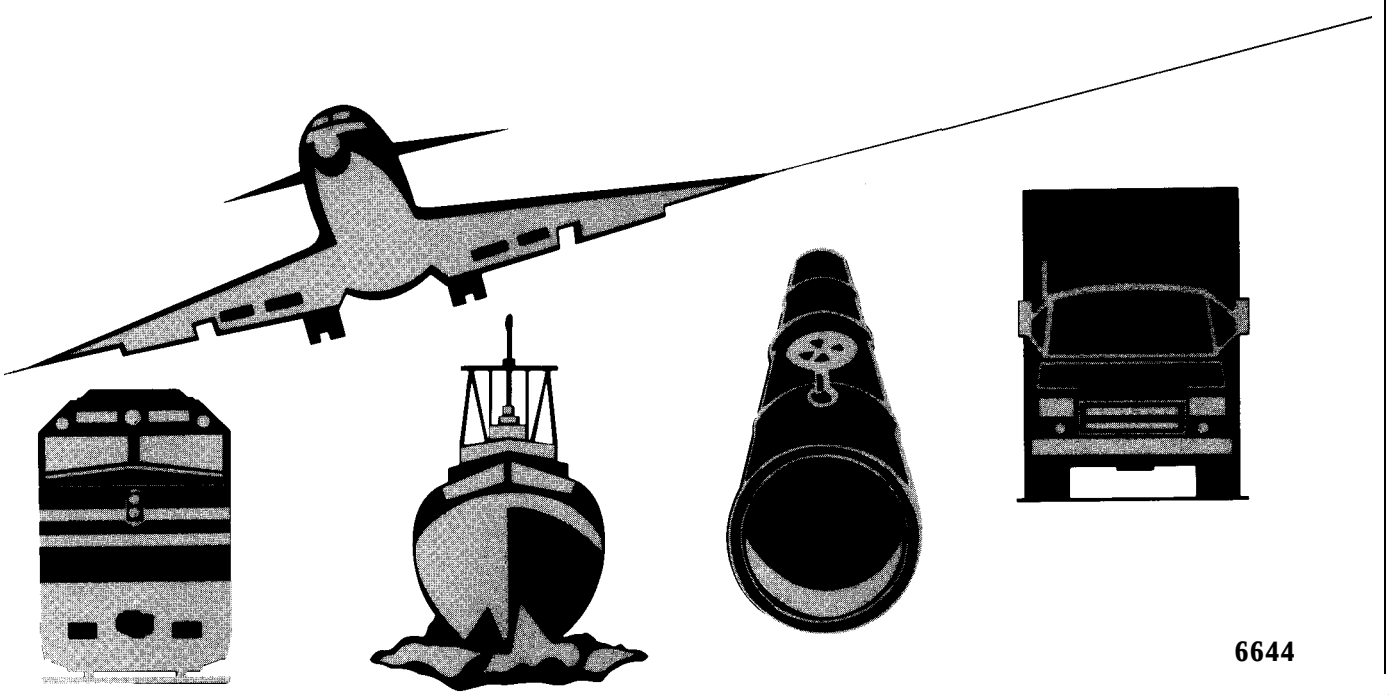
PB96-917001
NTSB/SIR-96/01

NATIONAL TRANSPORTATION SAFETY BOARD

WASHINGTON, D.C. 20594

SPECIAL INVESTIGATION REPORT

AIR TRAFFIC CONTROL EQUIPMENT OUTAGES



6644

The National Transportation Safety Board is an independent Federal agency dedicated to promoting aviation, railroad, highway, marine, pipeline, and hazardous materials safety. Established in 1967, the agency is mandated by Congress through the Independent Safety Board Act of 1974 to investigate transportation accidents, determine the probable causes of the accidents, issue safety recommendations, study transportation safety issues, and evaluate the safety effectiveness of government agencies involved in transportation. The Safety Board makes public its actions and decisions through accident reports, safety studies, special investigation reports, safety recommendations, and statistical reviews.

Information about available publications may be obtained by contacting:

National Transportation Safety Board
Public Inquiries Section, RE-51
490 L'Enfant Plaza, S.W.
Washington, D.C. 20594
(202)382-6735
(800)877-6799

Safety Board publications may be purchased, by individual copy or by subscription, from:

National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161
(703)487-4600

NATIONAL TRANSPORTATION SAFETY BOARD

WASHINGTON, D.C. 20594

SPECIAL INVESTIGATION REPORT

SPECIAL INVESTIGATION REPORT

AIR TRAFFIC CONTROL EQUIPMENT OUTAGES

Adopted: January 23, 1996
Notation 6644

Abstract: This report examines the outages involving computer and related equipment in certain air route traffic control centers (ARTCCs). The safety issues discussed in the report include the increasing frequency of outages involving the aging IBM 9020E computer equipment; other equipment outages involving power systems and communications equipment unrelated to the aging IBM computer systems; lack of controller proficiency with one of the backup computer systems; the increased likelihood that some ARTCC computer systems will be operated with compromised redundancy; and the adverse effect of the retirement of highly skilled airways facilities technicians on the Federal Aviation Administration's (FAA) ability to maintain and repair many air traffic control systems. Safety recommendations concerning these issues were made to the FAA.

this page intentionally left blank

Contents

this page intentionally left blank

Abbreviations

This is a list of abbreviations used in this report, followed by the number of the page on which they are explained, if explanation is needed.

AAS: Advanced Automation System, vi

ACEPS: ARTCC critical and essential power system, 25

AF: airways facilities, 3

AMIC: Area Manager In Charge, 17

ARTCC: air route traffic control center, 4

ATC: air traffic control, vi

BUEC: backup emergency communications, 21

CDC: computer display channel, 7

CE: computing elements, 7

DARC: direct access radar channel, 9

DCC: display channel complex, 7

DCCR: DCC Rehost, 24

DG: display generator, 7

DSR: Display System Replacement, 24

DYSIM: dynamic simulation, 19

FAA: Federal Aviation Administration, vi

FPL: full performance level, 4

IOCE: input/output control elements, 7

MSAW: minimum safe altitude warning, 9

NAS: National Airspace System, 4

NOM: NAS Operations Manager, 17

PAMRI: peripheral adapter module replacement item, 7

PVD: plan view displays, 7

RKM: radar keyboard multiplexer, 7

TRACON: terminal radar approach control, 4

VSCS: voice switching and control system, 25

Executive Summary

In the summer of 1995, the National Transportation Safety Board was asked to conduct a special investigation into the ongoing computer and related equipment outages experienced by the Federal Aviation Administration (FAA) en route air traffic control (ATC) system. The special investigation focused on the problems that had become visible to the public at the five air route traffic control centers (ARTCCs) with the oldest controller display computer systems. A team of investigators conducted interviews and research at these five ARTCCs and at one terminal radar approach control facility.

This report presents a basic overview of the ATC system and ARTCC computer systems, and discusses the maintenance and repair of aging display computers and the problem of outages involving these and other systems. The report also discusses a few ongoing FAA modernization programs to address these problems. Because of the limited scope (in time and resources) of its investigation, the Safety Board made no attempt to analyze the management of past modernization efforts, nor did the Board attempt to analyze scheduling or financial matters pertaining to current modernization projects.

The centerpiece of the FAA's efforts to modernize the ATC system was the Advanced Automation System (AAS), which was initiated in the mid-1980s and entirely restructured in June 1994 after a series of schedule slips and cost overruns. The FAA's current modernization efforts include portions of the restructured AAS. A computer and controller workstation modernization effort that was part of the AAS was scaled back and renamed the Display System Replacement (DSR). Another portion of the AAS, the voice switching and control system, was retained to enhance communications capabilities in en route facilities. The FAA also added a project called the Display Channel Complex Rehost, which will replace the older of the FAA's two display computer systems (the IBM 9020E) with off-the-shelf hardware until the DSR is implemented. The report discusses these projects as well as the ARTCC Critical and Essential Power System program, which is an upgrade project for facility electrical power systems.

The report concludes that while the en route ATC system is safe, the equipment failures examined have had a detrimental effect on the efficiency of air traffic movement. The report also concludes that the FAA's plans to upgrade the computer systems will be beneficial.

Safety issues in this report include:

- The increasing frequency of outages involving the aging IBM 9020E display channel complex equipment;
- Other recent equipment outages involving power systems and communications equipment;
- Lack of controller proficiency with the direct access radar channel (DARC)/Standalone mode of the backup computer system;
- The increased likelihood that some ARTCC computer systems will be operated with compromised redundancy, which increases the risk of outages; and

- The adverse effect of the retirement of highly skilled airways facilities technicians on the FAA's ability to maintain and repair many air traffic control systems.

The Safety Board issued safety recommendations concerning these issues to the FAA.

this page intentionally left blank

NATIONAL TRANSPORTATION SAFETY BOARD
WASHINGTON, D.C. 20594

SPECIAL INVESTIGATION REPORT

AIR TRAFFIC CONTROL EQUIPMENT OUTAGES

Introduction

On May 17, 1995, at 0805 central daylight time, the Federal Aviation Administration (FAA) air route traffic control center (ARTCC)[1] at Aurora, Illinois, experienced a major computer outage.[2] After preliminary attempts to restore the system were unsuccessful, a national ground stop of all departures destined for Chicago Center's airspace was initiated. The center had approximately 450 aircraft under its control at the time. Air traffic controllers continued to separate traffic using a backup system known as the direct access radar channel (DARC). Because certain computer features available under the primary system are not available to controllers using DARC, an ARTCC operating under DARC has a reduced traffic handling capacity. At 0910 the primary computer system was restored, and by about 0930 all traffic operations returned to normal.

No controllers reported a loss of standard aircraft separation, although a number of controllers said that the backup operation was "potentially" unsafe. The level of concern expressed by the controllers was dependent on the amount of traffic in and the complexity of the sector that they were working at the time of the outage. All controllers and the area manager indicated that they were very lucky that the outage occurred when it did. The center had just completed handling a large volume of traffic that slowed at 0800, and the next rush, which would normally not occur until about 0900, had been prevented by the national ground stop. Also, the fact that good weather prevailed on the morning of the outage was fortunate.

Because of this outage and similar recent outages[3] that have occurred in other air traffic control (ATC) facilities, the Safety Board began a special investigation of equipment outages within selected ARTCCs in the United States. During its history, the Safety Board has issued more than 100 safety recommendations and has conducted other special investigations concerning the ATC system. For example, the Board conducted such an investigation after several aircraft separation incidents occurred in rapid succession on October 7, 1980, near Hartsfield Airport in Atlanta, Georgia.[4] In 1981, in the wake of the dismissal of more than

[1] An ARTCC is often referred to as a "center" or an "en route facility."
[2] Generally speaking, a "failure" is said to have occurred when any element in a system becomes off line unexpectedly, but the system remains operational. If the entire system becomes unavailable, the failure is known as an "outage."
[3] See Appendix A for a list of recent outages.
[4] For more detailed information, read Special Investigation Report--"Aircraft Separation Incidents at Hartsfield Atlanta International Airport, Atlanta, Georgia, October 7, 1980" (NTSB-SIR-81-6).

11,000 striking Professional Air Traffic Controllers Organization controllers, the Board conducted an overall safety assessment of the ATC system.[5]

In 1987, the Safety Board investigated the following incident, which illustrates the potential dangers of ATC computer outages: On June 2, 1987, a near-midair collision occurred involving a Northwest Airlines Boeing 727 and a U.S. Air Force EC-135.[6] The incident occurred about 60 nautical miles east of Casper, Wyoming, at flight level 330. Both aircraft were operating in visual meteorological conditions on instrument flight rules flight plans being worked by controllers at Sector 32 of the Denver ARTCC. The traffic was described by controllers at that sector as heavy and extremely complex at the time that the incident occurred. Because of recurring computer hardware trouble, the facility had been using DARC often for several days. The crew of the military aircraft misunderstood an ambiguous control instruction issued by the developmental radar controller who was working the sector while receiving on-the-job training under the supervision of an experienced controller.

A conflict developed while the controllers turned their attention to other aircraft in their sector. The conflict alert feature was unavailable because the facility was using DARC. Although the controllers noticed the loss of separation and issued vectors to both aircraft, the pilot of the 727 reported that a collision would have occurred had he not noticed the other aircraft and taken evasive action. In his report of the incident, he said that the two aircraft passed no more than 1,000 feet from each other at the same altitude. The Safety Board determined that the partial failure of the en route radar system, excessive controller workload, and the inoperative conflict alert feature were factors in the incident.

The Safety Board's Investigation

The Safety Board conducted this special investigation to examine outages involving computer and related equipment in certain ARTCCs. Information about previous ATC modernization projects is presented in this report only to provide a framework for understanding current equipment troubles and staffing difficulties. Because of the limited scope (in time and resources) of this investigation, the Safety Board made no attempt to analyze the management of these projects, nor did the Board attempt to analyze scheduling or financial matters pertaining to current modernization efforts.

The FAA's ATC modernization efforts were begun in 1981. The nucleus of these efforts became the Advanced Automation System (AAS), which would have completely replaced existing ATC computer systems and controller workstations. However, after a series of schedule slips and cost overruns, the AAS was completely restructured in 1994. Because the FAA had been expecting the AAS to replace existing systems entirely, the FAA effectively shrank its capability to maintain and repair equipment, which has created a situation in which the number of qualified technicians is dwindling as the reliability of the aging equipment is deteriorating.

[5] For more detailed information, read Special Investigation Report--"Air Traffic Control System" (NTSB-SIR-81-7).
[6] For more detailed information, see Brief of Incident DEN87IA145.

This special investigation focused on the five en route facilities that rely on the older computer systems (Washington, Fort Worth, Cleveland, New York, and Chicago Centers). Of the 20 en route centers that operate in the contiguous United States, these five centers operate with the IBM 9020E computer display channel complex, which is more than 30 years old. The remaining 15 centers operate with the Raytheon 760 computer display channel system, which is more than 25 years old.

Also as part of its investigation, the Safety Board conducted a series of interviews with more than two dozen ARTCC managers and over 50 controllers in these facilities. Airways facilities (AF) staff in each of these centers gave Safety Board investigators detailed, technical tours. The Safety Board also interviewed staff from Loral Federal Systems, Inc., and BDM Federal, Inc., contractors for the FAA. FAA headquarters and Technical Center staff members briefed Safety Board investigators, and finally, Safety Board investigators visited a smaller ATC facility at the Edwards Air Force Base in California, the High Desert terminal radar approach control (TRACON) facility, which is using one of the most modern computer complexes in the ATC system.

As a result of its investigation, the Safety Board confirmed three basic, recurring problems affecting en route facilities:

(1) The well-publicized age of the equipment, particularly the IBM 9020E computer and some related components, contributes to the present difficulties. It is a difficult-to-maintain, old system with brittle wiring, thousands of difficult-to-repair special circuit boards, and a nearly total lack of direct manufacturer support.

(2) Facility backup power relay systems are also failing at an increasing rate. This appears to be a more important problem than 9020E failures, because it affects all electrically powered systems in a facility.

(3) Communication links, both radio communications to aircraft and land-line communications between ATC facilities, are also experiencing problems at a rate that concerns both the Safety Board and the FAA.

The following sections of this report provide an overview of the ATC system, with special emphasis on the en route environment. A discussion of each of the three recurring problems mentioned above follows. Finally, there is a discussion of the FAA's efforts to address the problems, and a discussion of the use of new technology at the High Desert TRACON facility and the potential it offers for the future.

System Overview

The ATC system comprises a complex network of highly trained personnel and sophisticated equipment that is designed to facilitate "...the safe, orderly, and expeditious flow of

air traffic..." through the National Airspace System (NAS).[7] Air traffic controllers provide a variety of services to aircraft from many different kinds of facilities located throughout the country. For example, ground and local controllers at airports direct ground movements of aircraft and provide takeoff and landing clearances to departing and arriving aircraft. Controllers in TRACON facilities, which are usually located at or near large airports, manage low-altitude arriving and departing airborne traffic operating near a terminal area. TRACONs also handle low-altitude traffic and traffic transitioning to or from the high-altitude en route air traffic system. Aircraft at higher altitudes en route from one terminal area to another are usually handled by en route controllers at ARTCCs.

An overriding responsibility placed upon all air traffic controllers is maintaining separation between aircraft operating in the system. At any moment, any given controller in the system has a certain number of aircraft under his or her control. Although only the pilots have physical control of these aircraft, the pilots share certain safety responsibilities with the air traffic controller. Using radar and other systems, the controller tracks aircraft through his or her assigned airspace segment (sector). The controller is required to ensure that aircraft under his or her control make efficient progress toward their destinations while operating within legal separation standards, which are defined in FAA Orders. Controllers use ground-to-air radio to deliver instructions to the pilots of aircraft under their control to ensure that these separation standards are maintained. As aircraft progress through the airspace, they cross from sector to sector, passing from one controller to the next. This process, called a handoff, is coordinated between the two controllers and involves a radio frequency change on the part of the pilots.[8]

Air traffic controllers at each facility are supported by a number of specialists such as meteorologists, traffic management specialists, and AF technicians who maintain and repair the equipment infrastructure of the ATC system. In addition to the display and control consoles used by controllers, this infrastructure includes computer systems of varying vintages, complex voice and data switching equipment, radio and microwave transmission systems, local and remote-located radio and radar systems, as well as environmental and electric power conditioning and backup systems, which are required by the equipment.

Controllers and AF technicians alike are highly trained and specialized. The typical new controller completes an initial training program at the FAA ATC academy in Oklahoma City, Oklahoma, before being assigned to a facility. On-the-job training of the "developmental" controller continues at the facility until he or she reaches "full performance level" (FPL) in a given specialty.[9] It may take 5 years or more for a controller to reach FPL. AF technicians

[7] Title 14 Code of Federal Regulations Section 1.1.

[8] Handoffs may be coordinated manually between controllers speaking over telephone connections, but in the en route environment handoffs are often accomplished using an automated handoff feature. This greatly reduces controller workload because a proposed handoff target is "flashed" to the adjacent controller, who can accept it with a simple keyboard entry.

[9] In the en route environment, a "specialty" is a set of sectors in a geographic area; thus, an FPL controller is one who is fully certified for each sector in a specialty. Developmental controllers may be certified on some of the sectors within the specialty. Developmentals are permitted to work independently at any radar position (sector) for which they hold certification.

complete a similar regimen of classroom and apprenticeship training. Many AF specialties also require a number of years of training. Just as controllers must be licensed by the FAA to control air traffic, certain ATC systems may only be maintained or repaired by FAA-certified technicians. It can take a new technician several years to earn this certification.

Along with the 20 ARTCCs that handle en route traffic in the contiguous United States, other en route facilities are located in Alaska, Hawaii, Guam, and Puerto Rico. The airspace jurisdiction of each of these facilities may encompass more than 100,000 square miles. Although staffing requirements are decidedly lighter at night, during peak hours more than 100 controllers may be on duty controlling traffic at an ARTCC. Until recently, AF technicians were also on duty around the clock to maintain and repair the system as needed. Currently, unstaffed AF shifts exist at several centers. Table 1 lists the locations of the contiguous U.S. ARTCCs, and Figure 1 is a map of these 20 facilities, showing their approximate geographic coverage areas.

Table 1: Names and locations of the 20 ARTCCs in the contiguous United States. Asterisks indicate facilities with IBM 9020E computers.

Albuquerque (Albuquerque, NM)	Kansas City (Olathe, KS)
Atlanta (Hampton, GA)	Los Angeles (Palmdale, CA)
Boston (Nashua, NH)	Memphis (Memphis, TN)
Chicago (Aurora, IL)*	Miami (Miami, FL)
Cleveland (Oberlin, OH)*	Minneapolis (Farmington, MN)
Denver (Longmont, CO)	New York (Ronkonkoma, NY)*
Fort Worth (Euless, TX)*	Oakland (Fremont, CA)
Houston (Houston, TX)	Salt Lake City (Salt Lake City, UT)
Indianapolis (Indianapolis, IN)	Seattle (Auburn, WA)
Jacksonville (Hilliard, FL)	Washington, D.C. (Leesburg, VA)*

ARTCC Computer Systems

Each ARTCC is equipped with a computer system that uses three main computers to drive controller workstations. Two of the computers (the Host computer and the display computer) comprise the primary system, which is used during normal operations, and the third is the backup (DARC). These computers are used to combine radar and flight plan data to present each controller with a dynamic display of relevant aircraft targets. The system correlates each of these targets with a moving three-line data block that displays flight information, such as the aircraft call sign, altitude, and ground speed. Redundant elements throughout the system serve to enhance its overall reliability.

Figure 1: Locations of the 20 continental air route traffic control centers and their approximate geographical coverage areas.

Figure 2 presents a block diagram that shows the interrelationships among the three main computers and other selected components used in the en route environment. Radar and flight plan information from a variety of sources enter the system through the peripheral adapter module replacement item (PAMRI). The PAMRI combines all of this information and sends it concurrently to the Host and DARC computers.

Installed in 1988, the Host is a dual-redundant IBM 3083.[10] The Host computer correlates radar data with flight plan data, which are continually updated and processed as aircraft progress through the airspace system.[11] These data are sent to the display computer and processed and buffered for display. The Host computer also prints paper flight progress strips at each sector about 45 minutes before aircraft are expected to enter that sector.

Depending on the facility, the display computer is either an IBM display channel complex (DCC) or a Raytheon 760 9020E computer display channel (CDC). Both the CDC and DCC display computers (and associated components) serve as a video processor and keyboard buffer for the main radar consoles known as plan view displays (PVD).[12] PVDs at all facilities are interfaced to the display computer (CDC or DCC) through a display generator (DG). A radar keyboard multiplexer (RKM) interfaces controller keyboards to the display computer.[13] Because the IBM 9020E can support more PVDs than the typical Raytheon 760 installation, it was installed at the five DCC facilities, which tend to have greater traffic densities than the CDC sites.

The typical IBM 9020E DCC system comprises four critical subsystems. A failure of any of these subsystems will cause a DCC outage. To enhance reliability, each subsystem has redundant elements. For example, each installation has two redundant input/output control elements (IOCE) that are used to communicate with the Host. If either one of these elements fails, the system is designed to continue functioning as long as the other remains operational. The system also contains three computing elements (CEs), one of which is redundant. The system is designed to function as long as two CEs are available. Each of these (and other) elements is located in its own large cabinet containing thousands of small circuit cards connected by aging, brittle wiring bundles. Each element has its own power supply unit. These components are accessed by opening a large cabinet door called a gate. Because of the age and frailty of the equipment, merely opening this gate can dislodge a circuit card or break a wiring bundle. A failure of any one of these cards or bundles can take an element off line, and lead to many hours of complex troubleshooting, which detracts from the substantial preventive maintenance tasks required by the equipment. As long as the failed element is redundant, the

[10] The term “dual redundant” means that two identical processors are available to drive the system, but the system can function with only one of these processors. Redundancy such as this is used to enhance the reliability of a system.

[11] Primary radar (skin paint) data are augmented with secondary radar data from airborne transponders (beacons). The secondary data include a beacon code and aircraft altitude. The beacon code is used to correlate aircraft target altitude, range, and bearing with a stored flight plan, if any.

[12] The PVD is a large cathode ray tube display device commonly termed a radarscope.

[13] Actually, multiple redundant RKMs and DGs are provided to enhance reliability. Three RKMs are installed in a typical ARTCC, two of which are required to drive radar position keyboards. Because each DG can drive six PVDs, a typical ARTCC installation includes 10 on-line DGs, plus two spares.

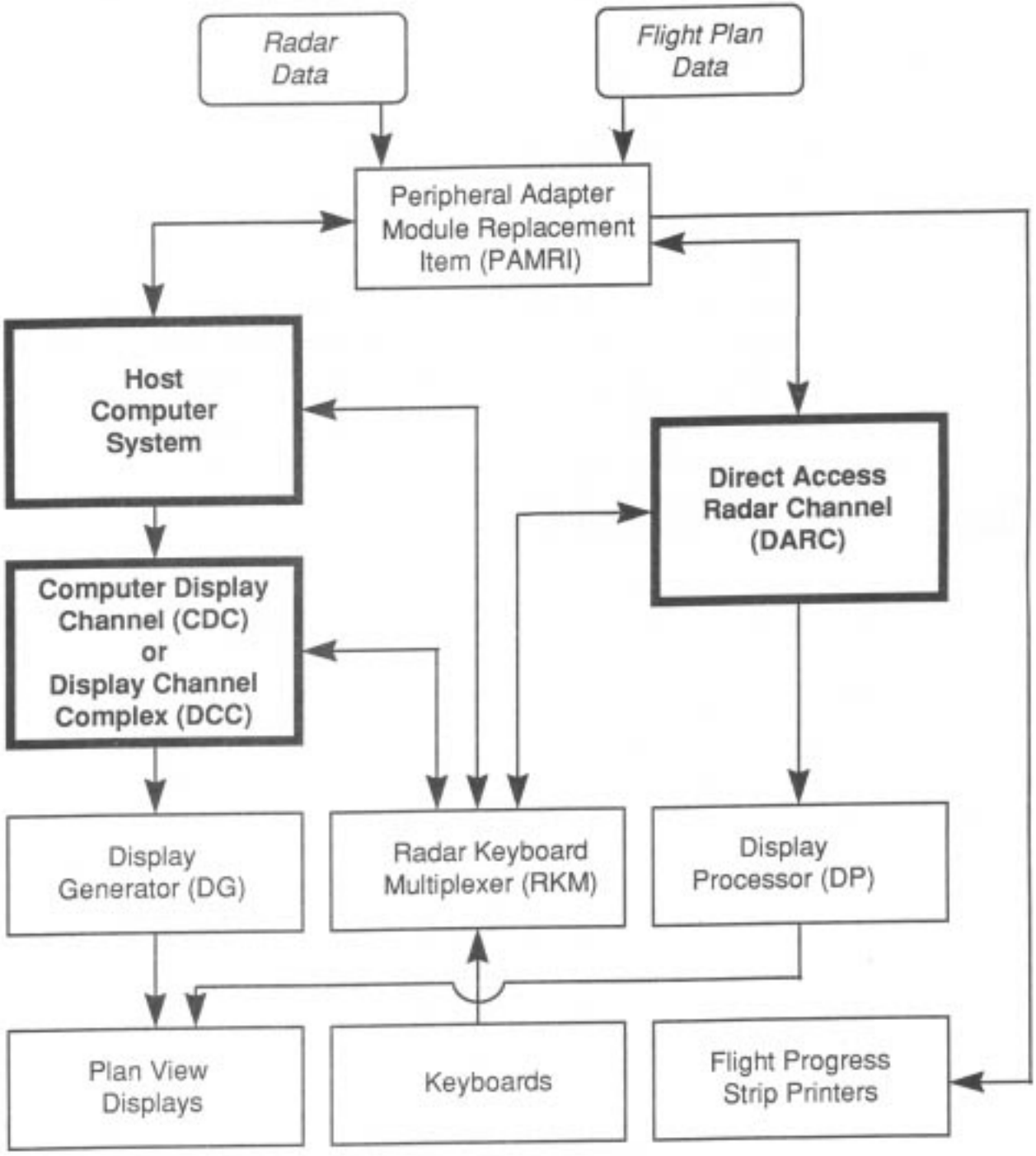


Figure 2: A simplified block diagram of major ARTCC computer components. Bold boxes indicate the three major computer systems, and the three boxes at the bottom show the major input/output devices available to controllers. Redundancy has been eliminated for simplicity.

computer can continue to operate; however, an outage occurs when a failure affects a nonredundant element. Historically, this redundant design has afforded the 9020E system a very high degree of reliability; however, the adequacy of this protection appears to be deteriorating as the equipment ages.

The DARC backup system is a dual-redundant computer that receives raw radar data through the PAMRI and correlates them with processed flight plan data supplied by the Host. Although both the Host and DARC can process raw radar data, only the Host can process raw flight plan data. A single button at each PVD switches between the primary system and DARC, which is continually available to controllers. The RKM is shared between the primary and backup systems, but the DARC system is interfaced to the PVDs through a display processor rather than a DG.

If either the Host system or the display computer fails (or if both fail), controllers must rely on DARC. In the event of a display computer outage, DARC delivers correlated radar and flight plan information to controller PVDs relying on the Host to process flight plan information. This mode of operation is referred to as "DARC/Host," and is similar to operation under the primary system; however, some features are not available to controllers. Five features that are not available during DARC/Host operation include: (1) conflict alert, a computer warning that safe aircraft separation has been compromised; (2) en route minimum safe altitude warning (MSAW), a computer warning that an aircraft is operating below a preset minimum altitude; (3) mode-C intruder alert, a computer warning that an untracked aircraft is operating in the airspace; (4) distance reference indicator, a moving 5-mile ring around aircraft targets that is used as a separation aide; and (5) route display, a feature that displays a lighted line along an aircraft's planned route of flight. Further, controllers must coordinate all handoffs to controllers at other facilities manually. The loss of features and increased workload do not alter a controller's responsibilities regarding aircraft separation or terrain clearance.

Regardless of the status of the display computer, if the Host should become unavailable, the backup system is used in "DARC/Standalone" mode. In this mode, in addition to the loss of the above five features and the automated handoff feature, no processed flight plan data are available, so operation is very different from that under the primary system.

If the traffic density is high, the transition from the primary system to DARC/Standalone can exacerbate an already-high controller workload. During this transition, controllers must select DARC at their PVDs, ensure that map displays for their sectors are properly displayed, and refer to flight progress strips to account for all aircraft under their control. This workload is further increased by the need to coordinate handoffs manually. Additionally, during DARC/Standalone operation, controllers are initially presented with limited data blocks for the aircraft under their control, and must reassemble and reenter the lost information referring to the flight plan information on the flight progress strips for each target. Also, because the flight progress strip printers are driven by the Host, as aircraft progress from sector to sector, flight progress strips must be manually passed between controllers or prepared by hand during the outage. Finally, during an extended period of DARC/Standalone operation, controllers will often

have to relay flight plan information during manual handoffs, because flight strips will not have been printed in adjacent sectors.

Equipment Maintenance

The ability to maintain the aging DCC equipment was described as a very big problem by FAA managers, AF technicians, and air traffic controllers. Many repairs require extensive troubleshooting and replacement of individual components on circuit boards. Many AF technicians and managers are concerned not only about parts and repairs, but also about the age of the wiring bundles, which require increasing care when any maintenance is done. There are also several instances of unique components manufactured for the 9020E computer, such as the read only system circuit board for which replacements can be obtained only by scavenging parts from the training computer at the FAA Air Traffic Academy in Oklahoma City, Oklahoma, or by using parts from two scrapped computers at the FAA supply depot.

An increasingly common failure mode involves metal-capped semiconductor components mounted on circuit cards.[14] These components (in effect, precursors to modern integrated circuit chips) are sealed with rubber gaskets and filled with a silicone lubricant. This lubricant permits differential expansion and contraction of the internal substrate and transistor components during temperature cycling. As the gaskets have aged, the rubber has deteriorated, allowing air into the components, which has given the lubricant an adhesive quality. This causes internal damage to the components when they are temperature cycled, which is inevitable when elements are powered up and down.

One of the most frustrating aspects of an AF technician's job concerns spare parts. Technicians and managers said that circuit boards, cathode ray tubes, and smaller electronic components are not only in very short supply, but are often nonfunctional when they arrive from several spare parts depots. Virtually no new parts are available for IBM 9020E systems. Most parts for the 9020E come from small untested stockpiles at various locations or are taken from training computers at the FAA Academy. Disabling or degrading the capability of training devices to keep operational devices on line is definitely a counterproductive, stop-gap measure. Frequently, remanufactured circuit cards, visibly heat scarred after years of component resoldering, arrive as spare parts. There is often no way to test the functionality of components such as these, other than by placing them in service in the live ATC system, which is quite undesirable. Many of these difficulties will persist until the 9020Es are decommissioned. However, efforts to improve the situation include a first-ever 9020E spare parts inventory, and the retention of two decommissioned 9020D computers for spare parts.

About 5 years ago, AF staff at Forth Worth conducted a risk assessment of the 9020E because of increasing concerns about spare parts and system maintenance in general. The repair

[14] At each ARTCC, the 9020E IOCE subsystem contains about 6,000 circuit cards and the other CE subsystem contains about 7,200 circuit cards. Storage and display elements also contain many circuit cards. Randomly selected circuit cards shown to investigators as examples contained five to 11 metal-capped components, each containing many semiconductors.

procedures that resulted from this risk assessment established specific 9020E repair hierarchies specially adapted for the age of the components. These hierarchies were designed to pose the least risk to the system. For example, the procedures prohibit access to certain areas within the computer during operations, and they specify the repairs that are permissible during operation and the repairs that require a shutdown of the system. One technician said that before the risk assessment was done, if one of the three CEs failed, the technicians would immediately start work on the failed element. Because this could conceivably disable the remaining two CEs, the plan now requires that they wait for a low traffic period to begin repairs. This example represents a conscious decision to continue operating with less-than-full redundancy because local technicians and managers believe that this is less risky than beginning immediate repairs.

When these procedures were described to the Safety Board, they had only been distributed to the FAA Technical Center. Technicians at other centers were unaware of them. Although FAA managers have the capability to implement and revise mandatory procedures in response to technician suggestions, no method exists for sharing useful suggestions of a nonmandatory nature. The Safety Board concludes that the conduct of the risk assessment by the Fort Worth AF staff is commendable and believes that useful suggestions and repair techniques should be evaluated by FAA management and shared with technicians at other facilities, as appropriate.

Technician Availability and Training

The IBM 9020E, a very complex piece of computer equipment no longer supported by its manufacturer, requires very highly trained and experienced FAA technicians to maintain and repair it. Because the system has aged and the number of 9020E certified technicians has declined, the ability to diagnose, maintain, and repair the equipment has deteriorated.

As an example, at the Fort Worth ARTCC, only four technicians are specifically assigned to the 9020E unit. Although six AF managers from other departments are available to support the four technicians (together known as a "tiger team") in an emergency, only four are available for routine maintenance--clearly insufficient to provide around-the-clock coverage. Technicians note that because of advancement and retirement, 9020E expertise at Fort Worth has declined sharply in the last 2 years. They also note that two of the four 9020E technicians are eligible to retire. According to the facility manager, one of them, who has 30 years of experience, "holds 50 to 60 percent" of the center's 9020E knowledge. This technician is expected to retire in about a year. Further, a 1994 FAA study of potential AF retirements through 1998, based on retirement eligibility alone, projects a steady downward decline of personnel in all facilities.

Also, in May 1995, the FAA completed a supportability review of its ability to continue maintaining and repairing DCC and CDC computers. The report concluded that the number of qualified technicians varies among the ARTCCs, and the authors noted that this situation is "…growing more critical." The study team wrote that some facilities are operating with only one or two technicians per shift, and that some shifts are not covered at all. Saying that the staffing situation is not likely to change, the authors noted that, "Training, vacations, sick leave are not coverable, much less the requirements of typically round-the-clock shift operations."

Because of dwindling expertise in the field, AF technicians are increasingly likely to call on the FAA Technical Center in Atlantic City, New Jersey, for assistance. If needed, a 9020E expert at the Technical Center is available to travel to provide troubleshooting and repair guidance. One of these experts told Safety Board investigators that he had typically made four or five such emergency trips for 9020E repairs each year; however, as of late September, he had made 12 such emergency site visits in 1995. He attributes this increased need for Technical Center engineering support directly to the retirement of several key technicians. To enhance their ability to provide IBM 9020E engineering support, FAA Technical Center managers have recently hired two additional IBM 9020E experts. These new technicians, who are highly qualified IBM retirees, will be available to provide telephone and on-site support for AF personnel in the field as needed.

Until recently, there has been no formal training on the IBM 9020E system since the last class was offered in 1990. Any informal training has been limited and entirely on the job. The FAA conducted an abbreviated 9020E training course during October 1995, which eliminated computer laboratory exercises and concentrated on the more important and basic repair techniques. Because it takes about 2 years to fully train a 9020E technician after basic schooling, these newly trained technicians will not become certified 9020E technicians until about the time that replacement computers are scheduled to be installed at the ARTCCs. Nonetheless, the newly trained technicians should be able to perform basic maintenance and repair tasks, freeing the more experienced technicians to perform more challenging troubleshooting and repairs. The Safety Board believes that such abbreviated courses could help to relieve the technician staffing problem. However, even though the number of technicians may be maintained or increased because of these courses, the overall experience level of the technician force will not.

FAA managers told the Safety Board repeatedly that it is very difficult to convince a technician who is eligible to retire to remain with the FAA when, because his or her numbers are dwindling through normal attrition, he will be "on call" virtually all the time. Several also said that they had restrictive overtime budgets that limit their ability to assign technicians as needed. Many highly trained, in a way irreplaceable, technicians said that they felt guilty whenever they went out of electronic pager range, even when they were officially off duty. Some said that they would remain with the FAA until the newer computer systems were up and running, but many others said that the enactment of any adverse changes to the current civil service retirement system would cause them to retire immediately.

An AF manager stated that pay incentives and a shiftwork credit towards retirement should be created to reward and retain the 9020E AF technical staff. However, he also expressed concern that if changes were made to the Federal retirement system, the shiftwork credit would encourage more retirements among eligible staff. He said that recent buyouts and personnel programs encouraging retirement have caused the facility to lose "people with the best technical knowledge in the building." He stated that as a possible solution, locality pay incentives could entice qualified staff from other parts of the country. The Safety Board shares this manager's concerns and urges the FAA to explore a variety of innovative personnel strategies to keep the maintenance and repair capability within the ARTCCs at an acceptable level. Such strategies

might include overtime pay, monetary and time-towards-retirement credit, and rehiring retired technicians as reemployed annuitants.

Equipment Reliability

FAA headquarters managers stated that the U.S. ATC system handles over 220 million flight operations annually. Of about 250,000 annual system delays, only 1.6 percent (or about 4,000) are ATC equipment related. Most of the other delays are weather related. FAA staff told the Safety Board for instance, that the ATC systems in general are 99.43 percent reliable over a measured 5-year timeframe. The Washington ARTCC managers stated that their equipment is fully operational 99.84 percent of the time. Chicago and New York Centers exhibit reliability figures of 99.39 percent and 99.43 percent, respectively. The Safety Board notes that while these figures indicate a very high reliability rate, they represent overall operating percentages for each facility.

The FAA's 1995 supportability review of the DCC and CDC computers was conducted to evaluate the near-term ability to support these systems. The supportability review project director wrote that his team examined these computer systems in "unprecedented" detail. The report concluded that systems failures "…are random and equally distributed between [ARTCC] sites." The authors also noted that "there are large periods of time where the systems are operating without any redundancy."

The FAA review team found that during the 18 months from January 1992 through June 1993, technicians at the New York ARTCC reported 90 DCC element failures in critical subsystems. Not all of these failures resulted in a complete DCC outage, but each one left the IBM 9020E system in a state of reduced redundancy. In fact, technicians calculated that the DCC system was operating with less-than-full redundancy 56 percent of the time during the period studied. By contrast, technicians reported 20 critical element failures involving the Host computer system, leaving it operating without full redundancy only 6.6 percent of the time during the same 18-month period.

The information in the FAA's supportability review about the DCC system performance was of particular interest to the Board because AF technicians had expressed concern that DCC systems were increasingly being operated with less-than-full redundancy. They noted that this tendency is not revealed by examining overall system availability data.

The FAA study team used FAA maintenance data to assess DCC and CDC system performance. The DCC system was evaluated at a greater level of detail than was the CDC system. Team members used maintenance data to compute quarterly availability[15] for each

[15] Availability as discussed in this report refers to the average amount of operational time within a quarter expressed as a proportion. For example, if a given element was operational 3/4 of the time during a quarter, its availability for that quarter was .75. One can also think of availability as a probability: If an element had an availability of .75 during a quarter, there was a 3 in 4 chance that it was operational at any given moment during that quarter.

element of the critical DCC subsystems. The FAA supportability review provided an appropriate first step at assessing subsystem availability, but no system-level data were presented.

The Safety Board conducted a probabilistic fault tree analysis[16] to determine system-level availability for the DCC computers using data presented in the FAA report. This analysis treated element failures as unrelated events, and it only included availability data provided by the FAA for the four critical DCC subsystems. Using the element-level availability data from the FAA report, the Safety Board computed quarterly availability statistics for each DCC computer. The results of this analysis are presented in Figure 3. The availability statistics in Figure 3 range from .9862 to 1. The DCC computers were operational more than 99 percent of the time in all but 1 of the quarters studied. The Board believes that this is an impressively high level of performance.

The DCC computer can operate either with full redundancy (all critical subsystem elements functioning) or with partial redundancy (no redundancy remaining in one or more critical subsystems). Because the data presented in Figure 3 do not reveal anything about how often the system was operated with full redundancy, the Board conducted a second fault tree analysis. This analysis determined quarterly availability of the DCC computers *with full redundancy*. The results of this analysis appear in Figure 4. This figure presents a different picture of DCC operational performance at the five DCC sites. It shows that fully redundant operational performance of the DCC computers has varied greatly among the facilities. For example, the DCC computer at the Washington, D.C., ARTCC has been fairly consistent: In all but 2 of the 12 quarters studied, the system was operated with full redundancy more than 90 percent of the time. The DCC system at the Cleveland ARTCC has performed almost as well: It was operated with full redundancy less than 90 percent of the time in only 4 of the 12 quarters. On the other hand, the fully operational availability of the other DCC computers has been more variable and less impressive. The DCC computer at the Chicago ARTCC was operational with full redundancy less than 70 percent of the time during 2 of the quarters studied, and the DCC computer at the Ft. Worth ARTCC was operational with full redundancy less than 70 percent of the time during 4 quarters.[17] The DCC computer at the New York ARTCC was operational with full redundancy less than 70 percent of the time during 5 quarters. In the second quarter of 1993, the system was never fully redundant because one element was off line during the entire period.

The Board's analysis showed that despite a number of element failures, the concept of redundancy continues to give the DCC systems a very high availability. On the other hand, the analysis confirmed that the DCC systems are often operating in a state of compromised redundancy. Based on statements made by AF technicians and managers, data presented in the

[16] Probabilistic fault tree analysis is an analytic technique that can be used to determine system-level availability from subsystem reliability data. For a discussion of fault tree analysis, see Henley, Ernest J. and Kumamoto, Hiromitsu, *Probabilistic Risk Assessment: Reliability engineering, design, and analysis*, IEEE Press: New York, 1992. For more information about the Safety Board's analysis, see Appendix B.

[17] The risk assessment and associated repair procedures at the Ft. Worth facility discussed earlier may have contributed to some of this nonredundant operation.

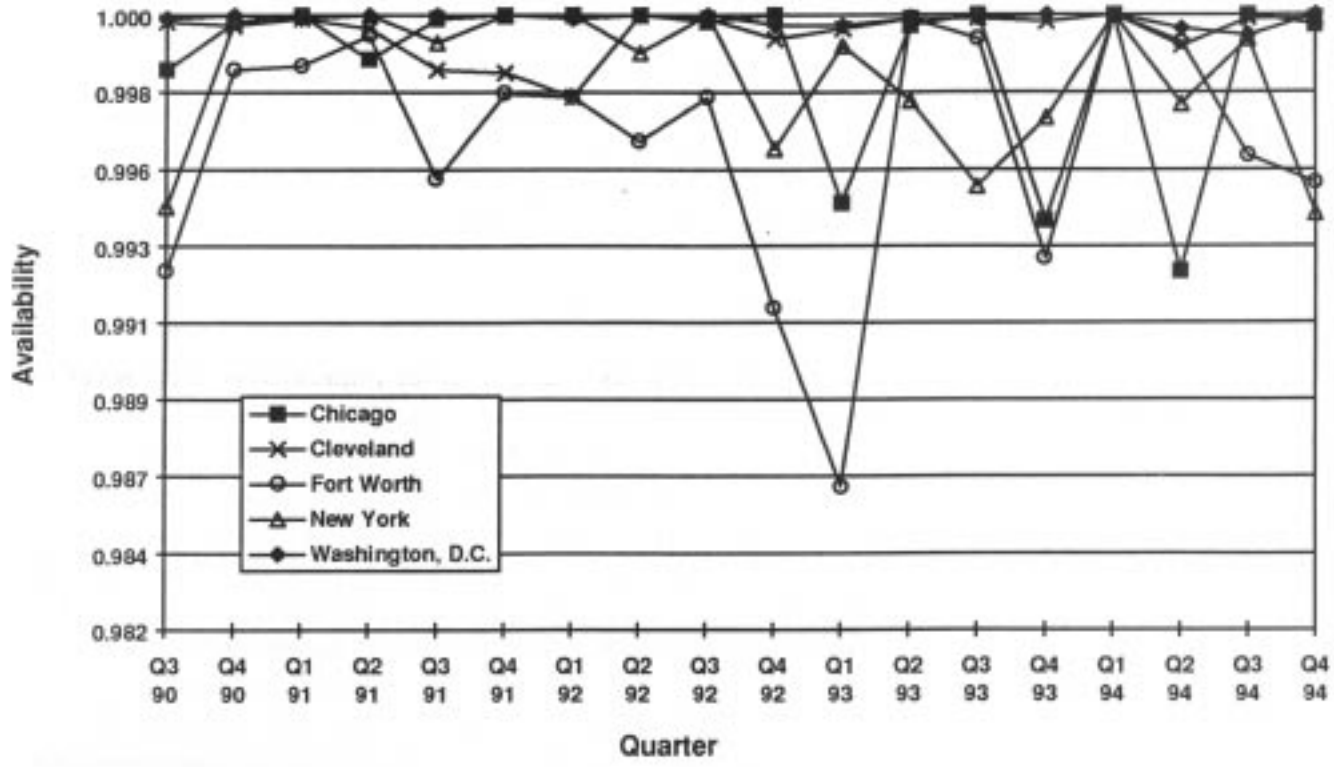


Figure 3: Quarterly DCC Availability by facility, 1990-1994.

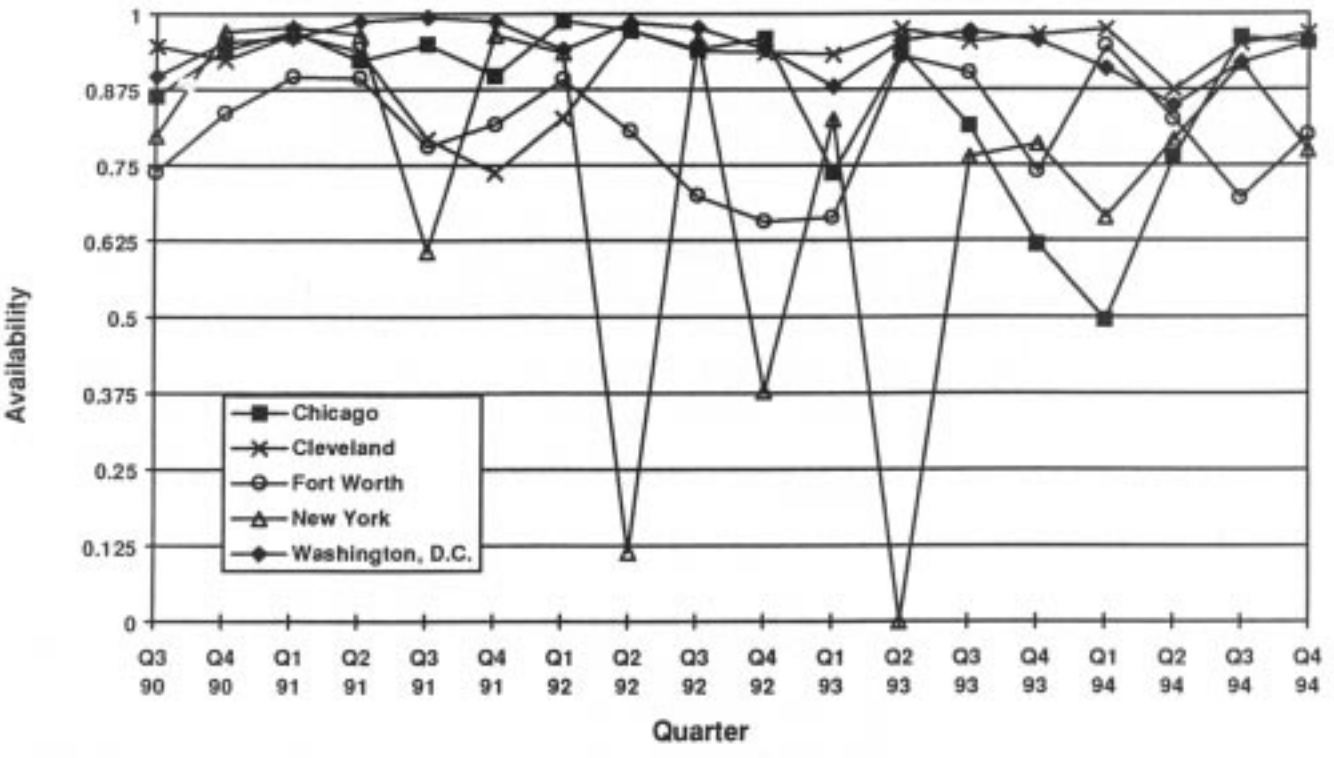


Figure 4: Quarterly DCC Availability with full redundancy, 1990-1994.

FAA supportability review, and the FAA's own statistical analysis, the Safety Board concludes that the DCC computers are increasingly likely to be operated with compromised redundancy. This increasing reliance on redundancy to keep the DCC system operational concerns the Safety Board because it increases the likelihood of an outage. Further, any time the system is operated with failed elements, technicians are working to make emergency repairs. Often, technicians work around the clock until repairs are complete. This limits their ability to complete routine maintenance tasks and less-serious repairs, and also heavily taxes their already-strained workforce.

Impact of Computer Outages

During this special investigation, Safety Board investigators found that the degree of reaction to a given equipment outage depended on the nature of the equipment failure and whether the person affected was a manager, a controller, or a repair technician. Interestingly, an IBM 9020E outage, the subject of so much current concern, is not considered to be a significant equipment problem by many air traffic controllers because the DARC/Host mode is very similar to the primary system. On the other hand, to an AF technician and his or her manager, a 9020E problem may mean hours or days of work with test equipment to identify a corroded contact on a 2-inch circuit board.

Computer outages can significantly alter a controller's normal working conditions. As mentioned, data block information is limited compared to the displays available when the primary system is available. For example, in DARC/Standalone, the controller is initially presented a target with only a beacon code, the airplane's call sign, and altitude information. All other data block information to be displayed must be manually entered by the controllers. In normal operations or under DARC/Host, these data are provided by the Host computer. When a controller switches to DARC/Standalone, as occurred on May 17, 1995, at Chicago Center, new data have to be entered manually via keyboard entries.

Depending on the number of radar targets and the complexity of the situation, working in DARC/Standalone mode can be very demanding and may result in extremely heavy workloads. The controller must maintain the relative "picture" of which flight was which and what each flight was doing at the time of the outage. The controller must attempt to rebuild the information from memory and flight progress strips with the assistance of another controller, if one is available. This involves performing additional functions while still communicating with all aircraft under the controller's jurisdiction and assuming the additional task of manual coordination with controllers in adjacent sectors.

An example is the computer outage on September 8, 1995, at Chicago Center, which resulted in a limited radar display for 8 minutes because a contractor inadvertently shorted a key relay with a screwdriver. The incident occurred during a busy traffic period; however, no incidents were reported. The contractor was conducting a scheduled equipment upgrade. The FAA later implemented expanded written procedures for all centers concerning upgrades, which better defined the procedures and assured that upgrades would not be attempted during heavy traffic periods.

The Safety Board's investigation into this outage revealed that the controllers did not have a firm understanding of the differences between normal system operation, DARC/Host, and DARC/Standalone. The level of knowledge of DARC varied among individual controllers, based on whether they had recently worked in the DARC modes during periods of routine computer maintenance. The most proficient were those controllers who had regularly worked the midnight shifts; however, even those controllers were not fully knowledgeable of the differences.

During interviews after the incident, the controllers stated that the first indication they received that the system had failed was when they noticed that their keyboards would not work and their trackball cursor was frozen. All controllers selected DARC on their own. Although a display that indicates the current operating mode is at the top of each PVD, none of the controllers interviewed remembered seeing this display or even consciously looking for it during the outage.

At one point, the primary computer system became available again for a short period and in one sector, the supervisor instructed the controllers to go back to the primary system. A controller responsible for numerous targets and a complex situation on his screen was manually rebuilding the track data when the primary system failed again. The controller switched back to DARC and again had to start rebuilding data. This controller stated that, fortunately, a controller who was not working a position started helping with coordination activities. The controller on the position had 40 to 50 aircraft awaiting departure releases and said that it was very fortunate that the outage did not occur after he had released these aircraft for departure.

The selection of normal radar display or DARC is made at each individual controller's PVD. Facility management determines whether the DARC is Standalone or DARC/Host mode based on available system capabilities. The Area Manager in Charge (AMIC), who supervises controllers during a given shift in an en route facility, advises the area supervisors when to change to or stay on DARC during planned transitions. In unplanned transitions, the controller makes the immediate decision so that a radar display is immediately available. As soon as possible after a failure, the NAS Operations Manager (NOM), who supervises AF technicians during a given shift in the facility, informs the AMIC of the situation and specifies the systems that are available. The AMIC then relays this information to the area supervisors. During the September 8 Chicago outage, instructions were issued to the AMIC for relay to the controllers. At this point during this incident, according to FAA officials, confusion and contradictory information was forwarded to the controllers. Controllers were switching from the DARC to the primary system. The Safety Board believes that they would have been better off remaining on DARC until the primary system was fully restored and certified.

DARC Training for Controllers

The Safety Board is concerned about the lack of knowledge about DARC/Standalone operations that appears to exist within the controller workforce, at Chicago and other ARTCCs visited. Training methodology on DARC/Standalone varies somewhat between ARTCCs, but can be characterized as classroom work and initial one-time on-the-job training certification.

Scheduled proficiency training occurs in some centers, but does not include DARC simulator training. Although unplanned DARC/Standalone operation is infrequent, it is a serious condition that controllers must be prepared to handle. The controller loses many features that are in fact safety enhancements. Most controllers today were initially trained on, and have become dependent on, those features mentioned earlier, such as automated flight plan processing, automated handoffs, the conflict alert feature, and the automatic generation of flight progress strips. The controllers said that only those who regularly work midnight shifts get effective, hands-on, DARC/Standalone experience. This access to DARC/Standalone occurs during planned outages that are usually scheduled for primary system maintenance. The controllers stated that the first call in the radar room during an unplanned daytime transition to DARC/Standalone operation is, "Help! Who has worked a mid [midnight shift] lately?" This suggests that although formal procedures for transition from normal operation to DARC/Host operation are not difficult, nor even very necessary, the procedures for transition from normal operations to DARC/Standalone, and vice versa, are not well established, or are not well understood.

A Safety Board investigator observed a planned outage that required DARC/Standalone operations during a midnight shift at Washington Center. The position under observation was a feeder position for JFK International Airport, and also included traffic for Philadelphia; Teterboro, New Jersey; and other facilities. The two controllers who worked these positions had been controllers for many years, and both had military ATC experience. Upon the investigator's arrival, about 15 airplanes were being worked at the position, but the traffic tapered off within the hour to three to five airplanes being worked at any one time. Before the outage, the supervisor circulated among all controllers and told them to expect a planned outage at 0030. Shortly thereafter, computer bells at each position in the control room signaled the start of the outage, and controllers selected DARC at their consoles. Without any prompting, the controller under observation took several rapid actions to configure his console for DARC/Standalone operation. These included calling up a flight list and relevant terminal area altimeter settings. He also verified that data blocks corresponding to all his active flight strips were present on DARC, and he made some adjustments to his radar map display.

An inter-facility automated handoff that had been initiated before the outage was completed successfully. This seemed to surprise one controller who had not realized that automated handoffs initiated under primary system could be completed successfully under DARC/Standalone. During the outage one controller showed two other controllers that the range/bearing feature is available during DARC/Standalone operations.[18] The two controllers had believed that this feature was unavailable. When asked, the controller demonstrating the use of the feature said that he had discovered it accidentally. While experimenting during the Safety Board's observation, that controller further learned that the feature apparently works only between two points selected with the controller's trackball--it does not allow the controller to

[18] Under primary system operation, controllers may select a tracked target (aircraft) and display the range and bearing to any position on their PVDs by indicating that position with their trackballs. Alternately, they may compute the range and bearing from a target to a facility such as an airport or navigational aid by keying in the facility identifier. Many controllers consider this feature useful, but are able to make these computations easily without computer assistance.

type in a facility identifier and have the computer automatically compute range/bearing to that facility, as it does during normal operation. The controllers demonstrated some additional DARC features to each other during the initial period of the outage.

Effective on June 1, 1995, a General Notice to all ARTCCs (GENOT RWA 5/66) required that all developmental controllers receive 1 hour of instruction on DARC. Although the exact type and method of this training were left to each facility air traffic manager to coordinate with labor representatives, generally, the facilities visited by Safety Board investigators satisfied this requirement by requiring developmentals to work a midnight shift during a planned outage, much like the outage described above. The Safety Board believes that on-the-job training familiarization such as that observed by investigators at Washington Center is a useful, but currently insufficient, way to train controllers on DARC operations.

Many controllers and training managers expressed a strong need for DARC training simulators. They noted that existing ARTCC dynamic simulation (DYSIM) laboratories, which are used to simulate primary system operation, cannot be used to simulate DARC, and that other training methods were only partially satisfactory. The Safety Board believes that no teaching method is as effective as full simulation. Safety Board investigators asked representatives from the FAA's Air Traffic Automation Software Policy and Planning Division if there were any plans to provide facilities with DARC simulation capability for training purposes. These representatives said that full DARC simulation (including transition procedures) is possible using equipment and software already in place at all ARTCC facilities, but it is not currently being used.

To simulate DARC, the Host's dual processors can be "split" to allow two configurations to exist at once: a live configuration and a training configuration. During split-Host operation, one of the Host processors is used to drive some PVDs in a live system, and the other processor drives the remaining PVDs in a simulated system. Full dynamic configuration of training scenarios is possible. This system was developed for use in the Denver ARTCC to train controllers on operations involving the new Denver airport. As designed, the split-Host configuration allowed the Denver facility to use the Host to conduct controller training without affecting live operation. Split-Host operation can be implemented at all ARTCC facilities immediately. Although there has been some reluctance to implement split-Host operation in ARTCCs because of initial cabling requirements that involve the DCC/CDC hardware, split-Host operation will be required at all facilities to install, test, and train controllers on the new Display System Replacement (DSR) hardware (the FAA's DSR program is described on page 24). Another concern regarding split-Host operation is that it bypasses the dual-redundancy of the Host. In the event of a failure involving the live Host processor, the redundant Host processor would not be available to maintain the operation of the primary system, so controllers using the live system would enter DARC/Standalone mode. During normal operation, controllers would enter DARC/Standalone only in the event of a failure of both Host processors.

The Safety Board is aware that FAA air traffic managers have recognized the need for operational compatibility between the primary and backup systems, and that over the years they have worked to enhance this compatibility through successive revisions of the DARC software.

Their goal had been to minimize the need for simulation by increasing the operational similarity between both systems. However, DARC remains a distinct system for which no simulator training has ever been made available to controllers, but is needed.

Given the success of split-Host operation as a training tool at the Denver ARTCC, and the notably high reliability of the Host, the split-Host operation could serve as an appropriate simulation tool for controller DARC training. Therefore, the Safety Board believes that the FAA should create a simulator-based training program using the simulation capabilities of split-Host operation during off-peak periods. The training program should include simulated transitions to and from DARC operating under both DARC/Host and DARC/Standalone modes. All controllers should be required to complete this new training program.

Impact of Communications Outages

Interestingly, controllers complained more frequently about communications problems than computer outages. The communications problems most frequently cited were not related to the automated radar displays, but to air-to-ground frequency degradations or failures. Most controllers and air traffic managers said that they were more concerned about radio frequency outages than computer outages because controllers can only issue instructions to pilots with whom they are in radio contact.

Radio frequency failures occur for many reasons. For example, a remote communications outlet may be struck by lightning, the telephone line connecting a remote outlet with an ATC facility may be cut, or interference may be introduced into a channel for a variety of reasons, such as noise from dirty connectors. AF technicians at one facility told investigators that a local telephone company once sent test tones into a live circuit being used by a controller to communicate with aircraft, rendering the frequency associated with this circuit useless. Managers told investigators that the available frequency spectrum is becoming very crowded, which has prompted a reduction in ATC radio transmitter power. They are concerned that frequency congestion could worsen if the available spectrum is further reduced, such as by auctioning portions of the spectrum to the private sector. The Safety Board shares this concern and plans to examine this issue further.

At Washington Center, one controller said that an aircraft in his sector lost an engine, began descending through lower altitudes under his control, and declared an emergency. The controller did not hear the mayday call, which was relayed to him by other aircraft under his control. The disabled aircraft apparently selected the emergency radio frequency (Guard) during the emergency, but the controller did not have emergency frequency transmit/receive capability at his position. A controller at another position monitoring Guard called the controller to ensure that he was aware of the emergency. Apparently the pilot of the disabled airplane restarted his engine at about 8,000 feet and continued flying, but the controller was never able to communicate with him. The controller said that the emergency frequency was available at only a limited number of controller positions at Washington Center.

At New York Center, controllers stated that communications "dead spots" are well known within some sectors. Controllers are unable to communicate with aircraft in these locations, so they routinely compensate by not issuing clearances to aircraft passing through known dead spots. AF staff noted that frequencies were generally free of dead spots when they were assigned, but holes have appeared in radio coverage because buildings and other obstructions such as cellular telephone towers and cranes have been erected. The reduction in transmitter power, which was intended to minimize signal bleedthrough, may have also further diminished radio coverage. Some controllers routinely use the backup emergency communications (BUEC) system[19] for enhanced coverage in known dead spots (especially low altitude feeder routes).

In the past, AF was able to restore lost frequencies relatively quickly. However, it is no longer able to provide the same level of service because some centers have resorted to unstaffed technician shifts because of technician shortages. At one location, the goal is to begin repairs within 24 hours of a failure. At some centers, radio frequency allocation specialists said that it might take as long as 6 months or more to correct a bleedthrough problem, such as that created by another ATC facility. AF staff also noted that when frequencies fail, it often takes a long time to get a replacement frequency released for the facility to use. Further, because off-duty technicians are not officially subject to recall and are not compensated for any on-call time, it can be difficult to locate an off-duty technician in a timely manner when a frequency (or any other equipment) failure occurs during an open shift. If the technician has consumed alcohol on his or her own time, for instance, he or she may not be legally able to report to work to make needed repairs.

AF technicians and controllers stated that because of such communications shortcomings, controllers are very dependent on the BUEC system. They also stated that controller positions have been added that have no access to BUEC. Recently, controllers have lost primary frequencies, and switched to BUEC only to find it already in use by another remote communications site. BUEC assigns controllers the use of remote communications sites in the order that the sites request BUEC operation. This means that when several controllers need BUEC at the same time, the site assigned to a particular position may not be the ideal one for the traffic being worked at that position. Supervisors will often ask all controllers to release BUEC, then coordinate the selection process so that priority remote communications sites are given to low altitude sectors.

The Safety Board is concerned that the overreliance on the BUEC system reveals deficiencies in the primary communications system, such as dead spots and interference. The Board is also concerned that some of these deficiencies may not be rectified by the FAA's ongoing communications modernization program, the voice switching and control system (VSCS). Therefore, the Safety Board believes that the FAA should identify and rectify safety

[19] The BUEC system is a system of remotely located transmit/receive radios at strategic locations throughout a particular center's area of responsibility. Signals from the centers to the BUEC sites do not go over commercial land lines (as do normal radio transmissions) but rather over the FAA's own data distribution network. The BUEC sites transmit at 25 watts strength, instead of the normal ATC radio's 10 watts.

deficiencies, such as failures, interference problems, and inadequate radio coverage, that are not currently being addressed in VSCS. Further, because ground-to-air communications are a vital link in the ATC system, all controllers should have immediate access to a backup communications system. Therefore, the Safety Board believes that the FAA should provide controllers access to the BUEC system at every controller console.

The Safety Board discovered that some ARTCC staff have concerns with the services of some of the nongovernment telecommunications providers.

Remote communications sites are linked to ATC facilities through third-party telephone lines, and much of the voice and data communications between facilities is carried over these third-party lines. Until 1992, AT&T had been the primary third-party telecommunications provider to the FAA. As required by Federal acquisition regulations, the FAA offered the ATC telecommunications contract for competitive bids. The bid submitted by MCI received the highest technical score and had the lowest cost; consequently, the contract was given in March 1992 to MCI. In June 1992, ATC facilities began switching over to MCI circuits. The ATC telecommunications contracts will be offered for competitive bid every 10 years; therefore, the current contract with MCI will expire in March 2002.

Safety Board investigators noted that staff at the ARTCCs they visited reported differing levels of satisfaction with MCI. Although staff at some of the facilities said that they had received a less-than-satisfactory level of service, staff at one facility said that they were quite happy with MCI's performance. AF management stated that any vendor that is new to the air traffic environment must be educated about the ATC function and the special demands of the ATC environment. The AF managers said that their relationship with AT&T developed over many years, and that AT&T personnel became very familiar with working on systems that are critical to the safety of flight. Those managers now believe that this appreciation of the importance of coordinated repair efforts is not at its previous level. However, uncoordinated repair efforts are decreasing as MCI's understanding of the ATC system is growing.

Problems sometimes also arise because any number of local service providers may interface with MCI in any given State. In one State, over 200 local telephone companies are connected to MCI. Repair service for a cable cut at a remote FAA communications outlet must be coordinated with the appropriate local provider through MCI, and this coordination can take a very long time. Occasionally, AF staff must call higher levels within MCI to facilitate faster repairs. An AF technician at one facility said that under AT&T, these routine service calls got upper-level AT&T attention from the outset. AF staff at one facility noted that it took 15 years to establish a strong working relationship with AT&T and to impress upon AT&T the importance of not manipulating a communications link without coordination. They said that they are attempting to educate MCI, and during the learning process, MCI has grown more cooperative and responsive. Nevertheless, AF technicians and managers are concerned that transitional service difficulties could reappear when the contract changes hands again.

At one ARTCC, AF staff indicated that the MCI changeover had been very successful. They said that the changeover was about 85-90 percent complete and that only about one or two

other centers are further along in the process. They have found MCI to be very reliable, cooperative, and reactive to their needs, and said that fixes to design elements that were engineered with less-than-adequate redundancy have been successfully coordinated with MCI, and that the entire changeover has been very successful. AF technicians at this facility said that MCI has provided a very reliable service with lower cost and greater reliability than when AT&T was the primary provider. The AF staff credit the successful changeover to good early planning and competent MCI technical liaisons.

Impact of Power Outages

Highest on the list of fears of ARTCC staff is a facility electrical power outage. As might be expected, when this occurs, and backup power systems do not go on line, controllers lose the ability to track aircraft targets on their PVDs and to communicate with flightcrews. Until radar and voice contact with airplanes is either reestablished or transferred to other adjoining radar facilities, the airborne flightcrews are solely responsible for midair collision avoidance. Total power outages have occurred for unavoidable reasons such as lightning strikes, or for avoidable reasons such as human error.

To illustrate the magnitude of such incidents, on September 14, 1994, while replacing a portion of the critical power system at the Chicago Center, the facility experienced a total loss of power for about 1 second. This brief interruption of power was the result of an inadvertent short circuit caused by a contractor technician while making power phase tests. This outage caused about 477 delays. More recently, on August 9, 1995, the Oakland Center experienced a total power failure when technicians took the facility off commercial power to make repairs. The two backup power systems then failed. It took workers about 15 minutes to restore radio contact between the center and pilots and almost an hour to restore radar. There was only one instance in which the separation standard was compromised; fortunately, the pilots of each aircraft saw one another and corrected their courses. Another incident occurred on August 12, 1995, at the Miami Center when the facility was struck by lightning, resulting in a loss of critical power, the Host computer, and radio communications. When the facility initiated a change to DARC operations, the system failed on 50 percent of the sectors. This outage resulted in about 90 to 100 delays.

FAA Efforts to Address the Problem

Because the system was beginning to age, in 1981, the FAA began its efforts to modernize the ATC computer, communications, and other systems. The centerpiece of this effort became the Advanced Automation System (AAS).[20] As conceived, the AAS would have completely replaced existing ATC computer systems and controller workstations and consolidated 203 TRACON facilities and 20 ARTCCs into 23 facilities. Design competition for the program began in 1984, and in 1988, the FAA awarded the AAS contract to IBM.

[20] For more information concerning the AAS and other related projects, refer to the May 1995 GAO report "Air Traffic Control: Status of FAA's Modernization Program," GAO/RCED-95-175FS. This report was the GAO's fifth annual report on the status of ongoing ATC modernization programs.

In anticipation of reduced technician staffing needs following the implementation of the AAS, the FAA allowed attrition, retirement, and buyouts to reduce AF staffing levels. The FAA also curtailed training efforts, especially on automation systems set for replacement. In effect, the FAA shrank its capability to maintain and repair aging systems in expectation of replacing these systems entirely.

Originally, the cost estimate for the AAS program was $2.5 billion, but design and development problems began to appear. By November 1992, the program had slipped 33 months behind schedule, and the program cost estimate had risen to $5.1 billion. In December 1992, the FAA announced a limited facility consolidation plan under AAS. The only portion of the AAS to be implemented was the Peripheral Adapter Module Replacement Item (PAMRI), which became operational at the last of the 20 ARTCCs in May 1993.

In June 1994, the AAS program was restructured entirely. The computer systems and controller workstations modernization efforts for the ARTCCs were scaled back and renamed the Display System Replacement (DSR). Another portion of the facility consolidation program, the voice switching and control system (VSCS), was retained. The FAA also added a project called the DCC Rehost (DCCR) to replace the IBM 9020E until the DSR is implemented.

Display Computer and Controller Workstations

As a part of the 1994 restructuring of the AAS, the FAA has two major ongoing programs to modernize much of the computer and workstation hardware in all of ARTCCs. The FAA has awarded an initial contract to Loral Corporation to begin producing and implementing the DCCR program. The DCCR program will replace the IBM 9020E computers with IBM 9221 devices at the five ARTCCs that have DCC equipment. The PVD, DG, and RKM hardware will remain in place. These new systems will be maintained and repaired by contract employees, which should lessen the demand on AF technicians. The first site (Chicago) is expected to become operational in October 1997. The remaining sites will follow until all DCC equipment has been taken off line (Ft. Worth, November 1997; Washington, December 1997; Cleveland, January 1998; New York, February 1998). Once operational, the FAA envisions that this system should serve as a bridge for the ATC system until the DSR project is completed.

The DSR, which has been referred to as the controller work station of the future, is slated to replace current en route ATC display system hardware and software. The current PVDs will be replaced with new controller workstations, which will locally process display information. The DGs will become obsolete, but the RKMs will remain for use with the DARC system. The IBM 9221 hardware at the DCCR sites and the CDC display computers at the other facilities will no longer be needed. The Host and DARC systems will remain in place as the primary and backup systems, respectively. The DSR system will include much off-the-shelf hardware and will provide controllers with many features not currently available, including easy-to-interpret color displays using industry-standard windowing, more reliable controller keyboards, and other advanced features. The FAA anticipates that this system will be operational at the first site in October 1998. The system should then become operational sequentially in each of the remaining sites until all ARTCCs have been converted by June 2000. The DSR is an appropriate upgrade

path for the existing display system, and the Safety Board believes that the FAA's decision to pursue the DCCR as an interim measure is prudent.

Planned DARC Software Upgrades

The FAA periodically updates the software that drives DARC. Currently version "M" is the production version of the software, and version "N" is being tested and debugged for National deployment. The FAA has specified several enhancements for DARC version "O," which is scheduled to be in place as the production version and to remain unchanged during DSR implementation. Version "O" of DARC will be deployed in two stages. Level 1 is set for deployment on or about June 1997. This upgrade will include the conflict alert, en route MSAW, mode C intruder alert, and route display features. Level 2 of version "O" will include the distance reference indicator feature. Level 2 may not be deployed before DSR depending on FAA resources and its impact on the DSR project. These features will be available in DARC/Host mode. The Safety Board concludes that adding these features to DARC will enhance the safety of operations conducted under DARC/Host and strongly believes that the FAA should make every effort to deliver these features in the summer of 1997, as planned. Because FAA managers expressed concern that resource limitations or competition from other agency programs could jeopardize these enhancements, the Safety Board will continue to monitor the progress of this project.

New Communications Technology

The voice switching and control system (VSCS) is currently being installed and tested at ARTCCs. VSCS is a digital communications switching system designed replace existing electromechanical switching technology currently installed at ARTCCs. VSCS will include panels at each controller workstation through which air-to-ground and ground-to-ground communications will be controlled. The system, originally intended to be part of the AAS facility consolidation plan, is designed to be expandable and highly reliable. Although the Safety Board is pleased that this system will rectify many communications problems, such as providing access to the emergency frequency to all controllers, the Board is concerned that VSCS will not correct all of the communications difficulties identified by controllers. The upgrades associated with VSCS are limited to equipment inside the ARTCCs. No remote communications sites or telephone company connections will be affected. Although VSCS will likely bring more communications flexibility to en route facilities, it was not designed to address such problems as inadequate radio coverage or signal interference from nearby stations.

Power Outages

A modernization program called the ARTCC Critical and Essential Power System (ACEPS) is also underway. This program is designed to take advantage of new design technology in backup power generation.

The current facility backup electrical system, manufactured by Garrett, Inc., is over 25 years old. As a result, it is very difficult to maintain for reasons that include a dwindling supply

of spare parts, such as output fuses. Because of their age, output fuses are very susceptible to overload and blow out easily. The ACEPS program provides a standard configuration in all centers to increase standby power capacity. This requires the installation of two 750 kilowatt generators, in addition to the four 550 kilowatt generators already in place at each center. In addition, a new Exide uninterrupted power system, routed through a series of output buses and ultimately through a new series of transformers, is installed. Once this array is in place, the old Garrett system is removed.

Further, ACEPS is designed to eliminate power spikes that can occur during the transition from commercial power to backup power. While inter- and intra-facility communications are not greatly affected by power spikes, which can last for as long as 1 second, the 9020E computer system cannot tolerate any significant power surge. The ACEPS system is designed to intercept a power fluctuation and within 200 microseconds, transition to the backup power supply. For the air traffic controller, the changeover from commercial to backup power should be transparent. Because several of the recent facility power outages have occurred during the installation and testing of the ACEPS hardware, the number of these outages should decline once the ACEPS installation is finished.

Alternative ATC Systems

The Safety Board visited an advanced FAA ATC system that is already in place and operational. In conjunction with the U.S. Air Force, the FAA developed a computer replacement system in the High Desert TRACON, to provide enhanced support to the Edwards Air Force Base Flight Test Center. Unlike most past ATC development programs (including DCCR and DSR), the High Desert TRACON upgrade program makes extensive use of commercially available, off-the-shelf hardware and software. The program development began in April 1990, and the FAA commissioned the equipment as fully operational in February 1994. The cost of the program to that point was 10.8 million dollars. The FAA plans to allocate another 3.8 million dollars for further development and safety enhancements such as conflict alert and MSAW programming.

The main processing and tracking functions of the system are accomplished on two redundant SUN SPARC 4/470 computers running identical computer codes written by BDM Federal, Inc. These two processors perform the identical central computer system functions of taking all of the radar information from the various radars and, through many software routines, develop tracking and flight following information.

For safety and reliability reasons, each computer is constantly processing the identical radar tracking and controller information. If one of the computers should fail, the remaining computer will assume the role of primary. When the failed computer is again available it will automatically update itself and assume a backup role. This whole process is initiated automatically and is transparent to the controllers, resulting in no service or data losses. There is no loss of controller features when the backup system is activated.

This entire central computing process was accomplished on unmodified commercially available computers. The computer code was written utilizing standard UNIX operating system program calls. The advantage to this approach, besides the low cost, is in the ability to replace the hardware with a newer system when the technology becomes available. For instance, the High Desert TRACON has a program underway to replace the central computer system computers with newer SUN SPARC 1000 servers. These new computers will triple the processing power of the older 4/470 computers, at a lower cost than the original stations. This will all be accomplished without having to rewrite a single line of operating software code.

The Safety Board does not mean to imply that a system similar to this could, or should, replace ongoing and well established DCCR and DSR plans. However, this project demonstrates that a small, FAA/Air Force/civilian contractor team can, in a relatively short period of time, develop a modern, small-scale ATC system in a very efficient and cost-effective manner. Thus, the effort and ingenuity associated with the development of the High Desert TRACON computer system replacement deserves consideration as a model for future air traffic development and procurement programs.

The Safety Board made no attempt to compare the appropriateness of the FAA's decision to pursue the DCCR/DSR ARTCC upgrade path to any competing strategy because of the limited scope of the Board's investigation, but concludes that it would be inappropriate to pursue any strategy that would further delay the replacement of the aging display computers. FAA management and technical personnel, as well as Loral management, all believe that DCCR is a workable replacement for the aging IBM 9020E systems and they are committed to its on-time implementation. The Safety Board has found no reason to question either of these decisions.

Summary

Despite the issues discussed in this report, the Safety Board believes that the U.S. ATC system is very safe and that the public should not be unduly alarmed by recent press accounts of specific ARTCC equipment malfunctions. In the vast majority of computer outages that have recently occurred, controllers were able to provide safe aircraft separation using a backup system similar to the primary system. On those rare occasions that computer capabilities were degraded further, the controllers were able to reroute planes and prevent aircraft departures. Although this likely causes significant economic impact, the system remains safe because there are fewer airplanes in the sky. In the extremely rare situation in which all electric power is cut off to an ATC facility, and radar and radio contact with airplanes is lost, the system in which adjacent facilities handle traffic has worked successfully. In addition, flightcrews are trained to utilize flight and timing procedures designed to ensure safe separation. Further, the installation of collision avoidance systems on commercial airplanes has provided an additional measure of safety.

Nonetheless, any degradation of radar and communications capability increases the complexity of the tasks facing both air traffic controllers and flightcrews, and it reduces the normal margin of safety afforded by the primary system. The Safety Board remains concerned about the aging computer problems, especially the increased tendency to operate the DCC

computer with less-than-full redundancy, which leaves the system more vulnerable to an outage. The Safety Board believes that the recent spate of ATC equipment problems has convinced the FAA that although procedures and training are in place to allow controllers to cope with the outages, it is prudent to further enhance these procedures and to increase the level of controller training on backup equipment.

The Board is also concerned about facility power outages and ATC communications deficiencies. Air traffic controllers told investigators that they believe these issues present the most significant safety concerns because they can result in a loss of radio contact with airplanes. The ACEPS and VSCS modernization programs are designed to enhance the safety and utility of both of these systems. The ACEPS program should improve ARTCC electrical power systems, reducing the incidence of power failures once its installation is complete. The new VSCS system should provide several important features to the communications system, but the Safety Board believes that the FAA should identify and address the communications deficiencies that are likely to remain even when the VSCS system is in use at all ARTCCs.

Findings

1. Outages involving the aging IBM 9020E DCC equipment are becoming more frequent. The effects of these outages are being exacerbated by extended restoration time because of the lack of qualified technicians and working spare parts.

2. Some of the IBM 9020E computer systems are increasingly likely to be operated with compromised redundancy, which increases technician workload and the risk of outages.

3. The retirement of highly skilled AF technicians has adversely affected the FAA's ability to maintain and repair many ATC systems; changes to the civil service retirement system could worsen this situation by hastening the retirement of many retirement-eligible technicians.

4. The FAA has hired additional IBM 9020E experts, is offering technician training, and is implementing DCCR, which should minimize the number and duration of the display computer outages.

5. The DSR will enhance the reliability of a number of components in the en route automation system. The DCCR will serve as an interim fix for the five facilities with IBM 9020E DCC equipment. The FAA's decision to pursue the DCCR in addition to the DSR upgrade path was prudent, given the aging condition of the existing equipment.

6. There is no method within the FAA for sharing useful suggestions and repair techniques of a nonmandatory nature to allow technicians at other ARTCCs to take advantage of such innovations.

7. Many controllers are not proficient with the DARC/Standalone mode of the backup computer system, because they receive limited training that does not include simulation training.

8. Split-Host operation is currently possible at all ARTCCs, and could be used as a simulator for DARC training.

9. The FAA plans to enhance the DARC backup system by adding conflict alert, en route minimum safe altitude warning, and other features on or about June 1997, enhancements that will enhance the safety of operations conducted under DARC.

10. Many recent outages have involved power systems and communications equipment unrelated to the aging IBM 9020E computer system; some of these will be fixed by ACEPS. These outages provide the most serious consequences; however, they occur infrequently.

11. Communications problems involving equipment failures, frequency failures, interference problems, radio coverage, and backup radio systems have also compromised the safety of the ATC system. These problems are also unrelated to the aging IBM 9020E computer system.

Recommendations

As a result of this special investigation, the National Transportation Safety Board makes the following recommendations:

--to the Federal Aviation Administration:

Explore innovative personnel strategies, such as overtime pay, monetary and time-towards-retirement credit incentives, and rehiring retired technicians as reemployed annuitants, to keep the maintenance and repair capability within air route traffic control centers at an acceptable level. (Class II, Priority Action) (A-96-1)

Create a program to evaluate suggestions and repair techniques proposed by technicians in the field and to share these innovations with technicians at other facilities, as appropriate. (Class II, Priority Action) (A-96-2)

Create a simulator-based training program using the simulation capabilities of split-Host operation during off-peak periods. The training program should include simulated transitions to and from the direct access radar channel (DARC) operating under both the DARC/Host and DARC/Standalone modes. All controllers should be required to complete this new training program. (Class II, Priority Action) (A-96-3)

Provide air traffic controllers access to the backup emergency communications system at every controller console. (Class II, Priority Action) (A-96-4)

Identify and rectify safety deficiencies, such as frequency failures, interference problems, and inadequate radio coverage, that are not currently being addressed in the FAA's voice switching and control system program. (Class II, Priority Action) (A-96-5)

BY THE NATIONAL TRANSPORTATION SAFETY BOARD

JAMES E. HALL
Chairman

ROBERT T. FRANCIS II
Vice Chairman

JOHN A. HAMMERSCHMIDT
Member

JOHN J. GOGLIA
Member

January 23, 1996

Appendix A--Partial Listing of Major ATC Equipment Outages
September 12, 1994 - June 6, 1995

Date	ARTCC	Event	Duration	Flight Delays	Operational Errors
Sep. 12, 1994	Chicago	Power Failure	1 hr 15 min	433	0
Apr. 6, 1995	New York	Power Failure	36 min	189	0
May 17, 1995	Chicago	Computer Problem	1 hr 5 min	234	0
May 25, 1995	New York	Power Failure	5 hrs 49 min	485	0
June 6, 1995	Washington	Computer Problem	40 hrs 59 min	1	0
July 17, 1995	Chicago	Computer Problem	44 min	161	0
July 19, 1995	Fort Worth	Computer Problem	31 min	6	0
July 23, 1995	Chicago	Computer Problem	25 min	28	0
July 24, 1995	Chicago	Computer Problem	122 hrs 34 min	42	0
Aug. 9, 1995	Oakland	Power Failure	1 hr 18 min	333	1
Sep. 12, 1995	Chicago	Computer Problem	20 hrs 46	83	0

Appendix B--Fault Tree Analysis of DCC Computers

Introduction

This appendix explains how the Safety Board calculated the availability statistics presented in the report for the IBM 9020E DCC computers. The appendix first presents a basic overview of the DCC system architecture, then presents calculations for computing availability and availability at full redundancy.

DCC System Architecture

The DCC system contains four critical subsystems, a failure of any of which will cause a DCC outage. Each subsystem has one redundant element. The computing element (CE) subsystem has three CE elements, the storage element (SE) subsystem has five SE elements, the input/output control element (IOCE) subsystem has two IOCE elements, and the display element (DE) subsystem has four DE elements. Any of these subsystems can tolerate a failure of one of its elements, but the subsystem will fail (causing a DCC outage) if more than one element in a subsystem fails. To depict this, the Board constructed the fault tree that is shown in Figure Al. The bottom-level events depicted in the fault tree correspond to the mutually exclusive set of events that can lead to subsystem failures (element failures within subsystems are not equiprobable events because the actual failure histories for each element were used in the analyses). Because any one subsystem failure will cause a DCC outage, the failure events are joined by OR gates at the top level. This fault tree was used as the basis for the probability calculations that follow.

DCC Availability

The FAA supportability review provided the number of failures and total down time by element for each quarter. These data were used to compute the mean time between maintenance (MTBM) and mean down time (MDT) for each element using Formulas 1 and 2:

$$MTBM = \frac{operational\ hours}{number\ of\ failures} \qquad [1]$$

$$MDT = \frac{total\ down\ time}{number\ of\ failures} \qquad [2]$$

MTBM and MDT were used to calculate availability using Formula 3:

$$Availability = \frac{MTBM}{MTBM\ -t\ MDT} \qquad [3]$$

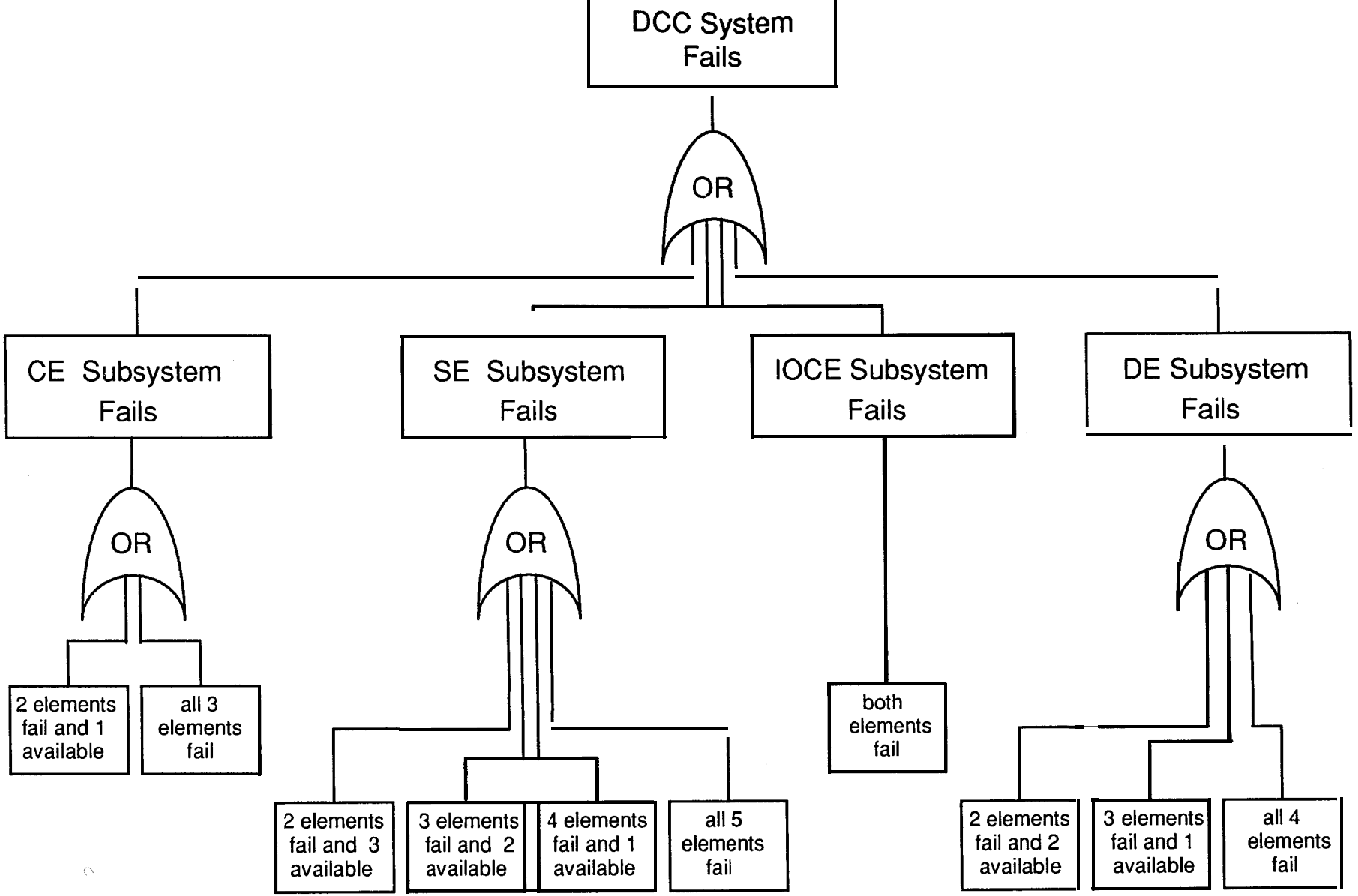


Figure A1: DCC system fault tree. (Note: Element failures within subsystems are not equiprobable events.)

For example, the FAA supportability review provided the information in Table Al for the computing element subsystem at the Chicago ARTCC for the third quarter of 1990.

Table Al: Total down time in hours and number of failures for DCC Computing Elements at the Chicago ARTCC during the third quarter 1990.

Performance measure	CE_1	CE_2	CE_3
Down Time	26.11	4.25	38.15
Failures	10	1	2

The Safety Board used Formulas 1, 2, and 3 and the data in Table Al to compute the data in Table A2.

Table A2: Mean time between maintenance, mean down time, and availability for DCC Computing Elements at the Chicago ARTCC during the third quarter 1990.

Performance measure	CE_1	CE_2	CE_3
MTBM	216.39	2185.75	1075.93
MDT	2.61	4.25	19.08
Availability	0.9881	0.9981	0.9826

In subsequent calculations, availability is treated as the probability that an element was functioning during the quarter. For example, the availability of CE_1 during the quarter was 0.9881, which can also be written as P(CE_1 available)=0.9881. The probability that the element failed during the quarter, P(CE_1 fails), is [1- P(CE_1 available)], so the probability of failure of that element was .0119.

According to the fault tree in Figure Al, for the computing element subsystem to fail, either two of the elements must fail or all three must fail. These events can be restated as equations:

El = CE_1 fails AND CE_2 fails AND CE_3 available,

Ez = CE_1 fails AND CE_2 available AND CE_3 fails,

Es = CE_1 available AND CE_2 fails AND CE_3 fails,

E4 = CE_1 fails AND CE_2 fails AND CE_3 fails,

Each of these four events can be written as a probability equation. Because element failures are independent, multiplication may be substituted for the ANDs. For example, E_1 can be restated as:

$$P(E_1) = P(CE_1 \text{ fails}) \text{ AND } P(CE_2 \text{ fails}) \text{ AND } P(CE_3 \text{ available})$$

$$= .0119 \times .0019 \times .9826$$

$$= .0000222$$

Similar calculations were made for each of the four events.[1] Because these events are mutually exclusive, addition can be used to determine the probability of any one of these events occurring during the quarter:

$$P(\text{CE fails}) = P(E_1) \text{ OR } P(E_2) \text{ OR } P(E_3) \text{ OR } P(E_4)$$

$$= .0000222 + .0002067 + .0000327 + .0000004$$

$$= .0002620$$

Similar computations were made for each of the other subsystems, and the failure probabilities were as follows: P(SE fails) = .0000075, P(IOCE fails) = .00004901, and P(DE fails)= .0012838. These data can be used to calculate the overall DCC availability:

$$P(\text{DCC available}) = P(\text{CE available}) \times P(\text{SE available}) \times P(\text{IOCE available}) \times P(\text{DE available})$$

$$= [1-P(\text{CE fails})] \times [1-P(\text{SE fails})] \times [1-P(\text{IOCE fails})] \times [1-P(\text{DE fails})]$$

$$= .99973800 \times .99999250 \times .99995099 \times .99871622$$

$$= .99839813$$

$$\cong .9984$$

Similar calculations were made for each quarter for each facility. The results of these calculations are presented in Table A3.

[1] Probabilities for three or more elements failing simultaneously had no effect on the final calculations, so they were omitted from the Safety Board's analysis for computational simplicity. Such events are shown in this appendix for completeness.

Table A3—Avai1ability of the DCC system by facility, 1990-1994

Quarter	Chicago	Cleveland	Fort Worth	New York	Washington
Q3, 1990	0.9984	0.9998	0.9925	0.9944	0.9999
Q4, 1990	0.9998	0.9997	0.9984	0.9998	1.000
Ql, 1991	1.0000	0.9999	0.9985	1.0000	0.9999
Q2, 1991	0.9987	0.9996	0.9994	1.0000	1.000
Q3, 1991	0.9999	0.9984	0.9952	0.9992	1.000
Q4, 1991	1.000	0.9983	0.9977	1.000	1.000
Ql, 1992	1.000	0.9976	0.9976	1.000	0.9999
Q2, 1992	1.000	1.000	0.9963	0.9989	1.000
Q3, 1992	0.9998	0.9999	0.9976	1.000	1.000
Q4, 1992	1.000	0.9993	0.9914	0.9961	0.9997
Ql, 1993	0.9945	0.9996	0.9862	0.9991	0.9997
Q2, 1993	0.9997	0.9999	0.9999	0.9975	0.9999
Q3, 1993	1.000	0.9999	0.9993	0.9950	0.9999
Q4, 1993	0.9940	0.9998	0.9929	0.9970	1.000
Ql, 1994	1.000	1.000	1.000	1.000	1.000
Q2, 1994	0.9925	0.9991	0.9992	0.9974	0.9996
Q3, 1994	1.000	0.9999	0.9959	0.9993	0.9994
Q4, 1994	0.9997	0.9999	0.9951	0.9942	1.000

DCC Availability at Full Redundancy

Computing the DCC availability at full redundancy is quite simple. A DCC system is available at full redundancy if each of the elements of its critical subsystems is available. The probability that a DCC system is available with full redundancy can be expressed as follows:

$$P(\text{DCC fully redundant}) = P(\text{CE fully redundant}) \text{ AND } P(\text{SE fully redundant}) \text{ AND } P(\text{IOCE fully redundant}) \text{ AND } P(\text{DE fully redundant})$$

$$= P(CE_1 \text{ available}) \times P(CE_2 \text{ available}) \times P(CE_3 \text{ available}) \times P(SE_l \text{ available}) \times P(SE_2 \text{ available}) \times P(SE_3 \text{ available}) \times P(SE_4 \text{ available}) \times P(SE_5 \text{ available}) \times P(IOCE_1 \text{ available}) \times P(IOCE_2 \text{ available}) \times P(DE_1 \text{ available}) \times P(DEZ \text{ available}) \times P(DE3 \text{ available}) \times P(DE_4 \text{ available})$$

Calculations such as these were made for each quarter for each facility. The results of these calculations are presented in Table A4.

Table A4—Availability of the DCC system at full redundancy by facility, 1990-1994.

Quarter	Chicago	Cleveland	Fort Worth	New York	Washington
Q3, 1990	0.8642	0.9463	0.7380	0.7976	0.8961
Q4, 1990	0.9400	0.9229	0.8346	0.9699	0.9525
Ql, 1991	0.9700	0.9651	0.8951	0.9774	0.9602
Q2, 1991	0.9223	0.9381	0.8930	0.9645	0.9869
Q3, 1991	0.9487	0.7926	0.7800	0.6062	0.9935
Q4, 1991	0.8972	0.7373	0.8171	0.9641	0.9865
Ql, 1992	0.9877	0.8265	0.8899	0.9349	0.9403
Q2, 1992	0.9720	0.9716	0.8059	0.1143	0.9845
Q3, 1992	0.9413	0.9384	0.6984	0.9563	0.9768
Q4, 1992	0.9591	0.9356	0.6566	0.3769	0.940.9
Ql, 1993	0.7373	0.9324	0.6628	0.8258	0.8794
Q2, 1993	0.9361	0.9744	0.9294	0.0000	0.9548
Q3, 1993	0.8143	0.9537	0.9011	0.7636	0.9708
Q4, 1993	0.6185	0.9646	0.7397	0.7846	0.9552
Ql, 1994	0.4942	0.9739	0.9458	0.6636	0.9086
Q2, 1994	0.7521	0.8741	0.8257	0.7916	0.8480
Q3, 1994	0.9608	0.9504	0.6955	0.9177	0.9190
Q4, 1994	0.9526	0.9670	0.7996	0.7738	0.9520