Embry-Riddle Aeronautical University Press.

Erzberger, H., & Nedell, W. (1988). *Design of automation tools for management of descent traffic*. NASA Technical Memorandum 101078. Moffett Field, CA: NASA-Ames Research Center.

Erzberger, H., & Nedell, W. (1989). *Design of automated system for management of arrival traffic* (NASA Technical Memorandum 102201). Moffett Field, CA: NASA-Ames Research Center.

Fadden, D. M. (1990). Aircraft automation challenges. In: *Abstracts of AIAA-NASA-FAA-HFS Symposium, Challenges in Aviation Human Factors: The National Plan*. Washington, DC.: American Institute of Aeronautics and Astronautics.

Fitts, P. M. (1951). *Human engineering for an effective air navigation and traffic control system*. Washington, D.C.: National Research Council.

Flight International (1990, October 31-November 6).Hard limits, soft options (Editorial), 138.

FSF (1982, January): *A safety appraisal of the Air Traffic Control system*. Report no. FSF-ATC 1142-1-82U. Arlington, VA, Flight Safety Foundation.

FSF (1994, December): Pinet, J., Enders, J.H.: *Human Factors in Aviation: A Consolidated Approach*. Arlington, VA: Flight Safety Digest.

Gilson, R.D., Garland, D.J., Koonce, J.M., eds. (1994): *Situational Awareness in Complex Systems*. Daytona Beach, FL, Embry-Riddle Aeronautical University Press.

Gorham, J. A. (1973, July). *Automatic flight control and navigation systems on the L-1011: capabilities and experiences*. Paper presented at the USSR/US Aeronautical Technology Symposium, Moscow, USSR.

Grunwald, A. J., Robertson J. B., & Hatfield J. J. (1980). *Evaluation of a computer-generated perspective tunnel display for flight path following* (NASA Technical Report 1736). Hampton, VA: NASA Langley Research Center.

Harwood, K., & Sanford, B. D. (1993). *Denver TMA assessment* (NASA Contractor Report 4554). Moffett Field, CA: NASA-Ames Research Center.

Hollnagel, E. (1993). *Reliability of cognition: Foundations of human reliability analysis*. London: Academic Press.

Honeywell Commercial Flight Systems Group (1990, September). *MD-11 Flight Management System Pilot's Guide* (PUB No. 28-3643-01-00). Phoenix, AZ.

Hopkin, V. D. (1994). Situational awareness in air traffic control. In: Gilson, R. D., Garland, D. J., Koonce, J. M. (Eds.), *Situational Awareness in Complex Systems*. Daytona Beach, FL.: Embry-Riddle Aeronautical University Press.

Hopkin, V. D. (1994, April). Human performance implications of air traffic control automation. In: M. Mouloua, & Parasuraman, R. (Eds.), *Human performance in automated systems: Current research and trends*. Hillsdale, N. J.: Erlbaum. (also Paper presented at the First Automation Technology and Human Performance Conference, Washington, D.C.)

Hopkins, H. (1990, October 24-30). Masterfully Digital (MD-) 11. *Flight International,* 138, pp.?

Hopkins, R. (1993, March 31-April 6). Backing up of approaches [Letter to the editor]. *Flight International,* p. 40.

Hughes, J.A., Randall, D., and Shapiro, D. (1992, November): *Faltering from Ethnography toward Design*. CSCW 92 Proceedings.

Hutchins, E. (1993, August). *An integrated Mode Management Display*. Paper presented at the NASA-Ames Mode meeting. Moffett Field, CA: NASA-Ames Research Center.

Hutchins, E., cited in AWST, 1995b, pp. 52-53.

IATA (1994, December): International Air Transport Association: *IATA Draft Requirements for Air Traffic Management in the Future Air Navigation System*. Montreal, International Air Transport Association, unpublished report.

Jordan, N. (1963). Allocation of functions between man and machines in automated systems. *Journal of Applied Psychology*, 47(3), 161-165.

Kelly, B. D., Graeber, R. C., & Fadden, D. M. (1992). *Applying crew-centered concepts to flight deck technology: The Boeing 777*. Paper presented at the Flight Safety Foundation 45th International Air Safety Seminar. Long Beach, CA.

Kerns, K. (1994, September): *Human Factors in ATC/Flight Deck Integration: Implications of Data Link Simulation Research.* McLean, VA: MITRE Corp. report MP 94W0000098.

Kinney, G. C., Spahn, J., & Amato, R. A. (1977). *The human element in air traffic control: Observations and analyses of the performance of controllers and supervisors in providing ATC separation services* (METREK Division of the MITRE Corporation., MTR-7655). McLean, VA.

Kraft, C. L., & Elworth, C. L. (1969, March-April). Night visual approaches. *Boeing Airliner*, pp. 2-4.

Laming, J. (1993, June 9-15). Who controls the aircraft? [Letter to the editor]. *Flight International,* p. 140.

Last, S., & Alder, M. (1991, September): *British Airways Airbus A320 Pilots' Autothrust Survey*. SP-885, SAE Aerospace Technology Conference, Long Beach, CA.

Lauber, J. K. (1989, March). *Remarks of John K. Lauber, member NTSB, before the Aero Club of Washington March Luncheon* (NTSB safety information pamphlet). Washington, D.C.: National Transportation Safety Board.

Lauber, J.K. (1993): *A Safety Culture Perspective.* Irving, TX, Flight Safety Foundation 38th Corporate Aviation Safety Seminar, April 14-16.

Lauber, J.K., Billings, C.E. Stevenson, J.E., Ruffell Smith, H.P., Cooper, G.E. (1976): *Simulation Studies of Air Transport Operational Problems.* Aircraft Safety and Operating Problems Conference, NASA SP-416, 1976.

Lauber, J. K., Bray, R. S., Harrison, R. L., Hemingway, J. C., & Scott, B. C. (1982). *An operational evaluation of head-up displays for civil transport operations: NASA/FAA Phase III final report* (NASA Technical Paper 1815). Moffett Field, CA: NASA-Ames Research center.

Lautmann, L. G., & Gallimore P. L. (1987, April-June). Control of the crew-caused accident: Results of a 12-operator survey, *Boeing Airliner,* Seattle: Boeing Commercial Airplane Company. Also in: Proceedings of the 40th Flight Safety Foundation International Air Safety Seminar (1987, October) Tokyo, Japan..

Layton, C., Smith, P.J., and McCoy, E. (1994): Design of a cooperative problem solving system for enroute flight planning: An empirical evaluation. *Human Factors* 36(1), 94-119.

Lee, L. (1992). *The day the phones stopped.* New York, NY: Donald I Fine, Inc.

Lenorovitz, J. M. (1990, June 25). Indian A320 crash probe data show crew improperly configured aircraft. *Aviation Week & Space Technology,* 132, pp. 84-85.

Mackworth, N. H. (1950). *Researches on the measurement of human performance* (Medical Research Council special report series, No. 268). London: Her Majesty's Stationary Office.

Malin, J. T., Schreckenghost, D. L., Woods, D. D., Potter, S. S., Johannesen, L., & Holloway, M. (1991). *Making intelligent systems team players: Case studies and design issues, Volume 2: Fault management system cases* (NASA Technical Memorandum 104738). Moffett Field, CA.: NASA-Ames Research Center.

Marthinson, H.F., Hagy, H.K. (1993, October-November): Boeing 737 Overruns: A Case History, Part I. *Air Line Pilot* 62(9), 27-31.

Marthinson, H.F., Hagy, H.K. (1993b, December): Boeing 737 Overruns: A Case History, Part II. *Air Line Pilot* 62(10), 25-27.

Maxim, H. S. (1908). *Artificial and natural flight.* New York: The MacMillan Co.

McMahon, J. (1978, July). Flight 1080. *Air Line Pilot.* Reprinted in: National Aeronautics and Space Administration (1983). *Restructurable Controls Conference* (NASA Conference Paper 2277). Washington, DC.

Mecham, M. (1994, May 9). Autopilot go-around key to CAL crash. *Aviation Week and Space Technology,* pp 31-32.

Mellone, V. J. (1993). *TCAS Incident reports analysis.* Paper presented at the second international TCAS Conference, FAA: Washington, D. C.

Ministere de l'equipment, des transports et du tourisme (1993, Novembre). *Rapport de la commission d'enquete sur l'accident survenu le 20 Janvier 1992 pres du Mont Sainte Odile (Bas Rhin) a l'airbus a320 immatricule F-GGED exploite par la compagnie Air Inter*, France.

Ministry of Planning, Housing, Transport and Maritime Affairs (1989). *Investigation Commission Final Report concerning the accident which occurred on June 26th 1988 at Mulhouse-Habsheim (68) to the Airbus A320, registered F-GFKC* (report 11/29/1989). Also extracted in *Aviation Week & Space Technology* 132: 6/4/90, p. 107; 6/18/90, p. 99; 6/25/90, p. 98; 133: 7/9/90, p. 60; 7/23/90, p. 90; 7/30/90, p. 90, 1990.

Ministry of Transport and Communications, Thailand (1993): *Lauda Air Boeing 767-300ER (accident at) Dan Chang Province, Thailand, 26 May 1991.*

Mohler, S. R., & Johnson, B. H. (1971). *Wiley Post, his Winnie Mae, and the world's first pressure suit.* Washington, D.C.: Smithsonian Institution Press.

Monan, W. P. (1986, March). *Readback related problems in ATC communications: the hearback problem* (NASA CR 177398). Mountain View, CA: Aviation Safety Reporting System Office.

Moray, N., Lee, J., & Hiskes, D. (1994). Why do people intervene in the control of automated systems? In: M. Mouloua, & R. Parasuraman (Eds.), *Human performance in automated systems: Current research and trends.* Hillsdale, N. J.: Erlbaum.

Moshansky, V. P. (1992). *Commission of Inquiry into the Air Ontario Accident at Dryden, Ontario* (Final Report (Volumes 1-4)). Ottawa, ON: Minister of Supply and Services, Canada.

Nagel, D.C. (1988). Human error in aviation operations. In: Wiener, E.L., & Nagel, D.C. (Eds.), *Human factors in aviation.* San Diego: Academic Press.

NASA Aviation Safety Reporting System (1976a). Incident report ACN 00026, Mountain View, CA: Aviation Safety Reporting System Office.

NASA Aviation Safety Reporting System (1976b). Incident report ACN 00362, Mountain View, CA: Aviation Safety Reporting System Office.

NASA Aviation Safety Reporting System (1986). Incident report ACN 59282, Mountain View, CA: Aviation Safety Reporting System Office.

NASA (1990). *Aviation Safety/Automation Program Plan* (NASA Information Sciences and Human Factors Division (unpublished document)), Washington, DC, National Aeronautics and Space Administration.

NASA (1991). *Advanced subsonic aircraft (capacity) initiative* (Information Sciences and Human Factors Division (unpubl. briefing document)). Washington, DC, National Aeronautics and Space Administration.

NTSB (1973). *Eastern Air Lines L-1011, Miami, FL, December 29, 1972.* (NTSB Report no. AAR-73-14). Washington, DC, National Transportation Safety Board.

NTSB (1974). *Delta Air Lines Douglas DC-9-31, Boston, MA, 7/31/73* (NTSB report no. AAR-74/03). Washington, DC, National Transportation Safety Board.

NTSB (1978a). *United Airlines Douglas DC-8 near Kaysville, UT, December 18, 1977.* (NTSB Report no. AAR-78-8). Washington, DC, National Transportation Safety Board.

NTSB (1978b). *National Airlines Boeing 727, Escambia Bay, Pensacola, FL, May 8, 1978.* (NTSB Report no. AAR-78-13). Washington, DC, National Transportation Safety Board.

NTSB (1979a): *United Airlines DC-8-61, Portland, OR, 12/28/78.* (NTSB Report no. AAR-79/07). Washington, DC, National Transportation Safety Board.

NTSB (1979b). *Swift Aire Lines Aerospatiale Nord 262, Marina Del Rey, CA, 3/10/79* (NTSB report no. AAR-79/13). Washington, DC, National Transportation Safety Board.

NTSB (1980). *Aeromexico DC-10-30 over Luxembourg, 11/11/79* (NTSB report no. AAR-80-10). Washington, D. C, National Transportation Safety Board.

NTSB (1981). *Aircraft Separation Incidents at Hartsfield Atlanta International Airport, Atlanta, GA, 10/7/80.* (NTSB report no. SIR-81-6). Washington, DC, National Transportation Safety Board.

NTSB (1982). *Air Florida B-737-222, Collision with 14th Street Bridge, near Washington National Airport, DC, 1/13/82* (NTSB report no. AAR-82-8). Washington, DC, National Transportation Safety Board.

NTSB (1984). *Scandinavian Airlines DC-10-30, J. F. Kennedy Airport, New York, 2/28/84* (NTSB report no. AAR-84-15). Washington, D. C, National Transportation Safety Board.

NTSB (1986). *China Airlines B-747-SP, 300 NM northwest of San Francisco, CA, 2/19/85* (NTSB report no. AAR-86/03).Washington, DC, National Transportation Safety Board.

NTSB (1986). *Delta Air Lines Lockheed L-1011-385-1, Dallas-Fort Worth Airport, TX, 8/2/85* (NTSB report no. AAR-86/05). Washington, DC, National Transportation Safety Board.

NTSB (1988a). *Delta Airlines B727-232, Dallas Fort Worth Airport, Texas, 8/31/88* (NTSB report no. AAR-89/04). Washington, DC, National Transportation Safety Board.

NTSB (1988b). *Northwest Airlines DC-9-82, Detroit Metro Wayne County Airport, Romulus, Michigan, 8/16/87* (NTSB report no. AAR-88/05). Washington, DC, National Transportation Safety Board.

NTSB (1991a). *Avianca, the Airline of Colombia, Boeing 707-321B, fuel exhaustion, Cove Neck, New York, Jan. 25, 1990.* (NTSB Report no AAR/91/04). Washington, DC, National Transportation Safety Board.

NTSB (1991b). *Northwest Airlines B-727 and DC-9, Detroit Metro Airport, Romulus, MI, 12/3/90* (NTSB Report no. AAR/91/05). Washington, DC, National Transportation Safety Board.

NTSB (1991c). *Runway Collision of US Air Boeing 737 and Skywest Fairchild Metroliner, Los Angeles, 2/1/91.* (NTSB Report no. AAR-91/08). Washington, DC, National Transportation Safety Board.

NTSB (1992a). Safety Recommendations A-92-31 through -35 (concerning *Evergreen International Airlines B747-100 upset at Nakina, Ontario, December 12, 1991.*) Washington, DC, National Transportation Safety Board, 14 May 1992. See also Aviation Occurrence Report no. A91H0014, Transportation Safety Board of Canada, *Flight Control System Malfunction.*

NTSB (1992b): *United Airlines Boeing 737 collision with terrain for undetermined reasons, Colorado Springs, CO.* (NTSB Report no. AAR-92/06). Washington, DC, National Transportation Safety Board.

NTSB (1994). Safety Recommendations A-94-164 through -166 (concerning *China Airlines Airbus A-300-600R accident at Nagoya, Japan, April 26, 1994*). Washington, DC, National Transportation Safety Board, 31 August 1994.

New York Times (1933, July 24).

Nolan, M. S. (1994). *Fundamentals of air traffic control.* Belmont, CA: Wadsworth Publishing Company.

Nordwall, B. D. (1993. March 8). Software problems delay ATC redesign 14 months. *Aviation Week & Space Technology*, p. 30.

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

Norman D. A. (1988). *Psychology of Everyday Things.* New York: Basic Books, Inc.

Norman, D. A. (1989, June). *The problem of automation: Inappropriate feedback and interaction, not "over-automation"*. Paper prepared for the discussion meeting, "Human Factors in High-Risk situations", the Royal Society (Great Britain). London, UK.

Ovenden, C. R. (1991). *Model-Based Reasoning applied to Cockpit Warning Systems* (Smiths Industries Aerospace and Defense Systems report). Cheltenham, UK.

Palmer, E. A., Mitchell C. M., & Govindaraj, T. (1990). *Human-centered automation in the cockpit: Some design tenets and related research projects.* Presented at the ACM SIGCHI Workshop on Computer-Human Interaction in Aerospace Systems, 1990. Washington, DC.

Pan American World Airways (1990, September). *Flight Check*, 68, p. 32.

Paulson, G. (1994). Global navigational satellite system for aviation, RAeS lecture (edited by B. Fitzsimons). *Aerospace*, 21(6), pp. 12-15.

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

Phillips, E.H. (1994a): ATR42/72 Review Focuses on Icing. *Aviation Week and Space Technology*, 141(20) November 14, p. 28.

Phillips, E.H. (1994b): NTSB Slates Hearing on Pittsburgh Crash. *Aviation Week and Space Technology*, 141(23) December 5, p. 28.

Phillips, E.H. (1994c): NTSB Links Detection-Delay Feature with DC-9 Crash. *Aviation Week and Space Technology*, 141(24) December 12/19, p. 30. See also *Aviation Week & Space Technology*, July 11, 1994, pp. 25-27)

Porter, R. F., & Loomis, J. P. (1981). *An investigation of reports of controlled flight toward terrain* (NASA Contractor Report 166230). Mountain View, CA: Aviation Safety Reporting System office.

Preble, C. (1987, July). Delta Air Lines officials baffled by series of unrelated mishaps. *Aviation Week & Space Technology*, 127, pp. 31-32..

President's Task Force on Crew Complement (1981, July). *Report of the President's task force on crew complement.* Washington, D. C.

Randle, R. J., Larsen, W. E., & Williams, D. H. (1980). *Some human factors issues in the development and evaluation of cockpit alerting and warning systems* (NASA Reference Publication 1055). Washington, D.C.: NASA.

Rasmussen, J. (1988). *Information processing and human-machine interaction: An approach to cognitive engineering.* New York, NY: North Holland.

Rauner, F., Rasmussen, L., & Corbett, J. M. (1988). The social shaping of technology and work: Human centred CIM systems. *AI & Society*, 2, 47-61.

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

Rodgers, M. D. & Nye, L. G. (1993). Factors associated with the severity of operational errors at air route traffic control centers. In: M. D. Rodgers (Ed.), *An examination of the operational error database for air route traffic control centers* (Office of Aviation Medicine, final report AM-93/22). Washington, D.C.: Department of Transportation/FAA.

Rogers, W. H. (1990). *Flight crew information requirements for fault management on a commercial flight deck.* NASA draft information requests task plan, Langley Research Center.

Roscoe, S. N. (1979). *Ground-referenced visual orientation with imaging displays: Final report* (Technical Report Eng. Psy-79-4/AFOSR-79-4). Urbana-Champaign, IL.: University of Illinois.

Rose, R. M., Jenkins, C. D., & Hurst, M. W. (1978). *Air traffic controller health change study* (report FAA-AM-78-39). Washington, DC: FAA Office of Aviation Medicine.

Roth, E. M., Bennett, K. B., & Woods, D. D. (1987). Human interaction with an "intelligent" machine. *Int. J. Man-Machine Studies*, 27, 479-525.

Rouse, W. B. (1980). *Systems engineering models of human-machine interaction.* New York: North Holland.

Rouse, W. B. (1988). Adaptive aiding for human/computer control. *Human Factors*, 30(4), 431-443.

Rouse, W. B. (1991). *Design for success.* New York: John Wiley & Sons.

Rouse, W. B., & Rouse, S. H. (1983). *A framework for research on adaptive decision aids* (Technical report AFAMRL-TR-83-082). Wright-Patterson Air Force Base, OH: Air Force Aerospace Medical Research Laboratory.

Rouse, W. B., Geddes, N. D., & Curry R. E. (1987). An architecture for intelligent interfaces: Outline for an approach supporting operators of complex systems. *Human Computer Interaction*, 3(2), pp. 87-122.

Rudisill, M. (1994). Flight crew experience with automation technologies on commercial transport flight decks. In: M. Mouloua, & Parasuraman, R. (Eds.), *Human performance in automated systems: Current research and trends.* Hillsdale, N. J.: Erlbaum.

Ruffell Smith, H. P. (1974, May). Pilots' activities immediately preceding a fatal accident. *Proceedings of the Annual Scientific Meeting, Aerospace Medical Association* 1984.Washington, DC.

Ruffell Smith, H. P. (1979). *A simulator study of the interaction of pilot workload with errors, vigilance and decisions* (NASA Technical Memorandum 78482). Moffett Field, CA: NASA-Ames Research Center.

Sanford, B. D., Harwood, K., Nowlin, S., Bergeron, H., Heinrichs, H., Wells, G., & Hart, M. (1993, October). Center/TRACON automation system: Development and evaluation in the field. *Proceedings of the Air Traffic Control Association Conference,* Nashville, TN.

Sarter, N.B. (1994): *"Strong, Silent, and Out of the Loop": Properties of advanced cockpit automation and their impact on human-automation interaction.* Dissertation, unpublished, The Ohio State University, Columbus, Ohio.

Sarter, N. B., & Woods, D. D. (1991). Situation awareness: A critical but ill-defined phenomenon. *International Journal of Aviation Psychology,* 1(1), 45-57.

Sarter, N. B., & Woods, D. D. (1992) Pilot interaction with cockpit automation: Operational experiences with the flight management system. *International Journal of Aviation Psychology,* 2, 303-321.

Sarter, N. B., & Woods, D. D. (1992, October). Mode Error in Supervisory Control of Automated Systems. In: *Proceedings of the Human Factors Society 36th annual meeting.* Atlanta, GA.

Sarter, N. B. & Woods, D. D. (1994, April). Decomposing Automation: Autonomy, Authority, Observability and Perceived Animacy. In: M. Mouloua, & Parasuraman, R. (Eds.), *Human performance in automated systems: Current research and trends.* Hillsdale, N. J.: Erlbaum.

Schroeder, D. J. (1982, October). The loss of prescribed separation between aircraft: How does it occur? *Proceedings of the Behavioral Objectives in Aviation Automated Systems Symposium,* P-114, (pp. 257-269). Society of Automotive Engineers.

Schroeder, D. J., & Nye, L. G. (1993). An examination of the workload conditions associated with operational errors/deviations at air route traffic control centers. In: M. D. Rogers (Ed.), *An examination of the operational error database for air route traffic control centers.* Office of Aviation Medicine, final report AM-93/22. Washington, D.C.: Department of Transportation/FAA.

Scott, B., Goka, T., & Gates, D (1987, October). *Design, development and operational evaluation of an MLS/RNAV control display unit.* Paper presented at the Tenth IEEE/AIAA Digital Avionics Systems Conference. Los Angeles, CA. See also: Federal Aviation Administration (1987). *Introduction to MLS.* Washington, DC.

Sheridan, T. B. (1984). Supervisory control of remote manipulators, vehicles and dynamic processes. *Advances in Man-Machine systems research,* 1.

Sheridan, T. B. (1987). Supervisory control. In: I. Salvendy (Ed.), *Handbook of human factors.* New York, NY: John Wiley and Sons.

Sheridan, T. B. (1988). Task allocation and supervisory control. In: M. Helander, (Ed), *Handbook of Human-Computer Interaction.* North-Holland: Elsevier Science Publishers, BV.

Shontz, W. D., Records, R. M., & Antonelli, D. R. (1992). *Flight Deck Engine Advisor: Final Report*. Boeing Commercial Airplane Group. Flight Deck Research, Seattle WA. NASA CR NAS1-18027.

Smith, P. J., McCoy, E., Layton, C., & Bihari, T. (1993). *Design concepts for the development of cooperative problem-solving systems* (CSEL paper). Columbus, OH.: The Ohio State University.

Stein, K. J. (1985, October 3). Human factors analyzed in 007 navigation error. *Aviation. Week & Space Technology*, 119, p. 165. (Also see relevant navigation routes in Aviat. Week & Space Technol. 119: 9/12/83, 18-23.)

Stein, K. J. (1986, December 1). Complementary displays could provide panoramic, detailed battle area views. *Aviation Week & Space Technology*, 125, pp. 40-44.

Stout, C. L., & Stephens, W. A. (1975, November). *Results of simulator experimentation for approach and landing safety*. Paper presented at the International Air Transport Association 20th Technical Conference "Safety in Flight Operations". Istanbul, Turkey.

Taplin, H. J. (1969). "George": An experiment with a mechanical autopilot. *Journal of the American Aviation Historical Society*, 4(4). 234-235.

Tarrell, R. J. (1985). *Non-airborne conflicts: the causes and effects of runway transgressions* (NASA Contractor Report 177372). Mountain View, CA: Aviation Safety Reporting System Office.

The Sperry Gyroscope Co. (1927). *The Sperry automatic pilot*. Brooklyn, NY: The Sperry Gyroscope Company.

Tobias, L. & Scoggins, J. L. (1986, June). Time-based traffic management using expert systems. In: *Proceedings of the American Control Conference* (pp. 693-700). Seattle WA.

Tolchin, M. (1994, April 14). *F.A.A. is threatening to cancel new air traffic system*. New York Times.

Uchtdorf, D., & Heldt, P. (1989, April). *Flight crew info; special issue: Survey on cockpit systems B737-200 and A310-200, 1986* (Lufthansa Flight operations division publication). Frankfurt, Germany: Lufthansa German Airlines.

Vortac, O.U., Manning, C.A. (1994): *Automation and Cognition in Air Traffic Control: An Empirical Investigation*. Washington, FAA Report DOT/FAA/AM-94/3.

Wiener, E. L. (1985a). *Human factors of cockpit automation: A field study of flight crew transition* (NASA Contractor report 177333). Moffett Field, CA: NASA-Ames Research Center.

Wiener, E. L. (1985b, October). *Cockpit automation: In need of a philosophy*. Paper presented at the Aerospace Technology Conference. Long Beach, CA.

Wiener, E. L. (1987). Fallible humans and vulnerable systems: lessons learned from aviation. In: J. A Wise, & A. Debons, (Eds), *Information systems: Failure analysis* (NATO ASI Series, Vol. F-32). Berlin: Springer-Verlag.

Wiener, E. L. (1989). *Human factors of advanced technology (Glass Cockpit) transport aircraft* (NASA Contractor Report 177528). Moffett Field, CA: NASA-Ames Research Center.

Wiener, E. L. (1993). *Intervention strategies for the management of human error* (NASA Contractor Report 4547. Moffett Field, CA: NASA-Ames Research Center.

Wiener, E. L., & Curry, R. E. (1980). *Flight-deck automation: Promises and problems* (NASA Technical Memorandum 81206). Moffett Field, CA: NASA-Ames Research Center.

Wilkinson, S. (1994): The November Oscar Incident. *Air & Space*, February/March, 1994, pp. 81-87.

Woods, D. D. (1984). Visual momentum: A concept to improve the cognitive coupling of person and computer. *International Journal of Man-Machine Studies*, 21, 229-244.

Woods, D. D. (1993a). Towards a theoretical base for representation design in the computer medium: Ecological perception and aiding human cognition. In: J. Flach, P. Hancock, J. Caird, and K. Vincente (Eds.),. *The Ecology of Human-Machine Systems*. Hillsdale, N. J.: Erlbaum.

Woods, D. D. (1993b). *Cognitive systems in context* (Cognitive Systems Engineering Laboratory Paper). Columbus, OH: The Ohio State University.

Woods, D. D. (1993c). *Cognitive Activities and Aiding Strategies in Dynamic Fault Management* (Cognitive Systems Engineering Laboratory Paper). Columbus, OH: The Ohio State University.

Woods, D. D. (1994a). *Visualizing Function: The Theory and Practice of Representation Design in the Computer Medium* (Cognitive Systems Engineering Laboratory book in progress). Columbus, OH: The Ohio State University.

Woods, D. D. (1994b, in press) *Decomposing Automation: Apparent simplicity, real complexity*. Proceedings of the 1st Automation technology and human performance conference. Hillsdale, NJ: Erlbaum Associates.

Woods, D. D., Johannesen, L. J., Cook, R. I., & Sarter, N. B. (1994). *Behind Human Error: Cognitive Systems, Computers and Hindsight*. State-of-the-art report for CSERIAC, Dayton, OH.

Index

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	February 1996	Technical Memorandum

4. TITLE AND SUBTITLE

Human-Centered Aviation Automation: Principles and Guidelines

5. FUNDING NUMBERS

NAG2-810

6. AUTHOR(S)

Charles E. Billings

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Ames Research Center
Moffett Field, CA 94035-1000

8. PERFORMING ORGANIZATION REPORT NUMBER

A-961056

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 TM-110381

11. SUPPLEMENTARY NOTES

Point of Contact: Charles E. Billings, Ames Research Center, MS 262-4, Moffett Field, CA 94035-1000; (415) 604-5320

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified — Unlimited
Subject Category 06

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This document presents principles and guidelines for human-centered automation in aircraft and in the aviation system. Drawing upon operational experience with highly automated aircraft, it describes classes of problems that have occurred in these vehicles, the effects of advanced automation on the human operators of the aviation system, and ways in which these problems may be avoided in the design of future aircraft and air traffic management automation.

Many incidents and a few serious accidents suggest that these problems are related to automation complexity, autonomy, coupling, and opacity, or inadequate feedback to operators. An automation philosophy that emphasizes improved communication, coordination and cooperation between the human and machine elements of this complex, distributed system is required to improve the safety and efficiency of aviation operations in the future.

14. SUBJECT TERMS

Aircraft automation, Human-centered automation, Advanced aircraft, Human factors

15. NUMBER OF PAGES

202

16. PRICE CODE

A10

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified		