

PHILADELPHIA ENQUIRER  
19 June 1970

TO: CS&E BOARD MEMBERS

FROM: WARREN C. HOUSE

# Schools Seek Aid to Improve Reading Skills

By JOHN P. CORR

*Inquirer Education Writer*

The public school system here is preparing to enter into "performance contracts" under which private firms will take over reading instruction in the schools and guarantee results.

The firms will not be paid for their services unless children progress as far as guaranteed each school year.

Although eight firms have submitted proposals, the one most likely to go into effect first — probably in September — costs \$40 per pupil.

### STANDARDS LISTED

The firm, Behavioral Research Laboratories of New York City, will receive no money, however, for any child who does not:

—Achieve at least a one-year advance in reading scores on standardized tests every year.

—Read at grade level — according to national norms approved by the school system — by the end of three years.

It is expected that about 20,000 children — all of them doing poorly in reading — will be included in the first program. Included will be children in kindergarten through grade six.

### FURTHER BEHIND

Now, the average child in the public schools here is a year and a half below national norms in reading. There are thought to be thousands at all grade levels who do not read at all.

Here, children in the public schools — according to standardized tests — fall further behind in reading the longer they stay in school.

The Board of Education, it was learned, soon will adopt minimum reading achievement standards for the school system. The action may come at Monday's regular meeting.

District superintendents of the city's eight school districts have been presented with the proposals of the eight private firms. In addition, seven other proposals for reading programs have been submitted to them by the system's curriculum office.

The district superintendents are expected to adopt one of the 15 proposals or to put forward his own plan for achieving the minimum achievement standards set by the Board of Education.

### SOLUTION UNTRIED

However, if the school system undertakes the contract being offered by Behavioral Research Laboratories and if BRL can fulfill its guarantees — contracts with private firms may be a real breakthrough throughout the system in a short time.

No American urban center has yet tried out the private contract solution to the pervasive problem of the failure of public schools in the big cities to educate poor children of all races and backgrounds.

Last September, Texarkana

— the city on the Texas-Arkansas border — entered into a similar performance contract with Dorset Educational Corporation, a small Midwest firm. Final testing has not been done yet, but optimism and enthusiasm are high.

The materials and methods of BRL have been tested successfully in some 70 American cities. This is the first time, however, that the company has offered "no-strings" guarantee of progress.

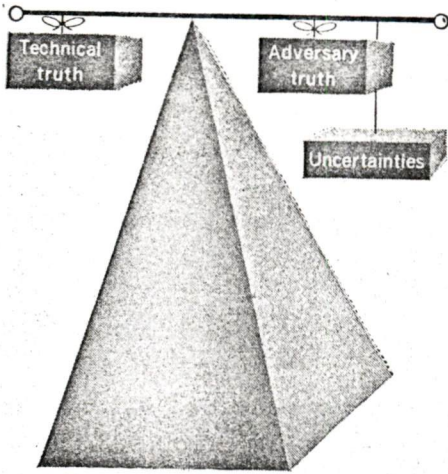
Under the proposal, BRL will provide all of the necessary books and materials, will train teachers and supply psychologists, consultants and program managers.

The company also will sponsor meetings to acquaint parents with its program.

The program takes the "linguistic" approach to reading instruction, concentrating on helping children to "break the code" and relate symbols to sounds.

from NAS  
CSSE

JUN 29 1970



## Engineering truth in competitive environments

*The success of decisions in both public affairs and industry depends today on the correct assessment of technical uncertainties. In an atmosphere of adversary confrontation, the efforts to hide them can prove the source of much harm*

**Raymond M. Wilmotte** *Management Consultant, Washington, D.C.*

The lack of understanding, analyzing, and communicating technological "uncertainties" are presented by the author as seriously undermining the effectiveness of decision-making in both public affairs and industry. Uncertainties are as important to truth as certainties and should be part of all forms of technical communication. "Technical truth," it is pointed out, is not developed in the legal process of adversary confrontation. On the other hand, "adversary truth," as presented by the contestants, is only part of the truth, for it excludes uncertainties, which are left to the perspicacity of the audience. In the well-publicized ABM controversy, the technical atmosphere had degenerated into that of an adversary confrontation, and technical truth with its uncertainties could not emerge. This basic and typical deficiency of the ABM controversy is not limited to public affairs: it exists strongly in industry and takes its toll in reducing the quality of decision-making in inefficient operations and in unnecessary crises, all carrying a burden of cost. It appears that the damaging effects of inattention to technical uncertainties could be radically reduced under a carefully worked out and nurtured environment.

In a recent article in IEEE SPECTRUM (August 1969), the late Seymour Tilson gave an outstandingly competent reporting of a controversy of national importance involving technology. The reporting had a message that took the form of a question. It was stimulated by a statement that the Director of Research and Engineering of the Department of Defense, Dr. John Foster, made in the midst of the controversy. "I want to point out," he said, "that one does not obtain a meaningful technical judgment by taking a vote of the scientific community, or even of Nobel Laureates." "How then," asked Seymour Tilson, "does one obtain a meaningful technical judgment?"

### A lesson from the ABM debate

This statement and question were made in the context of the ABM controversy, a controversy that split the Senate almost exactly 50:50—a split undoubtedly largely political, but affected also by the fact that the technical discussion left the Senate and the public better informed about some of the mechanics and critical features of the ABM, but confused as to the conclusions that could be drawn.

Tilson's question opens up an area of importance, one that is particularly critical to the scientific community today, when society is beginning to question the pragmatic value of technology. But the more important aspect of this question, as will be shown, is its bearing on the management of technology—on the relationship between decision-makers of government and industry on the one hand and scientists and engineers on the other. The ABM controversy is an important incident that brings this larger problem to the fore.

What are the practical conditions that would enable scientists and engineers, individually or as a community, to give the public and the decision-makers technical information and advice that is reliable, fully truthful, and of practical use? What were the conditions in the ABM controversy, for example, that inhibited the scientific community from providing the advice that society could reasonably expect of it? The expertise was there, but the technical foundation that would have been helpful for decision-making was not provided. What conditions are favorable for allowing engineers—individually and as a community—to give the most effective service to society? How can these conditions be provided?

The present analysis leads to the conclusion that favorable conditions are rare, but in many cases—possibly in most—it may be practical to set up a routine that will develop more meaningful technical judgment than was possible in the ABM debate.

Scientists and engineers used to be thought of as rather special people, different from others. It was generally believed that what they said was likely to be free from personal bias, that they could be depended on to present a balanced picture, and that they would reach a conclusion through an objective analysis of the facts, not by selecting the facts that support a predetermined conclusion. Their candor in technical areas was viewed as very special. What made them appear special was the way their thinking was structured in the limited area of their technical expertise—an area in which they often could talk at length and objectively because here their human emotions and personal interests were assumed not to be operative.

Others, when asked to do so, certainly would be willing to raise their right hands and swear to the truth, the *whole* truth, and nothing but the truth . . . and then to take advantage of a few socially accepted deviations, such as withholding aspects of the truth that might be damaging to one side of an argument, or introducing expressive adjectives that might create a more desirable impression than the bare facts might warrant, or avoiding explanations that might clarify a point that they hoped would remain misunderstood. Scientists and engineers, though, were expected to do more than merely use sentences that were true in themselves; they had the reputation for wanting also to communicate what they thought was the whole truth—without equivocation, subterfuge, or guile. The whole truth clearly is not limited to what one knows and to one's opinions; it includes also the *uncertainties* about one's knowledge and experience, so far as one is aware of them.

### Two ways of seeking truth

Scientists have been accustomed in their work to question anything about which they were unsure. Whenever they could, they would seek to remove their uncertainties. When they could not, they were expected to state what the uncertainties were, thus giving full information to their audience and possibly leaving members of that audience to fathom questions left unanswered. This is the way in which science uncovers the secrets of nature. In broad terms, the constant questioning—the delving into uncertainties in a continuous and systematic way—may be said to be the scientific process. Some aspects of the process are routine to all scientists and engineers. In the measurement of a physical quantity, it would be unheard of for a professional to question the necessity of giving a number without qualifying it with the accuracy (the uncertainty) of the measurement.

The mental attitude of the individual who sees that there is a gap in the truth when uncertainties are not expressed is altogether different from the attitude attending the process of finding the truth by the legal process of adversary confrontation, for that method in effect eliminates the voluntary disclosure of uncertainties. Scientists are inherently unsympathetic with this legal process, at least on technical matters. They would question the integrity of an engineer who would swear that a power line produced a force on a hand-held steel reinforcing rod a few feet away, without explaining that the force was a small fraction of an ounce. But the client—possibly others too—would admire the lawyer who obtained a large settlement from a power company by arguing the existence of this force and withholding mention of its

size.\* In fact, the lawyer might have been considered delinquent in his responsibilities if he had brought out that the size of the force was negligible! To do so was the responsibility of the opposing lawyer.

As scientists and engineers have encountered more and more the value system that controls political life, their natural bent on technical matters has given way with increasing frequency as their emotions and personal interests have become more closely involved.

The success of scientists and engineers in the development of technology—the complexity of the systems they can put together, their ability to analyze complex operations into elementary parts from which one can begin to understand the whole—moves them into social prominence. Their advice is sought by Presidents. They have begun to express opinions on all kinds of subjects, asserting the same degree of authority that they rightfully use in areas where they are truly expert.

It is not surprising, therefore, that on some matters of great national import involving technology, one now finds scientists and engineers espousing opposite contentions. One finds them presenting well-organized arrays of technical facts and analyses mixed with overtones of political opinions, and opposing groups reaching contrary conclusions. The public, which has begun to believe it possible that technology is doing more harm than good, has watched these encounters and is coming to the conclusion that scientists and engineers are not special people after all. They are much like everyone else.

"Technical truth" should be seen to be different from the "adversary truth" presented in adversary confrontation. The former includes both the findings and the uncertainties, the latter only a set of findings. Just as a technical measurement is not complete without an analysis and statement on the probability of error, so a technical conclusion is not complete without an analysis and statement of its uncertainties. The fact that uncertainties of measurement can be expressed quantitatively does not relieve the scientist from the responsibility of listing and explaining his nonquantifiable uncertainties. The importance of recognizing the difference between technical and adversary truth, as we shall see, is not limited to the political arena but carries over into industrial life.

The scientific process in the ABM controversy had all the earmarks of endeavoring to establish the truth on technical matters by adversary confrontation, which, though possibly best for legal proceedings, does not work out in the technical arena. It did not work with the ABM. In this case, well-known scientists, men who could be relied upon to know and understand the technical intricacies of the problem, presented for all to hear very different conclusions, not only on what action should be taken but also on the technical analyses undergirding their recommendations. How could the audience that they were addressing decide which set of analyses and conclusions was the correct one? Scientists as a community failed to give the country what it could reasonably expect—a reliable foundation of technical conclusions on which politicians could build their decisions.

In the technical arena, the truth requires an overwhelming consensus of the scientific community. Unless the consensus is overwhelming—that is, unless there are extremely few reasonable scientists likely to disagree

\* The legal case outlined actually took place.

when presented with the facts, analyses, and uncertainties—the “technical truth” in the area under consideration has not been reached. Where technical conclusions differ, the development of technical truth requires an effort to examine the uncertainties that are the basis of the differences, to try to reduce the gap or devise ways for so doing.

It is to be noted that there is little depth to an agreement unless it includes agreement on the nature of uncertainties. This concept brings out a basic difference between the processes for developing technical truth and adversary truth. In a technical controversy, technical truth is reached when the two sides have convinced each other what the truth is. In adversary controversy, there is no effort to have the two sides agree as to what is the truth. The truth is established by the *audience* whom the participants are addressing—Congress, a judge, a jury, or the public. The decision of the audience becomes the truth.

### The importance of uncertainties

The quality of the truth obtained with adversary confrontation depends heavily on the ability of the audience to fill in the information or uncertainties known to or obtainable by the participants, but not provided by them.

The controversy over the ABM involved some technical and some political factors. There was a wide gap of disagreement in both. One can well understand the difficulty of bridging the gap on questions in which the scientific community has no particular competence—such as the probable Soviet reaction to the building of the ABM—and recognize the impossibility of carrying out tests or reliable analyses that would be helpful to bridge them. But it is more difficult to understand why there was a wide gap on technical matters. It could have been helpful, for instance, for the two sides not only to give their opinion on the estimated performance of a Soviet attack and of the ABM defense against it, but for them to have also included their uncertainties, the reliability of the assumptions, and the facts and analyses they used, in terms that would be broadly understood. These should have been an essential part of the engineering process. With them, a better understanding of the reasons for the differences in conclusions could have been developed. But in the environment that existed this simple approach seemed impossible.

What could have been done? Probably nothing, in the environment that was allowed to develop. Probably a lot, in a different environment requiring only a slight change in discipline. The change may require consistent effort but should become so routine as to take place almost unconsciously.

*No scientific or engineering study should be considered complete without an “uncertainty analysis.” No system or component is really understood by its designer until he has carried out such an analysis.*

Uncertainty analysis is an important part of the design process and needs to be applied not once in a while, but routinely. In the case of the ABM, it should have been possible to reduce drastically a number of critically important technical differences—the difference between 25 percent and 5 percent in the estimates of the number of our Minuteman missiles surviving the first Soviet attack; the difference between the estimates of 4:1 and 1:1 in the cost ratio of defense to attack; the difference between

“hardly effective” and “seriously confusing” in the evaluation of penetration aids. It may be difficult to reduce the range of reasonable uncertainty on the reliability of ABM, particularly its computer, and the human problem of operating the system for the first time on a few minutes’ notice after years of being on the alert, but even there one could hope that the wide range of disagreement could be reduced, or analyzed into its component reasons.

Why was it not possible for the scientists on either side of the controversy to develop their uncertainties and establish the reasons for the differences in their conclusions? The answer is that the environment was that of adversary confrontation and the scientists in the controversy followed its well-established pattern. The controversy could not lead to the “technical truth” because the parties were not trying to reach a conclusion, but to prove one. They were addressing the public and its representatives, the nontechnical decision-makers. In such an environment, one side cannot admit uncertainties unless the other side reciprocates. The result is that description of uncertainties is avoided wherever possible. The whole truth could not, therefore, be developed. There is little doubt, however, that if it were routinely considered that good engineering requires an uncertainty analysis covering assumptions, facts, analyses, and opinions, reasons for differences would be clarified and the differences greatly reduced.

### What the ABM controversy can teach industry

In industry, the truth developed is sometimes the technical truth, but more often—and at considerable expense—it is the adversary truth that prevails, with the customer or a superior as the “audience.”

One can generalize from the example of the ABM that whenever the purpose of a technical presentation is to “sell” rather than communicate something, and competition exists, the foundation for a process of adversary confrontation is established.

In industry, the selling environment comes from what might be termed the “think-positive syndrome.” Corporate management is constantly “selling” the corporate image to customers; divisional vice presidents sell their capability to corporate management; middle-management people sell their ideas to divisional vice presidents; engineering managers sell their competence to the program manager—and so on, each seeking recognition and avoiding being the bearer of bad news.

At each level, the conditions are ripe for adversary confrontation. “Think positive” is the advice stated or implied that travels from each level to the next lower one. That advice is often interpreted to mean “concentrate on positive things” even though the most positive thing to do may be to concentrate on negative things.

The syndrome inevitably tends to obscure uncertainties until they become visible as deficiencies, to let negative things develop until they reach crisis proportions, to make difficult the introduction and operation of managerial feedback loops, to undermine attempts at measuring performance; in sum, to postpone the discovery of trouble. In large programs, it tends to hide from the program manager the true condition of his program. Near its end, he is often faced with urgent and competing demands from his managers for additional funds and more time, and has quite an inadequate background of information on which to judge the relative

merits of the demands—and usually has no time to acquire more. He becomes the “audience” of an adversary confrontation.

### Effects of the think-positive syndrome

The generalized effect of the syndrome is to distort all managerial feedback loops in which it is manifested. It thus degrades decision-making processes, for they all depend in one way or another on feedback of information. The effectiveness of feedback depends on assessing accurately and communicating speedily changes in a situation, in order to check whether the operation conforms with the plan and what uncertainties arise in their development. The syndrome tends to degrade both the accuracy and the speed. It always delays information, often injects errors, and may even prevent entirely the establishment of a communication channel.

It would clearly be desirable for uncertainties to be brought into the open, not to overemphasize them but to bring them into proper balance with other information. They would help guide the progress of a program, show where timely support might prevent the development of serious problems, and provide major support to decision-making generally.\* Schedule and cost controls are essential, but they cannot be fully effective without better information of the true state of a program, the hurdles that it faces and may face, and a better estimate of its probable outcome than is currently possible.

The effect of the “think-positive” syndrome on a program or an operation may be answered by asking a few questions such as the following.

It is generally admitted that many problems originate at managerial interfaces. Why then are much effort and many charts devoted to detailing line-managerial responsibilities and practices and hardly any to interface responsibilities and practices? Why do routine audits of operations concentrate on the adequacy of line operation and gloss over interface operations? Why does communication of defective interface operation have to go up the line, across, and down on the other side, leading to delays and distortions rather than in the first instance by a *routine* straight-across path? Is it that the circuitous path helps “control” the natural flow of negative information, of uncertainties, in the operation?†

Operations across managerial interfaces are a good example of some of the effects of the think-positive syndrome. A short discussion with a lower-level manager in charge of an operating unit typically develops the

\* An important application of this principle is in the communication of the results of mathematical modeling or simulation modeling to a decision-maker. For him to make effective use of the model and its outputs he must understand its assumptions, approximations, and sensitivities; in other words, its uncertainties. Without this information, the model can lead him seriously astray.

† Sometimes acting in accordance with the rules of the think-positive syndrome may appear to benefit an individual or even to be necessary to maintain his status within an organization. In most cases, however—possibly in every case—this is an illusion. The benefit, when it exists, is usually temporary. In the long run, the syndrome inevitably causes damage, and he who can consistently overcome it will be recognized and will benefit from this recognition. It is important when acting contrary to the rules of the syndrome that uncertainties be brought out in a forthright manner, free from a sense of explaining a deficiency, but rather from the point of view of presenting a fact and, where appropriate, the corrective action that appears desirable. Understanding, recognizing, and acting to counteract the syndrome’s damaging effects will help channel personal goals and emotional reactions along steady and constructive lines rather than along temporary and damaging ones.

following information: He knows what his unit is expected to produce, and who receives his product. He knows the expected costs and schedules. He knows the areas that interface with his unit, but when there are many he may forget some as he lists them. He will also know what flows across the interfaces but he will miss some items as he talks about them. It may be difficult to know whether he has left out anything important. He has made no list, nor does he keep a record of what flows or what fails to flow across the boundaries of his unit, unless it is connected with some hardware inventory for which he is accountable. He keeps close track of his output, personnel, costs; quality nearly always takes secondary place. When asked about his principal problem areas—what gets in his way in seeking to meet his cost and schedule assignments—he gives clear answers with examples of recent experiences. His analysis of the causes of his problems nearly always leads to the operation of an adjacent unit that does not provide what he needs at the time that he needs it, or provides something that is deficient. He has always been able, he explains, to wangle something to overcome these problems. He is proud of his success in some particularly difficult situations and the compliments he received. He is clearly better at fighting fires than at preventing them. When conditions grow bad beyond his endurance, he brings the matter up at the weekly staff meeting, following which something sometimes happens, sometimes not. By investigating the other side of an interface that appears to give trouble, it is usually easy to find the true nature of a problem. Not infrequently, other problems are uncovered at the same time. In many cases, it is relatively simple for the managers on either side of an interface to agree to some simple routine reporting giving each side information on the flow across the interface and the deficiencies encountered. For instance, the manager of a manufacturing shop could advise production control on the number of times each week his production has been hampered by failure to provide the planned accumulation of parts and materials. This simple information developed on a *routine* basis will speak more clearly than many orders from above.

### Curing the think-positive syndrome

Another common example is that of a unit whose responsibility is to issue reports—statistics, perhaps. The unit generally endeavors to demonstrate its importance by expounding on the number of reports distributed and the managerial ranks on the distribution list. Seldom does the unit make an analysis of the “uncertainties” of its activity—how well are the users’ needs or wants served, and to what extent does the report provide for them information that is useful in a form that is convenient and takes up a minimum of time to use? What the reports were planned to do is often known; what they actually do and what they could do are seldom known, certainly hardly ever reported. It is usually simple and requires no great effort to have from time to time *personal* interviews with a sample of key users, to discuss the uncertainties of those who prepare the report and thus be able to reduce them (the uncertainties, that is!) to a minimum.

An interesting case involved an area that was under review in a wide search for the reasons for problems that were besetting a large program. The area made a

self-audit. It uncovered some 50 places of defective operations, 48 of which originated outside the boundaries of the area. The audit was thorough and quite accurate. The interesting feature of the episode was not the audit itself or the effort that followed to correct the specific symptoms uncovered, but the lack of interest in answering the basic questions: Why had these defects originating across the interfaces remained uncovered and why had not those who knew of their existence taken steps to help correct them and, if they had, why had they been unsuccessful? Was it the syndrome's inhibiting power?

The preceding are examples of simple cases generally applicable to junior managers. There are many such throughout a major operation. Relatively little effort is needed to introduce routine corrective feedback that can counteract many of the syndrome's effects at these levels. Similar conditions in more complex form exist at higher levels. The common basis for operational problems appears to be the unwritten but generally accepted law that the mention of uncertainties should be avoided as much and as long as possible. The reason for this law lies in the fact that much of our activities take place in an atmosphere of adversary confrontation.

There is little doubt that the think-positive syndrome is damaging and costly. As a start at developing a corrective trend, scientists and engineers should make it a routine on technical matters to include an uncertainty analysis, to expect one from their peers, and, if necessary, to demand it.

#### A concluding note

It seems appropriate to apply a modicum of uncertainty analysis to the previous discussion. What are the uncertainties associated with the stated and implied recommendations for industry? Most of the analysis in this article is subjective reasoning and therefore open to criticism by those with different subjective thinking. There is, to date, little experimental verification of the effectiveness of such recommendations. What there is, follows.

Concentration on interface operations in managerial audits has been found to be an effective technique for locating problems—the degree to which managers did or did not understand their true responsibilities, their place in the scheme of things, and the irrationalities of some of their behavioral patterns. It is also consistently true in corporations that uncertainties in engineering design, though known, are not systematically passed up the line or communicated across the interface to inspection or test. These uncertainties are manifested in a lack of knowledge of areas that could not be inspected and of parts that are not fully exercised in final test. There is plenty of knowledge and documentation of what tests and controls can do, but little of what they cannot do and what remains undone. Usually, for example, little information is available on why a test procedure has failed to give warning of a defect in design. The lack of information on this negative side makes it difficult to assess the relative values of different test procedures.

More complex situations occur in design engineering. It is not uncommon for a subsystem manager, for instance, to supervise and review the design of the components of his subsystem and yet not know the weak spots that are known or suspected by the component de-

signers. The subsystem manager usually knows that certain desirable analyses and tests had to be discarded because of limitations of budget or schedule, but generally he has only a vague idea of the uncertainties introduced by their omission. It is even less common for plans, procedures, and implementation of final testing—qualification and acceptance tests—to reflect the existence of these uncertainties. The systematic transmission of uncertainty information could be very helpful, first to the subsystem manager, then to the system manager and to the manager of testing, and thence to the program manager, not only to direct the program as it progresses but also to develop a deeper understanding of exactly what has been designed and produced under their direction. This flow of uncertainty information takes the managers beyond the performance of the elements of the system and of the system itself as the work progresses, giving them greater ability to make rational projections of what is likely to occur. It will generally permit corrective action before it is too late or excessively costly, and at the end it will give a more accurate sense of the degree of confidence that can be placed in the system—that its performance will be maintained, that it can be safely duplicated, and how it can be improved.

As yet, there has been no opportunity to apply broadly the concepts and principles outlined here. Will behavioral patterns prevent an effective application? The answer to this question is not known and represents an important uncertainty. A subjective judgment is that they will often be a serious impediment, but that effective application can be developed in a suitable environment.

The author wishes to express his appreciation for interesting and valuable suggestions made by the late Seymour Tilson during the preparation of this paper.

**Raymond M. Wilmotte** (F, L) received B.A., M.A., and Sc.D. degrees in engineering from Cambridge University (Corpus Christi College), England. On graduating, he joined the National Physical Laboratory, the British equivalent of the National Bureau of Standards, engaged in research on antennas. Arriving in the United States in 1929, he worked on blind landing techniques for the Aircraft Radio Corp., Boonton, N.J. In 1932, as consultant to the broadcasting industry, he designed, built, and proved out the first directional antenna in the regular broadcast band to protect the service area of a station from the interference of another cochannel station. He has continued consulting throughout his career, first in broadcasting and subsequently with the government through the Wilmotte Laboratory, with contracts on radar, proximity fuze, antenna, and communications R&D. He was one of the first to correlate wide-band signals optically using ultrasonics.

In 1958, Dr. Wilmotte joined the advanced military systems group of RCA and became program manager responsible for the development and production of the "Relay" spacecraft, the first NASA communications satellite. During recent years, he has been a consultant on special aspects of management to major electronics corporations, non-profit organizations, and government agencies. Dr. Wilmotte has recently coauthored a study that was published by the ASCE on technology and decisions in transportation, using the problem of airport access as an example. He has received the Bureau of Ordnance Development Award from the Navy Department for his efforts in W.W.II, published over 50 professional papers, and been awarded more than 40 patents.



# Liberal Guidelines Proposed for CATV

TO ALL BOARD MEMBERS

FROM: W. C. House

By Robert J. Samuelson  
Washington Post Staff Writer

The Federal Communications Commission yesterday laid down the broad guidelines for the national regulations of cable television (CATV).

In a series of documents, the FCC formally:

- Proposed that cable systems — which transmit programs directly into subscribers' homes—be permitted to carry signals from four stations in addition to local stations.

- Prohibited television stations from owning cable systems in the same locality. Networks were also excluded from controlling CATV systems.

- Proposed that newspapers and radio stations also be barred from owning cable systems in the same area.

- Set April 1, 1971 as the date when cable systems with more than 3,500 customers must begin originating their own programs—instead of merely retransmitting either local or distant television programs via cable.

The CATV package also contained a proposal for providing permanent, long-term financing for educational television by assessing a 5 per cent annual levy on the gross revenues of cable systems. The money would go to the Corporation for Public Broadcasting, and, for every 10 million CATV subscribers, the FCC estimated, the CPB would receive \$30 million.

At the end of 1970 there were about 2,400 CATV systems, covering 4.5 million households, or about 7 per cent of the total U.S. television audience, according to the National Cable Television Association.

Nevertheless, the FCC's proposals—if and when they are finally adopted—could spur the growth of the industry and make it a major competitor of the existing over-the-air broadcasting system.

The key issue in the FCC's proposals is regarded as the authority for CATV systems to add "distant" television sig-

nals to the local programs already offered customers.

By adding these programs, the CATV systems theoretically should be able to attract more customers, who pay an average of \$5 a month for receiving the cable service.

With CATV households having a choice between local and "distant" programs (a Chicago station being shown over a Washington cable system, for example), local over-the-air broadcasters fear that their audiences will decline.

In the past, the FCC has been sympathetic to this position.

The agency now appears ready to make a quick reversal in its policy. It has called for comments on its "distant importation" proposal within 90 days and for reply comments 45 days after that; a final decision appears possible this year.

Other proposals will be handled on a more leisurely schedule, but yesterday's one final order—regarding CATV ownership—could have a wrenching effect on the fledgling industry.

In that order, television networks are given three years to dispose of any existing cable properties they own; both the Columbia Broadcasting System and the National Broadcasting Company have purchased CATV system as an apparent hedge against a decline in the value of over-the-air stations.

Moreover, according to the latest figures, television broadcasters have interests in 38.7 per cent of all existing CATV systems. The station owners, too, would have three years to eliminate conflicting holdings of cable and television properties in the same area.

Yesterday's FCC announcements also included a proposal to limit franchise fees imposed by the local governments to 2 per cent of a CATV system's gross revenues—a recommendation that is almost certain to be opposed by cities in search of new sources of funds.

The Commission's proposals on distant signal importation

could not take effect until Congress passed copyright legislation, giving copyright owners (such as movie studios) payments for programs snatched from the air by cable systems. Such a bill is now pending in the Senate.

The FCC suggested a copyright fee of .7 per cent (of gross revenues) for each additional "distant signal" used by a CATV system. If that formula were to be adopted by Congress, cable owners would face a 10 per cent charge on their incomes for various fees.

The breakdown is as follows:

5 per cent for educational television; 2 per cent for local franchise fees; 2.8 per cent for distant signals (four distant signals at .7 per cent for each one).

## Retail Sales Rise 4% During Week

Retail store sales rose sharply last week, up 4 per cent from the previous week and up seven per cent from a year earlier, the Commerce Department reported yesterday.

The year-to-year gain exceeded the 3 per cent average increase retail sales have been posting in 1970. Sales last week totaled \$7,370,000,000.

Durable goods sales were up 3 per cent at \$2,430,000,000, while over the past four weeks sales have suffered an average decline of 1 per cent.

During the four most recent weeks, sales of non-durable goods totaled \$4,950,000,000, 9 per cent ahead of a year earlier and exceeding the 5 per cent average rise in the past four weeks.

The largest year-to-year gains were the 18 per cent registered by department stores and the 16 per cent in the apparel group. Automotive sales were only 1 per cent above a year earlier.

The figures aren't adjusted for seasonal variation.

### Art Gallery Sells Computers As Art

The same company that recently auctioned the Cartier diamond and a Van Gogh masterpiece will put computer hardware on the block July 30.

The Parke-Bennet Galleries of New York, the nation's largest fine arts auction house, will put to bid items ranging from second and third generation computers and their associated components to simple card-handling equipment.

"People who own computers treat them with as much reverence as a work of art," said Joseph Kirby, the man who originated the idea.

26 June 1970

JUN 29 1970

TO ALL BOARD MEMBERS

FROM: W. C. House

## Judge Stays Army From Trying Sergeant in Mylai Massacre Case

By Bruce Galphin  
Washington Post Staff Writer

ATLANTA, June 25—U.S. District Judge Newell Edenfield temporarily restrained the Army from trying a sergeant on Mylai massacre charges after defense attorneys submitted 15 complaints, including an allegation that the Vietnam war is illegal.

It was the first time that the Mylai incident has come before a civilian court, and it was believed the first time a civilian court had enjoined a military court-martial.

Judge Edenfield issued a temporary restraining order and set a July 2 hearing on the petition of Sgt. Esequiel Torres, stationed at Ft. McPherson pending prosecution on two counts of murder and one of assault with intent to murder.

Torres' petition includes several of the defenses raised by Lt. William L. Calley Jr.'s attorneys, including the contention that President Nixon's remarks about Mylai, in effect, put pressure on courts-martial to bring in guilty verdicts.

But it was the first time in the Mylai cases that it was alleged court-martial proceedings in capital cases are illegal because the nation is not legally in a state of war.

Torres' petition also levels an attack on the court-martial

system itself, alleging that a commanding officer who already has determined that a soldier should be placed on trial chooses the court that tries him, thus violating the Fifth Amendment's due process guarantees.

Most of the points in Torres' complaint, if sustained, would bar prosecution of any of the defendants accused in the Mylai incident.

Torres was formally charged only today. Pvt. Gerald A. Smith, like Torres a member of Capt. Ernest Medina's rifle company, also was charged today with murder in connection with the March 16, 1968, incident.

Torres, a 22-year-old Texan with a heavy Latin accent, is living at Ft. McPherson with his wife and 10-month-old son. Sitting ramrod-erect, he attended a news conference this afternoon at which his attorney, former Rep. Charles Weltner, (D-Ga.), did most of the talking.

"I'm not guilty. I didn't commit no crime," Torres said.

Weltner alleged a general lack of jurisdiction for the Army to try Torres for actions in Vietnam because Congress had not declared war and the Army thus lacked authority to order him into combat.

Except "in time of war or public danger," according to

the Fifth Amendment, no person may be tried for a capital crime "unless on a presentment or indictment of a grand jury." This section, Weltner contended, overrules a court-martial.



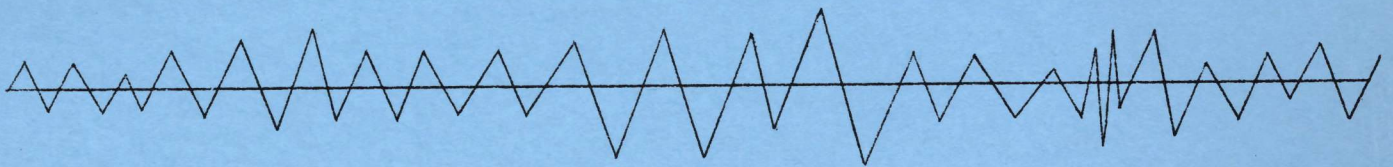
file

NAS

JUL 6 1970

*A Technical Analysis*  
*of*  
The Common Carrier/User  
Interconnections Area

*A Report of the*  
PANEL ON COMMON CARRIER/USER INTERCONNECTIONS  
COMPUTER SCIENCE AND ENGINEERING BOARD  
NATIONAL ACADEMY OF SCIENCES



To the  
Common Carrier Bureau  
Federal Communications Commission  
Washington, D. C.  
June 1970

*A Technical Analysis*  
*of*

The Common Carrier/User  
Interconnections Area

A Technical Analysis  
of  
THE COMMON CARRIER/USER INTERCONNECTIONS AREA

A Report of the  
PANEL ON COMMON CARRIER/USER INTERCONNECTIONS  
COMPUTER SCIENCE AND ENGINEERING BOARD  
NATIONAL ACADEMY OF SCIENCES

to the  
Common Carrier Bureau  
Federal Communications Commission  
Washington, D. C.

June 1970

FEDERAL COMMUNICATIONS COMMISSION

COMMISSIONERS

Dean Burch, Chairman

Robert T. Bartley                      Robert Wells  
Robert E. Lee                            Nicholas Johnson  
Kenneth A. Cox                          H. Rex Lee

OFFICIALS

Max D. Paglin, Executive Director  
Ben F. Waple, Secretary  
Henry Geller, General Counsel  
William H. Watkins, Chief Engineer  
Donald J. Berkemeyer, Chairman, Review Board  
Arthur A. Gladstone, Chief, Office of Hearing Examiners  
Leonidas P. B. Emerson, Chief, Office of Opinions and Review  
Leonard Weinles, Chief, Office of Information  
Sol Schildhause, Chief, CATV Bureau  
Bernard Strassburg, Chief, Common Carrier Bureau  
George S. Smith, Chief, Broadcast Bureau  
James E. Barr, Chief, Safety and Special Radio Services Bureau  
Curtis B. Plummer, Chief, Field Engineering Bureau

TABLE OF CONTENTS

	Page
LETTER OF TRANSMITTAL TO FEDERAL COMMUNICATIONS COMMISSION . . . . .	i
LETTER OF TRANSMITTAL TO COMPUTER SCIENCE & ENGINEERING BOARD. . . . .	v
ABSTRACT . . . . .	vi
SECTIONS	
1 BACKGROUND, SUMMARY AND CONCLUSIONS . . . . .	1
2 COMMUNICATIONS BACKGROUND . . . . .	15
3 TRANSMISSION AND PROTECTION CONSIDERATION . . . . .	21
4 NETWORK CONTROL SIGNALING . . . . .	33
5 PROTECTIVE DEVICES. . . . .	40
6 CERTIFICATION PROGRAM . . . . .	48
7 INNOVATION. . . . .	57
8 APPLICABLE EXPERIENCE . . . . .	65
9 INFORMATION AND ORGANIZATION. . . . .	75

NATIONAL ACADEMY OF SCIENCES

2101 CONSTITUTION AVENUE

WASHINGTON, D. C., 20418

10 June 1970

HONORARY G. OETTINGER, CHAIRMAN  
COMPUTER SCIENCE & ENGINEERING BOARD  
IN COMPUTATION LABORATORY  
HARVARD UNIVERSITY  
CAMBRIDGE, MASSACHUSETTS 02138

Mr. Bernard Strassburg, Chief  
Common Carrier Bureau  
Federal Communications Commission  
Washington, D. C.

Dear Mr. Strassburg,

I take pleasure in submitting this report of the Computer Science and Engineering Board's Panel on Communications/Interconnection.

This Panel was asked to make an assessment of the technical factors affecting the common carrier/user interconnection area of public communications. It was asked to develop technical and background information that might be useful to the Commission, common carriers, users and equipment manufacturers in reaching and implementing solutions to immediate problems, including a technical evaluation of various contending points of view regarding the common carrier/user interconnection area, of the various problems to which these views relate and of the various technical and policy alternatives for responding to these problems in the near future.

You stated on September 25, 1969 that "the essential technical questions to be considered by the NAS Panel now appear to be (1) the propriety of the telephone company-provided network control signalling requirements and various alternatives to the provision thereof by the telephone company, (2) the necessity and characteristics of telephone company-provided connecting arrangements and various alternatives to the provision thereof by the telephone company, and (3) basic standards and specifications for interconnection and the appropriate method to administer them".

The Computer Science and Engineering Board selected Mr. Lewis Billig, Technical Director - Communications, The MITRE Corporation, Bedford, Mass. to chair the Panel. After extensive consultations to identify the most competent people available with the required technical specialties, Mr. Billig nominated the fourteen people listed following this letter for appointment by the Board.

10 June 1970

The Board hereby commends to you these principal technical findings of the study:

1. Uncontrolled interconnection to the common carrier network as it now exists would be harmful.
2. The requirements of the tariff criteria limiting characteristics of interconnected lines are technically based and in accord with the operational limits of the common carrier network as it now exists.
3. The nature of potential harm, criteria for protection against such harm and the performance of various components of the telephone system can be specified explicitly enough to be understood and acted upon properly by people with normal technical competencies.

Having found that harm of various kinds can occur and that technical limitations on interconnection are therefore necessary, the Panel studied protective measures. On the technical basis of the third set of findings, the study concluded that the following two approaches -- used either alone or in parallel in such proportions as non-technical factors might determine -- can supply the required degrees of protection for the network, including network control signalling:

1. Protective arrangements as required by the tariffs
2. A properly authorized program of standardization and properly enforced certification of equipment, installation, and maintenance.

Analysis of potential harm and protection capabilities revealed no technical reasons why innovation would be significantly restricted by either of the two approaches alone or in combination. The choice clearly impinges on economic and social problems and on questions of industrial structure which are beyond the purview of the study.

Sincerely yours,

Anthony G. Oettinger  
Chairman  
Computer Science and Engineering Board

AGO:chm

Computer Science and Engineering Board  
2101 Constitution Avenue  
Washington, D. C. 20540

PANEL

PANEL CHAIRMAN

Lewis S. Billig  
Technical Director  
Communications  
The MITRE Corporation  
Bedford, Mass. 01730

Raymond M. Alden  
Executive Vice President -  
Operations  
United Utilities, Inc.  
Kansas City, Missouri 64112

Ronald Enticknap  
Associate Group Leader  
M.I.T. Lincoln Laboratory  
Lexington, Mass. 02173

James D. Babcock  
Chairman of the Board  
Allen-Babcock Computing, Inc.  
Los Angeles, California 90067

Charles L. Hutchinson  
Hutchinson Associates  
Wilmington, Delaware 19809

Jack A. Baird  
Vice President  
Bell Telephone Laboratories, Inc.  
Holmdel, New Jersey 07733

Robert C. Karvatt  
Director of Communications Services  
Penn Central Company  
Philadelphia, Pennsylvania

Ralph L. Clark  
Associate Director  
International Communications  
Office of Telecommunications  
Policy  
Washington, D. C. 20504

Jordan Kassan  
President  
Dynelec Systems Corporation  
Glen Rock, New Jersey 07452

Charles H. Elmendorf  
Assistant Vice President  
American Telephone &  
Telegraph Company  
New York, New York 10007

Herman Lukoff  
Director of Research and  
Advanced Techniques  
Univac Division of Sperry-Rand  
Blue Bell, Pennsylvania 19422

Bernard Rider  
President  
American Communications Corp.  
Arlington, Virginia 22209

Elmer B. Shapiro  
Senior Research Engineer  
Stanford Research Institute  
Menlo Park, California 94025

PANEL AIDES

George W. Gilman  
Senior Consultant  
The MITRE Corporation  
Bedford, Mass. 01730

John L. Wheeler  
Engineering Manager  
Xerox Corporation  
Rochester, New York 14604

Harry S. White, Jr.  
Chairman, American National  
Standards Institute (ANSI)  
National Bureau of Standards  
Washington, D. C. 20234

Victor Evans  
Consultant  
Office of Telecommunications  
Policy  
Washington, D. C. 20504

NATIONAL ACADEMY OF SCIENCES

COMPUTER SCIENCE & ENGINEERING BOARD  
2101 CONSTITUTION AVENUE  
WASHINGTON, D. C. 20418

15 April 1970

Professor Anthony G. Oettinger  
Chairman  
Computer Science and Engineering Board  
National Academy of Sciences  
Washington, D. C. 20418

Dear Professor Oettinger:

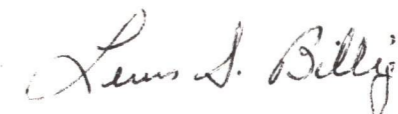
The Special Panel on the Common Carrier/Interconnection area of the Computer Science and Engineering Board was established to perform a technical analysis of certain factors in the common/carrier/user interconnections area in accordance with the terms of Contract No. RC-10091, dated 27 June 1969. It is a pleasure to transmit this report which represents the judgments of that Panel.

Both the timeliness of the report and its content reflect a high level of dedication and professional objectivity of the entire Panel throughout all phases of the study. The work of the Panel was possible only because of the cooperation of the many organizations and individuals in producing technical papers and presenting supplemental briefings which provided the basic information on which the Panel based its judgments. Many of the papers reflect special research undertaken in response to the request of the Panel for technical support. In addition to contributing to the report, the papers submitted constitute the bulk of the existing literature of the field for the common carrier/user interconnections area.

From the start, it was our aim to produce a report which reflected the best technical competence and experience available on the various aspects of this problem area. I believe that we have succeeded in this, and am pleased to commend this report to the Computer Science and Engineering Board.

This has been a rewarding experience for me, personally and professionally, and I believe the same is true for the members of the Panel.

Sincerely,



Lewis S. Billig  
Chairman  
Special Panel on  
Common Carrier/Interconnections

## ABSTRACT

This report represents the result of a study of the technical issues involved in the interconnection of user-owned terminal equipment to the regulated common carrier network. The pertinent characteristics of the network were analyzed to determine its susceptibility of harm to personnel, equipment, network performance, and degradation of service to other users. It was determined that such susceptibility does exist and that uncontrolled interconnection would indeed be harmful. The requirements of the tariff criteria limiting signal amplitude, waveform, and frequency distribution of interconnected lines were found to be in accord with the operational limits of the network and to be technically based. Several methods of protecting the network -- when interconnected to user-owned equipment -- from hazardous voltages, line unbalance, excessive signal levels, and improper network control signaling were investigated. The Panel concluded that the protective arrangements required by the tariffs can provide the basis for the required degree of protection. A properly-authorized program of standardization and enforced certification of equipment, installation and maintenance can be developed to provide the desired protection. The Panel concluded that innovation by carriers need not be significantly impeded by this program, while opportunities for innovation by users would be increased. The poor information exchange among carriers, users, and manufacturers has resulted in considerable misunderstanding and the Panel concludes that mechanisms are needed to address this problem.

## SECTION 1

### BACKGROUND, SUMMARY, AND CONCLUSIONS

#### BACKGROUND

The "Carterphone Decision" was widely recognized as potentially leading to a fundamental change in communications carrier/user relationships.

By this decision, the FCC ordered the American Telephone and Telegraph Company to delete general prohibitions against interconnection and customer attachments from its interstate message toll tariffs. In compliance, the AT&T, after consultation with representatives of the independent telephone companies, filed the following revised tariffs: #259 - "Wide Area Telecommunications Service"; #260 - "Private Line Service"; #263 - "Long Distance Message Telecommunications Service." These revised tariffs specify and define certain key limiting signal characteristics and "access arrangements" believed necessary by AT&T to protect telephone service and the telephone system, as well as those who come in contact with the system as employees or users.<sup>1</sup>

The FCC allowed these proposed tariffs to go into effect and requested comments from interested parties. It received a considerable number and range of responses. The technical portions of these responses ranged from complete acceptance, through challenges as to the basis of determination of the protection requirements, to complete rejection.

The FCC decided that a study should be made of the technical factors involving interconnection and user-provided attachments. The National Academy of Sciences, through its Computer Science and Engineering Board, agreed to undertake such a study.

The objective was to evaluate and report on the issues of "harm," and protection of the telephone network from "harm," under conditions of user-interconnection. The approach involved the following considerations:

- (a) Susceptibility of the network of "harm" in terms of hazards to personnel and equipment, network performance, and degradation of service to other users
- (b) Evaluation of the tariff criteria limiting signal amplitude, waveform, and frequency distribution of interconnected lines

---

<sup>1</sup>Section 3



- (c) Evaluation of the effectiveness of several methods of protecting the network
- (d) Evaluation of the impact of interconnection on innovation by carriers and user-manufacturers.

The charter of the Panel and the urgency of the problems of voice-band interconnection required that this report concentrate on the technical aspects of those problems, to the exclusion of other significant considerations involved in interconnection, such as:

- (a) Distribution of costs of interconnection among carriers, the general non-interconnected user, and the interconnected user
- (b) Reliability or adequacy of service obtained by a user from his own interconnected equipment
- (c) Effect on service when one party has carrier-provided equipment and the other party has his own interconnected equipment
- (d) Validity of the criteria for acoustic or inductive coupling

Final judgment by the FCC as to courses of action must, of course, include, in addition to the technical factors, such matters as rates, costs, legal implications, and basic economic policy. In this connection, it should be noted that future changes in costs or rates by the carriers for interconnection devices could have a significant impact on the interconnection situation.<sup>2</sup> This factor was not evaluated by the Panel. The principles that underlie the conclusions in this report may be applicable to other types and circumstances of interconnection.

Principal Conclusions

The principal conclusions arrived at by the Panel follow. Further detailed conclusions are included in the body of this section.

- (a) Uncontrolled interconnection can cause harm to personnel, network performance, and property.<sup>3</sup>

---

<sup>2</sup>Section 6

<sup>3</sup>Sections 3, 4, and 8

- (b) The signal criteria in tariffs 260 and 263 relating to signal amplitude, waveform, and spectrum are technically based and valid and, if exceeded, can cause harm by interfering with service to other users.
- (c) Present tariff criteria together with carrier-provided connecting arrangements are an acceptable basis for assuring protection.<sup>4</sup>
- (d) Present tariff criteria together with a properly authorized and enforced program of standards development, equipment certification, and controlled installation and maintenance are an acceptable basis for achieving direct user interconnection.<sup>5</sup>
- (e) Innovation by carriers need not be significantly impeded by a certification program. Opportunities for innovation by users would be increased.<sup>6</sup>
- (f) Mechanisms are needed to promote the exchange of information among carriers, users, and suppliers.<sup>7</sup>

STUDY PLAN

Organization

An initial analysis indicated that a broad range of experience should be represented in the membership of the Panel. The technical coverage included the following subjects:

- Switching Systems
- Transmission Systems
- Standards - Development and Use
- Equipment Manufacturing
- Privately Owned and Operated Communications Systems
- Communications-Oriented Computer Systems

---

<sup>4</sup>Section 5

<sup>5</sup>Sections 3, 4, and 5

<sup>6</sup>Section 7

<sup>7</sup>Section 9

Procedures

The Panel first reviewed the FCC files concerning interconnection and determined what additional data were necessary. Facts and opinions were accumulated from those who expressed their interest to the FCC and directly to the NAS Panel as a result of announcements, publicity, and direct solicitations. Organizations and individuals with knowledge of and experience in subjects of particular interest to the Panel were also contacted directly.<sup>8</sup> Among the organizations providing data were:

- Communication Common Carriers
- Telephone Equipment Manufacturers
- Computer Manufacturers
- Terminal Equipment Manufacturers
- Organizations with Private Communications Networks
- Regulatory Agencies
- U. S. Government Agencies
- Standards Agencies
- Foreign Communications Agencies
- Testing Laboratories
- Computer Service Organizations
- Installation and Service Organizations
- Trade Associations

In all, over fifty written technical communications were submitted, and over twenty-five organizational representatives, by Panel invitation, made supplemental oral presentations and responded to intensive questioning at closed panel sessions.

This study makes clear the need for improved communications between the carriers, users, manufacturers, and other members of the community in this field. On a number of occasions what were considered to be significant problems raised were apparently a matter of lack of, or poor, information.

EFFECTS OF INTERCONNECTION ON THE PERFORMANCE OF THE NETWORK

The objective of the Panel has been to determine how

<sup>8</sup>Section 8

interconnection can be achieved without impairment of service to users of the network, generally, and hazards to employees of the carriers. In its approach to this objective, the Panel has analyzed the appropriate portions of the carrier network to determine how harm can be caused and has then considered how this harm can be prevented.

Harmful Effects

Harm may arise through the introduction into the network of (a) voltages dangerous to human life, (b) signals of excessive amplitude or improper spectrum, (c) improper line balance, or (d) improper control signals.<sup>9</sup>

INCREASED EXPOSURE TO  
HAZARDOUS VOLTAGES CAN  
RESULT FROM UNCONTROLLED  
INTERCONNECTION<sup>10</sup>

Uncontrolled installation of user-owned terminal devices involving the use of 115 v AC and other hazardous voltages can introduce risks to telephone company installation and maintenance personnel. For maintenance and expansion of telephone service to be carried on without interruption of existing service, it is standard and efficient practice for cable and exchange plant workers to work bare-handed on pairs and junctions in the immediate proximity of hundreds of other pairs in normal use. To avoid increasing the hazard, it is mandatory that stringent measures be taken to ensure that hazardous voltages will not be applied at points of interconnection.

SIGNALS THAT VIOLATE THE  
CRITERIA RELATING TO SIGNAL  
AMPLITUDE, WAVEFORM, AND  
SPECTRUM IN TARIFFS 260 AND  
263 CAN CAUSE HARM BY INTER-  
FERING WITH SERVICE TO OTHER  
USERS<sup>11</sup>

<sup>9</sup>Section 2

<sup>10</sup>Section 3

<sup>11</sup>Section 3

The non-linear characteristics of transmission components, which are widely used in the telephone plant, require that inband signal power be limited to avoid deterioration of service to others due to cross-talk or overload. The signal-limiting characteristics of voice-frequency and carrier-transmission systems do not provide the required restraints on signal power. The signal powers specified in the tariffs represent reasonably optimized values for voice and data usage.

The limits on the inband signal-power spectrum are specified to avoid the possibility of interference with internal network signaling. The out-of-band power limits are based upon limitations of local cable plant and requirements for minimum interference with present and expected greater-than-voice-band services. The telephone plant does not supply this protection.

Signal criteria specified in the tariff must be observed for both voice and data services. Data services present the more serious problem, since, when transmitting data, the user has an incentive to exceed the signal-power criteria in order to reduce his error rate with possible degradation of service to others.

LINE BALANCE IS IMPORTANT  
TO NETWORK PERFORMANCE<sup>12</sup>

Imbalance in line terminations will render ineffective the careful electrical balance built into the pairs in the cables connecting users and the telephone company central offices. The resultant imbalances can cause loss of privacy and increased interference, not only to the unbalanced pair, but to other pairs in the cable as well. Terminal imbalance can occur due to poorly built equipment, improper installation, or inadequate maintenance.

IMPROPER NETWORK-CONTROL  
SIGNALING CAN IMPAIR TELE-  
PHONE SERVICE AND INCREASE  
COSTS<sup>13</sup>

<sup>12</sup>Sections 1 and 3

<sup>13</sup>Sections 1 and 4

Network-control signaling must be properly performed for correct system operation and message accounting. For example, in a telephone set, these signals are produced by the switchhook and the rotary dial or the touch-tone pad. Mechanisms for producing these signals, if not carefully designed, manufactured, installed, and maintained, can, in conjunction with the varying characteristics of the telephone loops, cause improper signals to be received at the central offices. Central offices vary in their tolerance to distorted control signals and in their ability to correct such signals before re-transmission into the network. In particular, dial-pulse signaling of poor quality can cause significant harm by the generation of wrong numbers, causing annoyance to others, wasteful use of central office equipment and transmission facilities, and improper billing. On the other hand, improper signals generated by touch-tone pads are inherently less harmful since, if a signal is out of tolerance, the central office equipment will not complete the call. Network-control signaling on multiparty lines is particularly difficult to define because of different practices with respect to ringing and line identification.

Protecting the Network

Several approaches for protecting the public telephone network were considered. Two which the Panel considers acceptable are:

- (a) Operation under present tariffs that call for common-carrier ownership, installation, and maintenance of connecting arrangements and adherence to tariff-specified signal criteria.
- (b) A program of enforced certification of equipment and personnel, with appropriate standards for safety and network protection. This approach would allow user ownership, installation, and maintenance of protective coupling units or complete terminal equipment.

PRESENT TARIFF CRITERIA AND  
CARRIER-PROVIDED CONNECTING  
ARRANGEMENTS ARE AN ACCEPT-  
ABLE WAY OF ASSURING NETWORK  
PROTECTION<sup>14</sup>

The present tariffs specify signal criteria for electrical, acoustic, and inductive coupling, and specify that the carrier provide

<sup>14</sup>Sections 3 and 5

connecting arrangements and network-control signaling. The signal criteria limit the signal inputs to the network to those considered to be harmless. The carriers, under the tariffs, assume responsibility for installation and maintenance of the connecting arrangements and for protection of carrier personnel and of the network itself. Technically, the Panel considers this to be an acceptable approach.

Carrier-provided connecting arrangements involve addition by the carrier of components between the user's terminal and the carrier's facilities. In some situations, these may duplicate components of the users' equipment; this redundancy in components and functions may, in principle, cause some loss in performance and some reduction in reliability. However, the Panel's analysis indicates that the added components, if well designed, should not significantly affect overall reliability or performance.

Concerning the need for some of the protective features, analyses of the presently available connecting arrangements indicate that they provide a degree of protection of voice-signal limiting that, in some cases, is unnecessary. Present carrier-provided coupling units are, in some instances, complicated and marginally effective and may degrade performance,<sup>15</sup> particularly in net-control signaling. According to AT&T, the problems relating to present protective equipment can be attributed to the rapid introduction of the connecting arrangements and lack of experience on which to base judgments. Further development should produce more effective units. Additionally, the sudden demand for interconnection and the need for time to determine the features required by a large number of users is a cause for present delays. Desired connecting arrangements are not yet available according to some users.

THE ESTABLISHMENT OF STANDARDS AND ENFORCED CERTIFICATION OF USER-SUPPLIED EQUIPMENT AND PERSONNEL CONSTITUTE AN ACCEPTABLE WAY OF ASSURING NETWORK PROTECTION<sup>16</sup>

It is important to note that the standards to be established cover only network-protection considerations such as personnel safety, signal levels, transmission, and network-control signaling, and do not include standards for user-equipment performance.

<sup>15</sup>Section 5

<sup>16</sup>Section 16

Despite some variability from installation to installation, there has been enough experience with the telephone network to provide a basis for standards for network protection. A standards-development program requires the resources of a qualified standards organization. The purpose here is to provide coordination, structural guidance, and staff services to those preparing the standards. Such organizations exist in both the private sector and government. Standards can be prepared by qualified representatives of the carriers, suppliers, and users. A definition of the interface between the user-owned equipment and the network, so far as protection is concerned, is part of the basis for standardization.

Finally, although general standards can be written to cover interconnection with various types of central offices and loops, each individual installation will be, to some extent, customized due to varying loop characteristics and other factors. Therefore, interconnected equipment should be provided with proper adjustment features to deal with individual case-by-case variations. Necessary adjustments can be worked out cooperatively at the time of installation between carrier and user. Cooperative guideline procedures should be formalized.

Type certification of equipment could be accomplished by government or by independent testing laboratories. It must include evaluating and monitoring each manufacturer and his specific products. Government and independent test laboratories exist which are capable of performing these functions in related fields. They could expand their resources to qualify for the program envisaged here. With a significant volume of work, costs of this program should not be prohibitive. Certification can be applied to couplers, to protective sections of larger equipment, or to the protective characteristics of entire units of equipment.

Equipment-type certification alone is not sufficient to protect the telephone network. The equipment must be installed and maintained by certified technicians. In addition, standards must make provisions for assurance that the network protection is maintained by documented periodic inspection.

Certification of the installation and maintenance of interconnected equipment will require a program of personnel training, development of tests and test equipment, and licensing of installation and maintenance personnel. On the last point, the Panel believes that a nucleus of support personnel exists in the servicemen and organizations who now install and service communications and computer equipment. They can be certified (or licensed) by examination, following procedures included in the overall certification program. Each certification (or license) would be endorsed as applicable to equipment of one or more classes.

Requirements for an Enforced Certification Program

AUTHORITY FOR A NATION-  
WIDE CERTIFICATION PRO-  
GRAM MUST RESIDE WITH  
THE FEDERAL AGENCY  
RESPONSIBLE FOR THE  
TARIFFS<sup>17</sup>

To be effective, a certification program must be recognized in the tariffs and the federal agency that approves these tariffs must assume responsibility for authorizing implementation of the overall certification program. This agency should develop and publish rules and procedures and propose timetables and sequence of applications.

Plans should be developed under control of the federal agency for the selection of the organization or organizations that will coordinate the preparation of standards, the procedures for the qualification of technicians, and the organizations to be given the authority to certify equipment.

Uniformity in standards and certification procedures for equipment and in personnel qualifications throughout the country is desirable, since installation and maintenance may be supervised and inspected locally. Therefore, coordination by federal and state agencies is necessary to establish policies which will permit the nationwide use of certified equipment and procedures for the certification of technicians.<sup>18</sup>

ENFORCED CERTIFICATION  
PROCEDURES MUST BE TAKEN  
AS A WHOLE

The Panel emphasizes that the development of standards and a program of certification requires a complete system of control, which will not be effective unless all elements of the system, as described in this report, are adopted. For example, the development of standards alone is inadequate. Certification of equipment without certification of installation, testing, and maintenance will be ineffective in protecting personnel, facilities, services, etc.

<sup>17</sup>Section 6

<sup>18</sup>Section 6

A CAREFULLY PLANNED  
STEP-BY-STEP EFFORT IS  
NECESSARY TO ENSURE THE  
SUCCESSFUL IMPLEMENTATION  
OF A CERTIFICATION PROGRAM<sup>19</sup>

Experience with interconnection is limited and has, for the most part, been with users with extensive experience and resources.<sup>20</sup> There is little applicable experience involving smaller, less sophisticated users or with large-scale public interconnection. A certification program is new to the telephone industry and to many of the major user industries.

Existing laboratories are not equipped to test and certify communications equipment in the quantities envisioned. The personnel needed by all parties for this kind of operation are in short supply.

There is much to be learned. If a start is made promptly, and if all concerned assign the task a high priority, the necessary certification programs and guidelines for qualifying personnel should be produced in reasonable time. The same effort should produce both standards for equipment and guidelines for qualifying personnel. Thereafter, when the personnel program has started to function, the certification of interface devices and equipment will permit their installation and operation by users according to the new standards.

The Panel believes that the certification program should be undertaken on an incremental basis in order to develop a meaningful base of knowledge and experience. The first implementation should be in an area with high probability of success and sufficient complexity to test the validity of the certification program. The first application should be to equipment with limited distribution and for which a knowledgeable technical base for manufacture, installation, and maintenance now exists (such as PBX). Application of the standards to one service can proceed while standards are set for others. Since the standards program is an iterative process, requiring procedures for continuous reconsideration and renegotiation of specifications, it is important that an organizational mechanism be set up to gather data and evaluate the progress of the program.

SELF-CERTIFICATION BY  
MANUFACTURERS OR USERS  
WILL NOT ENSURE AN ACCEPT-  
ABLE DEGREE OF NETWORK  
PROTECTION<sup>21</sup>

<sup>19</sup>Section 6

<sup>21</sup>Section 6

<sup>20</sup>Section 8

A self-certification program allows the manufacturer or user to test and approve his own equipment, installation, and maintenance. On the other hand, an enforced certification program separates the responsibility for certification from the organizations having direct financial involvement in the production or use of interconnected equipment.

Self-certification requires the user to procure and use equipment considered harmless and to operate in accordance with the tariffs. In the absence of some control system, it is inevitable that marginal equipment will make its way to the market and that there will be usage outside of the rules.

WE FIND NO PERSUASIVE ARGUMENTS FAVORING THE EXEMPTION OF WHOLE CLASSES OF USERS

The Panel endeavored to classify users, including utilities, right-of-way companies, agencies of the federal government, etc., in an effort to show that one or more classes might be permitted unrestricted interconnection without risk of impairment to the operation of the network. An analysis of information in the Applicable Experience section<sup>22</sup> and other information presented to the Panel led to a firm conclusion that this was not possible.

In a certification program that enables any user to qualify on reasonable terms, there is no reasonable basis, in the opinion of the Panel, for any class or group of users to be exempted from conforming.

EFFECTS OF INTERCONNECTION ON INNOVATION

THE PROPOSED CERTIFICATION PROGRAM SHOULD NOT SIGNIFICANTLY IMPEDE INNOVATION BY THE CARRIERS AND MAY PROMOTE INNOVATION BY USERS

Several opinions have been expressed to the Panel regarding the potential impact of interconnection on innovation.

<sup>22</sup>Section 8

The carriers have said that widespread interconnection will tend to impede innovation in the network, because, among other things, users will tend to oppose changes by the carriers that make the users' equipment obsolete or require it to be modified. They have also said that direct interconnection without carrier-owned interconnecting arrangement will further impede their innovation because it removes the carrier-controlled buffer with known characteristics between the network and the interconnected equipment.

Some users, especially the large ones and those in rapidly developing fields such as computer time-sharing, have expressed the opinion that, with the necessarily deliberate rate of innovation expected in the network, there will be no major problems in keeping up with the network innovation. They do not agree with the carriers' concerns regarding the need for a carrier-controlled buffer.

Some suppliers of equipment and services have expressed the opinion that the presence of the carrier-owned interconnecting arrangement will impede innovation on the user side of the interface where the goal is to optimize the users' system or use of equipment. Further, and perhaps more importantly, they question the ability of the carrier to respond rapidly enough to new situations in which new interconnection arrangements are required.

While data on which to base conclusions are limited, it is the opinion of the Panel that:

- (a) The advent of widespread interconnection itself, regardless of how it is implemented and controlled, will indeed have some effect on the rate of innovation by carriers, suppliers, and users. In some cases, it may impede innovation in the network; in others, it could conceivably promote innovation because of competition and the pressures of demand from users. It will certainly tend to increase the rate of innovation by suppliers and users.
- (b) The introduction of a certification program permitting direct interconnection should not significantly restrict carrier innovation if there is effective information exchange between carriers, suppliers, and users. On the other hand, the suppliers and users will have more freedom to innovate.
- (c) On balance, under the certification program, innovation in the overall system of carriers and users of interconnected equipment is likely to increase.

## INFORMATION INTERCHANGE

THE PANEL BELIEVES THAT MECHANISMS SHOULD BE ESTABLISHED TO PROMOTE THE EXCHANGE OF INFORMATION AMONG CARRIERS, USERS, AND SUPPLIERS<sup>23</sup>

As stated earlier, the Panel was continually reminded of the need for improved exchange of information among the parties concerned. There were instances of incorrect interpretations of conditions of use of the network by user and manufacturers, causing unnecessary confusion at both the technical and administrative levels. The carriers expressed strongly the need for more direct information exchange and a more comprehensive picture of user requirements. With the anticipated acceleration in innovation affecting data systems and telecommunications, the requirement for this improved exchange is even more pronounced. At present, no mechanism exists that adequately serves this function; such a mechanism should be established.

---

<sup>23</sup>Section 9

## SECTION 2

### COMMUNICATIONS BACKGROUND

#### TELEPHONE SYSTEM

In discussions of the interconnection situation, it is convenient to consider separately the exchange and long-distance parts of the telephone plant.

#### Exchange System

In its very simplest form this consists of a telephone, a "loop" to the central office, the automatic telephone exchange, and, perhaps, trunks running from the nearest central office either (a) to other central offices nearby; or (b) extending into the toll-telephone network.

#### The Telephone

The user interfaces with the telephone system at the telephone instrument. From the network-control viewpoint, the user performs as a highly adaptable logic and memory system that responds to incoming calls, initiates calls, and reacts reasonably predictably to a variety of situations encountered in using the telephone. The mechanisms he uses to exert this control in the simplest form of telephone are the switch hook and the dial. Lifting the handset closes electrical contacts in the switch hook to signal the central office. These switch-hook signals play an important role in subsequent operations. (One of them is establishing, for charging purposes, the times at which the call was initiated and terminated.) On receiving dial tone (which the user distinguishes from several other tones produced for his use), the user responds by operating the rotary dial or set of push buttons to correspond to the number he desires to reach, as read from the telephone directory or taken out of his memory (not always accurately). The user takes certain actions depending on whether, subsequently, he hears the voice of the wanted party, receives busy tone, continues to hear an unanswered audible ringing signal, reaches the wrong telephone, etc. At times he may hear a voice-recorded announcement and react accordingly, or he may reach an intercept operator with whom he converses. The user, in short, by manipulating the telephone instrument, plays a crucial role in the network-control signaling function of the telephone system. The telephone instrument, its controls, and the various signals from the system beyond the instrument to which the user responds are chosen in recognition of experience with the user's capabilities, limitations, and behavior patterns. The same is true of the quantity of switching equipment at the central office, which is chosen to fit traffic patterns as to calling frequency, duration of message, etc.

The various systems' solutions arrived at for the user/telephone combination at the point of access to the network may not necessarily be the same and certainly are not necessarily optimal where the combination is replaced in part or completely by machine or computer. Such a machine or computer, with or without interface devices, must reproduce most or all of the logical and memory operations now performed by the user. It may be conjectured that the machine is more accurate and more rapid, though not necessarily as versatile.

The primary function of the telephone instrument, of course, is to transmit and receive speech. The statistical distributions of levels and waveforms sent into the telephone system depend on the characteristics of both the user and the telephone instrument. The loops and long-distance trunks are designed to handle the range of levels encountered, without introducing crosstalk between pairs in multi-paired cable, or overloading the long-distance multiplexed system with its common amplifiers. To this end, there are limits both as to the output at the user station and the input to the trunks.

The telephone instrument is being used with increasing frequency to handle signals other than human voice, the telephone user's voice and ear being replaced by an acoustically or inductively coupled data set, cardiograph machine, facsimile machine, etc. Again, replacement of the user by a machine implies compromises. Specifically, the machine-generated signal levels and waveforms must be chosen to be both effective and non-interfering. This is accomplished in part by specification in the appropriate tariffs. In acoustic coupling, the signals are first converted to specified audible sounds and the telephone handset is fitted into a specified holder where these sounds are picked up. In inductive coupling, the electrical circuits within the handset pick up electromagnetic signals from the attached device. In both cases, the exact details of telephone-instrument design are important. Small changes in the telephone instrument may take obsolete acoustic and inductive coupling arrangements. Coordination between the designers of telephone instruments and the designers of acoustic and inductive couplers is required to avoid this.

A third function of the user's telephone installation is to protect the user, telephone employees, and the rest of the telephone system against harm. The telephone instrument and installation are insulated against contact with electric power sources. The telephone instrument contains a "click reducer" to eliminate the hazard of acoustic shock (a dangerously high level acoustic impulse to the listener's ear) etc. It is designed to maintain careful balance to ground on both sides of the telephone line, avoiding noise and cross-talk effects. It contains non-linear devices that limit energy levels, particularly on short loops to the central office.

Where the user telephone system is replaced by a machine, with or without interfacing equipment, the three basic functions of network control,

transmission, and protection must all be preserved.

Finally, these basic functions must be handled without mutual interference. Specifically, the network-control signaling function must be protected against interference from speech or other signals. As will be pointed out later, this consideration sets additional limits on the level and waveform of signals that can be transmitted throughout the system from the telephone.

#### The Loop

The "loop" connecting the telephone to the central office (or "trunk" connecting the PBX to the central office) is one of the major elements of total telephone-plant investment. The loop, for our purposes, includes the interior wiring in the users' premises, the "drop" from the premises to the point of attachment to the cable running to the central office, and a selected pair of wires in that cable, either assigned wholly for the use of a single user or shared with other users. Important characteristics of the loop are its length and the size of the copper conductors. Since a minimum of direct current, at least, must be drawn over these conductors to supply the microphone in the telephone and 20-cycle alternating current must be fed over them to ring the telephone bell, there are upper limits on length of loop and fineness of conductor gauge. Similarly, there are limits connected with the attenuation of voice signals, and the distortion to the direct-current signals used for switch-hook supervision and the detection at the central office of the fact that the called party has answered so that ringing may be "tripped." If considerations of limiting loop length and gauge are identical when the user/telephone subsystem is replaced by a machine, there need be no changes in loop design and layout. If not, some changes may eventually be indicated.

Loops and short-haul trunks are derived from copper-wire pairs in cables carrying several hundred or several thousand pairs. To hold cross talk between services carried over these pairs to a minimum, there must be strict control in cable manufacture to avoid structural imbalance. The effect of this careful control can be destroyed if improperly designed or improperly installed equipment is connected to the ends of the pairs. One of the basic requirements for any device connected to the telephone network, therefore, is that it not introduce imbalance<sup>1</sup> in impedance to ground from the two wires of the pair at the point of connection.

Cross talk (undesired coupling of signals from one channel to another) can also be created if excessively high signal levels are applied. To avoid cross talk from this source, limits are set on the output levels from the user station. Finally, cross talk in cables increases with

<sup>1</sup>Section 3



frequency. Since paired cables are used increasingly to handle communications involving higher frequencies (e.g., PICTUREPHONE), the limits on levels into these cables are set differently for frequency bands above the voice range.

#### Key Telephones and PBX's

Not all telephone instruments are connected directly to the central office over loops, particularly non-residence telephones for business, government, or professional use. In this case, additional switching systems are interposed between the telephone instrument (extension telephone) and the central office. These are manually operated key telephone systems and automatic (or sometimes manual) PBX's or PABX's (two acronyms for essentially the same thing). Some of these systems are of a size and complexity comparable to a telephone central office.

PBX's are sometimes, but not always, located on the user premises. In recent years there has been increasing use of Centrex service. In Centrex service, the PBX's switching may be done either on the customer's premises, or in the telephone central office. PBX extensions are reached directly by dialing from the telephone network (direct inward dialing). The telephone extension number becomes part of the nationwide numbering system. On outward calls from approved extensions, the called telephone is reached without the intervention of the PBX operator (direct outward dialing). The extension in some cases is identified automatically for billing purposes.

#### The Central Office

Dial central offices are of the step-by-step progressive-control type, or of the common control type (crossbar and most recently electronic switching). In a step-by-step office, the user more or less directly controls the switches in the central office when he operates the dial mechanism. Since these switches are mechanical devices with definite speed limitations, the dial-return mechanism is equipped with a speed governor, as a kind of buffer against an impatient user. In common-control offices, operation of the dial controls the condition of groups of relays or solid-state electronic circuits, which are made available for the user's sole use, when he gets a dial tone. These relay or electronic-circuit combinations then control the central office switches to set up the desired connection. In general, these latter arrangements are faster. In some cases this is taken advantage of by doubling the speed of the dial mechanism from 10 to 20 pulses per second.

Except for this, however, the same type of telephone instruments are used for all types of dial central offices. Push-button or Touch-Tone control will be referred to later.

#### Exchange and Toll Trunk Carrier Systems

Telephone switching offices are interconnected into a nationwide switching plan or hierarchy in which the local central office is at the lowest hierarchical level. The switching centers of the hierarchy are interconnected over short- and long-haul trunk circuits. These circuits are of voice-bandwidth (approximately 3,200 cycles) and handle two kinds of signals: 1) the message signal itself -- voice, data, etc.; and 2) the network control signals used in setting up and taking down connections, controlling switches, start of billing, and, in general, what is known as interoffice "handshaking," (exchange of call status information between switching offices by single-frequency [S.F.] signaling). It is important to good service that the message signals not produce false network-control signals. This can happen. For example, "talk-off" is a condition in which an unusual voice sound can be interpreted by the signaling equipment as an indication that the subscriber has hung up. When the system is used for other than voice, restrictions on energy level and waveform are imposed to avoid similar adverse effects. In certain trunk systems, a separate channel is used for network control-signals and these precautions are not required. The majority of trunks, however, use a single channel for both purposes. Restrictions on energy level and waveform are also required to avoid cross talk and noise among services sharing the same facilities.

Multi-channel carrier systems carry twelve to many thousands of voice channels through common amplifiers over paired cables, coaxial cables, microwave radio relay and (internationally) submarine cable and satellites. These common amplifiers can handle only limited signal power without overloading. The effect of overloading is to introduce noise and cross talk into many voice channels. The total available load capacity of the amplifiers are designed to be shared evenly by all the channels, whether they are handling voice or other communications. Specifications for individual channel loading have been established to be an optimum comprise between low levels where underlying system noises dominate and the higher levels where intermodulation noise and cross talk prevail.

#### Other Uses of the Telephone System

One of the uses of the telephone network for purposes other than switched message telephoning has been mentioned -- acoustic or inductive coupling to the telephone instrument for handling data, picture transmission, etc. This is only one of many non-telephone uses.

#### Private-Line Services

Uses of the telephone system fall into two broad categories: 1) private-line services, and 2) services provided on the switched network. Private-line channels may be terminated in either carrier-provided or customer-provided terminal equipment.

The loops and trunks of the telephone network have been made available to other services operated by large users of communications: Western Union, the railroads, large industries, government, etc. In some cases, these arrangements have involved interconnection between leased lines and equipment owned and maintained by the telephone companies, but operated by the user (for example, the 81-type teletype store-and-forward switching system). In other cases, Western Union for example, circuits only are provided -- the user attaches his own equipment.

#### Touch-Tone Services

There are over 1,000,000 telephone installations in which the rotary dial has been replaced by a 10- or 12-button "touch-tone" combination. The touch-tone signals, unlike the rotary-dial signals, can be used, not only to control the setting up of the connection, but also to transmit data once the connection has been set up.

### TRANSMISSION AND PROTECTION CONSIDERATIONS

#### INTRODUCTION

In this section we discuss the factors behind the carrier's tariff restrictions on the power and waveform of signals sent over the telephone networks (signal criteria),

THE PANEL HAS CONCLUDED THAT THE SIGNAL CRITERIA IN THE TARIFFS ARE REASONABLE. SIGNALS WHICH VIOLATE THESE CRITERIA CAN CAUSE HARM BY INTERFERING WITH SERVICE TO OTHER USERS

We discuss next the sources and effects of harmful voltages on personnel and plant, the exposures of the telephone system to these voltages, and the additional risks introduced by user-provided equipment.

THE PANEL CONCLUDES THAT INCREASED EXPOSURE TO HAZARDOUS VOLTAGES CAN RESULT FROM UNCONTROLLED INTERCONNECTION

Finally we discuss the subject of cross talk, and how this undesirable effect may be produced by unbalanced (to ground) attachments to telephone lines.

THE PANEL CONCLUDES THAT THE MAINTENANCE OF LINE BALANCE IS IMPORTANT TO GOOD SERVICE. LINE BALANCE CAN BE IMPAIRED IF POORLY DESIGNED OR IMPROPERLY INSTALLED AND MAINTAINED EQUIPMENT IS ATTACHED TO THE SYSTEM

The following paragraphs introduce the technical background appropriate to the later, more detailed discussion of signal criteria, protection criteria and line unbalance.

#### TECHNICAL FACTORS TO BE CONSIDERED IN THE INTERCONNECTION OF USER-OWNED TERMINALS TO THE PUBLIC NETWORK

The public telephone network has been engineered, on a statistical basis, to provide a variety of services to a large number of residential, commercial, military, and other users with different service requirements. The numbers and duration of the calls placed by these users cover a wide range.

Users are served by many types of telephone facilities at a range of distances from their serving central offices. The trunks that tie these offices into the long-distance portions of the network also vary statistically in type and length. Resultant ranges in transmission parameters of the loops and trunks produce variations in the overall end-to-end characteristics of switched connections through the network. The alternate routing of calls, which allows the automatic adjustment of traffic patterns to meet changing load requirements, can increase or decrease the number of links used in setting up successive calls between the same two locations. In short, both the service and the plant have been designed and can only be understood and treated on a statistical basis.

Because the numbers involved in telephone network are large, it is always possible to provide service to a small number of identified users whose requirements depart from the statistics in terms, for example, of the nature of signals to be transmitted. Special treatment might, for example, involve the selection of suitable pairs in local cables to minimize cross talk. It is clearly not economic, however, nor in some cases even possible, to provide special treatment to a very large portion of the total subscribers since the bulk of the service provided must match the capabilities of the bulk of the serving facilities. If, in addition, users whose signals depart from normal are not identifiable, there is no way to provide them with special treatment.

If the network is to accommodate large numbers of user-owned terminal equipment, it follows that signal amplitude, waveform, and energy distribution introduced by this equipment must continue to conform to the parameters used in the overall network design. Even a single user, whose signals are such as to cause cross talk or interference in multi-pair cable systems or cause overload in broadband carrier systems, can cause serious deterioration of service to a group of users.

#### Data and Voice

Motivation is one factor in the determination of the likelihood that generated signals will exceed the spectral power-handling capability of telephone facilities. Where voice transmission is involved, there is generally no motivation for exceeding design limits since the network components have been designed to accommodate the range of talker volumes and network links that will be experienced, with no advantage to excessive levels. In data communication, however, it is to the user's advantage to increase the signal-transmission level in order to improve his own error performance, albeit at the expense of degraded performance of other users. It is necessary, therefore, in this case to ensure that signals applied to the network do not exceed the transmission capabilities of the telephone facilities.

In addition to control of signal levels and waveforms, the interconnection of user-provided terminals involves other considerations. The first of these is the risk of voltages hazardous to personnel and to the network. The most important problem, of course, is the danger to telephone installation and maintenance personnel. Installation and maintenance must be carried on without interruption of existing service. It is the practice for cable and exchange plant workers to work barehanded on cable pairs and junctions in the immediate proximity of hundreds of other pairs and junctions in normal use.

There is potential hazard in this activity due to the adjacency of the telephone system to electric power systems. However, over the years the two systems have evolved effective measures to avoid injury. Similarly, effective measures must be evolved where there is interconnection of user-owned devices, to ensure that additional harmful voltages do not reach the telephone network from this source. Due to interconnection with the anticipated increase in user-owned terminal devices using 115 V AC and/or high DC voltages, the possibilities of harm due to poor initial design, improper installation, and/or inadequate maintenance are significant and must be faced in the interconnection of user-owned equipment.

Another situation in which service to other subscribers may be impaired is where the telephone line, normally well balanced, becomes unbalanced when a poorly designed, installed, or maintained device is attached to it.

Telephone cables are very carefully manufactured to minimize unwanted pickup of interference -- either from other telephone circuits or from nearby power systems. It is necessary to maintain this longitudinal balance at all times on all pairs. If this balance is degraded by some attached equipment, not only will interference be present on the unbalanced pair, but also other pairs in the same cable will be disturbed. Again, adequate provision must be made to ensure that user-owned terminals meet and maintain the longitudinal balance that is fundamental to maintaining the quality of network service, as do carrier-provided terminals.

Signal criteria, protection, and line balance are discussed in detail in the following paragraphs.

SIGNAL CRITERIA

The Panel has examined the basis of the signal criteria (as specified in the tariffs) that set limits on both "in-band" and "out-of-band" power. Criteria for in-band (below 3,995 Hz) signal-power levels are set to load the frequency-division multiplex carrier systems which furnish most long-haul voice-grade services, so as to optimize the signal-to-noise ratio for all users. The criteria for out-of-band signal-power levels are set to avoid interference to other pairs in the same cable, at frequencies above 3,995 Hz. Such cross talk between cable pairs increases at higher frequencies.

A third category of signal criteria sets limits on signal power in a specific region of the in-band range (2,450 to 2,750 Hz). These restrictions safeguard the operation of the 2,600 Hz in-band signaling system, which is almost universally used in long-distance telephone service. False operation of the in-band signaling system has serious results: improper billing, intermittent interruptions, insertion of a band-elimination filter in the transmission path, or even complete disconnection of a call.

As a part of this study, the Panel has examined the structure of the telephone-company plant and has determined that it does not provide protective mechanisms by either level limiters or filters to correct for signals exceeding criteria limits. We have also examined the operation of the telephone-company plant and have determined that the system is designed to operate in accordance with the criteria.

The derivations of the three classes of signal criteria, as set forth in the tariffs, are discussed under the following three subsections.

In-Band Signal-Power Criteria

The tariff requirements on in-band power<sup>1</sup> are as follows: FCC 259, FCC 263 -- the power of the signal at the central office not exceed 12 dB below one milliwatt when averaged over any three-second interval.<sup>2</sup> FCC 260 -- the power of the signal that may be applied by the user-provided equipment to the Telephone Company interface located on the user's premises

<sup>1</sup>In-Band power is defined as the total power in the band below 3,995 Hz.

<sup>2</sup>There is also a requirement that the signal applied to the loop plant not exceed 0dBm.

will be specified by the Telephone Company for each application to be consistent with the signal power allowed on the telecommunications network.

The above requirements on in-band power are based on interference considerations of long-haul<sup>3</sup> frequency division multiplex carrier systems. These systems include cable carrier systems with capacities ranging up to 3,600 channels and microwave radio carrier systems with up to 1,800 channel capacity. Virtually all voice-grade services longer than about 200 miles use these types of facilities.

These systems are designed to handle a per-channel load of -16dBm long-term average power measured at a network reference transmission level point. This -16dBm power is the maximum average power per 4kc channel that can be permitted without incurring a noise penalty (increase in total system noise power). Below the -16dBm per channel average signal power, the noise is predominantly thermal (or random) noise. In addition to this thermal noise (which is independent of total signal power), the broadband systems are also subject to intermodulation noise due to non-linearity of the carrier amplifiers. At these low levels, this increases with signal power and at the -16dBm average signal power per channel, the intermodulation noise and thermal noise are equal. At signal power above -16dBm, the noise is predominantly intermodulation noise, this increases at a faster rate than the signal power. Maximum signal-to-noise ratio is obtained with average signal power at -16dBm.

Since both directions of transmission normally are not used simultaneously and not all channels are active at the same time, it has been determined that an average power limit of -13dBm applied to all users of a system is consistent with the long-term loading objective of -16dBm. In developing the tariff criteria, this -13dBm three-second average power limit was translated to refer to a specific physically identifiable location. The selected location was the serving central office and the usual loss between this point and the equivalent network reference transmission level point is 1dB. Thus, the maximum signal power that may be permitted at the central office is -12dBm when measured over any three-second interval.

When this power level is exceeded, the effect on other users of voice and data services is increased noise and interference. Depending upon the nature and number of the excessive signals, this noise and interference may appear in the following forms:

- (a) Increased background noise or hiss on the channel
- (b) Crackling or static on the channel
- (c) Cross talk of other users' conversations into the channel. This cross talk may be either

<sup>3</sup>Section 2, p. 19.

intelligible or merely bursts of garbled speech

- (d) Increased error rates on data channels
- (e) Complete loss of service caused by catastrophic overload of line facilities

The network of long-distance facilities to which the in-band power criterion is applicable is used on almost all long-distance connections (over 200 miles in length). This network provides many diverse paths over which voice and data calls may be carried. Network-management techniques plus dynamic alternate routing plans vary the specific path (and specific broadband facility) that a particular point-to-point call will use. Similar changes in routing also occur on private-line services, particularly when a facility failure requires an alternate facility for service restoration. This need for facility flexibility necessitates that all channels be operated at equal signal levels. Hence, an equal apportionment of system power-handling capability to all channels is appropriate.

Out-of-Band Signal-Power Criteria

The tariff requirements on out-of-band<sup>4</sup> power are as follows: FCC 259, FCC 260, FCC 263 -- the signal that is applied by the customer-provided equipment to the Telephone Company interface located on the customer's premises meet the following limits:

- (a) The power in the band from 3,995 Hz to 4,005 Hz shall be at least 18dB below the stipulated maximum in-band signal power.
- (b) The power in the band from 4,000 Hz to 10,000 Hz shall not exceed 16dB below one milliwatt.
- (c) The power in the band from 10,000 Hz to 25,000 Hz shall not exceed 24dB below one milliwatt.
- (d) The power in the band from 25,000 Hz to 40,000 Hz shall not exceed 36dB below one milliwatt.
- (e) The power in the band above 40,000 Hz shall not exceed 50dB below one milliwatt.

<sup>4</sup>The out-of-band region is defined as those frequencies greater than 3,995 Hz.

Criterion (3,995-4,005 Hz)

The limitation on power in the band from 3,995 Hz to 4,005 Hz is based on potential interference in N3 carrier systems. This is an intermediate-range cable carrier system used to provide intercity circuits of 50 to 200 miles in length. By the end of 1968, there were almost 4,000,000 circuit miles of N3 carrier in the Bell System, which accounted for about 15 percent of all intercity circuits in the 50-200 mile distance range.

The interfering effect caused by power in excess of the criteria is a gain variation or flutter in another user's channel. In order to meet the overall system-flutter objective, it is necessary that the power of the interfering signal be 56dB below the power of the 4kHz carrier at the input to the carrier system's gain regulator. Based upon this requirement, the criterion for the 3,995 Hz to 4,005 Hz band is calculated as follows:

Spurious signal-to-carrier ration	-56dB
Carrier to maximum signal	+ 8dB
Average 4kHz suppression in channel filters	<u>+30dB</u>
Allowable 4kHz to in-band power ratio	<u>-18dB</u>

Criterion (4-10kHz)

The criterion for power in the band from 4,000 to 10,000 Hz is based on interference considerations in audio broadcast (radio and television) services. The most critical of these services, from a noise standpoint, is FM broadcast, which has an overall peak signal-to-noise requirement of 60dB. In order to meet this overall requirement, the studio-to-transmitter allocation of peak signal-to-noise is 65dB. Based on this signal-to-noise requirement and a peak transmitting level of +18dBm, the maximum channel noise permitted is -47dBm. Using this limit, the 4 to 10kHz criterion is calculated as follows:

Maximum noise	-47dBm
Correction for measuring techniques <sup>5</sup> and allowance for maintaining margin	-10dBm
Correction for multiple disturbers	- 3dB
System equalization	-25dB
Cross-talk coupling loss at 8kHz	<u>69dB</u>
Allowable 4 to 10kHz power on disturbing pair	<u>-16dBm</u>

<sup>5</sup>Broadcasters normally use nonweighted noise measurements and align their equipment at 400Hz, while the Telephone Company uses weighted noise measurements and aligns audio channels at 1,000 Hz.

The interference mechanism in the case of these channels is cable cross talk. The resulting user effect is noise or tones heard in the channel. Due to the large number of ultimate users affected by interference with audio broadcast services, it is very important to avoid such effects.

Criterion (10-25kHz)

The criterion for the 10 to 25kHz band is based on considerations of interference into the U1 carrier system, which uses the 14 to 22kHz band for transmission from the user to the central office.

The U1 subscriber carrier system is a relatively new system and is not widely used at present. However, looking ahead to increased copper costs and reduced electronic costs, it is expected that loop systems operating in this frequency range will likely be used to an increased extent.

To meet noise objectives for this system, the minimum carrier-to-interference ratio in this band is set at 75dB. Based upon this requirement, a maximum signal of 21dB below a milliwatt would be permissible on a single disturbing pair based upon cable cross-talk coupling characteristics alone. Because other noise and cross-talk sources can exist in a given cable, the criterion was set 3dB lower than the limit for a single disturbing source. This provides assurance that the system-noise objective will be met under most conditions. The criterion is computed, as follows:

Interference-to-carrier (18kHz) ratio for 15dBm noise at subscriber terminals	-75dB
Carrier level	-29dBm
Correction for multiple disturbers	- 3dB
Cross-talk coupling loss at 18kHz	<u>83dB</u>
Allowable 10-to-25kHz power on disturbing pair	<u>-24dBm</u>

Criterion (25-40kHz)

The criterion for the 25-to-40kHz band is also based on interference into the U1 carrier system. The U1 system uses the 26-to-34kHz band for transmission from the central office to the user.

The required carrier-to-interference ratio for this band is 77dB. To meet this requirement the criterion of 36dB below one milliwatt was established. It reflects consideration of both the increased cable cross-talk coupling and the greater transmission loss at these higher frequencies and also makes allowance for other noise and cross talk in the cable. The criterion is calculated as follows:

Interference-to-carrier (30kHz) ratio for 15dBm noise at subscriber terminals	-77dB
Carrier level	-34dBm
Correction for multiple disturbers	- 3dB
Cross-talk coupling loss at 30kHz	<u>78dB</u>
Allowable 25-to-40kHz power on disturbing pair	<u>-36dBm</u>

Criterion (Above 40kHz)

The criterion for power in the band above 40kHz is based on potential interference into PICTUREPHONE service and into cable carrier systems operating in that frequency range.

The effect of interference to PICTUREPHONE service on the user is snow in the picture or herringbone patterns superimposed on the desired picture, due again to cable cross talk.

Signal Criteria (Criteria for Distribution of In-Band Power)

The tariff requirements concerning distribution of power within the transmission band are: FCC 259, FCC 260, FCC 263 -- to prevent the interruption or disconnection of a call, or interference with network control signaling, it is necessary that the signal applied by the user-provided equipment to the Telephone Company interface located on the user's premises at no time have energy solely in the 2,450-to-2,750 Hz band. If signal power is in the 2,450-to-2,750 Hz band, it must not exceed the power present at the same time in the 800 to 2,450 Hz band.

In the 2,600 Hz single-frequency (SF)<sup>6</sup> signaling system, the SF receivers respond to signal power in a relatively narrow band nominally centered on 2,600 Hz. However, factors such as manufacturing tolerances, aging of components and ambient-temperature differences produce some variation in both the nominal bandwidth and the center frequency of the receiver-response band. In addition, a form of distortion termed "carrier shift," which may be encountered on certain types of transmission systems, causes small frequency changes in the signal and is another source of variation. When factors such as these are taken into account, we find that the effective SF response band lies between 2,450 and 2,750 Hz. The receivers are designed, however, not to respond to power in this band when an equal or greater amount of power is present at the same time in the 800-2,450 Hz portion of the voice band. This criterion applies at the user's terminal and includes allowances for the sources of variation cited before as well as differences in transmission loss for different frequencies in the voice band, over regular telephone connections.

<sup>6</sup>Section 2, p. 19.

### Harmful Voltages

In this section we discuss sources of harmful voltages appropriate to the interconnection issue network, exposures to these voltages, and effects produced by them. The major hazard of significance is to maintenance personnel. Equipment hazards are considered minor since only the single termination associated with each loop would be harmed in case of excessive voltage.

### Hazard to Personnel

This involves: (1) the effects of electric shock on human beings and (2) the extent to which network personnel may be exposed to such shock as a result of the connection of user-provided equipment and/or systems.

1. Effects of Electric Shock. Harmful effects are determined by the amount of current passing through the human body. The amount of current depends on several factors: the voltage on the electric conductor to which the body is exposed, the source impedance of the voltage, and the highly variable body resistance.

In many ways, the most dangerous source of potentially fatal currents is 110 or 220 volt AC. The major danger of this source stems from its ubiquity around users' premises and the fact that the protective devices that are presently connected to telephone lines will usually not operate if the line is exposed to 110 volts. Yet the presence of the voltage is potentially lethal to personnel who come in contact with that line.

2. Extent of Personnel Exposure. As explained, the telephone companies provide service to customers by means of physical conductors in the exchange plant. Each time service is installed, removed or repaired, telephone servicemen make physical contact with wire pairs and terminals at one or more points in the station equipment or at the terminal appearances of the wire pairs on customer premises in outside manholes or on poles, and in the central office building.

In general, the work operations require a hands-on type contact. The size of the wires, the terminal sizes and spacings, and the dexterity required, generally preclude the use of protective clothing or devices such as rubber gloves. This is not to say that rubber gloves are never worn. They are prescribed for many construction operations, particularly when working on joint-use poles shared with power companies. But they are inappropriate for such tasks as splicing together multi-conductor, fine-gauge cables.

The conductors that fan out from a wire center (or central office building) are carried in densely packed cables, ranging from as few as 6 to 2,700 pairs of conductors per cable, and they are spliced together and terminated on closely spaced terminals in cross-connection boxes and in sealed splices along the routes. Therefore, servicemen working on a single pair are exposed not only to that one pair at terminal field appearances, but also to additional pairs that are connected to adjacent terminals.

### Effects of Interconnection on the Harmful-Voltage Problem

The direct electrical connection of user-provided equipment and communications systems to telephone company lines adds an additional source for the introduction of potentially harmful voltages into the telephone plant. This can come about by a faulty equipment design or manufacture, or a faulty installation, both of which could cause 110 V AC or higher to appear on the loop. This potential hazard is also unique in that it is perhaps the easiest source to protect against in that the telephone-line exposure occurs specifically at the point of interface with the user equipment. Assured protection at the interface can provide suitable protection in both directions, i.e., protect the user from possible voltages on telephone lines and protect the telephone personnel from high voltages introduced by user-provided equipment or systems. In Section 5 we discuss protective mechanisms for this need.

### Loop Balance

Connections between customer premises and central offices are normally made by individual wire pairs in multi-paired cables. The wires, because of the close proximity to each other, have mutual capacitive and inductive coupling effects. Mutual coupling results in cross talk between adjacent pairs, which, if not controlled, increases the noise level on all circuits concerned. Cross talk, in aggravated instances, can produce interfering signals of an intelligible nature, which violates, or appears to violate, the privacy of one or more users.

### Cross Talk in Cables

To minimize electrical interactions among individual wire pairs within the cable, the pairs are twisted and balanced to ground. Twisting of the wire pairs reduces the effects of magnetic coupling to an insignificant factor. Capacitive coupling is, however, still a factor and has to be carefully controlled.

The longitudinal balance in cables is controlled in manufacturing so that the coupling loss between pairs is generally well over 100dB with about one percent of pairs having coupling losses of 80dB or less at 1,000 Hz. Since this coupling is primarily capacitive, the coupling loss will decrease (hence cross talk will increase) with increasing frequency at the rate of 6dB per octave. Tests have shown that if one conductor of one pair is grounded, cross talk will be worsened by 20dB, and if one conductor of each of two pairs is grounded, it will be worsened by as much as 60 dB. Therefore central-office circuits and telephone-station equipment and wiring in the telephone network are designed, installed, and maintained to ensure a high degree of balance to ground.

While cables are designed and controlled in manufacture to maintain balance and reduce cross talk, these controls become ineffective if equipment attached to the cable pairs is itself improperly designed, installed, or maintained. Cross talk will result if user-provided equipment is unbalanced to ground. This can occur if:

- (a) Equipment is poorly designed initially. Terminating the telephone pair in an unbalanced circuit is a common error.
- (b) Equipment is improperly installed so as to apply a ground to one side of the line. This may occur accidentally through insulation being scraped away or with nails or staples cutting through wires.
- (c) Equipment can fail in service. A component can break down and cause unbalance on the line.

Cross talk can be insidious and difficult to locate because the malfunction is partial rather than total. The user may or may not be aware that he is causing trouble to other parties, especially if his service appears normal. Thus, the deteriorated performance can exist for a long period before diagnosis and correction. It should be noted that, with multiple party-line operation, one side of the line is grounded through the ringer. However, the ringer impedance is high enough to avoid unbalance at voice frequencies.

NETWORK-CONTROL SIGNALING

INTRODUCTION

The network-control signaling functions are associated with the initiation, placing, answering, and charging of calls over the switched network.

Malfunctions can cause incompleting calls, or calls completed to other than the intended terminal. Processing such calls reduces the capacity of the network to serve "normal" calls. The effects of these malfunctions may be felt by all users of the system, not just those originating and answering imperfect calls.

The present state of the switched telephone network does not permit easy identification of the source of this kind of malfunction; that is, to locate it as occurring in the subscriber's station or in the central office. Carrier-maintenance personnel, tests, and administrative procedures become involved in the attempt to localize these malfunctions as they come to light.

Consequences of Improper Network-Control Signaling

The consequences of improper network signaling pervade the entire network and can be grouped into the following categories:

- (a) Wasteful use of central office and transmission facilities
- (b) Annoyance to other users
- (c) Incorrect billing
- (d) Wasted testing and maintenance effort
- (e) Added administrative expense

Following are examples of each category:

1. Wasteful Use of Central Office and Transmission Facilities. Wrong numbers caused by a faulty network-control signaling unit represent a waste of switching equipment and a source of annoyance to those who are wrongly called.



Furthermore, a wrong number resulting from faulty signaling can cause a call to end up in the wrong city. In the near future, a wrong number may tie up, for a time, a trans-atlantic cable or satellite trunk connection. There are other sources of faulty control signaling. If, when a call is completed, the switch hook contacts fail to open properly, or some extraneous impedance remains bridged across the line, it is arranged that the connection will release after a time-out of thirty seconds. This is thirty seconds during which the circuits are not available to other users.

2. Annoyance to Other Users. In the example mentioned above, in which the call is not released properly, the user himself will be unable to place calls during this interval and others trying to reach him will receive busy signals.
3. Incorrect Billing. On a two-party line, the billing equipment at the central office recognizes which party is making a call because there is a high-impedance DC connection to ground on one side of the line. If the connection is not made in the telephone, or if the telephone is installed or maintained improperly, the wrong party will be charged for some calls. On lines with more than two parties, more complex party identification schemes are used, which depend upon the telephone instrument having particular identifying characteristics that differ from the instruments on the same line.
4. Added Testing and Maintenance Effort. When excessive wrong numbers occur, action must be taken to identify the source. It might be on the loops, in the line circuit, or in the central office. On the other hand, it might be in the network-control signaling unit. The user unable himself to determine where the problem is located will normally call the telephone company. Faulty network contact signaling often shows up as an intermittent trouble. These are the hardest to trace and to diagnose.
5. Added Administrative Effort. Improper network-control signaling can result in customer demands for credit against his telephone bill due to false charges. Since the source of the trouble, as previously mentioned, is difficult to trace and correct, the added administrative effort required can be considerable.

Conclusions

Improper network-control signaling leads to inaccurate billing, wasteful use of the telephone plant and administrative effort, as well as

annoyance to other users. In planning for the use of user-owned network-control signaling devices, the quality of network-control signaling must be preserved.

AT&T Company Experience with Network-Control Signaling

The only available reliable source of information to the Panel on network-control signaling is experience with this function in the operation of the switched telephone network. In this section, information and data furnished by AT&T are summarized.

Dial-Pulse Signaling

Network-control signaling failures are largely related to the familiar rotary dial. Sources of trouble here are:

- (a) Finger wheel and stop
- (b) Contact
- (c) Mechanism
- (d) Noise
- (e) Other

The dial mechanism itself was the most frequent source of difficulty. The mechanism is required to operate at speeds nominally between 9.5 and 10.5 pulses per second and with a percentage break between 58 and 64 percent. Generally, the units used by the Bell System fail in such a manner as to fall outside the percentage-break tolerances. This type of failure can lead to dialing wrong numbers.

Data on units supplied by others is sketchy. AT&T and Bell Laboratories, however, had reported experience with some equipment they have tested and found deficient. For example, one unit tested had a low-priced "antique" telephone with these two faults:

- (a) Low ringer impedance
- (b) Percentage break 67 percent outside allowable range of 58 - 64 percent

The first fault is attributable to poor design. The second may indicate either poor design or maladjustment. Bell has also tested commercial answering machines and repertory dialers. Some answering machines had the characteristic of failing to disconnect promptly. One

repertory dialer tested exhibited improper percentage break as a function of line voltage, missed digits on low line voltage, and had inadequate interdigital time. A second repertory dialer exhibited dial speed and percentage-break characteristics that aged beyond specified limits.

On the other hand, general experience with telephones made by reputable manufacturers of telephonic equipment has indicated that the quality of network-control signaling units is on a par with those supplied by Bell. No comparative statistics are available.

Based upon the statistics provided AT&T, the mean time between failures for Bell station sets is 8.5 years. The mean time between failures for rotary dials is 46 years and for ringers 59 years. The combination of rotary dial and ringer has a mean time between failures of 26 years.

It is this kind of performance, or better, that must be realized where new devices and systems are attached to the telephone system if present network-control performance levels are not to be degraded.

Touch-Tone Signaling

Touch-tone signaling uses two tones per digit generated by pushing buttons on the telephone. One tone is selected from four frequencies between 697 and 941 Hz. The second tone is selected from four frequencies between 1,209 and 1,633 Hz. Both tones must be received by the central office for it to be accepted as a valid digit. Frequencies have a  $\pm 1.5$  percent tolerance. Output power is made a function of line current to regulate the received power at the central office for various loop lengths. Other tolerances are specified to hold the two sets of tones at appropriate power levels. The unit must operate within tolerance over a  $-30^{\circ}\text{C}$  to  $+55^{\circ}\text{C}$  temperature range and during its service life.

Reliable statistics on types and frequency of failures are not available on touch-tone dialers. Failure of the multi-frequency dialer due to improper frequency or power level, for example, will not be interpreted by the central office as a wrong number. The more likely condition is a register time-out due to its failure to recognize all the transmitted digits. This use of central office facilities is considered relatively insignificant as a harmful effect when compared to harmful effects due to malfunctioning rotary dials.

We conclude failure of touch-tone (multifrequency) signaling to be considerably less harmful to the network than failure of dial-pulse signaling.

Maintenance Data

In the switched telephone network, network-control signaling is exercised by the customer through the telephone instrument and over his wire loop to the central office. It is pertinent, therefore, to examine available data on station troubles and the costs associated with maintenance and trouble clearing. The following data were supplied to the Panel by representatives of AT&T.

In 1967, Bell had 42,586,551 customer-trouble reports - 27,392,760 troubles were found as a result. These troubles broke down as follows:

Station set	8,608,962	30.8%
Other station equipment	4,302,696	15.4%
Station wiring	4,802,760	17.2%
Outside plant	5,390,924	19.3%
Central office	2,485,913	8.9%
Customer action	1,801,505	6.4%

A Bell System study of station troubles made in 1966 showed the following breakdown:

	<u>Trouble rate/100 stations/month</u>
Cord	0.21
Dial	0.18
Ringer	0.14
Key and lamp	0.12
Mounting and plastic	0.12
Circuit	0.08
Receiver	0.03
Transmitter	0.03
Other	0.03

Whether these data reflecting carrier experience would be valid for customer-furnished station equipment, would depend on the performance of this equipment relative to that furnished by the common carrier. It would also depend on the extent of use of touch-tone control instead of rotary dial.

FAULTY NETWORK-CONTROL SIGNALING WITH USER-OWNED EQUIPMENT

It is difficult to evaluate the effect of interconnection on network-control signaling, since it is not known at present what precise instrumentalities users will employ for this function. Network-control signaling performance is closely related to the very detailed design and performance of the device used (switch hook, rotary dial, touch-tone pad).

The best that can be done, therefore, is to cite present experience of the carriers using their own devices. Starting from this as a reference point, it may be postulated that devices owned and used by customers will be either (a) as good as, or (b) poorer than, these carrier-furnished devices. The consequences of these assumptions are drawn in the following section.

ECONOMIC PENALTIES OF NET CONTROL SIGNAL-DEVICE FAILURES

Data on Bell System rotary dial and ringer units show a mean time between failures (MTBF) of 26 years. This is equivalent to a failure rate of 0.0385 per year.

Except for the special case in which competent maintenance personnel are continually at hand, trouble visits will be required and costs will be incurred and must be paid for.

Some vendors and users might be satisfied with a seemingly reasonable, though lower, MTBF. Reliability, however, has a profound impact on network operation and cost. Based on a large volume and using the Bell System experience of \$15 per maintenance visit, Table 1 shows the annual average per phone cost for maintenance alone as a function of MTBF. The distribution of this cost between the user and the carrier cannot be determined at this time; however, it represents a substantial factor to be considered in specifying the performance of network-control signaling units.

TABLE 1

MTBF	Annual Maintenance Cost Allocated to Each Phone
26 years	\$ .57
20 years	.75
15 years	1.00
10 years	1.50
5 years	3.00
1 year	15.00

Another cost (to the carrier) associated with improper network-control signaling failures is that attributed to wrong numbers, wrong toll charges, etc. It is difficult to estimate the frequency of such occurrences as a function of MTBF.

A third cost associated with network-control signal-unit failures

is that due to false calls for assistance by the user. Where limited free interconnection has been permitted in the past, it has been the experience of the carrier that he is frequently called to perform the maintenance when, in fact, the interconnected equipment is at fault. This phenomenon can be expected to persist with any form of interconnection in which a specific interface between vendor equipment and the telephone company is not clearly defined.

The three types of costs described are a function of the MTBF of the net-control signal unit. The costs are very significant when evaluated in terms of a large number of subscribers. These costs will be borne by both users and the carrier, since some costs cannot be easily allocated.

CONCLUSIONS

Net-control signaling is a critical element, and a high order of reliability is necessary to avoid loss of net performance and excessive costs to both carrier and user.

## PROTECTIVE DEVICES

## TARIFFS AND PROTECTIVE DEVICES

Unrestricted interconnection of user-owned communications devices or of privately owned unregulated communications systems to the public telephone network, as discussed in detail in Section 3, introduces the possibility of harm to the users of the networks in the form of degraded performance or an increase in the hazards of exposure of carrier personnel to dangerous voltages and currents.

As a safeguard against these potentially harmful effects, AT&T has incorporated in FCC tariffs 259, 260, and 263 not only protective criteria relating to levels, bandwidth, and signaling frequencies, but, in some cases, a requirement for carrier-furnished and installed protective and coupling arrangements to be placed between the telephone network and customer-owned and customer-maintained equipment and systems. Private-line customers obtaining service under FCC tariff 260 are not, in all cases, required to obtain protective devices.

This Section discusses this concept of protection along with alternative arrangements. At the present time, the selection of devices and priority of design and manufacture rests with the carrier. The number of different types of coupling devices available is limited and are intended to fill immediately-known requirements. They are to be followed by additional types as needs are identified, economics are justified, and as development is completed. Systems innovation and development of user-owned devices may be influenced by the willingness of the carrier to produce specialized interface units. This approach will be discussed in depth in later portions of this section.

## PROTECTION AFFORDED BY PRESENT CARRIER-FURNISHED DEVICES

It is not intended here to provide a detailed description of every available coupler. Each is described in detail in a Bell System Technical Reference. The couplers are similar in their basic functions, which are:

- (a) To isolate the line from hazardous voltages
- (b) To limit signal levels
- (c) To preserve longitudinal balance

- (d) To protect the network control and signaling functions

In its simplest form, the coupler is designed around an isolation transformer that interfaces directly, via a jack, with the user-owned equipment. This transformer serves three functions:

- (a) It ensures longitudinal balance on the loop regardless of any unbalance in the customer's equipment
- (b) It isolates DC currents in the customer's equipment from the loop
- (c) It prevents hazardous A.C. voltages from being impressed on the loop by virtue of its saturation capability

Varistors, shunted across the line side of the transformer, limit peak signal voltages. A capacitor in one side of the line blocks line current from saturating the transformer core.

Some of the more complex forms of coupler include a more sophisticated signal limiter designed to reduce distortion of data signals that exceed the allowable limits. Others include arrangements for signaling and supervision, either manual or automatic, answering only, or answering and calling. Coupler for interfacing customer-owned PBX equipment are much more complex units.

Degree of Protection

1. Hazardous Voltages. The major hazard is that involving personnel and the protection provided here is excellent in the carrier-furnished units. A saturable transformer is an effective method of protection. Fuses and circuit breakers rated for equipment protection do not provide personnel protection.
2. Signal Amplitude. The protection provided here also is excellent. The various types of limiter all ensure that proper levels are not exceeded.
3. Spectrum Limitations. No attempt is made in any of the couplers to limit signal spectrum. The couplers provide no protection against unwanted frequencies.

---

<sup>1</sup>Section 3

- 4. Longitudinal Unbalance. The isolation transformer provides excellent protection against any defects in the customer's equipment or installation that could cause unbalance on the user loop and consequent hazard of cross talk and noise.
- 4. Improper Network Control Signaling. The subject of network-control signaling and the consequences of improper control are dealt with in some detail in Section 4. In this section, conclusions are reached as to the effectiveness of the current carrier-provided interface arrangements in preventing improper network-control signaling.

The degree of protection afforded to customer-generated network-control signals is minimal. DC isolation is indeed provided between the customer's equipment and the loop, but since signals are usually merely repeated, there is no protection against dial-pulse speed variation, make-break ratio (in most cases), or repetitive dialing from a malfunctioning auto-calling device. In certain cases, particularly with relays that repeat dial pulses, the coupling device can, in fact, degrade the dial pulses by inferior timing characteristics of the relay. In another instance, the dial repeating function in one of the protective devices was less tolerant to dial pulse variation than if no protective device were used. In this latter case, AT&T is redesigning the unit.

#### IDENTIFIED ISSUES

##### Reliability

The protective arrangement or coupler introduce another electronic box into the system. What are the chances of failure occurring in a coupler with an attendant reduction in reliability? The answer, of course, depends on the complexity and soundness of design of the coupler. In the very simplest type of voice coupler, several solid-state diodes and an isolation transformer are all that is involved. Since all elements are solid-state, life under normal operating conditions is indefinitely long. Transformer-insulation failure at telephone-line voltage is extremely rare unless the quality of the insulation is initially poor.

At the next higher level of coupler complexity, the diodes are replaced by amplifiers and an AGC circuit with power supply. Additional resistors, capacitors, transistors, and diodes are introduced. Under normal conditions, the life of this sort of coupler should be comparable to the life of the attachment. Certain of these couplers use relays for

dial-pulse repeating. Relays are notably poorer in reliability than solid-state devices and can, therefore, be expected to have a somewhat higher, but still acceptable, failure rate.

##### Redundancy

Redundancy, for purposes of this discussion, means that essential functions are duplicated in the coupler and in the devices attached to it and the requirement for protection, in many cases, can cause such a redundant condition. For example, redundancy occurs in some of the couplers provided for use with PBX's. In these cases, all functions of the coupler are repeated within the PBX itself from transformer isolation to regeneration of subset dial pulses which themselves may meet the dial criteria.

One approach would be to delete the redundant features from the user equipment designed for interconnection to the common carrier network. A manufacturer, on the other hand, would then be required to supply two types of equipment -- one to interface with the carrier provided coupling unit and another where a coupler is not required. Another approach would be to allow interconnection under the provisions of a Certification Program.<sup>2</sup>

##### Transparency

Ideally, the protective device should be "transparent"; that is, its presence should have no effect upon normal system functions. In this connection, the present coupling units are not transparent in that they do not pass DC due to the transformer provided for line balance.

"Transparency" has another, and somewhat different, meaning to the designer of equipment attached to the telephone network. The ideal protective device to him is one that does not require that he make design changes in his equipment. For example, the AT&T CDH coupler for PBX's presents a manufacturer of PBX's with a ten-terminal interface, whereas a PBX is designed for a two-terminal connection direct to the carrier's line.

Certainly, the greater the transparency of the protective device, the fewer the problems presented to the designer and manufacturer of terminal equipment. As with the redundancy case, transparency can be improved by cooperative action by the carrier and the supplier of attachments to produce improved couplers or by incorporating the protection into a unit built under an enforced certification program.

---

<sup>2</sup>Section 6

Availability

Certain types of protective devices are said not to be available. AT&T states that the most frequently required types are available and the carrier is proceeding with the development of other varieties. They further state that the suddenness of the tariff filing created problems with regard to the supply of protective devices. A minimum number of types were ready for distribution at the time of, and shortly after, the filing. Nevertheless, a number of users have complained about lack of availability of announced units. Some have complained that, due to the difficulty in defining all protective requirements in advance, design and production of devices by the carrier could unduly delay installation of systems. There is also concern on the part of manufacturers that their desire and ability to innovate will be limited by the decisions of the carriers. At this time, availability is further complicated by a lack of a firm interpretation of tariff language. A lack of uniform interpretation among the many telephone companies and the various state Public Service Commissions is also a factor.

Power Supply Dependence

Protective arrangements (above the simplest level) require a source of power and typically commercial AC power is used. In the event of a power-line failure, therefore, the protective arrangement becomes inoperative. Communications within the customer's site can continue if the customer has provided emergency power for his own equipment, but communications with the outside world, where it is most needed, is cut off. This problem can be resolved and, fortunately, many solutions exist. Automatic means for bypassing the coupler in the event of an emergency is one possibility. The problem disappears, of course, if the protection is incorporated into the design of the user's equipment.

Glare

"Glare" is a condition that occurs on trunks or lines when the circuit is seized at both ends at, or nearly at, the same time (or during what is called the "unguarded interval"). When this happens, the switching machines at each end of the circuit are confused, each fruitlessly waiting for an answer from the other end. Early-type protective couplers were designed to a 1.5 second unguarded interval. The addition of this coupler introduced a three-fold increase in potential glare with customer-provided PBX's over normal operation. However, a field change order for all CDH units, which reduces their unguarded interval from 1.5 to .5 seconds, has been issued. The risks of glare with this change are no different with the protective coupler and user-provided PBX equipment than that with carrier-provided PBX's. The increase in glare incurred by the addition of the protective arrangement would, therefore, appear to be a minimal problem at this stage.

Transmission Degradation

Although the ideal protective arrangement should be without loss, coupler losses amounting to 2 db to 3 db are practically achieved. Normal variations of attenuation in the received signal of the line can vary over 10's of dB's due to differences of loop length and other circuit variables. Therefore, losses induced by the coupler are small compared to normal circuit variations. There is usually no problem in compensating for this additional loss. Most modems and other attachments have adjustments or taps by which these losses may be fully compensated.

Packaging

The carrier-supplied protective device now appears as a separate entity in its own cabinet or box. While clean-cut from the carrier's point of view, it represents to the user just another box that has to be put somewhere. Presently, the protective device cannot be physically located in the customer's equipment, although the carrier indicates it is willing to discuss this issue.

Integrated Protection

Assuming a Certification Program<sup>3</sup> to allow direct connection between carrier and users, the following are some factors involved in the inclusion of the protective arrangement within the equipment cabinet.

1. Redundancies can be removed in various ways; one way is through repackaging. A manufacturer, having complete control over both the protective device and his own attachment, will tend to eliminate all redundancies in order to get the best cost advantage.
2. There may be small maintenance advantages. An interface of two wires is easier to maintain than the interface of eight or more wires of the more complex couplers.
3. There are fewer hardware variations. Manufacturers of the user's equipment will build the protective arrangement from the same hardware building blocks that are used in the rest of this equipment. The number of types of spare assemblies needed for maintenance is consequently reduced.

<sup>3</sup>Section 6

4. The appearance of the installation is enhanced if there is one less box to contend with. The space occupied by the protective arrangement within the user equipment should be considerably less than as a free-standing box. The sharing of common facilities (power supplies, framework, etc.) will contribute to the better packaging efficiency.
5. No conclusions can be drawn with regard to manufacturing-cost advantages. It appears that a large-volume manufacturer would have a manufacturing-cost advantage through elimination of redundancies and the sharing of common facilities (as discussed in 1 and 3).
6. A built-in protective device has greater potential for mobility where that feature is important. Carrier-supplied protective devices would otherwise be required at each point of use of the portable attachment.

#### PROTECTION AT THE TELEPHONE CENTRAL OFFICE

This section discusses the feasibility of transferring the protection function to the telephone central office itself.

Perhaps the most significant observation to make about providing protection in the central office compared to protection of the customer's station is that no protection can be provided in the central office for certain effects. Protection at the central office cannot affect high-level signals that cause cross talk in exchange cables, high voltages that may be hazardous to those working on the loops, or unbalance which destroys the inherent balance of cables. Protection in the central office could, in principle, prevent excessive levels on carrier systems in the trunk plant. Present central-office designs, however, do not provide facilities to limit signals to the levels required to prevent overloading carrier systems or to prevent cross talk in loops or on voice-frequency intertrunks. In any case, such facilities, if provided, would also have to be provided on a per-loop basis or switched into service as required. At this writing, the Panel does not have enough information to make recommendations.

#### OTHER PROPOSED PROTECTION ARRANGEMENTS

Although the present coupling arrangements provide an acceptable way of providing protection from the hazards discussed in Sections 3 and 4,

there may well be other and better ways of accomplishing it. An approach proposed by one manufacturer provides partial protection. The exact nature of the protective device, which uses solid-state elements, is not disclosed by the manufacturer. Its virtue is apparently low cost. The device does not use transformer isolation, yet appears to guard against hazardous voltages and out-of-limit signals. The protection, however, is not complete in that capacitive unbalance can still exist.

#### CONCLUSIONS

The need for some forms of protection is well established. The questions are: How much? Where? and In what form? Clearly, there must be protection against harmful voltages, excessive signal amplitudes and longitudinal unbalance introduced by attached equipment. We draw the following conclusions:

1. Existing carrier-provided protective devices are indeed effective in providing protection for hazardous voltages, excessive signal amplitudes, and longitudinal unbalance from users.
2. Existing carrier-provided protective devices provide, on the whole, minimal protection against faulty network control and signaling.
3. A protective device obviously introduces another potential point of failure. Reliability of the protective devices under normal operating conditions, however, should be comparable to the attachment and should, therefore, present no great concern.
4. There are redundancies between the functions of the protective devices and those of certain user-provided equipments; e.g., PBX's.
5. Carrier-provided couplers are not inherently transparent.
6. The present dependence of some couplers on commercial power is a significant and probably unnecessary disadvantage.
7. Protective arrangements do not contribute to any significant performance degradation. Increase in glare is minimal. Transmission loss is a small effect.
8. Central-office protection cannot provide the same degree of protection as customer-site protection.

## CERTIFICATION PROGRAM

Certification procedures in the interest of safety are customary in areas where safety to personnel and equipment depends critically upon engineering design, installation, maintenance and inspection. The Federal Aviation Agency regulates private flying under such a program. The Federal Communications Commission regulates the operation of radio and television broadcasting stations through the issuing of station and personnel licenses. A certification of satisfactory inspection by an inspector, who is himself certified as competent, is required before an electric power utility will permit the connection of its power lines to a new home, office building or factory. There are other familiar examples in which certification procedures are in daily operation.

It is natural to inquire whether similar procedures can be applied to the interconnection of user-owned equipment with the telephone network. The Panel has studied this question and has concluded that:

ALTHOUGH EACH TELEPHONE  
INSTALLATION IS, TO SOME  
EXTENT, CUSTOMIZED BECAUSE  
OF DIFFERENCES IN LOOP AND  
SWITCH CHARACTERISTICS,  
NEVERTHELESS, THERE IS  
SUFFICIENT COMMONALITY TO  
ALLOW STANDARDIZATION

THE PANEL CONCLUDES THAT  
THE STATE OF KNOWLEDGE AS  
TO THE CHARACTERISTICS OF  
THE TELEPHONE PLANT AND  
THE DEMONSTRATED CAPABILITY  
OF REPUTABLE MANUFACTURERS  
AND USERS WILL ALLOW THE  
DEVELOPMENT AND CAREFULLY  
PHASED-IN IMPLEMENTATION  
OF A CERTIFICATION PROGRAM

A successful certification program for telephone interconnection must be made up of three principal functions. These cover the areas of:

- (a) Standards development
- (b) Equipment certification
- (c) Certification of installation and maintenance

## STANDARDS

No certification program, whether it be for equipment or for services, will work unless proper standards have been established. In the case of telephone interconnection, standards must be developed to cover certification for installation and maintenance of equipment and facilities, as well as for equipment manufacture, since all of these combine to determine the net effectiveness of the program.

The standards, as defined for this effort, cover those factors relating to protection of the telephone network and to personnel safety.

These limited performance and safety standards would not guarantee the performance that the use of user-owned and maintained equipment would receive. Programs for this area could be developed. However, they are not within the realm of this study, which is limited to the technical issues that have evolved from the Carterphone decision.

Since enforcement will require that the standards be referred to in the tariffs, final authority for the entire program should remain with the governmental agency having jurisdiction over the tariffs.

Standards Development

A standards-development program requires the resources of a qualified standards organization to provide coordination, structural guidance, and staff services to those writing standards. Such organizations exist within both the private sector and government. In addition, a standards-development program in this area requires the work of knowledgeable people with sufficient training and experience in the design, manufacture, installation, operation, and maintenance of modern complex communication equipment and systems. Without this depth of practical technical knowledge, the resulting standards will fall short of the requirements for a workable certification program. The technical expertise in this area resides with the carriers, users, and manufacturers, and these must all be involved in this program. In this connection, several organizations representing such expertise are now active in the United States in the preparation of standards for communication equipment, systems, and interfaces. They can contribute knowledge and experience toward the establishment of the program being considered.

Assuming federal government participation in the establishment and conduct of standards-development activity for telephone-interconnection certification programs, this participation should take several forms:

- (a) Establish the line of authority that gives weight to the enforcement of the standards. Cooperation between federal and state governments will be most important in this area.



- (b) As a large user of communications facilities and services, it should participate in the committees developing new standards.
- (c) Establish priorities and schedules to ensure that an orderly and expeditious development program proceeds.

Development of proper standards will take time. Even with qualified personnel working on their preparation, some standards have required more than a year before agreement could be achieved. If the program is recognized to be sufficiently urgent, the time required for development will be shortened. The importance of each standard influences the manner in which necessary qualified personnel are made available and the willingness of affected organizations to work out compromise agreements, and this, in turn, determines the time needed to arrive at an approved standard. In the opinion of the Panel such a standardization program can be successfully implemented.

#### EQUIPMENT CERTIFICATION

In addition to standards, procedures must be established and enforced to ensure that equipment meets those standards. The degree of inspection performed as a part of equipment certification determines the probability that the equipment will meet the standards.

An enforced equipment-certification program requires not only an evaluation of equipment samples but evaluation of the manufacturing organization to establish that procedures for quality of component procurement, manufacturing, testing, personnel training, and quality control ensure that there is a consistency of production quality.

In setting up an enforced certification program, overall organization responsibilities and relationships, therefore, need to be considered. One approach involves separating central management and administration of the certification and standards program from the day-to-day operation of test and inspection facilities. A central management organization might be continuously responsible to the government agency granting its authority. At the same time, performance of equipment testing and manufacturer inspection could be handled by government facilities or by many competing firms looking for more cost-effective methods of performing their tasks. There are a number of independent test laboratory companies in the United States today.

#### Certification of Installation and Maintenance

After a user obtains his certified terminals or other equipment, he must assume responsibility for their operation. As discussed earlier in this report, it is essential that the equipment be installed and connected to the telephone facilities correctly, and it must be maintained in a way which will not cause future harm to the telephone network. A complete certification program must, therefore, cover installation and maintenance, as well as manufacture, of the user-owned equipment.

An installation- and maintenance-certification program must include standards for, and inspection of, the equipment connection to each telephone line. In addition, consideration must be given to the qualifications and responsibility of the personnel who do the work. Minimum standard requirements will specify whether a given individual is authorized to carry out installation and maintenance of the equipment and to certify that the work has been properly completed.

A certification program for installation and maintenance would require that testing and licensing procedures be specified. In this case, licensing would follow examination under rules developed in the standards program with every license certificate endorsed to indicate its applicability to equipment of one or more classes.

The procedure for installing user-owned equipment will require close cooperation with telephone company personnel, since each case will require some degree of customer adjusting or fitting. This cooperative action will need to be recognized in a standard through the establishment of guideline procedures for installation and checkout.

In its simplest form, installation and maintenance certification would apply to a protective coupling unit designed to prevent harm to the public telephone network. If the protective features are not in a separate unit, but are incorporated into the user's equipment, then these procedures must apply to pertinent parts of equipment and facilities in the user system connected to the telephone line.

Inspection at the time of installation will not certify the installed user equipment indefinitely. Periodic inspection with appropriate documentation by licensed personnel must also be required by the standards for installation and maintenance.

Another area requiring careful consideration is the certification of equipment for resale to a second user. After connection and use at one installation and subsequent removal, it must be serviced and inspected by authorized personnel before it can be sold to a second user.

Maintenance requirements will include both routine and emergency service of the user's equipment. The correct type of routine or preventive maintenance can protect the network by preventing trouble before it starts. After trouble has been observed or suspected, optimum methods for fault isolation will help greatly in reducing the time needed to correct the trouble and to return the system to satisfactory operation. Responsibility and duties of those on each side of the common carrier-user interface must be spelled out in sufficient detail.

A maintenance organization, in order to secure certification, should carry the necessary stock of replacement units, spare parts, and other material needed for service of the equipment. Training programs for service personnel should also be implemented in a way that meets or exceeds minimum standard requirements.

#### PHASE-IN PROGRAM

In the Applicable Experience Section (Section 8) of this report, we point out that there has been considerable successful experience of U.S. carrier interconnection of large-scale organizations -- such as "right-of-way" companies. However, this experience is limited in scale relative to the overall telephone plant, and detailed data on the degree and specifics of this interconnection was not gathered. The past experience has been with large and technically capable organizations. There is no such equivalent experience with the larger-volume/smaller-user type of customer on a direct interconnection basis. As a matter of fact, since this whole area is so new, there is no large-scale experience of interconnection using the carrier-supplied connecting arrangements. As discussed earlier in this report, those elements are also new, relatively untried, and already some deficiencies are evident. All this leads to the caution that if a program for direct interconnection by the customer via a certification program is to be carried out, it should be done carefully and in a way planned to minimize risk to the success of the program. This program must be set up to gather data to provide feedback to the standards organization for further development of the program.

Therefore, the Panel feels that, as a first step of implementation, configurations involving smaller numbers of installations (such as PBX) should be certified. A ready technical base of servicemen exists, which could be certified. The equipment manufacturers and users are already familiar with telephone practices. This application would not represent a significant volume impact, so that if errors are made and lessons are learned they can be remedied. Following this, the next most widespread area can develop (probably data terminals), and then proceed to the remainder of the field. It must be emphasized that the development of the certification program for both equipment and personnel must proceed apace.

A number of installations, primarily the "right-of-way" companies,

are presently directly interconnected with the carrier system. Over a period of time, these existing interconnections should be certified or access arrangements used. The Panel has not investigated a schedule for this, but it could be considered as an element in the overall certification program.

#### SELF-CERTIFICATION

If a user-manufacturer sets up his own program for equipment certification and verifies that he, in fact, meets all the stated requirements of a producer of specific products, and that the finished product has been installed and inspected according to published standards, the resulting program would be called self-certification.

Limited self-certification has proved to be satisfactory in several areas. The FCC requires that manufacturers of radio transmitting equipment mark all such products in a way that certifies that particular standards are met. Although the units are not tested by a third party, provision is made for monitoring in case of interference and inspection when required. In a similar way, the U.S. Coast Guard requires that standards be met in the manufacture of equipment and accessories for small craft used in specified areas. Again, the manufacturers' own certification is sufficient. However, annual inspection of small craft equipment is required.

An enforced certification program formally separates the responsibility for inspection from the manufacturing, distributing, and using organizations that have a direct financial involvement in the outcome. In the case of direct electrical interconnection where intractable harm can be done, it is the considered opinion of the Panel that this risk cannot be avoided by self-certification. This is particularly so in the case where a large group of small users with little technical knowledge might buy lower-quality equipments (new or used) and cause serious harm to the rest of the using community. Faults in equipment quality, installation, maintenance, and operating procedures will have a high likelihood of occurrence in the absence of the controls of an enforced certification program.

#### Responsibility

It was pointed out that the allocation of responsibility for protection of personnel, equipment, and service is important to the success of a certification program.

At present the carriers are responsible for the safety of their personnel, equipment, and the services they provide, and the regulatory agencies (both federal and state) exert authority over these carriers.

The widespread interconnection of user-owned terminals and systems, without isolating protective interface devices (which assign responsibility to the carriers), would cause the dispersal of responsibility for service to include, in addition to the carriers, one or more of the following:

- (a) Users who own their own equipment
- (b) Manufacturers who assure that standards are met
- (c) Those who prepare standards
- (d) Those who test or certify products
- (e) The source of certifying authority
- (f) Those who certify the competence of individuals or organizations for installation and maintenance
- (g) Inspectors
- (h) Commission (directly, in contrast to present back-up responsibility) for system design

The Panel also believes that any significant dispersal of responsibility for service and cost would ultimately jeopardize the performance of the telephone network. The Panel also believes that this can be prevented by so structuring a program of standards and certification that the final authority for each segment of the program rests with the federal regulatory commission having jurisdiction over the carriers.

Installation and maintenance work will usually be performed at the request or direction of the user. The user therefore should be required to acknowledge his responsibility for abiding by rules he understands. The Panel believes that the vast majority of users will accept such responsibility if care is taken to be certain that each one is aware of the rules and limitations. Users who wish to interconnect directly with the network should be required, in the process of applying for such privilege, to affirm their acceptance and understanding of the provisions of the tariffs governing such interconnection. If the evidence of such awareness is provided in the form of an application for service, then the carriers and the commissions will have the necessary tools and authority to deal with problems on a case-by-case basis.

The question of jurisdiction among the several commissions, federal and state, must be considered. Equipment manufacturers cannot deal with a multiplicity of standards, and centralized authority is thus essential. Minimum standards for the certification of servicemen will be a parallel effort with the setting of standards for equipment, and the same uniformity

is needed. Nationwide service considerations would seem to require that practices be uniform, or nearly so, and certainly, certified equipment will be shipped from state-to-state. To retain the greatest practicable degree of centralized responsibility, the Panel recommends, therefore, that all standards and certifying organizations cooperating in the program derive their authority from the same federal regulatory agency having jurisdiction over the services of the common carrier. The tariffs would contain the provisions governing interconnections.

#### COSTS

The Panel has been requested to consider the technical aspects of interconnection with the telephone network, and of making recommendations on the basis of those considerations. At this time there is no available cost-data base for analysis. Nevertheless, every technical conclusion is associated with costs, and some general comments in this area would be worthwhile.

Many of the presentations made to this Panel have included protestations that this or that solution entailed an unnecessary cost burden. Consideration of any one cost by itself is easily transformed into a debate about who should bear the cost, or of how costs should be distributed among users and suppliers of telephone service. Such a debate is beyond the scope of the assignment given to this Panel.

What matters is that all costs that result from interconnection be recognized, and that they be held to a level that is reasonable in relation to the benefits expected to follow. While the directly connected user will have expenses for equipment purchase, installation and maintenance, the carriers will also have costs associated with direct connection. These will be primarily associated with changed maintenance and installation procedures and administrative tasks.

The apparent waste involved in requiring the use of protective interface devices in all cases, may be offset more or less by the reduction or elimination of other costs that are less visible, but just as real. The overall standardization-certification program will also entail costs. In this connection, a figure of \$1,000 has been suggested for test and evaluation of the production run for one manufacturer's small product. Final figures will depend upon volume as well as details of the equipment configuration.

It should be noted that the whole subject of rates has been outside the scope of this Panel's consideration. Nevertheless, rates are basic to this entire issue, as they will determine the degree of interest among users in any interconnection method beyond that presently authorized by the tariffs. Since there is as yet no experience with

direct interconnection, no conclusions in the area of rates are possible.

#### CONCLUSIONS

- (a) The establishment of standards and the enforced certification of user-supplied equipment and personnel form an acceptable way of ensuring network protection.
- (b) Authority for a nationwide certification program should reside with a federal regulatory agency responsible for the tariffs.
- (c) A carefully planned and timed step-by-step effort is necessary to ensure the successful implementation of a certification program.
- (d) Self-certification by manufacturers or users will not ensure an acceptable degree of protection.

#### INNOVATION

##### INTRODUCTION

For the purpose of this section, the term "innovation" will be taken to mean the introduction and use of new equipment, new uses of equipment, or new services. We are not concerned here with inventions or ideas per se, but rather with the ability to put inventions or ideas to practical use by the telephone companies or those who wish to interconnect.

The principal consideration here is interconnection with the Direct Distance Dial (DDD) network, although some of what is discussed is obviously applicable to the question of interconnection with private lines as well.

The impact of innovation has not been presented as a major issue before the Panel, but some concerns have been expressed. It is clear that many of those concerns are the result of interconnection itself and the fact that interconnecting parties and the carriers will have to cooperate in some way to reach solutions to problems when their interests do not coincide. The amount and kind of protection required for the network and the method of providing it tend to change the nature and degree of the problems, but do not solve them. Few, if any, of the problems are entirely technical in nature, although technical factors should be considered in any policy decision.

Although the discussions before the Panel have been addressed primarily to problems that might limit innovation, it seems clear that interconnection will have a positive influence on innovation in some cases. The Panel has made no systematic attempt to survey new technology and potential new developments. For our purposes, the material presented to the Panel in response to our inquiries seems adequate. For this reason, the references to new technology and new developments cited below should be considered only as examples of things that are reasonably well understood and which may have some impact in the not too distant future.

The incentive to innovate is usually economic, either directly or indirectly, whether it be to provide an existing service at lower cost or to provide a new service. The increasing dependence of the business community on communications in a variety of forms will provide ample incentive for continuing innovation in an era in which technology is likely to advance rapidly.

New Switching Systems

The move toward all-digital transmission in the long-distance plant will lead also to the switching of signals in digital form. Such switching already exists in special networks like that of Western Union. Since such a switch looks essentially like another digital-transmission link, it would have no additional effect on the criteria for interconnection.

In the local or exchange switching plant, the desire to go to solid-state electronic crosspoints in the switching network has been thwarted somewhat because of the need to pass the high voltages required for ringing the telephone. This is one example of a situation in which the system balance may change with integrated electronics. It may be that by putting a tone ringer and perhaps tone transmission of off-hook/on-hook signals in the telephone, even at added expense, the resulting impact on the local office, which might then make extensive use of electronics in the switching path, would more than offset the additional costs, if any, in the telephone. Such tradeoffs could, of course, have a significant impact on interconnection and the interface between user-owned and carrier-owned facilities.

New Signaling Systems

Currently, signaling in the DDD toll plant includes the use of a 2,600 Hz tone to indicate the busy or idle status of trunks. The tariff criteria are set up to protect this 2,600 Hz signaling system. The future direction of signaling appears to be toward systems that are separate from the voice-band path. Hence, with such systems, the protection of 2,600 Hz will no longer be necessary, but because of the very widespread use of the present system, it will be a significant factor for years to come.

NEW SERVICES

PICTUREPHONE

The Bell System has conducted trials of a switched see-while-you-talk service called PICTUREPHONE and has announced that a commercial service offering will be made in 1970. It has also advised the Panel that interconnection arrangements will be available at, or soon after, the introduction of the service.

This service will have, in addition to the normal audio pair in the loop, two pairs of wire for the video (one for each direction), with a transmission capability approaching 1 MHz. In the digital toll transmission plant, the voice and video will be multiplexed on a 6.4 MB/s bit stream.

The system clearly has capability for high-speed data.

Since the interconnection arrangements have not been announced, the Panel has no basis on which to make detailed comments. One observation, however, can be made. The audio pair is used for network-control signaling. The question of interconnection to the two video pairs should then be limited, in the technical sense, to transmission and physical-protection criteria.

DATA-PHONE 50

The Bell System has recently begun a 50 kilobit service called DATA-PHONE 50. No provisions have been made for interconnection and a few parties have suggested that interconnection be allowed. Although the Panel has not studied the characteristics of this service, it sees no technical reason why interconnection should not be permitted, consistent with the final decisions regarding interconnection for voice-band circuits. The use of this service will likely be primarily for computer-to-computer data transmission in load-leveling, national data banks, national network access for remote access users, etc. It will be desired to incorporate into computer communication hardware all automatic functions as opposed to manual functions most used today in voice-band data transmission.

OTHER NEW SERVICES

Other new services are likely to be offered in a way and form that can only be estimated at this time and which will depend not only on technical factors but also on actions by regulatory agencies. The offerings of the types recently proposed by MCI and the DATRAN service are examples. We have grouped such services under the general heading of customized common carriers. They will, in general, we believe, aim their offerings at the business community and perhaps especially at users of data services, where the rate of innovation will be high. In this connection, we observe that, from a technical point of view, many of them will depend on interconnection with the common carrier.

POTENTIAL RESTRICTIONS TO INNOVATION

Problems of Information Transfer

The need for more information to be exchanged between suppliers and users on the one hand and the carriers on the other was evident in the

presentations before the Panel. Users suggested arrangements to the Panel that the Bell System had already provided for, but about which the user was unaware. Other cases came up in which the Bell System stated its intent to the Panel to provide for connecting arrangements, but that intent was unknown to suppliers and potential users. Regardless of the procedures finally adopted for providing protection to the network, whether by interface boxes, by standards, or some other arrangement, some method should be worked out to allow for better interchange of information. Some of this will come naturally with time as all parties gain experience with interconnection, but the problem will remain to some degree. Further, it is evident to the Panel that many customer systems have or will have terminal points in independent companies, as well as Bell System territory, and better communication with the Bell System is not sufficient. This issue will be addressed further in Section 9.

#### Questions of Timing

Perhaps the most significant question of timing is that of the response time of carriers to new user requirements. Users have found that arrangements that are nominally available are not actually readily available in all Bell System companies when they want them and not available at all in some independent companies. This is inevitable in the initial stages of a change as significant as interconnection. Nevertheless, many people feel that the carriers will not be able to respond rapidly enough with new protective arrangements and that they could innovate faster if they included the protection in their terminals. They could then make it available on their equipment regardless of the location or company.

A second question of timing has to do with the changes in the carriers' system that might make user equipment obsolete. The Bell System has expressed concern that if a user has just purchased new equipment, he will be reluctant to accept a change in the telephone system that would require substantial change in his equipment.

Several users, especially those in fast-moving fields like computer communications and those who have historically interconnected with the carriers' private lines, suggest that the rate of innovation in the DDD network will pose no problem to them.

#### Questions of Cost

An important cost question from the suppliers point of view is the cost of a new connection arrangement for some new service or use he may want to offer. If he included the protection in his own design, he would be able to determine the total cost himself. If he must wait for a carrier tariff, the total cost of his service will be uncertain until the tariff is filed.

Another criticism of the present arrangement is that suppliers fear that the carriers can compete unfairly because, in their opinion, the added protective box makes customer-owned systems more expensive and less reliable than comparable carrier-owned systems. The Panel recognizes that the question of actual overall cost is a complex one and has made no evaluation of costs, including those of administration, etc., as they relate to different approaches. Section 6 discusses some of the general cost tradeoff areas in greater detail.

#### Restriction of Use

Present connection arrangements are on a per line basis and are tailored to a specific terminating arrangement. Some users may want to use a line for one purpose at one time (e.g., during the day) and something else at another time (e.g., during the night). This argues, in their opinion, for an arrangement that is physically a part of the terminal rather than the line. The Bell System has agreed that this may be possible using carrier-owned protective devices integrated into the customer equipment.

In a different vein, the carriers point to a potential use of characteristics of specific designs in the network that are incidental to its normal use and that may be different in subsequent generations of equipment. An interconnecting arrangement that takes advantage of such arrangements may unknowingly be made obsolete by new designs. An example brought before the Panel involved the use of single tones produced by pressing two touch-tone buttons simultaneously. The new integrated circuit version of the touch-tone generator does not produce the single tone since that feature was only incidental to the original design.

#### SUMMARY OF ISSUES AND CONCLUSIONS

The carriers have said that widespread interconnection will tend to impede innovation in the network, because, among other things, users will tend to oppose changes by the carriers that make the users' equipment obsolete or require it to be modified. They have also said that direct interconnection without carrier-owned interconnecting arrangement will further impede their innovation because it removes the carrier-controlled buffer with known characteristics between the network and the interconnected equipment.

Some users, especially the large ones and those in fast-moving fields such as computer time-sharing, have expressed the opinion that, with the necessarily deliberate rate of innovation expected in the network, there will be no major problems in keeping up with network innovation. They do

not agree with the carriers' concerns regarding the need for a carrier-controlled buffer.

Some suppliers of equipment and services have expressed the opinion that the presence of the carrier-owned interconnecting arrangement will impede innovation on the user side of the interface, where the goal is to optimize the users' system or use of equipment. Further, and perhaps more importantly, they question the ability of the carrier to respond rapidly enough to new situations in which new interconnection arrangements are required.

While data on which to base conclusions are limited, it is the opinion of the Panel that:

1. The advent of widespread interconnection itself, regardless of how it is implemented and controlled, may indeed have some effect on the rate of innovation by carriers, suppliers, and users. In some cases, it may impede innovation in the network and, in other cases, it could conceivably promote innovation because of the pressures of demand from users. It will certainly tend to increase the rate of innovation by suppliers and users.
2. The introduction of a certification program for direct interconnection will not significantly restrict carrier innovation if there is effective information exchange between carriers, suppliers, and users. On the other hand, the suppliers and users will have more freedom to innovate.
3. On balance, under the certification program, innovation in the overall system by carriers and users of interconnected equipment is likely to increase.

APPLICABLE EXPERIENCE

COMMON-CARRIER APPLICABLE EXPERIENCE

The common carriers have had extensive experience with interconnection between carrier systems and with non-carrier user-owned and user-maintained equipment and systems.

Interconnecting with Each Other

Communications carriers are extensively interconnected with each other. There are approximately 1,900 independent telephone systems connected with the Bell System. The Western Union Telegraph Company is interconnected with the Bell System and many of the independent telephone companies. The international communications carriers, including COMSAT, are interconnected with the Bell System. The Bell System, the international carriers, and COMSAT are interconnected with foreign carriers.

These interconnections are all arranged on a contractual basis with standardized interface arrangements developed by extensive inter-carrier committees and consultative groups. The Federal Communications Commission and forty-nine state regulatory commissions act as referees, or courts of appeal, if difficulties arise over the interconnection interface. However, the fifty or more years of experience the telephone industry has had in arranging interconnections from simple interfaces involving manual plug and jack telephone switchboard to the complex automatic systems providing for nationwide (and now international) Direct Distance Dialing (DDD) have resulted in a surprisingly small number of appeals to these commissions. Design procedures and the authority for interconnection have been formalized between the carriers and the regulatory commissions, such that these practices are well established and thoroughly understood throughout the telecommunications industry.

Equipment standards and practices are based on voluminous documentation prepared by joint industry committees. Equipments and practices developed by the Western Electric Company are widely used "standards" of reference throughout the industry and many manufacturers substantially duplicate this equipment for use by the independent telephone companies.

Standards for maintenance and repair and standard practices for installation and preventive maintenance have been established by the industry through experience with extensive analysis of equipment failures and faults. Technical equipment and system innovation promoted by both the carriers and the manufacturers of communications equipment is pursued on an industry-wide basis, with extensive consultation through the many joint

committees between the Bell System and the independent carriers. New services, when requiring new technical equipment, system practices, transmission standards, etc., are developed jointly between the AT&T and the independent companies. After new services have been tested experimentally, standard operating procedures, inter-company tariff agreements, and revenue-sharing arrangements are established.

The assignment of cost burdens between the several carriers is established on the basis of the current separations formulas, or through negotiation and action with the responsible regulatory commissions.

The experience of inter-carrier interconnection arrangements has applicability to the present study to the extent that two organizations operating on the opposite side of an interconnection interface can perform successfully when both operate to compatible or the same standards and are technically and operationally qualified, and when both are similarly motivated to provide efficient, economical service with minimum disruption due to interconnection difficulties. Common regulatory authority assures a degree of common motivation of all telephone carriers.

#### Non-Carrier Interconnections

There has been experience with a very considerable number of non-carrier interconnection arrangements. The largest of these users are the United States Government agencies, particularly the Department of Defense, which, for many years, has made extensive use of common-carrier systems, often providing its own terminal equipment, including PBX's. Another class of users has been the so-called right-of-way organizations (railroads, pipelines, electric utilities) who have operated their own communications systems with varying degrees of interconnection with the telephone carriers. Aeronautical Radio Incorporated (ARINC), serving the air-transport industry, has operated an extensive network and many localized interconnection arrangements. Most of these are on an allocated circuit (leased-line) basis, but there has been some use of interconnection with the switched network, theoretically only on an emergency basis.

User systems are designed, in most cases, with extensive consultation with the carrier involved and often with installation of test equipment and practices to protect the network.

In many cases in the past, the equipment employed has been Western Electric-manufactured or manufactured by other concerns on the basis of Western Electric's specifications and designs. Currently, equipment is being manufactured in accordance with accepted national or international standards by competent manufacturers and many satisfactory interface arrangements have resulted.

In most cases, the organizations concerned are adequately competent technically and motivated to maintain equipment to high standards of performance, and interconnection problems have been manageable.

There is applicability to the present study in these non-carrier interconnection arrangements, both from the standpoint that several have been highly successful and trouble-free, while others have resulted in troubles. Both of these cases will be discussed in greater detail later in this section.

#### Experience of Right-of-Way Companies with Carrier Interconnections

The right-of-way companies, to which might be added ARINC, have had extensive experience using carrier circuits as part of their systems. In many cases, these right-of-way companies own and operate private communications systems (microwave relays being the most important, but other systems are also included) which serve their principal operational locations. These locations include railroad switchyards and terminals, pipeline pumping stations and control centers, utility generating and distribution systems, substations, and other installations. In the case of ARINC, circuits are used to interconnect transmitter and receiver or transceiver sites with communications and control centers.

Much of the equipment used by the right-of-way and similar utility companies has been developed and procured in accordance with specifications or practices developed by carriers or manufacturers who are skilled in providing equipment for the telephone utilities. Interface problems have developed from time to time, but these are generally worked out amicably between the user and the carrier with satisfactory settlement of areas of responsibility.

One submission by such a user summarizes its experience with interconnection. It has nearly 500 unattended stations controlled over Bell System circuits by operating centers sometimes located several hundred miles away. The user also has an Electronic Switching System interconnected with over 800 Bell System circuits. This user had no reports of dangerous voltages or currents having been introduced into the carrier system through its operations, and, from the user's standpoint, service has been entirely satisfactory without the necessity of interface devices between the user and the carrier facilities. The user has extensive procedures and facilities for monitoring the nature of the signals introduced by it into the carrier network. It has also established rigorous preventive maintenance procedures with about sixty maintenance men and thirty fully-equipped maintenance trucks constantly visiting and checking facilities throughout the United States.

#### Experience of Foreign Communications Carriers

Foreign communications carriers have been concerned with the problem of interconnection of non-carrier equipment in varying degrees. The extent of the problem depends upon the policies of the carrier, the extent to which the carrier is able to meet urgent demands for switched telephone services, and the nature of its organization.



The applicability of the experience of foreign carriers to the specific problems facing the FCC and the U.S. carriers varies, both because of the widely differing circumstances under which different foreign carriers operate and the lag in the development of pressures for the use of the carrier networks for many non-telephone purposes.

In general, the carriers in the developed industrial countries have a monopoly of telecommunications services. This is achieved by the carriers, either being a ministry of government -- as in the case of the Bundespost and the PTT's in various countries -- or a chosen instrument government-chartered corporation, such as the Nippon Telephone and Telegraph Public Corporation or the British Post Office Corporation. The extent of the monopoly varies but, in general, it is quite complete and to challenge it is, in effect, to challenge the government.

Most of these foreign carriers are responsible for the total of domestic (and, in many cases, foreign) telecommunications services. This includes message telephone service, telegraph services including TELEX, the provision of leased lines for all services from narrow-band telegraph to television program relay. There are exceptions to the provision of television program distribution, such as the separate network of EUROVISION in Europe, but such exceptions are limited. In the case of the communications systems operated by government ministries, the ministry is, in effect, the FCC, the AT&T, the independent telephone companies, Western Union, private microwave services, etc., all incorporated in one organization. In general, the policies of such an organization can be challenged only through the national parliament. In the case of the recently established British Post Office Corporation, one of the objectives was to remove the carrier from detailed political surveillance by parliament and permit it to concentrate on the technical, operational, and business-management aspects of a major service business. In this case, to provide for customer or public influence or guidance in the operations of the carrier, several Country Councils and a National Council have been established.

In many countries, the primary orientation has been almost exclusively toward public message telephone and telegraph services and financial and plant resources have been inadequate to fulfill the demands for these services; hence, the carriers have been slow in permitting any extensive use of their facilities for other services. This has been particularly true of certain countries of Western Europe that have been loath to commit transmission facilities to private-line services when they are sorely needed for public message telephone service.

An advantage a government ministry or chosen instrument corporation has is the ability to rank order subscribers or using agencies giving preference to those adequately qualified. These include other government departments and agencies, the railroads or other right-of-way companies, and large technically qualified industries. The government department, or government-backed corporation, is in a strong position to

technically and motivated to performance, and interconnection

discontinue service if established specifications, practices, or standards are not adhered to.

These "monopoly" carriers can, and do, establish and enforce rules ensuring adherence to high standards in the procurement of customer equipment. They can establish specifications, require type approval of all equipment -- even to the extent of testing it in their own laboratories -- before manufacturers are permitted to sell to prospective users for interconnection. The British Post Office, for example, has long avoided the investment in large PBX's by requiring the user to procure his own, but it has type-approved only a few models produced by manufacturers who supply equipment to the Post Office and manufacture in accordance with Post Office specifications, practices, and standards. The PBX is then installed in accordance with the Post Office-established specifications and then maintained by Post Office personnel. The Post Office permits interconnection of automatic dialers and other devices for fire, burglary, high water, and other alarm services. However, these must be connected in parallel with a standard telephone installation, the device must pass a Post Office qualification test, and be maintained in accordance with established standards.

The ministry of telecommunications or a national telecommunications corporation can make any necessary decisions as to the placement of economic burden for provision of non-standard services for any interconnection arrangements or for other costs occasioned by user-provided equipment. The British Post Office requirement that the user provide large PBX's is a good example of this.

#### Experience with Extra-Legal Interconnections

Prior experience with unauthorized interconnection has given some indication of problems that might develop with formal arrangements for interconnection of user-provided equipment without some protective interface between customer-owned and customer-maintained equipment and the carrier facilities.

Amateur radio operators have long used "phone patches" for connecting amateur radio telephone stations to the switched network in order to permit their friends to communicate with distant parties through amateur radio. Most of the telephone companies have countenanced this "illegal" use of the system as a service to the amateurs and the public and relatively few cases of trouble have been experienced. In general, an amateur operator is a competent technician and the amateur's carrier-provided telephone is used to perform the signaling functions, and the phone patch is only connected while the call is in progress.

There is a body of experience of difficulties with user-installed extension telephones that usually shows up only when the telephone is defective or the mismatch between the characteristics of the "foreign"

manufacturers in the computer field occurred over ten years ago in the

telephone and the requirements of the loop are such as to result in a report of poor service or a failure of service.

A survey of state regulatory commissions indicates a limited accumulation of knowledge concerning troubles from interconnection of user-owned equipment, although a considerable number of examples were cited in which such equipment had been interconnected with telephone company facilities resulting in service calls and difficulties in clearing the trouble. One commission cited fifty-four trouble reports during a recent, but unspecified, period in which user-owned equipment was involved, of which forty-five were found to be faults in the user equipment. A second commission cited an example of computer time-sharing terminals connected through a local central office, which contributed to a serious overload condition. In this case, the holding time per call on the terminals was approximately ten times the holding time on regular business telephone lines. A number of other specific examples were cited by this commission.

The experience here is applicable to the present study to the extent that it indicates that a customer with inadequate technical and operational competence may create difficulties in the common-carrier network.

#### Experience in Other Areas

There is experience in other technical and service enterprises in which interconnections between systems or system components may be pertinent to the study of interconnection with telephone systems.

#### Computers (Main Frames and Peripheral Equipment)

A good example is the interconnection of peripheral equipment of one or several manufacturers with a computer main frame of another manufacturer.

The computing industry had to face the interconnection issue years ago. The large computer main-frame manufacturer maintained a strong sense of overall systems responsibility very similar to the common carrier's position, which has been altered by the Carterphone decision. The manufacturers maintained that they could not be responsible for the performance of the system if the customer uses other than the manufacturer's equipment and supplies. The issues are comparable in certain respects to those posed in the common-carrier interconnection case. Who is responsible for maintenance and installation? Will the attachment harm the system? The attachment may have greater capability, lower cost, etc.

The first departure from the entrenched position of the main-frame manufacturers in the computer field occurred over ten years ago in the

magnetic tape area. Computer manufacturers sold their approved magnetic tape, but the users started buying from other independent suppliers. In general, the tape worked quite well and it represented an appreciable cost saving to the user. Customers were warned, however, that they had now transferred the responsibility for tape-handler performance to themselves. When there was doubt as to whether the tape handler or the tape was at fault, the manufacturer's serviceman used a "good standard" tape to prove the case one way or the other. Even though the responsibility for tape performance was thus assumed by the user, he was willing to take this responsibility judging by the amount of magnetic tape being purchased from independent manufacturers today.

Within the past few years and with the fantastic growth of the computer industry, many independent peripheral device businesses have been spawned. More are being born each day. There are now a large number of organizations providing peripheral devices like punched-card readers and punches, high-speed printers, tape handlers, and disc handlers to customers in competition with computer main-frame manufacturers.

Interconnection of these attachments raised grave concerns among the computer main-frame manufacturers. The complexity of the interface between the peripheral device and the control unit or computer is such as to make the telephone interconnection interface seem much simpler in comparison. Signal frequencies are in the megacycles rather than cycles, levels are in the milli or microvolts, cross-talk problems are fierce, and timing-control sequences are much more complex and precise than the dial pulses or tones used in the telephone network-control system. Yet, users have decided of their own volition to risk the interface problem and incur the division of responsibility to accrue cost savings.

To the Panel's knowledge, the use of such attachments, especially disc and tape units, has been successful despite the complexities of the interface. The user will undoubtedly experience greater difficulty and delay in resolving a malfunction, but he apparently feels it is worth the cost differential. In the event of malfunction, the user will, in most cases, have to call the computer main-frame maintenance man to diagnose whether the problem is in the peripheral or in the system. If the problem is in the peripheral, he then has to call the peripheral service company, thus paying a double maintenance charge and incurring extra delay. If the problems are obviously in the peripheral, he need call only the one company. The same maintenance philosophy can apply to the interconnection of foreign attachments to the telephone lines.

It appears that foreign attachments will be a way of life for the computer industry. The weakness of the analogy pointed to above is that only the user may be harmed in the case of the computer attachment while many, who are generally unknown, may be harmed with a bad telephone attachment, although, with the advent of computer time-sharing, this may become less

true, but here again, it is the user or provider of the particular computer time-sharing service who accepts the degradation in service to reduce costs. Further, there is no comparable problem of hazard to personnel or property of other than the user of the computer.

#### Broadcast Interconnection Arrangement

There is considerable experience of some relevance in the broadcasting industry (sound as well as television) in the interconnection of user-owned equipment with the carrier facilities. These are almost exclusively leased-line situations with full-period or temporarily allocated circuits in use for broadcast purposes. These systems are operated without additional complex interface devices between the user and the carrier facilities.

#### Experience with Government Networks and Equipment

The largest single class of interconnected communications systems and terminals in the United States are those of U.S. Government agencies -- the largest being the Department of Defense.

#### Defense Communications Systems

There is a long complex history of a partnership between the Department of Defense and the U.S. domestic and international common carriers. In this connection, a wide latitude of interconnection of government-owned equipment and systems has been permitted by the common carriers as exceptions to normal tariff arrangements. Last year, the government obtained approximately one-half billion dollars of telecommunications services and facilities from these carriers. The largest single aggregation of such facilities is the Defense Communications System (DCS), which is being evolved from the systems of the three military services. When put together with systems of the other principal departments and agencies of the government, the whole becomes the National Communications System. Leased carrier facilities (particularly in the continental forty-eight states) comprise the bulk of the National Communications System (NCS). Major components of the NCS are:

1. The CONUS AUTOVON system, a leased telephone network provided by AT&T and the independent telephone companies. AUTOVON provides the backbone voice network for national security command-control communications.
2. A companion to AUTOVON is CONUS AUTODIN, a leased system provided by the Western Union

Telegraph Company, providing record-communications for the Department of Defense and certain other associated activities.

#### DCS Specifications

The Defense Communications Agency, with the advice and assistance of other agencies, has developed DCS and NCS specifications (in many cases, substantially equivalent to those descriptive of the public telephone network) to guide the evolution of the Defense Communications System and the National Communications System. These specifications include interface specifications for interconnection of the government-owned equipment with carrier facilities.

#### Government Systems Other Than Those Operated by Defense

There are a number of government systems other than those operated by Defense. Principal among these are:

1. The FTS (Federal Telecommunications System), a CCSA voice network administered by the General Services Administration and providing service to all government agencies, but primarily service to agencies other than DoD.
2. The ARS (Advanced Record System), a GSA-administered record-communications system leased from Western Union, provides these services for government agencies other than the DoD.

#### Preferential Treatment by Common Carrier

Because of the nature of government requirements, particularly those associated with national security activities, the space program, and other critical government activities, the carriers have afforded the government special treatment in regard to interconnection, such as the use of customer-provided equipment and the provision of special telecommunications arrangements to meet unique requirements. As was demonstrated to the Panel, these arrangements have not been without cost and difficulty. Although the DoD is probably the largest technical organization in the world with extensive capabilities for procurement, installation, and operation of telecommunications-type equipment, many problems have developed as a result

of interconnection arrangements without interface devices to shield the common carrier network from failure, malfunction, or deliberate misuse of user facilities.

It has been shown that DoD interconnection of user-owned and maintained equipment with the Bell System accounts for a disproportionate share of the troubles in terminal equipments and transmission arising through interconnection.

#### Conclusions

The review of the practices of certain foreign carriers and the experience of U.S. carriers with interconnections provides many lessons germane to the recommendations of the study Panel. The most comprehensive experience is that derived from interconnections of government-owned equipments and systems (primarily those of the U.S. Department of Defense) with systems of the common carriers.

There is also a large background of experience with interconnection of systems and equipments operated by the right-of-way companies, including the railroads, pipelines, electric utilities, etc., and with communications-service organizations such as ARINC. There is also some applicable experience with the connection of user-owned telephones and other terminal devices to carrier networks. There is, however, no experience applicable to large-scale interconnection of small, individual users, and the Panel concludes that it must be approached with great care.

The Panel also concludes that:

1. Interconnection without special interface devices is possible without service impairment or hazard to carrier personnel only under favorable conditions,
2. Such interconnections without restrictions could cause substantial service impairment,
3. Favorable conditions are necessarily associated with incentive, ability, responsibility, and user resources.

#### INFORMATION AND ORGANIZATION

The need for improved information transfer among carriers, users, and sponsors was demonstrated on numerous occasions during the study. This lack of information is felt by all and will grow more serious as the interconnection area evolves. It exhibits itself in the improper design of equipment, confusion as to rules, rates, and procedures, and a certain rigidity in the approach to mutual problems. At present, no formal organizational mechanisms exist to provide the desired information interchange. It is the opinion of the Panel that such mechanisms should be established in this area to cope with the problems that are sure to develop.

Existing inter- and intra-industry organizations should be encouraged to assist in improving the flow of technical information not only among the carriers, manufacturers, and users, but also within manufacturing and user organizations. It is especially important to expedite the process of obtaining agreement among the groups through technical and standardization meetings.

As discussed in the section on "Certification," certain organizational steps and mechanisms should be developed if that program is to be implemented. In that connection, organizational mechanisms may be similar to others but with a major difference, i.e., that of responsibility. Since the certification program will be reflected in tariffs, the Federal Regulatory agency responsible should ensure that the certification program reflects that responsibility. Such a new organizational mechanism should, therefore, be formally recognized to ensure that proper weights are attributed to its recommendations.

The Panel recommends that organizational mechanisms be established to:

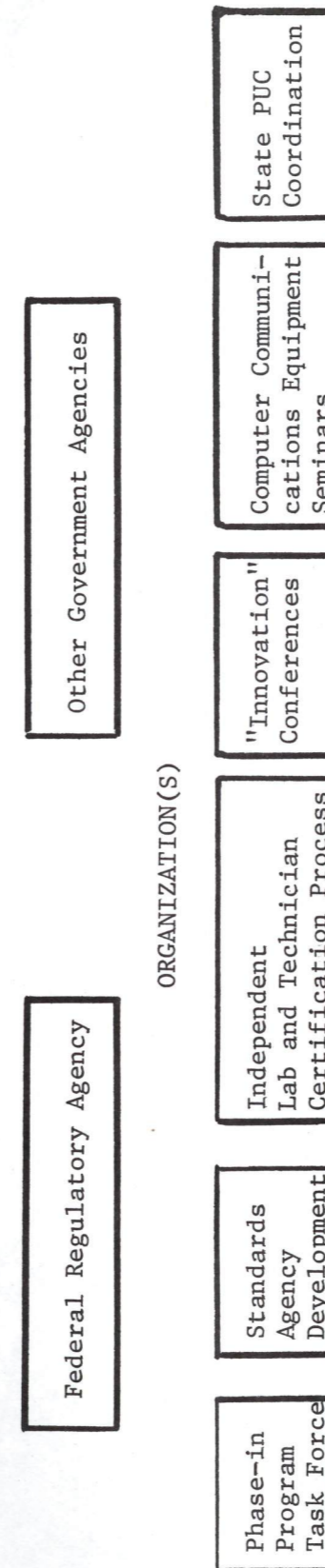
1. Promote a two-way exchange concerning problems of interconnection interfaces among users and suppliers and between them and the carriers. This exchange is vital to the problem of possible liberalization of interconnection and the resulting integrity of the public telephone network.
2. Promote and establish working groups that will be concerned with standards development, certification programs for equipment, licensing programs for installation and maintenance procedures, and finally, with the data gathering and analysis of technical interfacing problems. The various user groups should have a common, authoritative forum to which data are fed and reacted to in the coming decade. Other trade

and industrial organizations would probably welcome an independent atmosphere for discussions related to their specific positions on interconnection policy from a technical standpoint.

3. Develop recommendations to a federal regulatory agency as to the timing of the elements of a phasing-in process if a certification program is established. These recommendations should specify specific changeover interim periods for certain classes of users to minimize the impact of the new standards and certification programs.
4. Promote a workable atmosphere concerned with innovation problems in interconnection on a continuing basis. There are three areas of concern: (a) interchange of ideas and information before new concepts and equipment developments are implemented; (b) interchange of ideas and new approaches before installations are made (by the carrier or user); and (c) interchange of problems data after new services are installed in which unforeseen problems sometimes arise.

A possible structure of a possible new organization is noted in Figure 1. This structure is purely an example and is by no means meant to be definitive. Various standing committees on continuing problems could be organized and short-range ad hoc groups would function on specific problems such as the phasing-in period for the proposed standards and certification program for direct-connection equipment. Another important area is that of coordination with the state regulatory agencies to foster a degree of uniformity on technical matters.

FIGURE 1





**digital**

March 9, 1972

Dr. Sidney Fernbach  
Head, Computation Department  
Lawrence Radiation Laboratory  
University of California  
Box 808  
Livermore, California 94550

Dear Sid:

Tony Oettinger asked me to comment on the draft report, "Computer/Calculator Differentiation for Export Control Purposes", prepared by the panel you recently chaired.

I agree with the basic conclusions and recommendations outlined in this report. Relaxing the export licensing requirements to the bloc countries on calculators will enable more of the resources of the Office of Export Control to be devoted to the case-by-case analysis of export license applications for digital computers. Manufacturers of digital computers and the US balance of trade will both benefit if more expeditious processing of Communist Bloc export licenses becomes possible.

I realize that the Office of Export Control is at the moment overloaded with requests for export licenses for calculators to the bloc countries. This report recommends an approach that seems to be a sensible way of approaching the problem.

I would comment, however, that some provision should be made to establish a committee representing all the interests involved, to periodically review both the "boundary" value of the numerical processing rate and its concept to assure its continuing effectiveness.

I have not listened to the pro and con arguments for some time, but I think now is the time to drop all or almost all restrictions on export of computers.

Sincerely yours,

Kenneth H. Olsen  
President

MAR 6 1972

NATIONAL ACADEMY OF SCIENCES

COMPUTER SCIENCE & ENGINEERING BOARD  
2101 CONSTITUTION AVENUE  
WASHINGTON, D. C. 20418

March 1, 1972

Mr. Kenneth Olsen, President  
Digital Equipment Corporation  
146 Main Street  
Maynard, Massachusetts 01754

Dear Mr. Olsen:

Professor Anthony G. Oettinger, Chairman of the Computer Science and Engineering Board has asked us to request your assistance in commenting on the attached draft report for the Office of Export Control of the Department of Commerce, recently prepared by a Panel chaired by Dr. Sidney Fernbach.

The proposal governing the study is provided as background with the hope that you will be able to assist us in this regard. Should you find that you are unable to get your comments to Dr. Fernbach by March 9th, please let us know at your earliest convenience.

Dr. Fernbach's address is:

Dr. Sidney Fernbach  
Head, Computation Department  
Lawrence Radiation Laboratory  
University of California  
Box 808  
Livermore, California 94550

Your comments will be held in strict confidence. In fact, your comments may be made anonymous, if you so desire. The main point is that you feel you can express your judgments freely.

Sincerely,

  
J. F. Kettler  
Assistant Secretary

JFK:kmp

Enclosures:

As stated above.

P. S. PLEASE NOTE THAT THE ATTACHED PROPOSAL AND DRAFT REPORT ARE PROVIDED UNDER THE "NAS ACADEMY PRIVILEGED SYSTEM," MEANING ACCESS IS RESTRICTED AT THIS POINT TO YOURSELF AS A CONSULTANT TO THE NAS.



pdp11  
memo

TO: Ken Olsen  
FROM: Dick Finn/PDP-11 Sales Support

DATE: 8 March 1972

RE: Comments on attached National Academy of Sciences Draft Report

Presently, desk calculators are subject to most of the same regulations and procedures governing export of full-fledged digital computers. The attached draft report proposes that a boundary between calculators and computers be defined, and that the regulations governing the export of calculators be greatly relaxed. This is a good idea.

When the workload associated with licensing calculators on a case-by-case basis is eliminated, I see an immediate advantage to us. More of the limited resources of the Office of Export Control will become available to process the case-by-case type of export licensing application which will still be required for the communist bloc export of most of our products.

The only disadvantage this procedure might have is that the communist bloc countries might be able to get their hands on advanced LSI chips a little sooner than they might otherwise be able to do by buying them in calculators. It was rumored in the early days of integrated circuits that the communist bloc purchased instruments just to take out IC's and use them for other things. If technology of interest to the communist bloc becomes available in calculators the potential leakage of technology can be remedied simply by redefining the boundary between calculators and computers and placing advanced calculators under more strict export regulations again.

The definitions seem reasonable; ie, desk calculators should not have I/O connectors that can be used for controlling external devices or gathering external data. The panel has defined a quantity they call Numerical Processing Rate (NPR) defined on Page 9 of the report.

All machines which exceed 0.25 million bits per second, numerical processing rate would be considered computers and would be subject to computer export licensing procedures; those with NPR less than 0.25 million bits per second would be considered calculators. Applying this concept, the PDP-11 would require usual export licensing for bloc country export as I believe it should.

The proposal does not provide a mechanism for reviewing and perhaps redefining the value of the NPR which determines the boundary between calculators and computers. As desk calculators become more sophisticated, they may represent a means of exporting technology if the proposed procedures are not given constant review.

The report seems to be somewhat apologetic for defining a somewhat arbitrary quantity such as the numerical processing rate but they had to start somewhere and to me this seems to be a reasonable way of doing it.

Attached is a draft of a letter that you might want to consider when you reply to Dr. Fernbach.

j

8 March 1972

Dr. Sidney Fernbach  
Head, Computation Department  
Lawrence Radiation Laboratory  
University of California  
Box 808  
Livermore, California 94550

Dear Dr. <sup>sid</sup> ~~Fernbach~~:

~~Professor~~ <sup>Tony</sup> Oettinger asked <sup>me</sup> us to comment on the draft report "Computer/Calculator Differentiation for Export Control Purposes" prepared by the panel you recently chaired.

<sup>I</sup> We agree <sup>with</sup> that the basic conclusions and recommendation outlined in this report. Relaxing the export licensing requirements to the bloc countries on calculators will enable more of the resources of the Office of Export Control to be devoted to the case-by-case analysis of export license applications for digital computers. Manufacturers of digital computers and the US balance of trade will both benefit if more expeditious processing of communist bloc export licenses becomes possible.

<sup>I</sup> We realize that the Office of Export Control is at the moment overloaded with requests for export licenses for calculators to the bloc countries. This report recommends an approach that seems to be a sensible way of approaching the problem.

I would comment, however, that some provision should be made to establish a committee representing all the interests involved, to periodically review both the "boundary" value of the numerical processing rate and its concept to assure its continuing effectiveness.

~~We very much appreciate the opportunity to comment on these matters and if we can be of any further assistance to you, please do not hesitate to call upon us.~~

*I have not listened to the pro & con arguments for some time, but I think now is the time to drop all or almost all restrictions on export of computers.*

*Sincerely  
Ken*

COMPUTER/CALCULATOR DIFFERENTIATION  
FOR EXPORT CONTROL PURPOSES

I. BACKGROUND

The Office of Export Control in the Department of Commerce is responsible for the administration of the issuance of export licenses for computer systems. At present export licenses are required for computer systems as described in *Commodity Control list - 39* (Appendix A). Calculators fall under the heading "Other Digital Computers" and are described in CC1-399.1, as follows:

Digital computers operated by one or more common control units and capable of all of the following:

- (a) Accepting, storing, processing and producing and output in numerical and/or alphabetic form.
- (b) Storing more than 572 numerical and/or alphabetical characters or having an internal memory of more than 2048 bits.
- (c) Performing a stored sequence of operations that are modifiable by means other than a physical change in circuitry.
- (d) Selecting a sequence from a plurality of stored operations based upon data or on internally computed results.

Recently there has been a proliferation of calculators, bookkeeping and accounting machines having memories in excess of 2048 bits but depending on how the terminology is interpreted, meeting the other conditions of the above definition. Trade in these items is becoming so heavy that, unless they can be separated from computers that are of

NAS PRIVILEGED

concern, they will overwhelm the licensing capabilities of the Office of Export Control.

The Department of Commerce is concerned that handling the growing volume of calculators, accounting machines, and even small computers is taxing resources that could better be applied to more significant transactions. It, therefore, sought with the assistance of the Computer Science and Engineering Board a definition of a minimum computer that could clearly, without ambiguity, distinguish it from more significant computers.

The Computer Science and Engineering Board organized a conference with the intent of including: (a) Those people on both sides of the boundary in industry and business, particularly those concerned with technological and systems developments; (b) Those officers engaged in administering the export control program, those officers concerned with operating and policy aspects of East-West trade; (c) Those officers concerned with general diplomatic relations between the U. S. and nations affected by the U. S. export control program; (d) Those officers concerned with current international negotiations with the COCOM apparatus; (e) Those officers currently studying the U.S. balance of trade problem in both the near- and mid-term; (f) and those officers concerned with national policy regarding the export from the U.S. of high technology products and of high technology itself.

The conference was held on October 12, 1971, in Washington, D. C. The attendees (Appendix B) represented most of the parties listed above. The information exchange at this meeting was very useful and served to set the tone for several working sessions involving mainly those persons

NAS PRIVILEGED

NAS PRIVILEGED

in industry on both sides of the boundary. It was at the follow-on meetings that the technology involved in the "lower" bounds of computers was reviewed and the technical differences between the calculator and computer were argued.

Initially a list of criteria was proposed that contained the major considerations for distinguishing most calculators from most computers. These included the questions of whether the device has an "internally-stored program" or not. A computer generally is distinguished by the fact that it is operable under program control, this program being stored inside the computer, being alterable by modifying the contents of storage without altering the machine's circuitry, and finally being capable of modifying itself.

Unfortunately, this criterion is not adequate to satisfy the intent of the U.S. Government in setting its bounds for embargoing the shipment of certain computing devices to the Communist Bloc nations. The difficulties stem from the fact that the technical computer/calculator boundary does not fall at the same plane as the boundary for the strategic/non-strategic digital processor. There are computers as defined above that are so slow as to have no strategic value and, furthermore, there are some devices that are not computers as defined above but do have strategic value. Hence, one is forced to consider other criteria such as measures of performance or capacity which are relative and arbitrary. The cut off level of performance could then be determined by comparison with devices considered to be of strategic importance in the U.S. military environment.

*Handwritten signature*

NAS PRIVILEGED

NAS PRIVILEGED

II. DIGEST OF PANEL DISCUSSIONS

A. The Problems

It is clear that a definition for the boundary between calculator and computers can be framed. However, for the purpose of strategic consideration in export control, the definition may not be too useful. The reason is that any good modern electronic calculator with some modification can be made useful in some military application.

When fire control and guidance control computers were first designed, they had a fairly well defined range of capability. This range was considerably below the capabilities of the general purpose computers of the period. For example, they generally use fixed point arithmetic, and have fairly limited file handling capabilities. On the other hand, the requirements were far more sophisticated than calculators could provide in the 50's and early 60's. In the last decade, computer capabilities have extended on the low end, and a whole new class of machines, the mini-computers, have come into existence. In a similar way, electronic calculator capabilities have gone up to include sophisticated programmable calculators. The computer and the calculator applications now have considerable overlap. The military requirements fall entirely in the range of the overlap. So long as this is the case, the end use must be considered in this overlap area.

Although, in the United States, decisions on release of technical information can be made independently of the items being described,

NAS PRIVILEGED

NO PRINTED

this is not the case with all governments involved in the international export control of commodities to Communist Bloc countries. It is perhaps more important to protect the technology for producing the computer than the computer itself. This may not be possible if the level of control is set too high. It is recognized that the purpose of the meetings was to establish a way of removing from the administrative burden of case-by-case licensing commercial computing devices in such a way that the embargo on export of technology, direct design and engineering assistance.

B. State of the Art

The present generation of desk top calculators incorporate one to six LSI chips to perform all of the logic. It is interesting to note that at present the mini-computers which pose the most difficulty to the boundary definition are constructed with conventional TTL and MSI primarily because desired speed could not be achieved with LSI.

Two areas of advancement will affect the present status. First, the semiconductor companies are developing LSI mini-processors which incorporate speed and computing power comparable (approx. 1/2 to 1/3) to present TTL mini's. Secondly, the cost per bit of semiconductor memory will be lowered with competition and improving production rates as core memory replacement between now and 1975.

ROUGH DRAFT

NO PRINTED



The LSI mini-processors to be announced within the next few months will incorporate 8 to 12 general registers and up to 32 words of push down stack. They will operate under complex micro-programmed control and be able to perform an add or load immediate in approximately 4  $\mu$ s (3.3 - 5.2  $\mu$ s) depending of course on the speed of memory. These 3 to 5 chip mini's are intended for the point of sale, crt terminal, complex programmatic calculator, and TTL mini-replacement markets. Therefore, we can accurately predict that EXACTLY the same processor will appear as both a calculator and a computer. The primary differences will lie in the functions performed, the use of the micro-programming, and the quantity of memory.

It can be predicted that small desk top and hand held calculators realizing only the four basic functions will continue to use LSI to tailor and minimize the logic for the specific task. There will be a great emphasis on reducing the number of chips to one. There now exists at least six different single chip designs of which one is a 5 digit unit that performs all the functions of a slide rule plus add and subtract. The introduction of the LSI mini and the ability to "get more on the chip" combined with the introduction of silicon gate, ION implant, and other processes which result in a natural gain in speed and will certainly close any gap that existed between boundaries.

The question of how much memory a calculator of the future will have on the quantity of memory is difficult to answer. Experts in

NAS PRIVILEGED

the field of semiconductor memory have found it difficult to predict exactly when core will be replaced. The evolution has already taken place in the crt terminal area. The cost effectiveness of core is still predominant on larger systems. If predictions are correct, then they would suggest an increased interest in utilizing a greater quantity of memory for the "complex" calculator. Also note that bi-polar ROMS are predicted to be competitive with MOS ROMS. The impact of cost competitive bi-polar ROMS on system speeds will be significant.

III. RESOLUTION OF THE PROBLEM

Recognizing the fact that the computer/calculator boundary and the strategic/non-strategic boundary could not be reconciled by a simple definition, it was decided to seek a solution that would permit the general licensing of classes of computers in the lower performance range, leaving those in the more strategic range to be considered on a case-by-case basis.

To accomplish this aim and to leave flexibility in the "moveable" boundary that would be decided by consideration of strategic importance, it is suggested that the lower end of computer definition be left virtually as is.

The first change recommended is to strike out item (c) as specified in Comodity Control List - 339.1 paragraph 714(5)A. The section currently

NAS PRIVILEGED

-8-

WAS PRIVILEGED

reads:

"Other digital computers, and statistical machines used in conjunction with punched cards or tape (including auxiliary machines), operated by one or more common control units and capable of all of the following: (a) accepting, storing, processing, and producing an output in numerical or alphabetical form; (b) storing more than 512 numerical and/or alphabetical characters or having an internal memory of more than 2048 bits; (c) performing a stored sequence of operations that are modifiable by means other than a physical change in circuitry; and (d) selecting a sequence from a plurality of stored operations based upon data or an internally computer result; and specially designed parts and accessories, n. e. c. (specify name, model number, and systems characteristics. Also see 376.10.)"

Item (c) sometimes called the von Neumann criteria could be construed as allowing the uncontrolled shipment of guidance and control computers whose programs are in read only memory. The recommendations to eliminate item (c) thus helps protect the strategic interests of the United States and would not affect calculator exports.

The second change would have the effect of easing the administrative burden of exporting calculators that are controlled commodities due to 714(5)A. The recommendation is that a new export licensing procedure be followed. The licensing authorities should review a specific model of a computing device to determine whether the device could be exported

WAS PRIVILEGED

under a general license without further review on a case-by-case basis. As a guide to the licensing authorities the following was proposed as a "movable" boundary on devices which would not be eligible for general license.

"Other digital processors capable of all of the following: (a) numerical processing rate\* exceeding 0.25 million bits per second; (b) accepting electrical input signals; and (c) providing electrical output signals. It is further provided that the devices have been designed specifically for identifiable civil applications and by nature of design or performance are substantially restricted to the particular application for which they have been designed."

The intent of these conditions is to permit shipment of programmable calculators including those with integral devices such as magnetic cards or magnetic cassettes or displays or alphanumeric printers. There is not to be an I/O connector for information transfer; i. e., without major physical modification, the device cannot be used for both generally controlling external devices and electrically inputting external data. Detachable peripherals are to be individually considered under their own embargo regulations if any.

\* The definition of numerical processing rate (NPR) is given as

$$(NPR) = \text{Data word size} / (0.9 \times \text{average add time} + 0.1 \times \text{average multiple time})$$

If data word size exceeds 32 bits, 32 is used in the formula

NAS PRIVILEGED

The complete set of proposed changes to the existing commerce regulations described in CCL 399.1 appears in Appendix G. The only parameter involved in defining the boundary between the general and case-by-case licensing is the numerical processing rate. The recommendation is that it be established at 250 thousand bits per second. The number was chosen on the basis of comparison with numerical processing rates for existing aero space computers determined from a compilation of such prepared by Don Baechler of Bell Comm., Inc. Only three computers of the 87 listed (see Appendix) fall below the selected figure. These are the IBM Gemini Guidance computer at 155 and the General Precision AN/ASN-24 at 26, both of which appeared in 1963 and GPI Kearfott GPK-10 at 193 which appeared in 1967. The recommended figure of 250 could be altered to suit the requirements of the U.S. Government. It is not expected that the calculator manufacturers will introduce machines that have an NPR in excess of 100 thousand bits/sec for several years. There is no doubt that this number will be exceeded within the next five years, 250 seems to be a reasonable compromise.

NAS PRIVILEGED

Department of Commerce Export Control Commodity Number and Commodity Description	Unit	Processing Number	Validated License Required for Country Groups Shown Below	GLV's Value Limits for Shipments to Country Groups.			Special Provisions List
				T	V	X	

712(8)C Commodities not listed above, classified .....<sup>1</sup> 203 SZ — — —  
 under Schedule B Nos. 712.1095 through 712.9965.  
 (Also specify 7-digit Schedule B No.)

714(1)D Electric typing devices capable of being .....<sup>2</sup> 618 SWXYZ — — 100  
 connected to and operating over a wire communi-  
 cation circuit; and parts and accessories, n.e.c.

714(2)A Analog computers with one or more of .....<sup>4</sup> 621 QSTVWXYZ 500 500 0 R  
 the following characteristics: (a) with summers,  
 inverters, or integrators with (i) static accuracy better than 0.02 percent, or (ii) total error at 1 KHz better  
 than 0.15 percent; (b) with multipliers with (i) static accuracy better than 0.1 percent, or (ii) total error at  
 1 KHz better than 0.25 percent; (c) with fixed function generators (including Log X and sine/cosine, etc.)  
 with static accuracy better than 0.1 percent; (d) more than 75 operational amplifiers; or (e) more than four  
 integrator time scales switchable during one program; and specially designed parts and accessories, n.e.c.  
 (Specify name, model number, and systems characteristics. Also see § 376.10.)<sup>5</sup>

714(3)A Other analog computers capable of ac- .....<sup>4</sup> 621 QSTVWXYZ 500 500 0 R  
 cepting, processing, and putting out data in the  
 form of one or more continuous variables and capable of incorporating a total of at least 20 summers,  
 integrators, multipliers, or function generators with facilities for readily varying the interconnection of these  
 components; and specially designed parts and accessories, n.e.c. (Specify name, model number, and systems  
 characteristics. Also see § 376.10.)<sup>5</sup>

714(4)A Digital computers with one or more of the .....<sup>4</sup> 621 QSTVWXYZ 500 500 0 R  
 following characteristics: (a) the CPU imple-  
 ments floating point operations by hardware; (b) the sum of either the "I/O bus rate" or the "total effective  
 bit transfer rate," whichever is less, and the "CPU bus rate" exceeds 10.8 million bits per second; (c) the in-  
 ternal memory has a total connected capacity (excluding parity, word marker, and flag bits) of more than 0.5  
 million bits; (d) the computer is equipped with peripheral memory devices, as follows: (i) more than 12, or (ii)  
 the "total effective bit transfer rate" (excluding data channels not equipped with peripheral memory units) ex-  
 ceeds 0.7 million bits per second, or (iii) any magnetic tape transport with: (1) more than 800 bits per inch per  
 track, (2) more than 75 inches per second tape speed, (3) more than 9 tracks per 1/2 inch tape width, or (4)  
 more than 1/2 inch tape width, or (iv) for peripheral memory devices other than magnetic tape transports: (1)  
 total connected "net capacity" exceeds 3 million bits, or (2) "total number of accesses exceeds 120 per second;  
 (e) the computer is equipped with "terminal devices" located remote from the "computer operating area," as fol-  
 lows: (i) the "total effective bit transfer rate" (excluding parity, word marker, and "flag bits") as limited by  
 any communications channel exceeds 1,400 bits per second, or (ii) the "effective bit transfer rate" of any "ter-  
 minal device" exceeds 1,200 bits per second; (f) the computer has interface equipment for which: (i) the "effec-  
 tive bit transfer rate" of any interfaced "communications channel" exceeds 200 bits per second; or (ii) any in-  
 terfaced "communication channel" is not dedicated full time to the given application; (g) computers with cath-  
 ode ray tube display units, as follows: (i) using alpha-numeric and similar data or information, excluding those  
 displays for which circuitry and character-generation devices external to the tube limit displays to alpha-numeric  
 characters in fixed formats or to graphs composed only of the same basic elements as used for alpha-numeric  
 character composition (this exclusion is limited to graphic displays for which the sequence of symbols and basic  
 elements of symbols are fixed by the format and character generators in the unit and cannot be generated arbi-  
 trarily by the computer), or (ii) with light gun or other graphic input devices, excluding those which are parts  
 of displays for which circuitry and character-generation devices external to the tube limit displays to alpha-numeric  
 characters in fixed formats or to graphs composed only of the same basic elements as used for alpha-numeric  
 character composition; and specially designed parts and accessories, n.e.c. (Specify name, model number,  
 and systems characteristics. Also see § 376.10.)<sup>5</sup>

\* For explanation, see "General Information Regarding Commodity Control List" at beginning of § 329.1.  
<sup>1</sup> See § 371.1(c) for commodities which do not require a validated license for export to the People's Republic of China.  
<sup>2</sup> Report unit for each commodity in accordance with Schedule B requirement.  
<sup>3</sup> Report machines in "number."  
<sup>4</sup> Report computers in "number."  
<sup>5</sup> Computers bearing a military designation, or designed or modified for use in airborne vehicles, missiles, or space vehicles, require export  
 authorization from the U. S. Department of State, see Supplement No. 2 to Part 376.

NAS PRIVILEGED

Department of Commerce Export Control Commodity Number and Commodity Description	Unit	Processing Number	Validated License Required for Country Groups Shown Below	GLV & Value Limits for Shipments to Country Groups			Special Provisions
				T	V	X	
714(5)A Other digital computers, and statistical machines used in conjunction with punched cards or tape (including auxiliary machines), operated by one or more common control units and capable of all of the following: (a) accepting, storing, processing, and producing an output in numerical or alphabetical form; (b) storing more than 512 numerical and/or alphabetical characters or having an internal memory of more than 2048 bits; (c) performing a stored sequence of operations that are modifiable by means other than a physical change in circuitry; and (d) selecting a sequence from a plurality of stored operations based upon data or an internally computed result; and specially designed parts and accessories, n.e.c. (Specify name, model number and systems characteristics. Also see § 376.10.) <sup>1</sup>		621	QSTVWXYZ	500	500	0	R
714(6)A Other computers (for example, hybrid) capable of operating in both analog and digital modes, and related equipment; and specially designed parts and accessories, n.e.c. (Specify name, model number and systems characteristics. Also see § 376.10.) <sup>1</sup>		621	QSTVWXYZ	500	500	0	R
714(7)G Other analog or digital computers, n.e.c.; and parts and accessories, n.e.c. (Specify name, model number, and systems characteristics. Also see § 376.10.) <sup>1</sup>		628	SZ	—	—	—	—
714(9)A Machines specially designed for use with electronic computers; and specially designed parts and accessories, n.e.c. (Specify by name and model number.) <sup>4</sup>		621	QSTVWXYZ	500	100	0	R
714(10)A Magnetic recording and/or reproducing equipment specially designed for electronic computers; and specially designed parts and accessories, n.e.c. (Specify by name and model number.) [Report magnetic tape and other magnetic recording media in No. 891.] <sup>4</sup>		621	QSTVWXYZ	500	250	0	R
714(11)A Input/output devices and other peripheral equipment for electronic computers, including terminal devices capable of being remotely interfaced with computers; and specially designed parts and accessories, n.e.c. (Specify by name and model number. Also see § 376.10.) <sup>4</sup>		621	OSTVWXYZ	500	500	0	R
714(12)G Commodities not listed above, classified under Schedule B Nos. 714.1010 through 714.9295. (Also specify 7-digit Schedule B No.) Machines and machine tools for working metals [Report parts in No. 7195]:		218	SZ	—	—	—	—
71510(1)A Machine tools incorporating Laser, Maser, or Iraser devices. [Report Lasers, Masers, or Irasers exported as replacements or accessories in No. 7299.]		421	QSTVWXYZ	500	500	0	R

<sup>1</sup> For explanation, see "General Information Regarding Commodity Control List" at beginning of § 399.1.  
<sup>2</sup> Computers bearing a military designation, or designed or modified for use in airborne vehicles, missiles, or space vehicles, require authorization from the U. S. Department of State. See Supplement No. 2 to Part 376.  
<sup>3</sup> Report computers and machines in "number."  
<sup>4</sup> Report machines in "number."  
<sup>5</sup> See Supplement No. 2 to Part 376 for commodities which require export authorization from the U. S. Department of State.  
<sup>6</sup> Report recording and/or reproducing equipment in "number."  
<sup>7</sup> Report devices and peripheral equipment in "number."  
<sup>8</sup> See § 714.1101 for commodities which do not require a validated license for export to the People's Republic of China.

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED

Those attending the first Computer/Calculator Boundary Conference:

Dr. Sidney Fernbach  
Livermore Laboratory

Dr. Ronald Finkler  
IDA

Mr. Sherman Abrahamson  
Office of Export Control  
Department of Commerce

Mr. Ned Chang  
Wang Laboratories, Inc.

Mr. Thomas Bun  
Smith Corona Marchant

Mr. E. A. Kritzer  
Office of Export Control  
Department of Commerce

Mr. John Collins  
Office of Export Control  
Department of Commerce

Mr. George Lindamood  
Center for Computer Sciences & Technology  
National Bureau of Standards

Mr. Edward Dawson  
Texas Instruments

Mr. Thomas Osborne  
Hewlett-Packard

Mr. Clark Dilks  
Burroughs Corporation

Mr. Saul Padwo  
U. S. Department of Commerce

Mr. Gaymond Schultz  
American Micro Systems

Mr. Jean Tartter  
Office of East-West Trade  
Department of State

Additional people attending Computer/Calculator Boundary Panel Meetings:

Mr. Daren Appelt  
Texas Instruments

Mr. E. W. Pughe  
Raytheon

Mr. Jorge Hernandez  
Smith Corona Marchant

Dr. Michael Schneider  
Data General Corporation

Mr. Ray Holt  
American Micro Systems

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED



NAS PRIVILEGED

## PROPOSED CHANGES TO COMMERCE REGULATIONS

1. Change subitem 714(5)A(b) of CCL 399.1 to read:

"(b) Storing in fixed or alterable memory more than 512 numerical and/or alphabetical characters or having a fixed or alterable internal memory of more than 2048 bits."
2. Delete subitem 714(5)A(c) of CCL 399.1.
3. Renumber subitem 714(5)A(d) of CCL 399.1 to subitem 714(5)A(c) and change to read:

"(3) Selecting a sequence from a plurality of operations stored in fixed or alterable memory based upon data or an internally computed result;"
4. Add a new note in the appropriate location with the following intent:

"Distribution (general) licenses may be issued for digital computers and/or devices embargoed by subitem 714(5)A of CCL 399.1 provided that:

  - (a) The digital computers and/or devices have been designed specifically for identifiable civil applications and, by nature of design or performance, are substantially restricted to the particular application for which they have been designed;

NAS PRIVILEGED

NAS PRIVILEGED

- (b) The manufacturer submits details of such devices to the Commerce Department, who has agreed that the particular digital computers and/or devices should be eligible for such a license;
- (c) The digital computers and/or devices are not capable of all of the following:
  - (1) Having a "numerical processing rate" exceeding 0.25 million bits per second;
  - (2) Accepting electrical input signals; and
  - (3) Producing electrical output signals;
- (d) Exports of technology are embargoed.

5. Add a new note as follows:

"Definitions of the terms of Note - above:

- (a) "Numerical processing rate" is the product of the number of bits in an "operand" and the "processing rate."
- (b) "Processing rate" is the reciprocal of the sum of:
  - (1) 0.9 times the average "execution time" of an addition, and
  - (2) 0.1 times the average "execution time" of a multiplication.
- (c) The "operand" length and "execution times" of the above operations are based on:
  - (1) Either fixed point or floating point operands and execution times or if both are provided then whichever type yields the greater numerical processing rate;

NAS PRIVILEGED

NAS PRIVILEGED

- (2) For operand lengths in excess of 32 bits, a value of 32 bits shall be used as the operand length;
- (3) The fetching of the one or more instructions necessary to perform an arithmetic operation from memory (for CPUs simultaneously fetching more than one instruction in a memory word, the execution time shall be the average over the possible locations of the instruction(s) within the fetch word);
- (4) One operand being in the accumulator(s) or a location in memory acting as the accumulator(s);
- (5) The second operand being in the most accessible portion of memory;
- (6) The result being left in the same accumulator or a location in memory acting as the accumulator;
- (7) The instruction(s) and operands being in optimum locations in memory;
- (8) No indexing or indirect operations being included."

NAS PRIVILEGED

NAS PRIVILEGED

TABLE 1 - CHARACTERISTICS OF AEROSPACE COMPUTERS\*

BELLCOMM, INC.

NAME DATE INTRODUCED	DATA FLOW	DATA TYPE	NO. OF INSTRUCTIONS	COMPUTING TIME, $\mu$ SEC			TYPE	MEMORY				IN/OUTPUT		PHYSICAL CHARACTERISTICS				COMMENTS	NPR (KBITS/SEC)	
				ADD	MULT	DIV		WORD SIZE (BITS)	CAPACITY (WORDS)		ACCESS TIME ( $\mu$ SEC)	CYCLE TIME ( $\mu$ SEC)	NO. OF CHANNELS	NO. OF INTERRUPTS	TYPE OF HARDWARE	WEIGHT (LBS)	SIZE (CU. FT.)			POWER (WATTS)
BURROUGHS D210 PRE 1962	P	Fx	16	30	500	600	DRO CORE CORE ROPE CORE ROPE	24 16 50	256 1K 256	1K 16K 1K	10 10	15	2	1	MAGNETIC LOGIC	19	0.25	100	USES CORE MULL-DECODER REGISTERS FOR LOGIC. INSTRUCTIONS ARE 16 BITS, DATA IS 24 BITS. 50-BIT ROPE USED FOR MICROPROGRAMMING.	232 198 376
UNIVAC ADD-1000 PRE 1962	P	Fx	16	12	711	837	DRO THIN FILM WORD THIN FILM	24 24	256 7K		3	3		4	DISCRETE COMPONENTS	88	1.1	262	WORD MEMORY HAS 50 MILLISEC WRITE TIME FROM EXTERNAL EQUIPMENT.	293 293
ARMA MICRO COMPUTER MID 1962	S	Fx	19	27	135	324	WORD CORE	22	2K	8K		27	2		DISCRETE COMPONENTS	20	0.4	50	REGISTERS ARE DELAY LINES. MEMORY USES TWO-APERTURE CORES.	582
HUGHES HCM-201 MID 1962	P	Fx	30	6	120	120	DRO CORE WORD CORE OR DRUM	24 24 24	4K 16K 1500K			6		1	DISCRETE COMPONENTS	51		150	CHOICE OF ONE OF THE THREE MEMORIES AVAILABLE.	1379 1379 1379
IBM GEMINI GUIDANCE COMPUTER EARLY 1963	S	Fx	16	140	420	840	WORD CORE	39	4K			4	5	0	DISCRETE COMPONENTS	59	1.65	85	CONCURRENT MULTIPLY/DIVIDE. 13 BITS OF MEMORY WORD ARE READ-ONLY. INSTRUCTION WORD, 13 BITS; DATA WORD, 26 BITS.	155
GENERAL PRECISION ANVASH-24 MID 1963	S	Fx	12	624	44	4K	DRUM	25	4K				1	0	DISCRETE COMPONENTS	100	1.2	420	HAS INDEPENDENT, PROGRAMMABLE INTEGRATOR. USES TWO ADDRESSES, OPERAND AND NEXT INSTRUCTION. ALSO PACKAGED AS GPN-33 FOR SPACE APPLICATIONS.	26
HUGHES HCM-202 MID 1963	P	Fx	30	6	120	120	DRO CORE WORD THIN FILM	24 24	512 1024	4K 8K		6 6		1	HYBRID THIN FILM	51		150	OTHER MEMORY TYPES ARE AVAILABLE. THIS WAS LATER CALLED HCM-204.	1379 1379
IBM SATURN 1B/V LVDC MID 1963	S	Fx	14	82	328	656	DRO CORE	25	4K	32K	25		1	1	DTL HYBRID	80	2.1	138	REGISTERS ARE GLASS DELAY LINES. CONCURRENT ADD AND MULTIPLY. TWO PARITY BITS IN MEMORY WORD.	263
MIT BLOCK I AGC LATE 1963	P	Fx	11	23.4	117	210	DRO CORE CORE ROPE	16 16	1K 10K			11.4 11.4		8	DCTL IC	87	1	125	SOME I/O HANDLED THROUGH COUNTER INTERRUPTS. PREDECESSOR OF BLOCK 11 APOLLO GUIDANCE COMPUTER.	488 488
UNIVAC 1824 LATE 1963	P	Fx	41	8	92	128	DRO THIN FILM WORD THIN FILM	24 48	512 4K		0.7		8		DTL IC	31.5	0.47	110	DATA WORD, 24 BITS; INSTRUCTION WORD, 16 BITS.	1463 1951
BURROUGHS DB4 MID 1964	P	Fx	47	6	25		DRO CORE	24	4K	32K		3			IC	166	3.6	150	WEIGHT, SIZE AND POWER ARE GIVEN FOR 4K MEMORY	3038
SAAB CK 37 MID 1964	P	Fx	48	5.6	23.8	44.8	DRO CORE	26	8K		1.2	2.8		6	RTL IC	80	1.3	200	MOST COMMON OPERATIONS USE 13-BIT INSTRUCTION WORD, WITH 13-BIT OPERAND STORED IN OTHER HALF OF THE WORD.	1752
LITTON L-304 EARLY 1965	P	Fx	63	5.6	61		DRO CORE	32	4K	131K		1.8		1	TTL IC	34	0.26	100	DATA WORD, 16 BITS; INSTRUCTION WORD, 32 BITS	1436
NORTRONICS NDC-1051 EARLY 1965	P	Fx	51	8	70	176	DRO CORE	24	2K	8K	2			4	IC	29	0.5	94	WEIGHT, SIZE, AND POWER ARE GIVEN FOR 2K MEMORY.	1690
LEAR-SIEGLER DIVAC MID 1965	S	F		12	360		CORE ROPE DRO CORE	30 30		6K 512					IC	40		160	BASIC CONCEPT OF DIGITAL COMPUTER WITH SPECIALIZED ANALOG CIRCUITRY WAS BUILT INTO A VARIETY OF SYSTEMS INCLUDING AN/AYN-1.	641 641
AUTOMETICS D26J LATE 1965	P	Fx	30	8	18	18	DRO CORE	12	4K	8K			4	4	DTL IC	35	0.21	200	SIZE, WEIGHT AND POWER ARE GIVEN FOR 4K MEMORY AND INCLUDE EXTENSIVE I/O SIGNAL CONDITIONING BUILT AS D24-J-41, 43 AND 44. D26J-103 HAS 24 BIT WORD, 16K MEMORY AND USES TTL DEVICES.	1333

SEE ATTACHED EXPLANATION OF HEADINGS

NAS PRIVILEGED

**TOP SECRET**

TABLE 1 - CHARACTERISTICS OF AEROSPACE COMPUTERS (CONTINUED)

BELLCOMM, INC.

NAME	DATE INTRODUCED	DATA FLOW	DATA TYPE	NO. OF INSTRUCTIONS	COMPUTING TIME, $\mu$ SEC			MEMORY					IN/OUTPUT		PHYSICAL CHARACTERISTICS				COMMENTS	NPR (KBITS/SEC)		
					ADD	MULT	DIV	TYPE	WORD SIZE (BITS)	CAPACITY (WORDS)		ACCESS TIME ( $\mu$ SEC)	CYCLE TIME ( $\mu$ SEC)	NO. OF CHANNELS	NO. OF INTERRUPTS	TYPE OF HARDWARE	WEIGHT (LBS)	SIZE (CU. FT.)			POWER (WATTS)	
HONEYWELL HDC-801	LATE 1965	P	Fx	89	4	14	32	DRO CORE	24	4K	64K	1	2			MLTTL IC	65	1.2	150	OPTIONS INCLUDE DRO CORE WITH 1 $\mu$ SEC CYCLE TIME, AND BUFFERED I/O WITH 7 CHANNELS. ALSO DESIGNATED AN/ATK-5. FORMERLY CALLED ALERT.	4800	
NORTRONICS NDC-1051A	EARLY 1966	P	Fx	51	6	26	50	DRO CORE	14	8K	32K		2	8	DTL IC	38	0.87	225	WEIGHT, SIZE, AND POWER ARE GIVEN FOR 16K MEMORY.	1750		
SPERRY MARK XII	EARLY 1966	P	Fx	13	18	60		DRO CORE	21	6K				1	IC	64	1.5	250	MEMORY CAN BE PARTIALLY HARD-WIRED.	946		
TRW MARCO 4418	EARLY 1966	P	Fx	27	10	70	73	DRO CORE	18	4K	8K		5	0	DTL IC	34	0.4	75	MEMORY CAN BE PARTIALLY HARD-WIRED.	1125		
ARMA MICRO D	MID 1966	S	Fx	18	18	342	342 (12) (200)	DRO CORE	18	4K	31K		3.3		2	TTL IC	5.75	0.07	30	(AVAILABLE WITH FAST CLOCK)	357 (584)	
CDC 5360	MID 1966	P	Fx	41	12	90	90	DRO CORE	24	4K	32K	1.5	8		1	IC	26	0.6	95	WEIGHT AND SIZE EXCLUDE POWER SUPPLY.	1212	
COMPUTING DEVICES OF CANADA AN/UYK-501	MID 1966	P	Fx	110	8	110	118	DRO CORE	24	4K	32K	1	2		1	64	IC	82	0.96	240	WEIGHT, SIZE, AND POWER ARE GIVEN FOR 8K MEMORY. HAS ALTERABLE MICROPROGRAM.	1319
SPERRY MARK XIV	MID 1966	P	Fx	13	18	60		DRO CORE	21	6K				1		IC	64	1.5	250	MEMORY CAN BE PARTIALLY HARD-WIRED.	946	
TI 2501	MID 1966	P	Fx	36	4	27	37	DRO CORE	32	4K	16K		2		32	IC	65	1.1	350	WEIGHT, SIZE AND POWER ARE GIVEN FOR 4K MEMORY.	5079	
UNIVAC 1830-A	MID 1966	P	Fx	72	4	20	34	DRO CORE	30	4K	131K		2		1	IC	200	2.65	567	ALSO HAS DRO THIN FILM CONTROL MEMORY AND 64-WORD CORE ROPE BOOTSTRAP MEMORY. SUCCESSOR TO 1830.	5357	
AC ELECTRONICS MAGIC 321	LATE 1966	S	Fx	22	15	121	323	DRO CORE	32	4K	32K				1	3	IC	23	0.44	120	WEIGHT, SIZE AND POWER ARE GIVEN FOR 8K MEMORY. DATA WORD, 31 BITS - PARITY; INSTRUCTION WORD, 15 BITS - PARITY.	1250
CDC 5400	LATE 1966	P	Fx	73	3.1	25	275	DRO CORE NDRO THIN FILM	24 96	4K 3K			2.5 2.5	5	16	IC	60	1.1	140	4-WORD (96-BIT) READOUT FROM NDRO MEMORY TO AN INSTRUCTION LOCK-AHEAD MEMORY.	4537 6049	
HONEYWELL HDC-501	LATE 1966	P	Fx	53	4	24	24	DRO CORE	20	2K	16K	0.65	2.0		5	1	DTL IC	28	0.49	92	HAS DOUBLE PRECISION ADD INSTRUCTION. FORMERLY CALLED SIGN III	3333
HUGHES HCM-205	LATE 1966	P	Fx	42	4	24	25	DRO CORE	18	2K	8K		2.0		1	1	DTL IC	16	0.2	110	WEIGHT, SIZE AND POWER ARE GIVEN FOR 2K MEMORY.	3000
IBM 4 PI/CP	LATE 1966	P	Fx	34	6.6	29.1		DRO CORE	32	8K	32K	0.9	2.5		3	5	TTL IC	57	.85	250	HAS 1024-2048 WORD MICROPROGRAMMING MEMORY. 70 BITS/WORD, 155 NSEC ACCESS TIME. AVAILABLE WITH 51 OR 77 INSTRUCTIONS. AVAILABLE AS CP-2 WITH HARDWARE DECODE INSTEAD OF MICROPROGRAM.	3616
IBM 4 PI/EP	LATE 1966	P	FL	135	5.8	9.5	18.3	DRO CORE	36	8K	128K	0.9	2.5		3	5	TTL IC	62	0.9	303	3K x 100 BITS MICROPROGRAMMING MEMORY. FLOATING POINT OPTION. 32-BIT DATA WORD. 1 PARITY BIT PER 8-BIT BYTE.	5186

**TOP SECRET**

TABLE 1 - CHARACTERISTICS OF AEROSPACE COMPUTERS (CONTINUED)

BELLCOMM, INC

NAME DATE INTRODUCED	DATA FLOW	DATA TYPE	NO. OF INSTRUCTIONS	COMPUTING TIME, $\mu$ SEC			MEMORY					IN/OUTPUT		PHYSICAL CHARACTERISTICS				COMMENTS	NPR (KBITS/SEC)	
				ADD	MULT	DIV	TYPE	WORD SIZE (BITS)	CAPACITY (WORDS)		ACCESS TIME ( $\mu$ SEC)	CYCLE TIME ( $\mu$ SEC)	NO. OF CHANNELS	NO. OF INTERRUPTS	TYPE OF HARDWARE	WEIGHT (LBS)	SIZE (CU. FT.)			POWER (WATTS)
MIT BLOCK II AGC LATE 1966	P	Fx	34	23.4	46.6	81.9	DRO CORE CORE ROPE	16 16	2K 36K			11.4 11.4	15	10	DCTL IC	58	1.0	100	HAS DOUBLE PRECISION ADD. BUILT BY RAYTHEON. USED AS COMMAND MODULE COMPUTER AND LUNAR MODULE COMPUTER IN THE APOLLO PRIMARY GUIDANCE AND NAVIGATION SYSTEM.	622 622
SPERRY MARK XVI LATE 1966	P	Fx	14	12	34		DRO CORE	21	8K	16K		6	4	IC	60	1.5	250	MEMORY CAN BE PARTIALLY HARD-WIRED.	1479	
AC ELECTRONICS MAGIC 301 EARLY 1967	S	Fx	12	24	96	280	DRO CORE	8	2K	8K		4	2	1	TTL IC	5.0	.08	45	HARDWIRED PROGRAM STORAGE OPTION. DATA WORD, 16 BITS; INSTRUCTION WORD, 8 BITS.	513
AC ELECTRONICS MAGIC 311 EARLY 1967	S	Fx	28	19	104	332	DRO CORE	13	6K			2.6	1	1	TTL IC	22	0.44	110	DATA WORD, 24 BITS + 2 PARITY; INSTRUCTION WORD, 12 BITS + PARITY.	873
AC ELECTRONICS MAGIC 331 EARLY 1967	P	Fx	23	4.5	34.5	94.5	DRO CORE	16	4K	32K		3	1	1	IC	23	0.35	115	DATA WORD, 31 BITS + PARITY; INSTRUCTION WORD, 15 BITS + PARITY.	4133
CDC 449 EARLY 1967	P	Fx	36	28	604		DRO THIN FILM DRO .BIAX	24 24	256 3840			1	1	1	IC	12	.083	4.0	INCLUDES BATTERIES, KEYBOARD AND DIAL READOUT. 12-BIT PARALLEL, 2 BYTE SERIAL.	280 280
ELLIOTT MCS 920 M EARLY 1967		Fx	23	19	38		DRO CORE	18	8K	65K		5	2	0	DTL IC	30	0.61	60	WEIGHT, SIZE AND POWER ARE GIVEN FOR 8K MEMORY.	861
IBM 4 PI/TC EARLY 1967	P	Fx	54	15	51		DRO CORE	8	16K			2.5	15	2	TTL IC	27	0.48	138	2 BYTE SERIAL, 8-BIT PARALLEL. MEMORY SIZE GIVEN IN TERMS OF 8-BIT BYTES. DATA WORD IS 2 BYTES AND INSTRUCTION WORD IS 1, 2 OR 3 BYTES. THE IC HAS BEEN BUILT IN SEVERAL CONFIGURATIONS.	860
RCA VIC-36A EARLY 1967	P	FL		9.3	66		DRO CORE DRO CORE	38 38	4K 512	32K	.650 .326	3.0 0.6	4	4	IC	120	3.0	525	SOME DISCRETE COMPONENTS USED. VARIABLE. INSTRUCTIONS CONTROL MICROFORM. WEIGHT, SIZE AND POWER GIVEN FOR 4K MEMORY.	2138 2138
UNIVAC 1818 EARLY 1967	P	Fx	28	4	22	22	DRO CORE CORE ROPE	18 18	1K 4K	8K		2 2	12	10	IC	35	0.7	197	WEIGHT, SIZE AND POWER ARE GIVEN FOR 8K MEMORY.	3103 3103
COLLINS C-8311A-1 MID 1967	S	Fx	12	13			DRO CORE	12	4K		0.727	3	8	1	TTL IC	15	0.3	72	DEVICE CONTROL COMPUTER. PROGRAM IS LOADED BY A TAPE CARTRIDGE. ALSO BUILT AS C-8311A-2 A-3 AND B-1. ALL HAVE EXTENSIVE I/O.	UNDEFINED
CPI KEARFOTT GPK-29 MID 1967	S P	Fx	32	20	100		DRO CORE	10	4K	16K	1	4	5	4	DTL IC	25	0.35	85	HAS ADDITIONAL I/O FOR DISCRETES. PULSE RATE INPUTS. DATA WORD, 20 BITS; INSTRUCTION WORD, 5, 10, 15 OR 20 BITS.	714
NORTRONICS NDC-1060 MIG 1967	P	Fx	51	6	26	50	DRO CORE	14	8K	32K	1	2	2	1	DTL IC	38	0.87	180	WEIGHT, SIZE, POWER ARE GIVEN FOR 8K MEMORY.	1750
TELEDYNE SERIES 20000 MID 1967	P	Fx	29	8	32	41	DRO CORE	20	1K	8K		4	4	4	IC	12	0.18	70	PHYSICAL CHARACTERISTICS ARE FOR ONE IN THE SERIES.	1923

TABLE 1 - CHARACTERISTICS OF AEROSPACE COMPUTERS (CONTINUED)

BELLCOMM, INC.

NAME DATE INTRODUCED	DATA FLOW	DATA TYPE	NO. OF INSTRUCTIONS	COMPUTING TIME, $\mu$ SEC			MEMORY					IN/OUTPUT		PHYSICAL CHARACTERISTICS				COMMENTS	NPR (KBITS) SEC		
				ADD	MULT	DIV	TYPE	WORD SIZE (BITS)	CAPACITY (WORDS)		ACCESS TIME ( $\mu$ SEC)	CYCLE TIME ( $\mu$ SEC)	NO. OF CHANNELS	NO. OF INTERRUPTS	TYPE OF HARDWARE	WEIGHT (LBS)	SIZE (CU. FT.)			POWER (WATTS)	
47. CDC 540GB LATE 1967	P	Fx	73	2	10	11	DRO MOROTIM FILM	24 24	8K 24K			1 1	1	3	TTL IC	75	1.4	189	ADD TIME 1 $\mu$ SEC WITH INSTRUCTION LOOK AHEAD	8571 8571	
48. GPI KEARFOTT GPK-10 LATE 1967	S	Fx	37	70	1025	1055	DISC	32	16K					8	IC	31	0.46	100	PHYSICAL CHARACTERISTICS INCLUDE POWER SUPPLY. HAS ADDITIONAL I/O FOR DISCRETES. PULSE RATE INPUTS.	193	
49. RAYTHEON RAC-230 LATE 1967	P	Fx	16	4.6	13.8	13	CORE OR PLATED WIRE CORE	24 24	4K 2K			2 2	8	8	TTL IC	20	0.4	95		4348 4348	
50. ARMA PORTABLE MICRO D EARLY 1968	P	Fx	36				CORE ROPE	18	4K			2			IC	14	0.195		ALSO CALLED CELESTIAL DATA PROCESSOR. WEIGHT AND SIZE INCLUDE BATTERIES AND I/O DEVICES.	UNDE- FINED	
51. CDC 5100 EARLY 1968	P	Fx	36	18	210		DRO CORE	16	4K 64K			3	1	2	TTL IC	30	0.54	70	FAST MULT OF 24 $\mu$ SEC AVAILABLE AS AN OPTION. ADD TIME IS FOR ADD TO MEMORY. DOUBLE PRECISION CAPABILITY. DIRECT MEMORY ACCESS.	430	
52. NORTRONICS NDC-1070 MID 1968	S/P	Fx	53	6	8	32	DRO CORE	16	8K 64K	1		2	2	1	TTL IC				HAS DOUBLE PRECISION ADD, REGISTER-REGISTER OPERATIONS.	258	
53. TI 2540 MID 1968	P	Fx	29	4	13.5		DRO CORE	32	4K 32K			2	4	16	IC	50	0.96	310	DATA WORD, 16 BITS; INSTRUCTION WORD, 32 BITS. ALSO AVAILABLE IN SHIPBOARD CONFIGURATION AS CP-967.	3232	
54. TI 2550 MID 1968	P	Fx	78	4	36	53	DRO CORE	32	4K 32K			2	4	16	IC	50	0.96	310	DATA WORD, 16 BITS; INSTRUCTION WORD, 32 BITS.	2221	
55. CNES ROSEAU COMPUTER LATE 1968	S	Fx	29	68			FIXED	16 16	64K 1000	4				16	IC		0.4	10	DESIGN COMPLETED IN LATE 1968. APPLICATION NOT REALIZED.	UNDE- FINED	
56. RAYTHEON RAC-250 LATE 1968	P	Fx	55	2.4	9.4	23.7	CORE	32	8K 64K			1	35	256	TTL LSI	20	0.4	120	WEIGHT, SIZE AND POWER ARE GIVEN FOR 8K MEMORY. HALF-WORD INSTRUCTIONS USED FOR REGISTER-REGISTER OPERATIONS. FORMERLY CALLED ARGUS MULTIPROCESSOR. EVOLVED INTO RAC-251.	1032	
57. WESTINGHOUSE OBP LATE 1968	P	Fx	55	6.25	45	90	DRO CORE	18	4K 64K			2.2	1	16	LPDTL IC	20	0.3	35	WEIGHT, SIZE AND POWER ARE GIVEN FOR 4K MEMORY EXCLUDING POWER SUPPLY.	1778	
58. ARMA 1808 EARLY 1969	P	Fx	56	6.6	26.4	26.4	DRO CORE	18	4K 32K			0.7	3.3	2	1	TTL IC	6.6	0.096	55	WEIGHT, SIZE, AND POWER ARE GIVEN FOR 4K MEMORY.	2098
59. UNIVAC 1819 EARLY 1969	P	Fx	77	6	24	24	DRO CORE	18	4K 32K			2		1	IC	35	0.7	197	WEIGHT, SIZE AND POWER ARE GIVEN FOR 4K MEMORY	2308	
60. WESTINGHOUSE WADSP 1822 EARLY 1969	S/P	Fx	37	3.2	23.2	34	DRO CORE	18	4K 64K			1	2		TTL ECL	50	1	200	ALSO CALLED AN/AYK-8 WEIGHT, SIZE AND POWER GIVEN ARE MAXIMUMS AND INCLUDES POWER SUPPLY. INTERRUPTS ARE IN INTERFACE EQUIPMENT.	3462	

NRS PRIVILEGED

TABLE 1 - CHARACTERISTICS OF AEROSPACE COMPUTERS (CONTINUED)

NAME	DATE INTRODUCED	DATA FLOW	DATA TYPE	NO. OF INSTRUCTIONS	COMPUTING TIME, $\mu$ SEC	MULT	DIV	MEMORY			NO. OF CHANNELS	NO. OF INTERRUPTS	TYPE OF HARDWARE	PHYSICAL CHARACTERISTICS			COMMENTS	NPR (KBITS)	SEC	
								WORD SIZE (BITS)	CAPACITY (WORDS)	ACCESS TIME ( $\mu$ SEC)				POWER	SIZE (CU. FT.)	WEIGHT (LBS)				TYPE OF HARDWARE
1. AUTONICS 020-1	MID 1969			8	105	112		MOS	24	2K	2			128	6	CU. IN.	10	WEIGHT, SIZE, POWER ARE GIVEN FOR 4K MEMORY AND INCLUDES POWER SUPPLY.	1333	
2. CDC ALPHA	MID 1969			3	9.7	17		DRD CORE	32	4K	16K	0.35	1	LSI	54		250	FIXED POINT ADD, MULTIPLY AND DIVIDE TIMES ARE 2 $\mu$ SEC. 11 $\mu$ SEC. AND 21 $\mu$ SEC. WITH A 16K WORD FIRM MEMORY. THE WEIGHT, SIZE AND POWER ARE 40 LBS, 0.572 FT <sup>3</sup> , AND 165 WATTS. HAS SERIAL OPERATION CAPABILITY.	8719	
3. LITTON-L-350	MID 1969			3.3	6	92		DRD CORE	32	8K	131K	1.6	1	IC	40		40	WEIGHT, SIZE AND POWER ARE GIVEN FOR 8K MEMORY. INSTRUCTION WORD ADDRESSES A MEMORY OPERAND, A REGISTER OPERAND AND AN ANSWER REGISTER.	8964	
4. HOLYWELL HOC-201	LATE 1969			9	100			IC ROM	12	1K	0.900	0.900	12	IC ROM	12	655	32	18 BIT WORD OPTION AVAILABLE. PROGRAM MEMORY IS 16K WORDS. 256 WORDS AND SCRATCH-PAD. 32 INSTRUCTIONS. 256 WORDS AND SCRATCH-PAD. 32 WATTS. WEIGHT, SIZE AND POWER ARE GIVEN FOR 4K MEMORY.	663	663
5. LEAR-SIEGLER LS-50	LATE 1969			3	32	21	116	MOS ROM	16	8K	2	0.05		TTL IC	11		50		525	525
6. RCA 200 SERIES	LATE 1969			3.3	7	10.5		CORE ROM CONTROL	32-4	16K	262K	0.6	1.5	IC	280	9.5	1400	IS 150 MSEC. MULTIPROCESSOR CAPABILITY. UPWARD COMPATIBLE WITH RCA SPECTRA AND IBM 350. PHYSICAL CHARACTERISTICS ARE GIVEN FOR PCA 195A, SMALLEST OF THE 200 SERIES.	8719	8719
7. AC ELECTRONICS MAGIC 351	EARLY 1970			6	24	30		DRD CORE	19	4K	32K	3	8	TTL MSI	22		120	ALSO AVAILABLE WITH 24 BITS - PARALLEL - WEIGHT, SIZE AND POWER ARE GIVEN FOR 16K MEMORY, CPU, PS AND I/O INTERFACE CARD.	2436	2436
8. MIT DIGITAL COMPUTATION ASSEMBLY (DCA)	EARLY 1970			8	20	35		DRD CORE	28	4K	8K	0.5	1.0	TTL IC	1		200	EXAMINER MODEL BUILT. HAS 2K, 20 BIT WORDS OF MICRO-PROGRAM. HAS AUTOMATIC SINGLE INSTRUCTION REGISTER FOR HARDWARE DETECTED FAILURES. HAS SERIAL MULTIPLEXED I/O BUS.	3043	3043
9. ROMA 1501	EARLY 1970			5.9	9.7	9.7		DRD CORE	16	4K	12K	0.9	2.6	IC	40	0.6	70	WEIGHT, SIZE AND POWER ARE GIVEN FOR 4K MEMORY.	2548	2548
10. TELETYPE TDY 300	EARLY 1970			6	22.5	23.0		DRD CORE	24	4K	65K	3	5	HYBRID LSI	25	0.27	110	ONE OF A SERIES. TDY 310 HAS 1/4 SEC ADD TIME.	3137	3137
11. TI 2502 LSI	EARLY 1970			4	11	20		DRD CORE	32	4K	32K		12	LSI	46	0.45	200	DATA WORD, 32 BITS; INSTRUCTION WORD, 16 BITS.	6809	6809
2. HOLYWELL HOC-601	MID 1970			4	12			MOS PLATED WIRE	16	8K	32K	2	20	TTL IC	30	0.7	125	MULTIPLAZED VERSION OF AND COMPLETELY COMPATIBLE WITH THE DDP-516. WEIGHT, SIZE, AND POWER ARE GIVEN FOR 8K MEMORY.	3333	3333
3. RAYTHEON PAC-251	MID 1970			2.4	14.4	27.0		DRD CORE	32	4K	64	1.4	10	BIPOLAR LSI	14	0.23	110	HAS BIPOLAR LSI FOR MICROPROGRAMMED CONTROL. HAS 16 AND 32 CHANNELS AND OPTICAL ADDRESSING. ASSOCIATED CHANNEL MICROPROCESSOR BIT INSTRUCTION AND DATA WORDS. PLATED WIRE MEMORY AND 22 VERSION IS AVAILABLE.	8081	8081
4. AC ELECTRONICS MAGIC 341	DEVELOPMENT			5	20	20		DRD CORE	16	2K	65K	1	2.5	IC	10	0.35	50	BOTH VERSIONS AVAILABLE WITH MICROPROGRAMMED INSTRUCTIONS. HAS STANDARDIZED I/O SIGNAL CONDITIONING MODULES. WEIGHT, SIZE ARE GIVEN FOR 4K MEMORY, CPU, PS AND I/O INTERFACE CARD.	2462	3556

BELLCOMM, INC.

P. 54

NRS PRIVILEGED



TABLE 1 - CHARACTERISTICS OF AEROSPACE COMPUTERS (CONTINUED)

BELLCOMM, INC.

NAME DATE INTRODUCED	DATA FLOW	DATA TYPE	NO. OF INSTRUCTIONS	COMPUTING TIME, $\mu$ SEC			MEMORY					IN/OUTPUT		PHYSICAL CHARACTERISTICS				COMMENTS	NPR (KBITS/SEC)	
				ADD	MULT	DIV	TYPE	WORD SIZE (BITS)	CAPACITY (WORDS)		ACCESS TIME ( $\mu$ SEC)	CYCLE TIME ( $\mu$ SEC)	NO. OF CHANNELS	NO. OF INTERRUPTS	TYPE OF HARDWARE	WEIGHT (LBS)	SIZE (CU. FT.)			POWER (WATTS)
AUTONETICS D200-10 DEVELOPMENT	P	Fx	66	2	11	19	MOS	16	4K	32K	0.5	1.0	64		MOS	4	0.05	15	ONE OF SERIES. D200-30 HAS 24 BIT WORD, D200-50 HAS 32 BIT WORD. FOUR INSTRUCTION CODES AVAILABLE FOR OPTIONAL TRIG FUNCTIONS, VECTOR ROTATION, ETC.	5517
AUTONETICS D200-15 DEVELOPMENT	P	Fx	66	2	11	19	MOS	16	4K	32K						0.5	8 CU. IN.	10	WEIGHT, SIZE AND POWER INCLUDES POWER SUPPLY AND COOLING. DIMENSIONS ARE 2" x 2" x 2", AND VARY DEPENDING ON MEMORY SIZE.	5517
BUNKER-RAMO BR-1018 DEVELOPMENT	P	Fx	43	5	33	43	PLATED WIRE	18	4K	131K	0.8		3	1	MOS LSI	4.5	0.04	35	WEIGHT, SIZE & POWER ARE FOR 4K MEMORY, I/O INCLUDES DMA, PARALLEL, & CONTROL CHANNELS	2308
CDC 459 DEVELOPMENT	P	Fx	42	2.4	10.4	30.4	PLATED WIRE	18	512	65K	1.0	1.6	3		MOS	2.7	34.3 CU. IN.	<10	DOUBLE PRECISION ADD, 3.6 $\mu$ SEC. WEIGHT, SIZE & POWER ARE FOR 4K VERSION.	5000
COLLINS C864A-1 DEVELOPMENT	S	Fx	61	3.4	4.0	7.0	DRO CORE	32	4K	16K	0.6	2.0	8		TTL IC	37	1.0	540	HAS FLOATING POINT OPTION. BYTE ORIENTED. UP TO TWO I/O CHANNELS CAN BE IMPLEMENTED AS TIME DIVISION MULTIPLEX CHANNELS.	9249
GEMC CP-32A DEVELOPMENT	P	Fx	70	1.3	8.5	14.6	PLATED WIRE	32	8K	128K	0.387	1.0	1	32	TTL MSI/LSI	40	0.7	395	I/O FOR BOTH PROGRAMMED AND DIRECT MEMORY ACCESS WITH 16 MULTIPLEXED CHANNELS EACH. TWO GROUPS OF 16 GENERAL REGISTERS. 16 OR 32 BIT INSTRUCTION AND DATA FORMATS.	15842
GPI KEARFOTT SKC-2000 DEVELOPMENT	P	F1	113	2.62	5.32	8.12	DRO CORE	16/32	4K	131K	1.0	2.5	64	16	TTL MSI	19.7	0.32	150	LSI SCRATCHPAD AVAILABLE, PROVIDES 0.75 $\mu$ SEC ADD, 4 $\mu$ SEC MULTIPLY. FORMERLY CALLED FOCUS KP.	5536/ 11072
HONEYWELL HOC-701 DEVELOPMENT	P	Fx	56	2.4	10.8	21.4	PLATED WIRE	32	4K	16K	0.6		1	8	IC	50	1.2	270	HAS MICROPROGRAMMED CONTROL.	9877
HUGHES HCM-231 DEVELOPMENT	P	Fx	81	2	5.5	15	DRO CORE PLATED WIRE SEMICONDUCTOR THIN FILM	24	4K	131K		1-2	3	24	MSI	45	0.75	760	PHYSICAL CHARACTERISTICS INCLUDE 4 I/O MODULES AND A 12K WORD CORE MEMORY. HAS FLOATING POINT OPTION.	10213
IBM AP-1 DEVELOPMENT	P	Fx	76	2.25	7	11	DRO CORE	32	8K	24K		1	4	9	TTL IC	48.5	0.8	240	PHYSICAL CHARACTERISTICS ARE FOR CPU, 16K MEMORY, POWER SUPPLY AND I/O.	11743
LITTON L-3070 DEVELOPMENT	P	Fx	103	2.5	2.5	10.0	DRO CORE	32	16K	131K	0.4	1.0	5	64	LSI	142	3.4	300	LSI VERSION OF L-2050. BASIC BOX HOLDS 131K MEMORY WORDS; 33K WORDS ARE DIRECTLY ADDRESSABLE. PHYSICAL CHARACTERISTICS ARE FOR 16K MEMORY AND INCLUDE I/O UNIT.	12800
NORTHROP HOC-1071 DEVELOPMENT	P	Fx	31	3	20	50	DRO CORE	16	4K	16K		1	1		IC	16	0.27	150	WEIGHT, SIZE AND POWER ARE FOR 4K MEMORY, NO I/O. FLOATING POINT OPTION IS AVAILABLE. CONTROL IS MICROPROGRAMMED USING LSI ROM. ALSO CALLED NORTHROP'S DELTA I.	3404
UNIVAC 1832 DEVELOPMENT	P	F1	137	1.5	8	10	THIN FILM	32	65K	262K		.750	2	2	TTL IC	A 240 B 550 C 650	5 13.5 15	1 KW 2.6KW 3.4KW	MEMORY OVERLAP REDUCES ADD TIME. I/O CHANNELS ARE FOR ONLY 0 CONTROL. MORE CAN BE ADDED. SOME MSI CIRCUITS USED. PHYSICAL CHARACTERISTICS: A IS FOR SINGLE PROCESSOR, I/O, 32K MEMORY; B IS FOR DUAL PROCESSOR, I/O, 131K MEMORY; C IS FOR THREE PROCESSORS, THREE I/O, 131K MEMORY.	14884

# NAS PRIVILEGED

TABLE 1: CHARACTERISTICS OF AEROSPACE COMPUTERS (CONTINUED)

\*EXPLANATION OF HEADINGS:

● NUMBER: PROVIDES CROSS-REFERENCE FROM ALPHABETICAL LIST TO THIS CHRONOLOGICAL LIST.

● NAME: MANUFACTURER'S NAME, FOLLOWED BY OTHER IDENTIFYING NAMES OR NUMBERS. DATE OF INTRODUCTION IS DATE THAT MANUFACTURER HAD WORKING HARDWARE.

● DATA FLOW: S = SERIAL, OR P = PARALLEL, INDICATES THE WAY DATA FLOWS IN THE ARITHMETIC UNIT; S/P INDICATES A COMBINATION OF SERIAL AND PARALLEL, AND IS EXPLAINED IN THE "COMMENTS" COLUMN.

● DATA TYPE: Fx = FIXED POINT, FL = FLOATING POINT.

● NO. OF INSTRUCTIONS: THIS THE NUMBER OF INSTRUCTIONS IN THE INSTRUCTION SET, AND DOES NOT INCLUDE VARIATIONS OF BASIC INSTRUCTIONS.

● COMPUTING TIMES: NO MEMORY OVERLAP IS ASSUMED. ONE INSTRUCTION FETCH AND ONE OPERAND FETCH FROM MEMORY IS INCLUDED.

● MEMORY: "CAPACITY (MIN)" IS THE STANDARD MEMORY SIZE FOR THE MACHINE, AND "CAPACITY (MAX)" IS THE MAXIMUM SIZE OF DIRECTLY ADDRESSABLE MEMORY ATTAINABLE BY ADDING STANDARD MODULES.

● INPUT/OUTPUT: THESE NUMBERS WERE OBTAINED FROM MANUFACTURER'S DESCRIPTIONS. DIFFERENT MANUFACTURERS DEFINE "CHANNEL" IN DIFFERENT WAYS, AND INTERRUPTS LISTED IN SPECIFICATIONS SOMETIMES INCLUDE INTERNAL INTERRUPTS AS WELL AS EXTERNAL INTERRUPTS. THEREFORE, CARE SHOULD BE TAKEN IN USING THE NUMBERS LISTED.

● PHYSICAL CHARACTERISTICS: UNDER "TYPE OF HARDWARE" THE FOLLOWING ABBREVIATIONS ARE USED:

MOS - METAL OXIDE SEMICONDUCTOR

IC - INTEGRATED CIRCUITS

DCTL - DIRECT-COUPLED TRANSISTOR LOGIC

DTL - DIODE-TRANSISTOR LOGIC

TTL - TRANSISTOR-TRANSISTOR LOGIC

HL - HIGH LEVEL, AS IN HLTL.

LSI - LARGE SCALE INTEGRATION

THE WEIGHT, SIZE, AND POWER REQUIREMENTS ARE GIVEN FOR A MACHINE WITH A "STANDARD SIZE" MEMORY.

● COMMENTS: COMMENTS DESCRIBE UNIQUE OR INTERESTING FEATURES, OR FURTHER EXPLAIN AN ENTRY IN THE PRECEDING COLUMN.

● NPR - Numeric Processing Rate

$$NPR = \frac{\text{Data Word Size}^*}{0.9 \times \text{Add Time} + 0.1 \text{ Multiply Time}}$$

\* If data word size exceeds 32 bits, 32 is used in this formula. As indicated in COMMENTS column, data word size might differ from value given in WORD SIZE column.

## ABOUT THE AUTHOR



Don Baechler, a Member of Technical Staff of Bellcomm, Inc., Washington, D.C., is a member of the Institute of Electrical and Electronics Engineers. He has an M.S.E. degree from the George Washington University, where, as a member of the part-time staff, he teaches undergraduate computer design courses and graduate courses in computer systems and automata theory. He is a registered Professional Engineer and a member of the National Society of Professional Engineers and of Sigma Tau.

# NAS PRIVILEGED

22 June 1971

NATIONAL ACADEMY OF SCIENCES  
COMPUTER SCIENCE AND ENGINEERING BOARD  
Washington, D. C.

PROPOSAL

TO: Office of Export Control  
Bureau of International Commerce  
U. S. Department of Commerce

- FOR:
1. A Study to Define the Boundaries Dividing Computers, Components, and Peripherals From Calculators and Similar Equipments; and,
  2. A Review and Evaluation of the Previous and Current Work Relating to the Measurement of the Strategic Potential of Computer Systems.

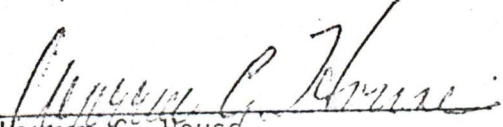
DURATION: 15 June 1971 through 31 December 1971

Contract Administrator

---

B. L. Kropp  
Deputy Business Manager  
961-1213

Program Administrator

  
Warren C. House  
Executive Secretary, CS&EB  
961-1834

PROPOSAL TO  
STUDY AND DEFINE THE BOUNDARIES DIVIDING COMPUTERS,  
COMPONENTS AND PERIPHERALS FROM CALCULATORS  
AND ASSOCIATED EQUIPMENTS  
AND TO  
REVIEW AND EVALUATE THE PREVIOUS AND CURRENT WORK  
RELATING TO THE MEASUREMENT OF THE STRATEGIC  
POTENTIAL OF COMPUTER SYSTEMS

The administration and execution of U.S. export policies covering computers, components, and peripherals is becoming increasingly important to (1) the U.S. government in relation to general export policy and foreign relations; (2) to the operating departments responsible for reaching judgments regarding the exportability of computer systems; (3) to the operating departments concerned with the application of guidelines to the measurement of the existing and potential strategic value of work done by a given computer system; and, (4) to the various computer companies marketing computer systems in the international area. The rising importance derives, in part, from the sharpening competition in the world market among computer manufacturers, from the greater complexity of U.S. computer systems being exported, and from the recent arrival of the latest generation of computer technology.

In regard to the sharpening competition in the international market, it is becoming increasingly difficult to use the existing criteria to distinguish consistently between computer systems, on the one hand, and

calculators and similar equipments, on the other hand. This difficulty arises in part from an irregular ebb and flow among the various technologies which at any given point in time are included in computer systems, calculating and processing systems, data handling equipments and general communications equipments. The desired combination of the above technologies and equipments reflects the operating requirements of an organization at a given point in time. These requirements have their own "drift" or "float". For example, on-coming combinations of calculators and associated equipments possess some properties previously found in small computer systems. Small, specialized computer systems often possess one or more capability or capacity that raises them above the export control threshold. Re-defining the boundaries would be a task of considerable complexity, including both technical and operational aspects of systems applications.

Devising a feasible method for consistently and reliably measuring the capacity of a computer system to perform work of strategic value involves three separate sets of action. The first has to do with general and specific technology evaluations and would include (1) the overall evaluation of the "new generation technology" as technology, per se, and as an interactive force within the current computer systems technology package, and (2) the evaluation of measurable and viable "elements of technology" within the

new generation and an updating of the evaluation of "elements of technology" carried forward to current systems from preceding generations. The second has to do with the functional criteria currently being used to measure the capacity of computer systems to perform work of strategic value, and would include re-evaluation of the functional criteria used and possible modifications in light of the experience of the past few years and of the new generation technology. The third has to do with the "administrability" of any given formula or method and would include a comparative evaluation of the current method with any newly developed method.

The Computer Science and Engineering Board proposes to undertake the first task of defining the boundaries dividing computer systems from calculators and similar equipments and to evaluate previous and current work relating to the second as a combined technical analysis in support of the President's Special Assistant for Science and Technology, the Department of State, the Department of Defense, the Department of Commerce, and other government elements having interests and responsibilities in the computer export area.

The two studies would be handled as separate, but concurrent and closely related activities. A special sub-Panel of the CS&E Board would be established to do the technical analysis to distinguish more clearly the line separating computer systems from calculators and similar equipments. The

pertinent information, experience and expertise within the government and the private sector will be utilized, as appropriate. The results will be issued and distributed to those government activities having priority concern with the problem. Further distribution of this report, or generalized version, may be made as mutually agreed upon.

The work to develop a technically reliable method for consistently measuring the capacity of a computer system to perform work of strategic value would be undertaken concurrently by a second special sub-Panel of the CS&E Board. The work would be performed in two stages. The first stage would include, but not necessarily be limited to, a survey and evaluation of previous and current work in the field relating to the measurement of the strategic potential of computer systems. The outcome could take the form of consultations, informal briefings and perhaps an informal paper, as mutually agreed upon. If the outcome of stage one indicates the need for further work to develop a satisfactory method for measuring the strategic potential of computer systems, a supplemental proposal will be submitted outlining the nature of the additional work to be undertaken, a new time period for performance and the additional funding schedule. As in the case of task one, i.e., computer systems vs. calculators, the pertinent information and expertise within the government and the private sector would be brought to bear.

The decision to move into stage two could occur at any time during the course of the initial inquiry that is mutually agreed upon.

Page Five  
Export Control Proposal  
22 June 1971

These two concurrent efforts would take place between 15 June 1971 and 31 December 1971. Interim or preliminary papers, technical consultations, briefings or conferences would be provided as mutually agreed upon. Close liaison will be maintained with the elements of government concerned with various aspects of the problem in order to assure the timing and focus that would be most useful to those government activities having policy and implementation responsibilities.

Attached is a proposed budget showing the total funds needed and the estimated expenditures within that total.



file

OCT 16 1972

NATIONAL ACADEMY OF SCIENCES  
2101 CONSTITUTION AVENUE  
WASHINGTON, D. C., 20418

ANTHONY G. OETTINGER, CHAIRMAN  
COMPUTER SCIENCE & ENGINEERING BOARD  
AIKEN COMPUTATION LABORATORY  
HARVARD UNIVERSITY  
CAMBRIDGE, MASSACHUSETTS 02138

11 October 1972

PREFACE

and

SUMMARY

of the

Project on Computer Databanks  
and of its report

DATABANKS IN A FREE SOCIETY

TO BE PUBLISHED IN NOVEMBER, 1972

by

Quadrangle Books

A New York Times Company

## PREFACE

Due process and privacy have long been matters of fundamental importance to all Americans. At its inception in July 1968, the Computer Science and Engineering Board of the National Academy of Sciences invited one of its members, Alan F. Westin, Professor of Public Law and Government at Columbia University, to discuss issues of due process and of privacy in the context of trends toward increasing computerization of personal records. Because of the sparseness of information, the board concluded that the public interest would be served by searching out and publishing a comprehensive body of facts about the actual effects that computers, communications, and allied information technologies have had on creating, sharing, and using files on individuals.

This goal was to be reached through firsthand observations in depth of as broad a cross-section of private and public files as resources would permit. In keeping with the board's policy, commitment to this goal implied looking not merely at file technology, but also at the nontechnical factors shaping its use: it implied estimating technological trends and developing the future implications of these trends for individual and public policy choices on matters of due process and of privacy. Including classified government files in the study was precluded by legal limitations on access to these files and, when access is granted, on freedom to publish findings. Attempting, as an alternative, to develop implications for public policy choices from the fragmented and unverifiable information publicly available seemed unwise.

Professor Westin, with Dr. Launor Carter, Vice-president and Manager of the Public Systems Division of the Systems Development Corporation; Dr. John R. Meyer, President of the National

## *DATABANKS IN A FREE SOCIETY*

Bureau of Economic Research and Professor of Economics at Yale University; Dr. John R. Pierce, then Executive Director of the Research Communications Sciences Division at Bell Laboratories and now Professor of Engineering at the California Institute of Technology; and Dr. J. Barkley Rosser, Professor of Mathematics and Director of the Mathematics Research Center at the University of Wisconsin, developed a study plan for review and approval by the board.

Sharing as they do the board's interest in the interrelation of law, the behavioral sciences, and technology, Russell Sage Foundation and its President, Orville G. Brim, Jr., were receptive to our plan. In February 1969, Russell Sage Foundation accepted a formal study proposal submitted by the Computer Science and Engineering Board and approved by the President and Council of the National Academy of Sciences. Named Project Director, Alan Westin, with the advice of the board, assembled a staff well versed in computer science, economics, journalism, law, political science, psychology, and sociology. Based on the contributions and critical comments of the entire project staff, the final report was written by Alan F. Westin and Michael A. Baker.

To assure that major viewpoints and contrasting positions on basic issues involved in databanks would influence the planning, research, and reporting of the project, the board appointed a National Advisory Group to the project. With the understanding that their role was advisory and that responsibility for this report rests with the authors, the Computer Science and Engineering Board and the National Academy of Sciences, these people gave fully and freely of their advice and their criticism at several stages of the work. This report owes much to their probing and their prodding.

A distinguishing mark of this report is its fascinating first-hand accounts of 14 out of over 50 site visits made by the project director and his staff to public and private organizations whose files on people are in transition from manual to computer technology. The staff was welcomed with courtesy over extended and, occasionally, repeated visits. To each organization and to every individual in it who met with the staff and answered their questions, the board expresses its thanks.

Those who answered the questionnaires used in the study were pledged anonymity. In their privacy, they too have our

*Preface*

thanks, along with the anonymous reviewers of this report selected by the National Academy of Sciences' Report Review Committee.

The board closely supervised the study throughout its course. Alan Westin and his staff gave of themselves unstintingly in developing the factual base for their findings and analyses. The board deeply appreciates their efforts and is pleased to commend this report to all Americans.

Computer Science and Engineering Board

By \_\_\_\_\_

Anthony G. Oettinger  
Chairman

## SUMMARY

The United States has become a records-oriented society. In each major zone of personal and civic life (education, employment, credit, taxation, health, welfare, licensing, law enforcement, etc.), formal, cumulative records are assembled about each of us by hundreds of private and government record-keeping organizations. These personal histories are relied on heavily by the collecting organizations in making many decisions about our rights, benefits, and opportunities, and informal networks for sharing record-information among public and private organizations become a common feature of organizational life heavily dependant on credentials.

During the past two decades, as most government agencies and private organizations have been computerizing their large-scale files, the American public has become concerned that dangerous changes might be taking place in this record-keeping process. Because of the computer's enormous capacities to record, store, process, and distribute data, at great speeds and in enormous volumes, it is feared that far more personal data might be assembled about the individual than it had been feasible to collect before; that much greater sharing of confidential information might take place among the computerized record holders; and that there might be a lessening of the individual's ability to know what records have been created about him, and to challenge their accuracy or completeness.

DATA BANKS IN A FREE SOCIETY is the report of the first nationwide, factual study of what the use of computers is actually doing to record-

keeping processes in the United States, and what the growth of large-scale databanks, both manual and computerized, mean for the citizen's constitutional rights to privacy and due process.

It also outlines the kinds of public policy issues about the use of databanks in the 1970's that must be resolved if a proper balance between the individual's civil liberties and society's needs for information, is to be achieved.

#### HOW THE STUDY WAS CONDUCTED

The Project on Computer Data Banks was a three year research study conducted under the auspices of the Computer Science and Engineering Board of the National Academy of Sciences, under grants of \$164,000 from Russell Sage Foundation. The Director of the Project was Dr. Alan F. Westin, Professor of Public Law and Government, Columbia University, and author of the well-known book, Privacy and Freedom, published in 1967. An interdisciplinary staff of seven scholars from the fields of law, computer science, and the social sciences collaborated in the research. The project received continuing guidance not only from the Computer Science and Engineering Board but also a special Advisory Board of 18 prominent figures in public life whose views spanned the full spectrum of opinion on issues of databanks and civil liberties.\* The final report of the project was written by Dr. Westin and Mr. Michael A. Baker, Assistant Director of the Project and an Instructor in Sociology at Brooklyn College of the City University of New York.

The major sources collected and used by the Project include:

1. Documentary materials on computerized record systems in more

\* Names of staff and Advisory Board members appear later in this summary.

than 500 government agencies and private organizations.

2. Detailed on-site staff visits to 55 of the most advanced computerizing organizations, ranging across the most sensitive fields of personal record-keeping.

3. Replies from over 1500 organizations in a national mail survey of developments in computerization and record-keeping among government agencies and private organizations.

4. Extensive interviews with officials from computer companies, software houses, systems consulting firms, industry associations, civil liberties groups, labor unions, consumer organizations, minority-rights organizations, and professional associations.

5. Legal, legislative and regulatory-agency materials dealing with databank issues in 25 distinct major fields of personal record-keeping.

6. Materials and interviews on the state of databank developments and regulatory controls in 23 foreign nations, for purposes of comparison with the United States.

#### ORGANIZATION OF THE REPORT

The Report is organized into five parts:

Part I presents a brief, orienting discussion of computer systems and civil liberties concepts for general readers.

Part II consists of "profiles" of 14 governmental, commercial, and private organizations, drawn from 55 to which the Project staff made site visits. Each profile describes the nature and function of the organization, its pre-computer record-keeping, its move into computer usage, the effect of automation on its record-keeping about people, previous

civil liberties issues involving the organization's manual record-keeping, the effect of computerization on civil liberties protections, and the organization's plans for further computerization in the next five years.

The 14 organizations given this detailed treatment are:

The U.S. Social Security Administration  
 The F.B.I.'s National Crime Information Center  
 Kansas City (Missouri) Police Department  
 New York State Department of Motor Vehicles  
 City of New Haven, Connecticut  
 Santa Clara County, California  
 Bank of America  
 T.R.W. - Credit Data Corporation  
 Mutual of Omaha Insurance Company  
 R.L. Polk & Company  
 Massachusetts Institute of Technology  
 Church of Latter Day Saints  
 Office of Research, American Council on Education  
 Kaiser-Permanente Health Plan

Part III has three chapters which present and analyze the Project's principal findings. These include an overview of what kinds of files have and have not been computerized in advanced organizations; an analysis of computer effects on civil liberties that are not taking place as yet; and a description of those changes in record-keeping that the use of computers and communication systems is producing in these organizations.

Part IV is an analysis of the way in which the reception of computer technology is affected by organizational, legal, and socio-political factors, followed by a forecast of developments in new computer and communications technologies that are likely to occur in the remainder of the 1970's, and an analysis of their implications for civil liberties.

Part V discusses public policy choices in the 1970's in light of the project's findings and forecasts. The first chapter analyzes the larger



socio-political significance of the computer's arrival in the late 1950's and 1960's; it goes on to suggest the basic civil liberties principles that ought to be followed when seeking to safeguard citizen rights in large-scale record systems, especially in the increasingly computerized sectors of American organizational life. The final chapter of the report presents an agenda for the 1970's, identifying six areas of priority for public policy and civic action.

Three appendixes to the report present the results from the Project's survey of organizations, an analysis of public opinion literature on privacy and the computer, and information about the experience of other advanced industrial nations in dealing with the databanks-and-privacy problem.

#### HIGHLIGHTS OF THE REPORT

1. A great many commentators have warned that the spread of computers is fundamentally altering the balance between information policies of organizations and individual rights to privacy that marked past eras of record-keeping. Compared to what was done in the manual era, it is said, the new capacities of the computer inevitably lead organizations to collect more detailed and intrusive personal information about individuals; to consolidate confidential information from previously separate files; and to share confidential personal data with government agencies and private organizations that had not received it before. The Project's findings from visits to 55 organizations with highly advanced computer applications is that computerization is not yet having such effects in the overwhelming majority of such organizations. For a combination of technological and organizational reasons, central databank developments are far from being as advanced as many public commentaries have assumed. Organizations have

so far failed to achieve the "total" consolidation of their information about individuals which raised civil liberties alarms when such goals were announced in the 1960's by various government agencies or private organizations.

Further, in computerizing their records on individuals organizations have generally carried over the same policies on data collection and sharing that law and administrative traditions in each field had set in the pre-computer era. Where new law or practices have evolved to protect individual liberties over the past decade, organizations with computerized systems have followed such new policies as fully as those that still use manual files and procedures. Even the most highly computerized organizations continue to rely heavily on manual record keeping and retain in their paper files the most sensitive personal information they possess.

2. Another widely held fear is that computerization makes it more difficult for the individual to know what is in the file about him, to have errors corrected, or have the data erased where public policy specified that certain information about an individual's past should be ignored. The Project's inspection of advanced systems showed that notice to the individual about a record's existence, opportunity to inspect and challenge that record, and policies as to the removal of out-of-date or irrelevant information were not being substantially altered by computerization. Where policies affording individuals rights of due process such as the above had been provided in an organization prior to computerization, those rules are being followed in the new computerized systems as well. Where no such rights were given, the adoption of computers has not made

the situation either worse or better. Neither has computerization introduced impersonal decision making in systems where this was not present before, nor forced organizations into greater reliance on "the record" in making decisions about clients, customers or citizens. Where abuses along these lines were present in computerized systems -- raising serious due process questions -- they had been carried over from the high-volume "processing" of people in the manual era.

Over and over again, the Project's findings indicate profound public misunderstanding about the effect of computers on large scale record systems. To some extent, the inflated claims and proposals of organizational managers about the capacities of their computer systems helped to generate what were in fact baseless privacy concerns on the part of the public. In addition, as the Report shows with respect to law enforcement uses and airline-reservations and charge-card systems, many commentators on computers and privacy issues have failed to do adequate research into the actual operations of systems about which they write, and have presented entirely incorrect pictures to the press and public about how these computer systems work. The danger in this, the report points out, is that we may give up the fight in the belief we have already lost. "If we assume that computer users are already doing things that they are not, we risk surrendering without a fight the border between properly limited and surveillance-oriented computer applications... The question of what border control measures should be adopted can hardly be understood and properly considered...if the public and opinion leaders assume that the borders have already been obliterated."

3. Computerization in advanced organizations is producing changes in record-keeping methods that can increase the efficiency with which organizations carry out their basic decision making about the people

they process or serve. Computerization is making it possible for many organizations to maintain more up-to-date and complete records; obtain faster responses to inquiries about a given individual; and make more extensive use of information already in the files. Computers have also made possible dramatic expansion of networks for exchange of data among organizations that have shared data since pre-computer days; and the creation of some large data bases of information about people that would not have been feasible without automation. These changes have been felt already in police information systems, national credit reporting systems, charge card systems, and others.

4. Looking at technological trends for the remaining years of the 1970's, the Report forecasts that while there will be important continued increases in computer capabilities, no developments are now foreseeable that will alter the technological, organizational, and socio-political considerations that presently frame the databanks and civil liberties issue. Organizations will have more flexible, reliable, and cost-effective computer systems to use in pursuit of their policies, but these will not represent a radical departure from the computer capabilities presently available. The most important development with implications for civil liberties will be an increase in the ease with which data can be shared among organizations which have computers, coupled with a reduction in the cost of doing so. This will make it imperative that legal boundaries as to data-sharing are set as clearly as possible.

5. The Project concluded that the real issue of databanks and civil liberty facing the nation today is not that revolutionary new capacities for data surveillance have come into being as a result of computerization. The real issue is that computers arrived to augment the power of

organizations just when the United States entered a period of fundamental debate over social policies and organizational practices, and when the traditional authority of government institutions and private organizations has become the object of wide-spread dissent. Important segments of the population have challenged the goals of major organizations that use personal records to control the rights, benefits, and opportunities of Americans. There is also debate over the criteria that are used to make such judgments (religious, racial, political, cultural, sexual, educational, etc.), and over the procedures by which the decisions are reached, especially those that involve secret proceedings and prevent individuals from having access to their own records. Computers are making the record keeping of many organizations more efficient precisely at the moment when trust in many large organizations is low and when major segments of the American population are calling for changes in values that underly various social programs, for new definitions of personal rights, and for organizational authorities to make their decision-making procedures more open to public scrutiny and to the review of specific individuals involved.

6. Despite the rapid spread of computers, there has been little so far by way of new legislation, judicial rulings, regulatory-agency rules, or other legal remedies defining new rights to privacy and due process in major record systems. The Report stresses that, because of the increased efficiency of record-keeping and the growing intensity of the public's concern, the middle 1970's is the moment when law-makers and the public must confront both long-standing and newly raised civil liberties issues, and evolve a new structure of law and policy to apply principles of privacy

and due process to large-scale record keeping.

7. The Report identifies six areas of priority for public action, and presents examples of specific policy measures under each of these that ought to be seriously considered by policy makers:

A. Development of laws to give the individual a right of access and challenge to almost every file in which records about him are kept by city, county, state, or government agencies. At stake here is the possibility that, denied access to records being used for decisions about himself, the citizen is left with "feelings of powerlessness and the conviction that government authority is fundamentally arbitrary."

At the very least, citizens ought to know what record systems exist in government agencies. A Citizen's Guide to Files, published at every appropriate level of government jurisdiction, should "provide the citizen with a thorough, detailed and non-technical directory of the record systems that contain information about him, and the general rules under which it is being held and used." Providing adequate due process protection in government files, the Report suggests, is best achieved by assuming that individuals should be able to see and get a copy of any records used to affect them personally -- with the record keeping agency "bearing the burden of proving that some specific public interest justifies denying access."

B. Development of explicit laws or rules balancing confidentiality and data-sharing in many sensitive record systems that today do not have clearly defined rules. Among these would be rules governing the provision of information to law enforcement agencies from bank accounts, travel and entertainment card records, airline and hotel reservation systems,

etc. The Report predicts that one or two large systems will come to dominate in each of these areas. "This development will make the individual's account record more comprehensive and a very inviting target for investigators of all kinds. With that rise in sensitivity and attractiveness ought to go legislative enactments spelling out retention and destruction policies, confidentiality rules, and procedures for protecting individual rights when outsiders seek to obtain access for what are asserted to be lawful and necessary purposes."

As a case study in how not to build new record systems, the Report discusses some of the major Administration and Congressional proposals for national welfare reform, which generally hinge on the availability of computers for massive data storage and exchange. Several of the welfare system proposals contain "sweeping authorizations for data collection and sharing but almost nothing by way of confidentiality standards and due-process review procedures." The Report points out that we may be "creating one of the largest, most sensitive, and highly computerized record systems in the nation's history, without explicit protections for the civil liberties of millions of persons whose lives will be profoundly affected..."

C. Limit the collection of personal information where a proper regard for the citizen's right to privacy suggests that records ought not to be maintained at all by certain organizations, or never furnished for certain uses in the society. Among the examples are the use of arrest-only records in licensing and employment decisions, and the selling to commercial advertising services of names and addresses collected by government under its licensing and regulatory powers, unless the individual

specifically consents to such use.

In the case of arrest records, the Report stresses that "a democratic society should not allow arrest records to be collected and circulated nationwide with increasing efficiency without considering directly the actual social impact of their use in the employment and licensing spheres, and without examining the possibility that dissemination beyond law-enforcement agencies represents an official stigmatization of the citizen that ought to be either forbidden by law, or closely regulated."

D. Increased work by the computer industry and professionals within it on technological safeguards which will make it possible to implement confidentiality policies more effectively than is now feasible. The Report notes that "No 'technological fix' can be applied to the databank problem." Protection of privacy is a matter of social policy, on which "computer professionals are fellow citizens, not experts." But the Project calls for more research, development, and testing efforts to be undertaken by the computer industry to see that the computer's capacities for protection of confidentiality and insurance of proper citizen access are turned into "available and workable products." Law and public pressure, the Report suggests, require that such measures be taken by managers of sensitive record systems when they are computerized, thereby stimulating the "user demand" to provide a practical market for such devices and techniques.

E. Reconsideration by congress and the executive branch of the current permissive policies toward use of the social security number in an increasing number of government and private record systems. The Report notes that having such a number is not a prerequisite for linking files within or between organizations, but notes that a common numbering system clearly makes record linkage easier and cheaper. Further, the Project



concludes that resolving the critical civil liberties issues in record keeping "will require that a minimum level of trust be maintained between American citizens and their government. Under these conditions, adopting the social security number as a national identifier or letting its use spread unchecked cannot help but contribute to public distrust of government."

F. Experimentation with special information-trust agencies to hold particularly sensitive bodies of personal data. For example, the Report suggests that the handling of both national crime statistics and summary criminal histories ("rap sheets") might be taken away from the Federal Bureau of Investigation and placed in an independent national agency under control of a board that would have public representatives as well as law enforcement officials on it. Such an agency would have to be established "with a clear legislative mandate to be a 'guardian' institution," paying attention to civil liberties interests as well as law enforcement needs.

The Report stressed that the next five years would be a critical period in the reception and control of sensitive personal record systems, especially those managed by computers. More sensitive areas of record-keeping are being entered by many computerizing organizations, many larger on-line (instant access) networks are being brought into operations, and more consolidations of presently scattered records about individuals can be seen as a trend in certain areas, such as criminal justice, credit and financial transactions, and welfare. The Report stresses that unless law makers and organizational managers develop proper safeguards for privacy and due process, and create mechanisms for public scrutiny and review, the record systems they are

building could sharpen the already serious debate in American society over the way to apportion rights, benefits, and opportunities in a credential-oriented society, and leave organizational uses of records to control individual futures too far outside the rule of law.

In its closing paragraphs, the Report sums up the databanks and civil liberties problem as follows:

"If our empirical findings showed anything, they indicate that man is still in charge of the machines. What is collected, for what purposes, with whom information is shared, and what opportunities individuals have to see and contest records are all matters of policy choice, not technological determinism. Man cannot escape his social or moral responsibilities by murmuring feebly that "the Machine made me do it."

"There is also a powerful tendency to romanticize the pre-computer era as a time of robust privacy, respect for individuality in organizations, and "face-to-face" relations in decision-making. Such arcadian notions delude us. In every age, limiting the arbitrary use of power, applying broad principles of civil liberty to the troubles and challenges of that time, and using technology to advance the social well-being of the nation represent terribly hard questions of public policy, and always will. We do not help resolve our current dilemmas by thinking that earlier ages had magic answers.

"Computers are here to stay. So are large organizations and the need for data. So is the American commitment to civil liberty. Equally real are the social cleavages and cultural reassessments that mark our era. Our task is to see that appropriate safeguards for the individual's rights to privacy, confidentiality, and due process are embedded in every major record system in the nation, particularly the computerizing systems that promise to be the setting for most important organizational uses of information affecting individuals in the coming decades."

#### STAFF AND ADVISORY BODIES TO THE PROJECT

Staff Associates for the Project were:

Robert F. Boruch, Assistant Professor, Department of Psychology,  
Northwestern University

Howard Campaigne, Professor of Mathematics, Slippery Rock State  
College

Gerald L. Grotta, Associate Professor of Journalism, Southern Illinois University

Lance J. Hoffman, Assistant Professor of Electrical Engineering and Computer Sciences, University of California, Berkeley

Charles Lister, Attorney at Law, Washington, D.C.

The Project had during its existence an Advisory Group that provided the staff with a wide range of diverse viewpoints on the databanks and civil liberties issue and helped shape the project's studies. Members of the Advisory Group were:

Edgar S. Dunn, Jr.  
Resources for the Future, Inc.

The Honorable Cornelius E. Gallagher  
House of Representatives

Richard Freund  
First National City Bank

Justice Nathan L. Jacobs  
New Jersey Supreme Court

Nicholas deB. Katzenbach  
Vice President and General Counsel  
IBM Corporation

John H. Knowles  
President, Rockefeller Foundation

Arthur R. Miller  
Professor of Law  
Harvard University Law School

George A. Miller  
Institute for Advanced Study  
Princeton, New Jersey

Ralph Nader  
Attorney, Washington, D.C.

Arthur Naftalin  
Professor of Public Affairs  
University of Minnesota

Anthony G. Oettinger  
Harvard University

John R. Pierce  
California Institute of Technology

The Honorable Ogden R. Reid  
House of Representatives

L. F. Reiser  
Corporate Director  
Personnel and Industrial Relations  
CPC International Inc.

Richard Ruggles  
Department of Economics  
Yale University

Roderick O. Symmes  
Director, Data Systems & Statistics Staff  
U.S. Dept. Housing and Urban Development

Roy Nutt  
Vice President  
Computer Sciences Corporation

Following this summary are a list of the members of the Computer Science and Engineering Board who supervised the Project throughout its operations, and brief biographies of the Report's authors, Professor Westin and Mr. Baker.

Computer Science and Engineering Board

Anthony G. Gettinger, Harvard University - Chairman  
Jerrier Haddad, IBM - Vice-chairman

Stephen Ailes - President, American Association of Railroads  
Walter S. Baer - Consultant to the Rand Corporation, Los Angeles (1972)\*  
Lewis S. Billig - Technical Director of Strategic and Communications Systems,  
Mitre Corporation  
Howard Campaigne - Mathematics department, Slippery Rock College  
Launor F. Carter - Vice-president, Systems Development Corporation  
Wesley A. Clark - Computer Systems Laboratory, Washington University (1971)  
Fernando J. Corbato - Professor of Electrical Engineering, Massachusetts  
Institute of Technology  
Harvey Cragon - Manager, Advanced Design Department, Digital Systems Division,  
Texas Instruments, Inc.  
Guy Dobbs - Vice-president, Xerox Computer Services  
Hugh Donaghue - Special Assistant to the President, Control Data Corporation  
David C. Evans - Director of Computer Science, University of Utah (1970)  
Sidney Fernbach - Head, Computation Department, Lawrence Radiation Laboratory  
Martin Greenberger - Chairman, Computer Science Department, Johns Hopkins  
University  
D. Brainerd Holmes - Executive Vice-president, Raytheon Company  
Wayne D. Holtzman - President, Hogg Foundation for Mental Health Research  
William Knox - Director, National Technical Information Service, Department  
of Commerce (1971)  
Cecil E. Leith, Jr. - Head, Dynamics Department, National Center for  
Atmospheric Research  
J.C.R. Licklider - Director, Project MAC, Massachusetts Institute of Technology  
(1971)  
Donald A. Lindberg - University of Missouri Medical Center  
William L. Lurie - Vice-president, International Strategy Planning and Review  
Operations (1971)  
Max V. Mathews - Bell Telephone Laboratories  
John R. Meyer - President, National Bureau of Economic Research  
George A. Miller - Institute for Advanced Study (1972)  
William F. Miller - Vice-president and Provost, Stanford University (1971)  
N.M. Newmark - Department of Civil Engineering, University of Illinois (1969)  
Roy Nutt - Vice-president, Computer Sciences Corporation  
Robert J. O'Keefe - Senior Vice-president, Chase Manhattan Bank  
Kenneth Olsen - President, Digital Equipment Corporation (1971)  
Alan J. Perlis - Professor of Computer Science, Yale University (1971)  
John R. Pierce - Professor of Engineering, California Institute of Technology (1971)  
J. Barkley Rosser - Director, Mathematics Research Center, University of  
Wisconsin (1971)  
Alan F. Westin - Professor of Public Law and Government, Columbia University  
Ronald L. Wigington - Director of Research and Development, Chemical Abstracts  
Service

\* Date indicates end of term.

Alan F. Westin is Professor of Public Law and Government at Columbia University, and a member of the District of Columbia Bar. For the past two decades he has written about the law and politics of civil liberties and civil rights. His work has appeared in periodicals ranging from the Columbia Law Review and the Communications of the Association for Computing Machinery, to the New York Times Magazine and Playboy.

In 1968 he received three national awards for Privacy and Freedom, a comprehensive study of the social and political functions of privacy in a democratic society, and the dangers to these interests posed by technological advances in physical, psychological, and data surveillance. As an associate of the Harvard Program on Technology and Society, he has been conducting studies of the impact of information technology on government decision-making; in 1971, he published a collection of readings on this topic, Information Technology in a Democracy. He is also a member of the National Academy of Sciences' Computer Science and Engineering Board.

Professor Westin is Chairman of the American Civil Liberties Union's Privacy Committee, and a member of the ACLU National Board; has served as a consultant on privacy to the New York State Identification and Intelligence System, and appears frequently as an expert witness in federal congressional hearings on invasion of privacy and constitutional rights. Between 1969 and 1972 he served as Director of the National Academy of Science's Project on Computer Databanks.

Michael A. Baker is a member of the sociology faculty at Brooklyn College of the City University of New York and is currently completing work on his Ph.D. in sociology at Columbia University. Between 1970 and 1972 he served as Assistant Director of the Project on Computer Databanks.

He is among the authors of POLICE ON CAMPUS, a study of the 1968 mass police actions at Columbia University, published in 1969, and serves as a member of the American Civil Liberties Union's Privacy Committee. He has written on "Record Privacy as a Marginal Problem: the Limits of Consciousness and Concern" in the Winter 1972 Columbia Human Rights Law Review.

NATIONAL ACADEMY OF SCIENCES

2101 CONSTITUTION AVENUE

WASHINGTON, D. C., 20418

13 May 1970

ANTHONY G. OETTINGER, CHAIRMAN  
COMPUTER SCIENCE & ENGINEERING BOARD  
AIKEN COMPUTATION LABORATORY  
HARVARD UNIVERSITY  
CAMBRIDGE, MASSACHUSETTS 02138

*G. Oettinger*  
MAY 18 REC'D

Dear Warren,

Enclosed are the articles I promised you for distribution to  
the Board prior to the June meeting.

Sincerely yours,

*Anthony G. Oettinger*  
Anthony G. Oettinger

AGO:chm

encl.

# Hardware aspects of secure computing

by LEE M. MOLHO

*System Development Corporation  
Santa Monica, California*

## INTRODUCTION

It makes no sense to discuss software for privacy-preserving or secure time-shared computing without considering the hardware on which it is to run. Software access controls rely upon certain pieces of hardware. If these can go dead or be deliberately disabled without warning, then all that remains is false security.

This paper is about hardware aspects of controlled-access time-shared computing.\* A detailed study was recently made of two pieces of hardware that are required for secure time-sharing on an IBM System 360 Model 50 computer: the storage protection system and the Problem/Supervisor state control system.<sup>1</sup> It uncovered over a hundred cases where a single hardware failure will compromise security without giving an alarm. Hazards of this kind, which are present in any computer hardware which supports software access controls, have been essentially eliminated in the SDC ADEPT-50 Time-Sharing System through techniques described herein.<sup>2</sup>

Analysis based on that work has clarified what avenues are available for subversion via hardware; they are outlined in this paper. A number of ways to fill these security gaps are then developed, including methods applicable to a variety of computers. Administrative policy considerations, problems in security certification of hardware, and hardware design considerations for secure time-shared computing also receive comment.

## FAILURE, SUBVERSION, AND SECURITY

Two types of security problem can be found in computer hardware. One is the problem of hardware failure.

\*The relationship between "security" and "privacy" has been discussed elsewhere.<sup>3,4</sup> In this paper "security" is used to cover controlled-access computing in general.

This includes not only computer logic that fails by itself, but also miswiring and faulty hardware caused by improper maintenance ("Customer Engineer") activity, including CE errors in making field-installable engineering changes.

The other security problem is the cloak-and-dagger question of the susceptibility of hardware to subversion by unauthorized persons. Can trivial hardware changes jeopardize a secure computing facility even if the software remains completely pure? This problem and the hardware failure problem, which will be considered in depth, are related.

### *Weak points for logic failure*

Previous work involved an investigation of portions of the 360/50 hardware.<sup>1</sup> Its primary objective was to pinpoint single-failure problem locations. The question was asked, "If this element fails, will hardware required for secure computing go dead without giving an alarm?" A total of 99 single-failure hazards were found in the 360/50 storage protection hardware; they produce a variety of system effects. Three such logic elements were found in the simpler Problem/Supervisor state (PSW bit 15) logic. A failure in this logic would cause the 360/50 to always operate in the Supervisor state.

An assumption was made in finding single-failure logic problems which at first may seem more restrictive than it really is: A failure is defined as having occurred if the output of a logic element remains in an invalid state based on the states of its inputs. Other failure modes certainly exist for logic elements, but they reduce to this case as follows: (1) an intermittent logic element meets this criterion, but only part of the time; (2) a shorted or open input will cause an invalid output state at least part of the time; (3) a logic element which exhibits excessive signal delay will appear to have an invalid output state for some time after any input transition; (4) an output wire which has been con-



nected to an improper location will have an invalid output state based on its inputs at least part of the time; such a connection may also have permanently damaged the element, making its output independent of its input. It should be noted that failure possibilities were counted; for those relatively few cases where a security problem is caused whether the element gets stuck in "high" or in "low" state, two possibilities were counted.

A situation was frequently encountered which is considered in a general way in the following section, but which is touched upon here. Many more logic elements besides those failed would cause the storage protection hardware to go dead if they failed, but fortunately (from a security viewpoint) their failure would cause some other essential part of the 360/50 to fail, leading to an overall system crash. "Failure detection by faulty system operation" keeps many logic elements from becoming security problems.

#### *Circumventing logic failure*

Providing redundant logic is a reasonable first suggestion as a means of eliminating single failures as security problems. However, redundancy has some limits which are not apparent until a close look is taken at the areas of security concern within the Central Processing Unit (CPU). Security problems are really in control logic, such as the logic activated by a storage protect violation signal, rather than in multi-bit data paths, where redundancy in the form of error-detecting and error-correcting codes is often useful. Indeed, the 360/50 CPU already uses an error-detecting code extensively, since parity checks are made on many multi-bit paths within it.

Effective use of redundant logic presents another problem. One must fully understand the system as it stands to know what needs to be added. Putting it another way, full hardware certification must take place before redundancy can be added (or appreciated, if the manufacturer claims it is there to begin with).

Lastly, some areas of hardware do not lend themselves too easily to redundancy: There can be only one address at a time to the Read-Only-Storage (ROS) unit whose microprograms control the 360/50 CPU.<sup>5,6</sup> One could, of course, use such a scheme as triple-modular redundancy on all control paths, providing three copies of ROS in the bargain. The result of such an approach would not be much like a 360/50.

Redundancy has a specialized, supplementary application in conjunction with hardware certification. After the process of certification reveals which logic elements can be checked by software at low overhead, redundant

logic may be added to take care of the remainder. A good example is found in the storage protection logic. Eleven failure possibilities exist where protection interrupts would cause an incorrect microprogram branch upon failure. These failure possibilities arise in part from the logic elements driven by one control signal line. This signal could be provided redundantly to make the hardware secure.

Software tests provide another way to eliminate hardware failure as a security problem. Code can be written which should cause a protection or privileged-operation interrupt; to pass the test the interrupt must react appropriately. Such software must interface the operating system software for scheduling and storage-protect lock alteration, but must execute in Problem state to perform its tests. There is clearly a tradeoff between system overhead and rate of testing. As previously mentioned, hardware certification must be performed to ascertain what hardware can be checked by software tests, and how to check it.

Software testing of critical hardware is a simple and reasonable approach, given hardware certification; it is closely related to a larger problem, that of testing for software holes with software. Software testing of hardware, added to the SDC ADEPT-50 Time-Sharing System, has eliminated over 85 percent of present single-failure hazards in the 360/50 CPU.

Microprogramming could also be put to work to combat failure problems. A microprogrammed routine could be included in ROS which would automatically test critical hardware, taking immediate action if the test were not passed. Such a microprogram could either be in the form of an executable instruction (e.g., TEST PROTECTION), or could be automatic, as part of the timer-update sequence, for example.

A microprogrammed test would have much lower overhead than an equivalent software test performed at the same rate; if automatic, it would test even in the middle of user-program execution. A preliminary design of a storage-protection test that would be exercised every timer update time (60 times per second) indicated an overhead of only 0.015 percent (150 test cycles for every million ROS cycles). Of even greater significance is that microprogrammed testing is specifiable. A hardware vendor can be given the burden of proof of showing that the tests are complete; the vendor would have to take the testing requirement into account in design. The process of hardware certification could be reduced to a design review of vendor tests if this approach were taken.

Retrofitting microprogrammed testing in a 360/50 would not involve extensive hardware changes, but some changes would have to be made. Testing microprograms would have to be written by the manu-

facturer; new ROS storage elements would have to be fabricated. A small amount of logic and a large amount of documentation would also have to be changed.

Logic failure can be totally eliminated as a security problem in computer hardware by these methods. A finite effort and minor overhead are required; what logic is secured depends upon the approach taken. If microprogram or software functional testing is used, miswiring and dead hardware caused by CE errors will also be discovered.

### *Subversion techniques*

It is worthwhile to take the position of a would-be system subverter, and proceed to look at the easiest and best ways of using the 360/50 to steal files from unsuspecting users. What hardware changes would have to be made to gain access to protected core memory or to enter the Supervisor state?

Fixed changes to eliminate hardware features are obvious enough; just remove the wire that carries the signal to set PSW bit 15, for example. But such changes are physically identical to hardware failures, since something is permanently wrong. As any functional testing for dead hardware will discover a fixed change, a potential subverter must be more clever.

In ADEPT-50, a user is swapped in periodically for a brief length of time (a "quantum"). During his quantum, a user can have access to the 360/50 at the machine-language level; no interpretive program comes between the user and his program unless, of course, he requests it. Thus, a clever subverter might seek to add some hardware logic to the CPU which would look for, say, a particular rather unusual sequence of two instructions in a program. Should that sequence appear, the added logic might disable storage protection for just a few dozen microseconds. Such a small "hole" in the hardware would be quite sufficient for the user to (1) access anyone's file; (2) cause a system crash; (3) modify anyone's file.

User-controllable changes could be implemented in many ways, with many modes of control and action besides this example (which was, however, one of the more effective schemes contemplated). Countermeasures to such controllable changes will be considered below, along with ways in which a subverter might try to anticipate countermeasures.

### *Countermeasures to subversion*

As implied earlier, anyone who has sufficient access to the CPU to install his own "design changes" in the hardware is likely to put in a controllable change, since

a fixed change would be discovered by even a simple software test infrequently performed. A user-controllable change, on the other hand would not be discovered by tests outside the user's quantum, and would be hard to discover even within it, as will become obvious.

The automatic microprogrammed test previously discussed would have a low probability of discovering a user-controllable hardware change. Consider an attempt by a user to replace his log-in number with the log-in number of the person whose file he wants to steal. He must execute a MOVE CHARACTERS instruction of length 12 to do this, requiring only about 31 microseconds for the 360/50 CPU to perform. A microprogrammed test occurring at timer interrupts—once each 16 milliseconds—would have a low probability of discovering such a brief security breach. Increasing the test rate, though it raises the probability, raises the overhead correspondingly. A test occurring at 16 microsecond intervals, for example, represents a 15 percent overhead.

A reasonable question is whether a software test might do a better job of spotting user-controllable hardware changes. One would approach this task by attempting to discover changes with tests inserted in user programs in an undetectable fashion. One typical method would do this by inserting invisible breakpoints into the user's instruction stream; when they were encountered during the user's quantum, a software test of storage protection and PSW bit 15 would be performed.

A software test of this type could be written, and as will be discussed, such a software test would be difficult for a subverter to circumvent. Nevertheless, the drawbacks of this software test are severe. Reentrant code is required so that the software test can know (1) the location of the instruction stream, and (2) that no instructions are hidden in data areas. Requiring reentrant programs would in turn require minor changes to the ADEPT-50 Jovial compiler and major changes to the F-level Assembler. A small microprogram change would even be required, so that software could sense the difference between a fetch-protect interrupt and an execute-protect interrupt. Changes would be required to the ADEPT-50 SERVIS, INTRUP, DEBUG, and SKED modules. Were such a software test implemented, run-time overhead would likely be rather high for frequent breakpoint-insertions, since each breakpoint inserted would require execution of 50 or more instructions at run time. Lastly, programmers might not always like having to write reentrant code.

These implementation problems, though described for one specific test approach, are likely to extend to any test which attempts to interrupt running user pro-

grams via software, since any such test must isolate and augment every user's instruction stream.

Although the above does not demonstrate that detecting user controllable subversion hardware is impossible, it should indicate that by no means is such detection trivial. It is even harder than the above may suggest, for, as the next section indicates, while the subverter is busily building his controllable changes into the CPU he may add insult to injury by inactivating anti-failure and anti-subversion hardware.

#### *Defeat of countermeasures*

Hardware countermeasures that are easy to install are easy to remove. Redundant logic can be disabled with the same wire cutters or wire-unwrapper as other logic. This is also true of state-testing and parity-check logic. Alternatively, a clever subverter may add logic that picks up a test signal and uses it to inactivate his own logic while the test is performed. The subverter may, alternatively, arrange things so that tests always pass during his quantum.

Microprogrammed countermeasures are somewhat more difficult for the subverter to inactivate, since he must decode particular ROS addresses to know that a microprogrammed test routine has begun. Once he has done this, though, he may proceed as if he were dealing with hardware, since on a short-term basis, microprogram contents and addresses do not change. The net result of putting countermeasures in ROS rather than in logic is to raise the "work function" for subversion; that is, the subverter must do more work to achieve his goal, but he can reach it.

On the other hand, a thorough software test, such as the breakpoint test previously described, would be nearly impossible to defeat by hardware techniques. This is because of the transient nature of software: a subverter would have to decode program variables such as addresses via hardware; then even minor changes in the breakpoint-placing routines would make that hardware useless. One must recall, however, the large implementation and overhead problems inherent in a user-interrupting software test. In summary, countermeasures can be devised which have a high "work function," but they entail major costs in implementation and system efficiency.

Two assumptions have been inherent in this discussion; namely, that the subverter has both knowledge of system hardware (including subversion countermeasures) and means of changing the hardware. This need not be the case, but whether it is depends on administrative rather than technical considerations. Administrative considerations are the next subject.

#### *Administrative policy*

Special handling of hardware documentation and engineering changes may be worthwhile when commercial lines of computers are used for secure time-sharing. First, if hardware or microprograms have been added to the computer to test for failures and subversion attempts, the details of the tests should not be obtainable from the computer manufacturer's worldwide network of sales representatives. The fact that testing is done and the technical details of that testing would seem to be legitimate security objects, since a subverter can neutralize testing only if he knows of it. Classification of those documents which relate to testing is a policy question which should be considered. Likewise, redundant hardware, such as a second copy of the PSW bit 15 logic, might be included in the same category.

The second area is that of change control. Presumably the "Customer Engineer" (CE) personnel who perform engineering changes have clearances allowing them access to the hardware, but what about the technical documents which tell them what to do? A clever subverter could easily alter an engineering-change wire list to include his modifications, or could send spurious change documentation. A CE would then unwittingly install the subverter's "engineering change." Since it is asking too much to expect a CE to understand on a wire-by-wire basis each change he performs, some new step is necessary if one wants to be sure that engineering changes are made for technical reasons only. In other words, the computer manufacturer's engineering changes are security objects in the sense that their integrity must be guaranteed. Special paths of transmittal and post-installation verification by the manufacturer might be an adequate way to secure engineering changes; there are undoubtedly other ways. It is clear that a problem exists.

Finally, it should be noted that the 360/50 ROS storage elements, or any equivalent parts of another manufacturer's hardware that contain all system microprogramming, ought to be treated in a special manner, such as physically sealing them in place as part of hardware certification. New storage elements containing engineering changes are security objects of even higher order than regular engineering-change documents, and should be handled accordingly, from their manufacture through their installation.

#### GENERALIZATIONS AND CONCLUSIONS

Some general points about hardware design that relate to secure time-sharing and some short-range and long-range conclusions are the topics of this section.

*Fail-secure vs. fail-soft hardware*

Television programs, novels, and motion pictures have made it well known that if something is "fail-safe," it doesn't blow up when it fails. In the same vein, designers of high-reliability computers coined the term "fail-soft" to describe a machine that degrades its performance when a failure occurs, instead of becoming completely useless. It is now proposed to add another term to this family: "Fail-secure: to protect secure information regardless of failure."

The ability to detect failures is a prerequisite for fail-secure operation. However, all system provisions for corrective action based on failure detection must be carefully designed, particularly when hardware failure correction is involved. Two cases were recently described wherein a conflict arose between hardware and software that had been included to circumvent failures.\* Automatic correction hardware could likewise mask problems which should be brought to the attention of the System Security Officer via security software.

Clearly, something between the extremes of system crash and silent automatic correction should occur when hardware fails. Definition of what *does* happen upon failure of critical hardware should be a design requirement for fail-secure time-sharing systems. Fail-soft computers are not likely to be fail-secure computers, nor vice versa, unless software and hardware have been designed with both concepts in mind.

*Failure detection by faulty system operation*

Computer hardware logic can be grouped by the system operation or operations it helps perform. Some logic—for example, the clock distribution logic—helps perform only one system operation. Other logic—such as the read-only storage address logic in the 360/50—helps perform many system operations, from floating point multiplication to memory protection interrupt handling. When logic is needed by more than one system operation, it is cross-checked for proper performance: Should an element needed for system operations A and

\*At the "Workshop on Hardware-Software Interaction for System Reliability and Recovery in Fault-Tolerant Computers," held July 14-15, 1969 at Pacific Palisades, California, J. W. Herndon of Bell Telephone Labs reported that a problem had arisen in a developmental version of Bell's "Electronic Switching System." It seems that an elaborate setup of relays would begin reconfiguring a bad communications channel at the same time that software in ESS was trying to find out what was wrong. R. F. Thomas, Jr. of the Los Alamos Scientific Laboratory, having had a similar problem with a self-checking data acquisition system, agreed with Herndon that hardware is not clever enough to know what to do about system failures; software failure correction approaches are preferable.

B fail, the failure of system operation B would indicate the malfunction of this portion of operation A's logic.

Such interdependence is quite useful in a fail-secure system, as it allows failures to be detected by faulty system operation—a seemingly inelegant error detection mechanism, yet one which requires neither software nor hardware overhead. Some ideas on its uses and limitations follow.

The result of a hardware logic failure can usually be defined in terms of what happens to the system operations associated with the dead hardware. Some logic failure modes are detectable, because they make logic elements downstream misperform unrelated system operations. Analysis will also reveal failure modes which spoil only the system operation which they help perform. These failures must be detected in some other way. There are also, but more rarely, cases where a hardware failure may lead to an operation failure that is not obvious. In the 360/50, a failure could cause skipping of a segment of a control microprogram that wasn't really needed on that cycle. Such failures are not detectable by faulty system operation at least part of the time.

Advantage may be taken of this failure-detection technique in certifying hardware to be fail-secure as well as in original hardware design. In general, the more interdependencies existing among chunks of logic, the more likely are failures to produce faulty system operation. For example, in many places in a computer one finds situations as sketched in Figure 1. Therein,

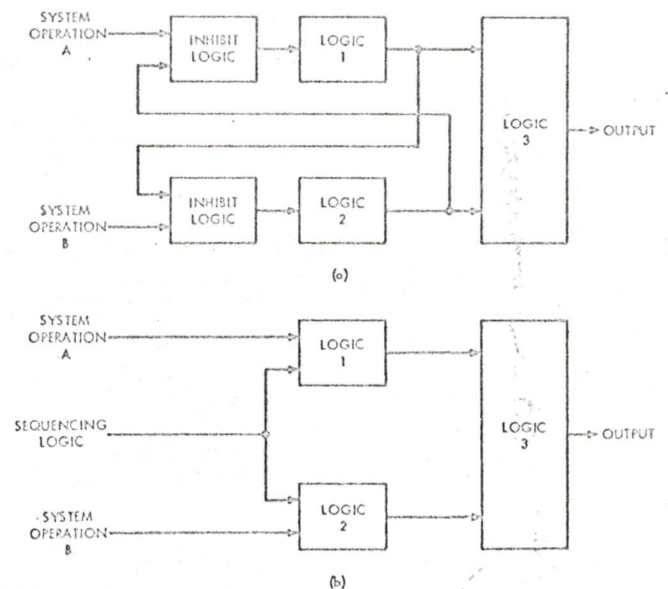


Figure 1—Inhibit logic vs sequencing logic

TABLE 1—Control Signal Error Detection by Odd Parity Check on Odd-Length Data Field

DATA BITS		MEANING
012 P		
000 0		data error or control logic error*
000 1		0
001 0		1
001 1		data error
010 0		2
010 1		data error
011 0		data error
011 1		3
100 0		4
100 1		data error
101 0		data error
101 1		5
110 0		data error
110 1		6
111 0		7
111 1		data error or control logic error**

\*Control logic incorrectly set all bits to zero.

\*\*Control logic incorrectly set all bits to one.

System Operation A needs the services of Logic Group 1 and Logic Group 3, while System Operation B needs Logic Group 2 and Logic Group 3. Note at this point that, as above, if System Operation A doesn't work because of a failure in Logic Group 3, we have concurrently detected a failure in the logic supporting System Operation B.

A further point is made in Figure 1. Often System Operations A and B must be mutually exclusive; hardware must be added to prevent simultaneous activation of A and B. Two basic design approaches may be taken to solve this problem. An "inhibiting" scheme may be used, wherein logic is added that inhibits Logic Group 1 when Logic Group 2 is active, and vice versa. This approach is illustrated by Figure 1(a). Alternatively, a "sequencing" scheme may be used, wherein logic not directly involved with 1 or 2—such as system clock, mode selection logic, or a status register—defines when A and B are to be active. This approach is illustrated by Figure 1(b).

Now, "inhibit" logic belongs to a particular System Operation, for its function is to asynchronously, on demand, condition the hardware to perform that System Operation. It depends on nothing else; if it fails by going permanently inactive, only its System Operation is affected, and no alarm is given. On the other hand, "sequencing" logic feeds many areas of the machine; its failure is highly likely to be detected by faulty system operation.

A further point can be made here which may be somewhat controversial: that an overabundance of "inhibit"-type asynchronous logic is a good indicator of sloppy design or bad design coordination. While a certain amount must exist to deal with asynchronous pieces of hardware, often it is put in to "patch" problems that no one realized were there till system checkout time. Evidence of such design may suggest more thorough scrutiny is desirable.

System Operations can be grouped by their frequency of occurrence: some operations are needed every CPU cycle, some when the programmer requests them, some only during maintenance, and so on. Thus, some logic which appears to provide a cross-check on other logic may not do so frequently or predictably enough to satisfy certification requirements.

To sum up, the fact that a system crashes when a hardware failure occurs, rather than "failing soft" by continuing to run without the dead hardware, may be a blessing in disguise. If fail-soft operation encompasses hardware that is needed for continued security, such as the memory protection hardware, fail-soft operation is not fail-secure.

#### Data checking and control signal errors

Control signals which direct data transfers will often be checked by logic that was put in only to verify data purity. The nature and extent of this checking is dependent on the error-detection code used and upon the length of the data field (excluding check bits).

What happens is that if logic fails which controls a data path and its check bits, the data will be forced to either all zeros or all ones. If one or both of these cases is illegal, the control logic error will be detected when the data is checked. (Extensive parity checking on the 360/50 CPU results in much control logic failure detection capability therein.) Table 1 demonstrates an example of this effect; Table 2 describes the conditions for which it exists for the common parity check.

TABLE 2—Control Signal Error Detection by Parity Checking

DATA FIELD LENGTH:	PARITY:	CONTROL LOGIC ERROR CAUSES:	
		all zeros	all ones
even	odd	CAUGHT	MISSED
even	even	MISSED	CAUGHT
odd	odd	CAUGHT	CAUGHT
odd	even	MISSED	MISSED

## CONCLUSIONS

From a short-range viewpoint, 360/50 CPU hardware has some weak spots in it but no holes, as far as secure time-sharing is concerned. Furthermore, the weak spots can be reinforced with little expense. Several alternatives in this regard have been described.

From a longer-range viewpoint, anyone who contemplates specifying a requirement for hardware certification should know what such an effort involves. As reference, some notes are appropriate as to what it took to examine the 360/50 memory protection system to the level required for meaningful hardware certification. The writer first obtained several publications which describe the system. Having read these, the writer obtained the logic diagrams, went to the beginning points of several operations, and traced logic forward. Signals entering a point were traced backward until logic was found which would definitely cause faulty machine operation outside the protection system if it failed. During this tedious process, discrepancies arose between what had been read and what the logic diagrams appeared to show. Some discrepancies were resolved by further study; some were accounted for by special features on the SDC 360/50; some remain.

After logic tracing, the entire protection system was sketched out on eight  $8\frac{1}{2} \times 11$  pages. This drawing proved to be extremely valuable for improving the writer's understanding, and enabled failure-mode charting that would have been intractable by manual means from the manufacturer's logic diagrams.

For certifying hardware, documentation quality and currentness is certainly a problem. The manufacturer's publications alone are necessary but definitely not sufficient, because of version differences, errors, oversimplifications, and insufficient detail. Both these and machine logic diagrams are needed.

Though the hardware certification outlook is bleak, an alternative does exist: testing. As previously described, it is possible to require inclusion of low-overhead functional testing of critical hardware in a secure

computing system. The testing techniques, whether embedded in hardware, microprograms, or software, could be put under security control if some protection against hardware subversion is desired. Furthermore, administrative security control procedures should extend to "Customer Engineer" activity and to engineering change documentation to the extent necessary to insure that hardware changes are made for technical reasons only.

Careful control of access to computer-based information is, and ought to be, of general concern today. Access controls in a secure time-sharing system such as ADEPT-50 are based on hardware features.<sup>7</sup> The latter deserve scrutiny.

## REFERENCES

- 1 L MOLHO  
*Hardware reliability study*  
SDC N-(L)-24276/126/00 December 1969
- 2 R LINDE C WEISSMAN C FOX  
*The ADEPT-50 time-sharing system*  
Proceedings of the Fall Joint Computer Conference Vol 35  
p 39-50 1969  
Also issued as SDC document SP-3344
- 3 W H WARE  
*Security and privacy in computer systems*  
Proceedings of the Spring Joint Computer Conference  
Vol 30 p 279-282 1967
- 4 W H WARE  
*Security and privacy: Similarities and differences*  
Proceedings of the Spring Joint Computer Conference  
Vol 30 p 287-290 1967
- 5 S G TUCKER  
*Microprogram control for system/360*  
IBM Systems Journal Vol 6 No 4 p 222-241 1967
- 6 G C VANDLING D E WALDECKER  
*The microprogram control technique for digital logic design*  
Computer Design Vol 8 No 8 p 44-51 August 1969
- 7 C WEISSMAN  
*Security controls in the ADEPT-50 time-sharing system*  
Proceedings of the Fall Joint Computer Conference Vol 35  
p 119-133 1969  
Also issued as SDC document SP-3342

## Security and privacy: similarities and differences

by WILLIS H. WARE  
*The RAND Corporation*  
Santa Monica, California

For the purposes of this paper we will use the term "security" when speaking about computer systems which handle classified defense information, and "privacy" in regard to those computer systems which handle non-defense information which nonetheless must be protected because it is in some respect sensitive. It should be noted at the outset that the context in which security must be considered is quite different from that which can be applied to the privacy question. With respect to classified military information there are federal regulations which establish authority, and discipline to govern the conduct of people who work with such information. Moreover, there is an established set of categories into which information is classified. Once information is classified Confidential, Secret, or Top Secret, there are well-defined requirements for its protection, for controlling access to it, and for transmitting it from place to place. In the privacy situation, analogous conditions may exist only in part or not at all.

There are indeed Federal and State statutes which protect the so-called "secrecy of communication." But it remains to be established that these laws can be extended to cover or interpreted as applicable to the unauthorized acquisition of information from computer equipment. There are also laws against thievery; and at least one case involving a programmer and theft of privileged information has been tried. The telephone companies have formulated regulations governing the conduct of employees (who are subject to "secrecy of communication" laws) who may intrude on the privacy of individuals; perhaps this experience can be drawn upon by the computer field.

Though there apparently exist fragments of law and some precedents bearing on the protection of information, nonetheless the privacy situation is not so neatly circumscribed and tidy as the security situation. Privacy simply is not so tightly controlled. Within computer networks serving many companies, organi-

zations, or agencies, there may be no uniform governing authority; an incomplete legal framework; no established discipline, or perhaps not even a code of ethics among users. At present there is not even a commonly accepted set of categories to describe levels of sensitivity for private information.

Great quantities of private information are being accumulated in computer files; and the incentives to penetrate the safeguards to privacy are bound to increase. Existing laws may prove inadequate, or may need more vigorous enforcement. There may be need for a monitoring and enforcement establishment analogous to that in the security situation. In any event, it can not be taken for granted that there now exist adequate legal and ethical umbrellas for the protection of private information.

The privacy problem is really a spectrum of problems. At one end, it may be necessary to provide only a very low level of protection to the information for only a very short time; at the opposite end, it may be necessary to invoke the most sophisticated techniques to guarantee protection of information for extended periods of time. Federal regulations state explicitly what aspect of national defense will be compromised by unauthorized divulgence of each category of classified information. There is no corresponding particularization of the privacy situation; the potential damage from revealing private information is nowhere described in such absolute terms. It may be that a small volume of information leaked from a private file may involve inconsequential risk. For example, the individual names of a company's employees is probably not even sensitive, whereas the complete file of employees could well be restricted. Certainly the "big brother" spectre raised by recent Congressional hearings on "invasion of privacy" via massive computer files is strongly related to the volume of information at risk.

Because of the diverse spread in the privacy situation, the appearance of the problem may be quite different from its reality. One would argue on principle that maximum protection should be given to all information labeled private; but if privacy of information is not protected by law and authority, we can expect that the owner of sensitive information will require a system designed to guarantee protection only against the threat as he sees it. Thus, while we might imagine very sophisticated attacks against private files, the reality of the situation may be that much simpler levels of protection will be accepted by the owners of the information.

In the end, an engineering trade-off question must be assessed. The value of private information to an outsider will determine the resources he is willing to expend to acquire it. In turn, the value of the information to its owner is related to what he is willing to pay to protect it: Perhaps this game-like situation can be played out to arrive at a rational basis for establishing the level of protection. Perhaps a company or governmental agency—or a group of companies or agencies, or the operating agent of a multi-access computer service—will have to establish its own set of regulations for handling private information. Further, a company or agency may have to establish penalties for infractions of these regulations, and perhaps even provide extra remuneration for those assuming the extraordinary responsibility of protecting private information.

The security measures deemed necessary for a multi-processing remote terminal computer system operating in a military classified environment have been discussed in the volume.\* This paper will compare the security situation with the privacy situation, and suggest issues to be considered when designing a computer system for guarding private information. Technology which can be applied against the design problem is described elsewhere.†

First of all, note that the privacy problem is to some extent present whenever and wherever sharing of the structures of a computer system takes place. A time-sharing system slices time in such a way that each user gets a small amount of attention on some periodic basis. More than one user program is resident in the central storage at one time; and hence, there are obvious opportunities for leakage of information from one program to another, although the problem is alleviated to some extent in systems operating in an interpretive software mode. In a multi-programmed

computer system it is also true that more than one user program is normally resident in the core store at a time. Usually, a given program is not executed without interruption; it must share the central storage and perhaps other levels of storage with other programs. Even in the traditional batch-operated system there can be a privacy problem. Although only one program is usually resident in storage at a time, parts of other programs reside on magnetic tape or discs; in principle, the currently executing program might accidentally reference others, or cause parts of previous programs contained on partially re-used magnetic tape to be outputted.

Thus, unless a computer system is completely stripped of other programs—and this means clearing or removing access to all levels of storage—privacy infractions are possible and might permit divulgence of information from one program to another.

Let us now reconsider the points raised in the Peters\* paper and extend the discussion to include the privacy situation.

(1) The problem of controlling user access to the resource-sharing computer system is similar in both the security and privacy situations. It has been suggested that one-time passwords are necessary to satisfactorily identify and authenticate the user in the security situation. In some university time-sharing systems, permanently assigned passwords are considered acceptable for user identification. Even though printing of a password at the console can be suppressed, it is easy to ascertain such a password by covert means; hence, repeatedly used passwords may prove unwise for the privacy situation.

(2) The incentive to penetrate the system is present in both the security and privacy circumstances. Revelation of military information can degrade the country's defense capabilities. Likewise, divulgence of sensitive information can to some extent damage other parties or organizations. Private information will always have some value to an outside party, and it must be expected that penetrations will be attempted against computer systems handling such information. It is conceivable that the legal liability for unauthorized leaking of sensitive information may become as severe as for divulging classified material.

(3) The computer hardware requirements appear to be the same for the privacy and security situations. Such features as memory read-write protection, bounds registers, privileged instructions, and a privileged mode of operation are required to protect

\*Peters, B., "Security Considerations in a Multi-Programmed System".

†Petersen, H. E., and R. Turn, Systems Implications of Privacy."

\*Peters, B., *loc cit.*



information, be it classified or sensitive. Also, overall software requirements seem similar, although certain details may differ in the privacy situation because of communication matters or difference in user discipline.

(4) The file access and protection problem is similar under both circumstances. Not all users of a shared computer-private system will be authorized access to all files in the system, just as not all users of a secure computer system will be authorized access to all files. Hence, there must be some combination of hardware and software features which controls access to the on-line classified files in conformance with security levels and need-to-know restrictions and in conformance with corresponding attributes in the privacy situation. As mentioned earlier, there may be a minor difference relative to volume. In classified files, denial of access must be absolute, whereas in private files access to a small quantity of sensitive information might be an acceptable risk.

(5) The philosophy of the overall system organization will probably have to be different in the privacy situation. In the classified defense environment, users are indoctrinated in security measures and their personal responsibility can be considered as part of the system design. Just as the individual who finds a classified document in a hallway is expected to return it, so the man who accidentally receives classified information at his console is expected to report it. The users in a classified system are subject to the regulations, authority, and discipline of a governmental agency. Similar restrictions may not prevail in a commercial or industrial resource-sharing computer network, nor in government agencies that do not operate within the framework of government classification. In general, it would appear that one cannot exploit the good will of users as part of a privacy system's design. On the other hand, the co-operation of users may be part of the design philosophy if it proves possible to impose a uniform code of ethics, authority, and discipline within a multi-access system. Uniform rules of behavior might be possible if all users are members of the same organization, but quite difficult or impossible if the users are from many companies or agencies.

(6) The certifying authority is certainly different in the two situations. It is easy to demonstrate that the total number of internal states of a computer is so enormous that some of them will never prevail in the lifetime of the machine. It is equally easy to demonstrate that large computer programs have a large number of internal paths, which implies the potential existence of error conditions which may appear rarely or even only once. Monitor programs

governing the internal scheduling and operation of multi-programmed, time-sharing or batch-operated machines are likely to be extensive and complex; and if security or privacy is to be guaranteed, some authority must certify that the monitor is properly programmed and checked out. Similarly, the hardware must also be certified to possess appropriate protective devices.

In a security situation, a security officer is responsible for establishing and implementing measures for the control of classified information. Granted that he may have to take the word of computer experts or become a computer expert himself, and granted that of itself his presence does not solve the computer security problem, there is nonetheless at least an assigned, identifiable responsible authority. In the case of the commercial or industrial system, who is the authority? Must the businessman take the word of the computer manufacturer who supplied the software? If so, how does he assure himself that the manufacturer hasn't provided "ins" to the system that only he, the manufacturer, knows about? Must the businessman create his own analog of defense security practices?

(7) Privacy and security situations are certainly similar in that deliberate penetrations must be anticipated, if not expected; but industrial espionage against computers may be less serious. On the other hand, industrial penetrations against computers could be very profitable and perhaps safer from a legal viewpoint.

It would probably be difficult for a potential penetrator to mount the magnitude of effort against an industrial resource-sharing computer system that foreign agents are presumed to mount against secrecy systems of other governments. To protect against large-scale efforts, an industry-established agency could keep track of major computing installations and know where penetration efforts requiring heavy computer support might originate. On the other hand, the resourceful and insightful individual can be as great a threat to the privacy of a system. If one can estimate the nature and extent of the penetration effort expected against an industrial system, perhaps it can be used as a design parameter to establish the level of protection for sensitive information.

(8) The security and privacy situations are certainly similar in that each demands secure communication circuits. For the most part, methods for assuring the security of communication channels have been the exclusive domain of the military and government. What about the non-government user? Could the specifications levied on common carriers in their

implied warranty of a private circuit be extended? Does the problem become one for the common carriers? Must they develop communication security equipment? If the problem is left to the users, does each do as he pleases? Might it be feasible to use the central computer itself to encode information prior to transmission? If so, the console will require special equipment for decoding the messages.

(9) Levels of protection for communications are possibly different in the two situations. If one believes that a massive effort at penetration could not be mounted against a commercial private network, a relatively low-quality protection for communication would be sufficient. On the other hand, computer networks will inevitably go international. Then what? A foreign industry might find it advantageous to tap the traffic of U.S. companies operating an international and presumably private computer network. Might it be that for reasons of national interest we will someday find the professional cryptoanalytic effort of a foreign government focused on the privacy-protecting measures of a computer network?

If control of international trade were to become an important instrument of government policy, then any international communications network involved with industrial or commercial computer-private systems will need the best protection that can be provided.

This paper has attempted to identify and briefly discuss the differences and similarities between computer systems operating with classified military information and computer systems handling private or sensitive information. Similar hardware and software and systems precautions must be taken. In most respects, the differences between the two situations are only of degree. However, there are a few aspects in which the two situations genuinely differ in kind, and on these points designers of a system must take special note. The essential differences between the two situations appear to be the following:

(1) Legal foundations for protecting classified information are well established, whereas in

the privacy situation a uniform authority over users and a penalty structure for infractions are lacking. We may not be able to count on the good will and disciplined behavior of users as part of the protective measures.

- (2) While penetrations can be expected against both classified and sensitive information, the worth of the material at risk in the two situations can be quite different, not only to the owner of the data but also to other parties and to society.
- (3) The magnitude of the resources available for protection and for penetration are markedly smaller in the privacy situation.
- (4) While secure communications are required in both situations, there are significant differences in details. In the defense environment, protected communications are the responsibility of a government agency, appropriate equipment is available, and the importance of protection over-rides economic considerations. In the privacy circumstance, secure satisfactory communication equipment is generally not available, and the economics of protecting communications is likely to be more carefully assessed.
- (5) Some software details have to be handled differently in the privacy situation to accommodate differences in the security of communications.

It must be remembered that since the Federal authority and regulations for handling classified military information do not function for private or sensitive information, it does not automatically follow that a computer network designed to safely protect classified information will equally well protect sensitive information. The all important difference is that the users of a computer-private network may not be subject to a common authority and discipline. But even if they are, the strength of the authority may not be adequate to deter deliberate attempts at penetration.

*Chairman's Introduction to the SJCC Session*

## Security and privacy in computer systems

by WILLIS H. WARE  
The RAND Corporation  
Santa Monica, California

### INTRODUCTION

*Information leakage in a resource-sharing  
computer system*

With the advent of computer systems which share the resources of the configuration among several users or several problems, there is the risk that information from one user (or computer program) will be coupled to another user (or program). In many cases, the information in question will bear a military classification or be sensitive for some reason, and safeguards must be provided to guard against the leakage of information. This session is concerned with accidents or deliberate attempts which divulge computer-resident information to unauthorized parties.

Espionage attempts to obtain military or defense information regularly appear in the news. Computer systems are now widely used in military and defense installations, and deliberate attempts to penetrate such computer systems must be anticipated. There can be no doubt that safeguards must be conceived which will protect the information in such computer systems. There is a corresponding situation in the industrial world. Much business information is company-confidential because it relates to proprietary processes or technology, or to the success, failure, or state-of-health of the company. One can imagine a circumstance in which it would be profitable for one company to mount an industrial espionage attack against the computer system of a competitor. Similarly, one can imagine scenarios in which confidential information on individuals which is kept within a computer is potentially profitable to a party not authorized to have the information. Hence, we can expect that penetrations will be attempted against computer systems which contain non-military information.

This session will not debate the existence of es-

spionage attempts against resource-sharing systems. Rather, it is assumed that the problem exists, at least in principle if not in fact, and our papers will be devoted to discussing technological aspects of the problem and possible approaches to safeguards.

First of all, clarification of terminology is in order. For the military or defense situation, the jargon is well established. We speak of "classified information," "military security," and "secure computer installations." There are rules and regulations governing the use and divulgence of military-classified information, and we need not dwell further on the issue. In the non-military area, terminology is not established. The phrase "industrial security" includes such things as protecting proprietary designs and business information; but it also covers the physical protection of plants and facilities. For our purposes, the term is too broad. In most circles, the problem which will concern us is being called the "privacy problem."

The words "private" and "privacy" are normally associated with an individual in a personal sense, but *Webster's Third New International Dictionary* also provides the following definitions:

Private: . . . intended for or restricted to the use of a particular person, or group, or class of persons; not freely available to the public

Privacy: . . . isolation, seclusion, or freedom from unauthorized oversight or observation.

We are talking about restricting information within a computer for the use of a specified group of persons; we do not want the information freely available to the public. We want to isolate the information from unauthorized observation. Hence, the terminology appears appropriate enough, although one might hope that new terms will be found that do not already have strongly established connotations. For our purposes today, "security" and "classified"

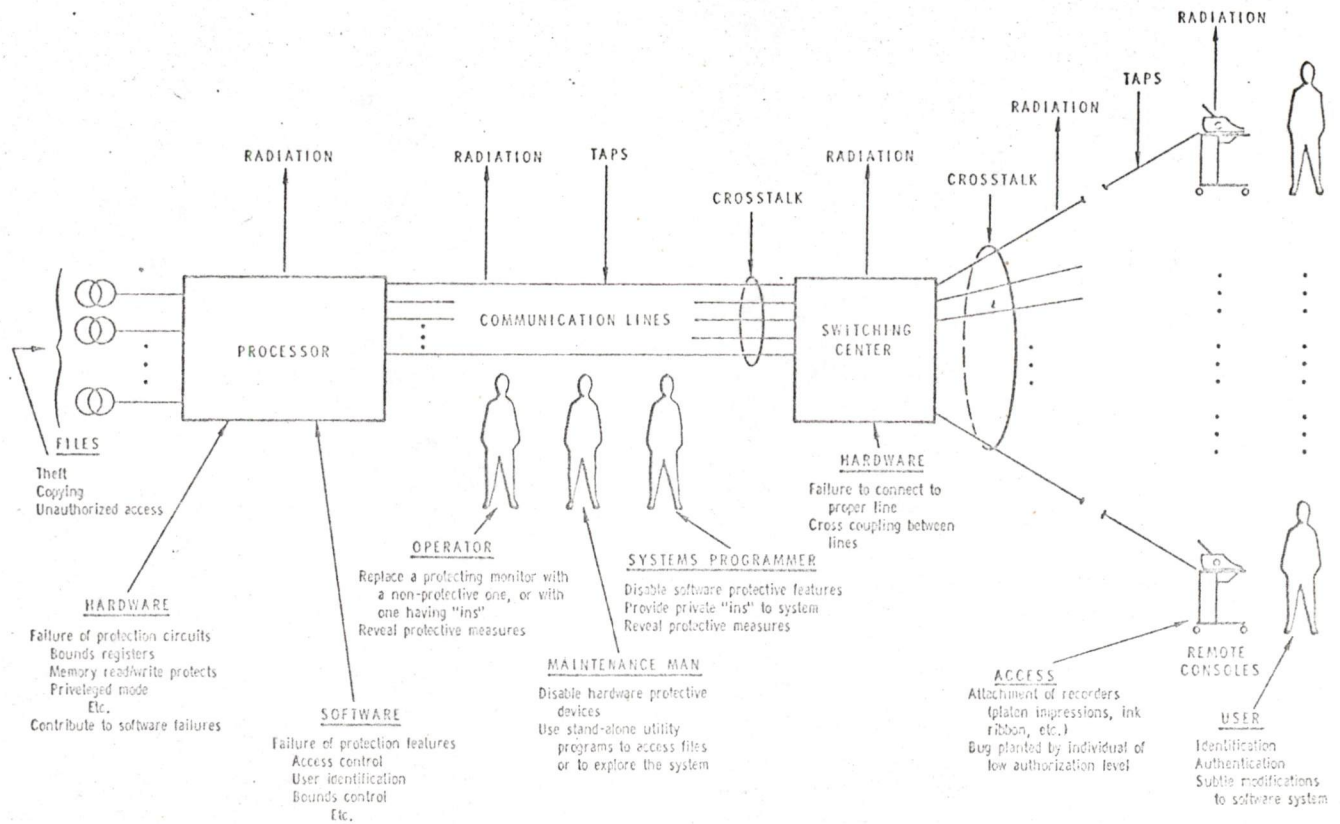


Figure 1—Typical configuration of resource-sharing computer system

will refer to military or defense information or situations; "private" or "privacy," to the corresponding industrial, or non-military governmental situations. In each case, the individual authorized to receive the information will have "need to know" or "access authorization."

We will do the following in this session. In order to bring all of us to a common level of perspective on resource-sharing computer systems, I will briefly review the configuration of such systems and identify the major vulnerabilities to penetration and to leakage of information. The following paper by Mr. Peters will describe the security safeguards provided for a multi-programmed remote-access computer system. Then I will contrast the security and privacy situations, identifying similarities and differences. The final paper by Dr. Petersen and Dr. Turn will discuss technical aspects of security and privacy safeguards. Finally, we have a panel of three individuals who have faced the privacy problem in real-life systems; each will describe his views toward the problem, and his approach to a solution. In the end, it will fall upon each of you to conceive and implement satisfactory safeguards for the situation which concerns you.

A priori, we cannot be certain how dangerous a given vulnerability might be. Things which are serious

for some computer systems may be only a nuisance for others. Let us take the point of view that we will not prejudge the risk associated with a given vulnerability or threat to privacy. Rather, let us try only to suggest some of the ways in which a computer system might divulge information to an unauthorized party in either the security or the privacy situation. We'll leave for discussion in the context of particular installations the question of how much protection we want to provide, what explicit safeguards must be provided, and how serious any particular vulnerability might be.

The hardware configuration of a typical resource-sharing computer system is shown in Figure 1. There is a central processor to which are attached computer-based files and a communication network for linking to remote users via a switching center. We observe first of all that the files may contain information of different levels of sensitivity or military classification; therefore, access to these files by users must be controlled. Improper or unauthorized access to a file can divulge information to the wrong person. Certainly, the file can also be stolen—a rather drastic divulgence of information. On the other hand, an unauthorized copy of a file might be made using the computer itself, and the copy revealed to unauthorized persons.

The central processor has both hardware and software components. So far as hardware is concerned, the circuits for such protections as bound registers, memory read-write protect, or privileged mode might fail and permit information to leak to improper destinations. A large variety of hardware failures might contribute to software failures which, in turn, lead to divulgence. Since the processor consists of high-speed electronic circuits, it can be expected that large quantities of electromagnetic energy will radiate; conceivably an eavesdropping third party might acquire sensitive information. Failure of the software may disable such protection features as access control, user identification, or memory bounds control, leading to improper routing of information.

Intimately involved with the central computer are three types of personnel: operators, programmers, and maintenance engineers. The operator who is responsible for minute-by-minute functioning of the system might reveal information by doing such things as replacing the correct monitor with a non-protecting one of his own, or perhaps with a rigged monitor which has special "ins" for unauthorized parties. Also, he might reveal to unauthorized parties some of the protective measures which are designed into the system. A co-operative effort between a clever programmer and an engineer could "bug" a machine for their own gain in such a sophisticated manner that it might remain unnoticed for an extended period. ("Bug" as just used does not refer to an error in a program, but to some computer equivalent of the famous transmitter in a martini olive.) Bugging of a machine could very easily appear innocent and open.

Operator-less machine systems are practical, and in principle one might conjecture that a machine could be bugged by an apparently casual passerby. There are subtle risks associated with the maintenance process. While attempting to diagnose a system failure, information could easily be generated which would reveal to the maintenance man how the software protections are coded. From that point, it might be easy to rewire the machine so that certain instructions appeared to behave normally, whereas in fact, the protective mechanisms could be bypassed.

While some of the things that I've just proposed require deliberate acts, others could happen by accident.

Thus, so far as the computing central itself is concerned, we have potential vulnerabilities in control of access to files; in radiation from the hardware; in hardware, software, or combined hardware-software failures; and in deliberate acts of penetration or accidental mistakes by the system personnel.

The communication links from the central processor to the switching center, and from the switching center to the remote consoles are similarly vulnerable. Any of the usual wiretapping methods might be employed to steal information from the lines. Since some communications will involve relatively high-frequency signals, electromagnetic radiation might be intercepted by an eavesdropper. Also, crosstalk between communication links might possibly reveal information to unauthorized individuals. Furthermore, the switching central itself might have a radiation or crosstalk vulnerability; it might fail to make the right connection and so link the machine to an incorrect user.

A remote console might also have a radiation vulnerability. Moreover, there is the possibility that recording devices of various kinds might be attached to the console to pirate information. Consideration might have to be given to destroying the ribbon in the printing mechanism, or designing the platen so that impressions could not be read from it.

Finally, there is the user of the system. Since his link to the computer is via a switching center, the central processor must make certain with whom it is conversing. Thus, there must be means for properly identifying the user; and this means must be proof against recording devices, pirating, unauthorized use, etc. Even after a user has satisfactorily established his identity, there remains the problem of verifying his right to have access to certain files, and possibly to certain components of the configuration. There must be a means for authenticating the requests which he will make of the system, and this means must be proof against bugging, recorders, pirating, unauthorized usage, etc. Finally, there is the ingenious user who skillfully invades the software system sufficiently to ascertain its structure, and to make changes which are not apparent to the operators or to the systems programmers, but which give him "ins" to normally unavailable information.

To summarize, there are human vulnerabilities throughout; individual acts can accidentally or deliberately jeopardize the protection of information in a system. Hardware vulnerabilities are shared among the computer, the communications system, and the consoles. There are software vulnerabilities; and vulnerabilities in the system's organization, e.g., access control, user identification and authentication. How serious any one of these might be depends on the sensitivity of the information being handled, the class of users, the operating environment, and certainly on the skill with which the network has been designed. In the most restrictive case, the network might have to be protected against all the types of

invasions which have been suggested plus many readily conceivable.

This discussion, although not an exhaustive consideration of all the ways in which a resource-sharing computer system might be either accidentally or deliberately penetrated for the purposes of unauthor-

ized acquisition of information, has attempted to outline some of the major vulnerabilities which exist in modern computing systems. Succeeding papers in this session will address themselves to a more detailed examination of these vulnerabilities and to a discussion of possible solutions.

# Security controls in the ADEPT-50 time-sharing system

C. WEISSMAN

System Development Corporation  
Santa Monica, California

*"Authority intoxicates/And makes mere  
sots of magistrates" -- Butler*

## FOREWORD

At present, the system described in this paper has not been approved by the Department of Defense for processing classified information. This paper does not represent DOD policy regarding industrial application of time- or resource-sharing of EDP equipment.

## INTRODUCTION

Computer-based, resource sharing systems are, and contain, things of value; therefore, they should be protected. The valuables are the information data bases, the processes that manipulate them, and the physical plant, equipment, and personnel that form the system plexus. An extensive lore is developing on the subject of system protection.<sup>1,2</sup> Petersen and Turn<sup>3</sup> discuss in considerable detail the substance of protection of non-military information systems in terms of threats and countermeasures. Ware<sup>4,5</sup> contrasts "security" and "privacy" for viewing protection in military systems as well. This paper describes the security controls implemented in the ADEPT-50 time-sharing system<sup>6</sup>—a resource sharing system designed to handle sensitive information in classified government and military facilities.\*

Our approach to security control is based on a set

theoretic model of access rights. This approach appears natural, since the important objects of security are sets of things—users, terminals, programs, files—and the operators of set theory—membership, intersection, union—are easily programmed for, and quickly performed by, computer. The formal model defines time-sharing security control of user, terminal, job and file security objects in terms of equations of access based upon their security profiles—a triplet of Authority, Category, and Franchise property sets. The correspondence of these properties to government and military Classification, Compartments, and Need-to-Know is demonstrated. Implementation of the model in the ADEPT-50 Time-Sharing System is described in detail, as are features that transcend the model including initialization of the security profiles, the LOGIN decision procedure, system integrity checks, security residue control, and security audit trails. Other novel features of ADEPT security control are detailed and include: automatic file classification based upon the cumulative security history of referenced files; the "security umbrella" of the ADEPT job; and once-only passwords. The paper concludes with a recapitulation of the goals of ADEPT security control, approximate costs of implementation and operation of the security controls, and suggested extensions and improvements.

Historically, protection of a sensitive computer facility has been attained by limiting physical access to the computer room and shielding the computer complex

\* Development of ADEPT was supported in part by the Advanced Research Projects Agency of the Department of Defense.

from electromagnetic radiation. This "sheltered" approach promotes one-at-a-time, batch usage of the facility. Modern hardware and software technology has moved forward to more powerful and cost/effective time-shared, multi-access, multiprogrammed systems. However, three features of such systems pose a challenge to the sheltered mode of protection: (1) concurrent multiple users with different access rights operating remote from the shielded room; (2) multiple programs with different access rights co-resident in memory; and (3) multiple files of different data sensitivities simultaneously accessible. These features appear to violate traditional methods of accountability based upon a single user (or multiple users with like clearances) operating within strictly controlled facilities. The problem is of such magnitude that no time-sharing system has yet been certified for use in the manner described! However, some multi-access systems are in operation in a classified mode,<sup>7,8</sup> and a number of design approaches have been suggested.<sup>9,10,11,12</sup>

In addition to the usual goal of building an effective time-sharing system,<sup>13</sup> the ADEPT project began with a number of security objectives as well:

1. Build a security control mechanism that supports heterogeneous levels and types of classifications.
2. Design the security control mechanism in such a manner that it is itself unclassified until primed by security configuration parameters, a point strongly supported by Baran<sup>14</sup> regarding communications security.
3. Construct the security control mechanism as an isolated portion of the total time-sharing system so that it may be carefully scrutinized for correctness, completeness, and reliability.
4. Do the above in as frugal a manner as possible, considering costs to design, fabricate, and operate. Good system performance is our principal criterion in selecting among alternative technical solutions, as noted by the author elsewhere.<sup>15</sup>

In approaching our task, we recognize security as a total system problem involving hardware, communication, personnel, and software safeguards. However, our focus is primarily on monitor software, and its interfaces with the other areas. This view is not parochial: our hardware is a standard IBM 360 model 50; communication security is an established field of study with considerable technological know-how;<sup>14</sup> and the policy, doctrine, and procedures for personnel behavior in classified environments are extensive, with legal founda-

tions. Thus, our only degree of freedom is the control we build into the time-sharing executive software.

#### *A security control formalism*

A formal model of software security control for access to sensitive portions of ADEPT is developed here.

#### *Security objects*

Four kinds of security objects are to be managed by our model: user, terminal, job, and file. Let  $u$  denote some user;  $t$  some terminal;  $j$  some job; and  $f$  some file.

#### *Security properties*

Each security object is described by a security profile that is an ordered triplet of security properties—Authority (A), Category (C), and Franchise (F). Authority is a set of hierarchically ordered security jurisdictions. Category is a set of discrete security jurisdictions. Franchise is a set of users licensed with privileged security jurisdiction.

The property "Authority" is defined as a set  $A$ , where

$$A = \{a^0 < a^1 < \dots < a^n\} \quad (1)$$

and the specific members,  $a^i$ , of the set are security jurisdictions hierarchically ordered.

"Category" is a discrete set of specific compartments,  $c^i$ ,

$$C = \{c^0, c^1, \dots, c^y\} \quad (2)$$

Compartments are mutually exclusive security sanctuaries with discrete jurisdictions.

"Franchise" is a security jurisdiction privileged to a given set of users, i.e.,

$$F = \{u | u \text{ is a user}\} \quad (3)$$

For a given terminal,  $t$ , let a given Authority set,  $A$ , be denoted by  $A_t$ , or in general, let a given security object,  $\alpha$ , denote a given property,  $P$ , for  $\alpha$  as  $P_\alpha$ . Hence we can speak of  $A_u$ , or  $C_j$ , etc., to mean the specific Authority set for a given user,  $u$ , or the specific Category set for a given job,  $j$ , respectively.

Four important sets (of users) arise with respect to the Franchise property, namely, Franchise for files, terminals, jobs, and users. To distinguish the sense in which a given user is being considered, we subscript  $u$  by the security object under consideration. Hence,  $u_f$  means the user with jurisdiction to file  $f$ ;  $u_t$  and  $u_j$  are similarly defined. For completeness, we define  $u_u$  as



reply  $u$ . We can now define Franchise for each security object.

$$F_u = \{u\} \quad (4)$$

$$F_t = \{u_t^0, u_t^1, \dots, u_t^\lambda\} \quad (5)$$

$$F_j = \{u_j^0, u_j^1, \dots, u_j^\mu\} \quad (6)$$

$$F_f = \{u_f^0, u_f^1, \dots, u_f^\nu\} \quad (7)$$

Equation (4) states that the Franchise for a user is restricted to himself; his jurisdiction is unique, and no other user is so endowed. Equation (5) states that the terminal Franchise is possessed by  $\lambda$  different users who have jurisdiction over the terminal  $t$ . Likewise, equations (6) and (7) define the job and file Franchise sets.

In security discussions, one hears the familiar phrase, "he needs a higher-level clearance." We can now define "higher level" with our model.

Let  $\alpha$  and  $\beta$  be security objects and let  $\rho$  be some function such that  $\rho(A_\alpha) \in A$ .

Then,

$$A_\alpha \geq A_\beta \leftrightarrow \rho(A_\alpha) \geq \rho(A_\beta) \quad (8)$$

$$C_\alpha \geq C_\beta \leftrightarrow C_\alpha \supseteq C_\beta \quad (9)$$

$$F_\alpha \geq F_\beta \leftrightarrow F_\alpha \supseteq F_\beta \quad (10)$$

Equation (8) claims that the Authority of a security object,  $A_\alpha$ , is at a "higher level" than another security object  $A_\beta$  when the specific authority,  $a_\alpha$ , is greater than the specific authority,  $a_\beta$ .

It is implicit in equations (1) and (8) that the specific authorities,  $a_i$ , must be numerically encoded for the magnitude relationships to hold. Equations (9) and (10) define  $P_\alpha$  to be greater than  $P_\beta$  if and only if  $P_\beta$  is a subset of  $P_\alpha$ .

Events may alter the membership of property sets. Let  $P_j^e$  be the  $e$ th  $P_j$  in a given context.

Define the Authority history,  $A_h$ , at the  $e$ th event as

$$A_h(0) = a_j^0 \quad (11)$$

$$A_h(e) = \max(A_h(e-1), \rho(A_j^e)), e > 0 \quad (12)$$

Likewise, define the Category history  $C_h$ , at the  $e$ th event as

$$C_h(0) = \phi \quad (13)$$

$$C_h(e) = C_h(e-1) \cup C_j^e, e > 0 \quad (14)$$

Equations (11) through (14) recursively define two useful sets that accumulate a history of file references as a function of file reference events,  $e$ . A history of the highest Authority,  $A_h$ , is defined by equation (12) as either the previous set,  $A_h(e-1)$ , or the current set,  $\rho(A_j^e)$ , whichever is larger in the sense of equation (8). Equation (11) gives the initial condition as some low specific file authority,  $a_j^0$ . Equation (14) defines the highest Category history as the union of the previous set,  $C_h(e-1)$ , and the current set,  $C_j^e$ ; while equation (13) states that the union is initially the empty set.

Though  $F_h$  could be defined in our model, no need is seen at this time for a Franchise history. More will be said about these history sets later.

### Property determination

Table I presents in a  $3 \times 4$  matrix a summary of the rules for determining the security profile triplets,  $P_{\alpha\epsilon}$ . We shall examine these rules here. For the user  $u$ ,  $A_u$  and  $C_u$  are given constants, and  $F_u$  is given by equation (4). For the terminal  $t$ ,  $A_t$  and  $C_t$  are given constants, and  $F_t$  is given by equation (5). Given  $A_u$  and  $A_t$ , we determine  $A_j$  as:

$$A_j = \min(A_u, A_t) \quad (15)$$

Likewise, given  $C_u$  and  $C_t$ , we determine  $C_j$  as:

$$C_j = C_u \cap C_t \quad (16)$$

Equation (6) gives  $F_j$  to complete the job security profile triplet.

An existing file has its security profile predetermined with  $A_j$  and  $C_j$  as given constants, and  $F_f$  as given by equation (7). However, a new file—one just created—derives its security profile from the job's file access history according to the following:

$$A_f = A_h(e) \quad (17)$$

$$C_f = C_h(e) \quad (18)$$

$$F_f = u_f^e \quad (19)$$

From equations (11) through (14) we see how the Authority and Category histories accumulate as a function of event  $e$ . These events are the specific times when files are accessed by a job. To maintain security

TABLE I—Security property determination matrix

Object \ Property	Authority A	Category C	Franchise F
User, u	Given Constant	Given Constant	u
Terminal, t	Given Constant	Given Constant	u <sub>t</sub> <sup>i</sup>
Job, j	min(A <sub>u</sub> , A <sub>t</sub> )	C <sub>u</sub> ∩ C <sub>t</sub>	u <sub>j</sub> <sup>i</sup>
File, f	<i>Existing file</i> Given Constant	<i>Existing file</i> Given Constant	u <sub>f</sub> <sup>i</sup>
	<i>New file</i> max(A <sub>h</sub> (e-1), ρ(A <sub>f</sub> <sup>i</sup> )), e > 0	<i>New file</i> C <sub>h</sub> (e-1) ∪ C <sub>f</sub> <sup>i</sup> , e > 0	u <sub>f</sub> <sup>i</sup>

integrity, these histories can never exceed (i.e., be greater than) the job security profile. This is specified as,

$$A_h(\infty) \rightarrow A_j \quad (20)$$

$$C_h(\infty) \rightarrow C_j \quad (21)$$

For  $e=0$ , we see the properties initialized to their simplest form. However, as  $e$  gets large, the histories accumulate, but never exceed the upper limit set by the job.  $A_h(e)$  and  $C_h(e)$  are important new concepts, discussed in further detail later. We speak of them, affectionately, as the security "high-water mark," with analogy to the bath tub ring that marks the highest water level attained.

The Franchise of a new file is always obtained from the Franchise of the job given by equation (6). When  $i = \mu = 0$ , the job is controlled by the single user  $u_j$  who becomes the owner and creator of the file with the sole Franchise for the file.

#### Access control

Our model is now rich enough to express the equations of access control. We wish to control access by a user to the system, to a terminal, and to a file. Access is granted to the system if and only if

$$u \in U \quad (22)$$

where  $U$  is the set of all sanctioned users known to the system.

Access is granted to a terminal if and only if

$$u \in F_t \quad (23)$$

If equations (22) and (23) hold, then by definition

$$u = u_t = u_j \quad (24)$$

Access is granted to a file if and only if

$$P_j \geq P_f \quad (25)$$

for properties A and C according to equations (8) and (9), and

$$u_j \in F_f \quad (26)$$

If equations (25) and (26) hold, then access is granted and  $A_h(e)$  and  $C_h(e)$  are calculated by equations (12) and (14).

#### Model interpretation

Three different dimensions for restricting access to sensitive information and information processes are possible with the security profile triplet. The generality of this technique has considerable application to public and military systems. For the system of interest, however, the Authority property corresponds to the Top Secret, Secret, etc., levels of government and military security; Category corresponds to the host of special control compartments used to restrict access by project and area; such as those of the Intelligence and Atomic Energy communities; and the Franchise property corresponds to access sanctioned on the basis of

need-to-know. With this interpretation, the popular security terms "classification" and "clearance" can be defined by our model in the same dimensions--as a min/max test on the security profile triplet. Classification is attached to a security object to designate the minimum security profile required for access, whereas clearance grants to a security object the maximum security profile it has permission to exercise. Thus, legal access obtains if the clearance is greater than or equal to the classification, i.e., if equation (25) holds.

Another observation on the model is the "job umbrella" concept implied by equations (22) through (26); i.e., the derived clearance of the job (not the clearance of the user) is used as the security control triplet for file access. The job umbrella spreads a homogeneous clearance to normalize access to a heterogeneous assortment of program and data files. This simplifies the problem of control in a multi-level security system. Also note how the job umbrella's high-water mark (equations (11) through (14)) is used to automatically classify new files (equations (17) and (18)); this subject is discussed further below.

A final observation on the model is its application of need-to-know to terminal access, equation (23). This feature allows terminals to be restricted to special people and/or special groups for greater control of personnel interfaces--i.e., systems programmers, computer operators, etc.

#### *Security control implementation*

The selection of a set theoretic model of security control was not fortuitous, but a deliberate choice biased toward computational efficiency and ease of implementation. It permits the clean separation and isolation of security control code from the security control data, which enables ADEPT's security mechanisms to be openly discussed and still remain safe--a point advocated by others.<sup>14,16</sup> We achieve this safety by "arming" the system with security control data only once at start-up time by the SYSLOG procedure discussed later. Also, the model improves the credibility of the security system, enhancing its understanding and thereby promoting its certification.

#### Security objects: Identity and structure

Each security object has a unique identification (ID) within the system such that it can be managed individually. The form of the ID depends upon the security-object type; the syntax of each is given below.

#### User identification

For generality of definition, each user is uniquely identified by his *user:id*, which must be less than 13 characters with no embedded blanks.

The *user:id* can be any meaningful encoding for the local installation. For example, it can be the individual's Social Security number, his military serial number, his last name (if unique and less than 13 characters), or some local installation man-number convention. The set of all *user:ids* constitutes the universal set,  $U$ .

#### Terminal identification

All peripheral devices in ADEPT are identified uniquely by their IBM 360 device addresses. Besides interactive terminals, this includes disc drives, tape drives, line printer, card reader-punch, drums, and 1052 keyboard. Therefore, *terminal:id* must be a two-digit hexadecimal number corresponding to the unit address of the device.

#### Job identification

ADEPT consists of two parts: the Basic Executive (BASEX), which handles the allocation and scheduling of hardware resources, and the Extended Executive (EXEX), which interfaces user programs with BASEX. ADEPT is designed to operate itself and user programs as a set of 4096-byte pages. BASEX is identified as certain pages that are fixed in main core, whereas EXEX and user programs are identified as sets of pages that move dynamically between main and swap memory. A set of user programs are identified as a job, with page sets for each program (the program map) described in the job's environment area, i.e., the job's "state tables." Every job in ADEPT has an environment area that is swapped with the job. It contains dynamic system bookkeeping information pertinent to the job, including the contents of the machine registers (saved when the job is swapped out), internal file and I/O control tables, a map of all the program's pages on drum, *user:id*, and the job security control parameters. The environment page(s) are memory-protected against reading and writing by user programs, as they are really swappable extensions of the monitor's tables.

The *job:id* is then a transitory internal parameter which changes with each user entrance and exit from the system. The *job:id* is a relative core memory address used by the executive as a major index into central system tables. It is mapped into an external two-digit number that is typed to the user in response to a successful LOGIN.

### File identification

ADEPT's file system is quite rich in the variety of file types, file organization, and equipment permitted. There are two file types: temporary and permanent.

Temporary files are transitory "scratch" disc files, which disappear from the system inventory when their parent job exits from the system. They are always placed on resident system volumes, and are private to the program that created them.

Permanent files constitute the majority of files cataloged by the system. Their permanence derives from the fact that they remain inventoried, cataloged, and available even after the job that created or last referenced them is no longer present, and even if they are not being used. Permanent files may be placed by the user on resident system volumes or on demountable private volumes.

There are six file organizations from which a user may select to structure the records of his file: Physical-sequential, S1; non-formatted, S2; index-sequential, S3; partitioned, S4; multiple volume fixed record, S5; and single volume fixed record, S9. Regardless of the organization of the records, ADEPT manages them as a collection, called a file. Thus, security control is at the file level only, unlike more definitive schemes of sub-element control.<sup>5,10-12</sup>

All the control information of a file that describes type, organization, physical storage location, date of creation, and security is distinct from the data records of the file, and is the catalog of the file.

All cataloged ADEPT files are uniquely identified by a four-part name; each part has various options and defaults (system assumptions). This name, the *file:id*, has the following form:

$$file:id ::= name, form, user:id, volume:id$$

*Name* is a user-generated character string of up to eight characters with no embedded blanks. It must be unique on a private volume as well as for Public files (described below).

*Form* is a descriptor of the internal coding of a file. Up to 256 encodings are possible, although only these seven are currently applicable:

- 1 = binary data
- 2 = relocatable program
- 3 = non-relocatable program
- 4 = card images
- 5 = catalog
- 6 = DLO (Delayed Output)
- 7 = line images

*User:id* corresponds to the owner of the file, i.e., the creator of the file.

*Volume:id* is the unique file storage device (tape, disc, disc pack, etc.) on which the file resides. For various reasons, including reliability, ADEPT file inventories are distributed across the available storage media, rather than centralized on one particular volume. Thus, all files on a given disc volume are inventoried on that volume.

### Security properties: Encoding and structure

Implementation of the security properties in ADEPT is not uniform across the security objects as suggested by our model, particularly the Franchise property. Lack of uniformity, brought about by real-world considerations, is not a liability of the system but a reflection of the simplicity of the model. Extensions to the model are developed here in accordance with that actually implemented in ADEPT.

### Authority

Authority is fixed at four levels ( $\omega = 3$  for equation (1)) in ADEPT, specifically, UNCLASSIFIED, CONFIDENTIAL, SECRET, and TOP SECRET in accordance with Department of Defense security regulations. The Authority set is encoded as a logical 4-bit item, where positional order is important. Magnitude tests are used extensively, such that the high-order bits imply high Authority in the sense of equation (8).

### Category

Category is limited to a maximum of 16 compartments ( $\psi \leq 15$  for equation (2)), encoded as a logical 16-bit item. Boolean tests are used exclusively on this datum. The definition of (and bit position correspondence to) specific compartments is an installation option at ADEPT start-up time (see SYSLOG). Typical examples of compartments are EYES ONLY, CRYPTO, RESTRICTED, SENSITIVE, etc.

### Franchise

Property Franchise corresponds to the military concept of need-to-know. Essentially, this corresponds to a set of *user:ids*; however, the ADEPT implementation of Franchise is different for each security object:

1. User: All users wishing ADEPT service must be known to the system. This knowledge is imparted by SYSLOG at start-up time and limited to approximately 500 *user:ids* ( $\max(U) \leq 500$ ).

2. Terminal: Equation (5) specifies the Franchise of a given terminal,  $F_t$ , as a set of *user:ids*. In ADEPT,  $F_t$  does not exist. One may define all the users for a given terminal, i.e.,  $F_t$ ; or alternatively, all the terminals for a given user. Because SYSLOG orders its tables by *user:id*, the latter definition was found more convenient to implement.
3. Job: The Franchise of a job is the *user:id* of the creator of the job at the time of LOGIN to the system. Currently, only one user has access to (and control of) a job ( $\mu = 0$  for equation (6)).
4. File: Implementation of Franchise for a file ( $F_f$ ), is more extensive than equation (7). In ADEPT, we wish to control not only who accesses a file, but also the quality of access granted. We have defined a set of four exclusive qualities of access, such that a given quality,  $q$ , is defined if

$$q \in \{\text{READ, WRITE, READ-AND-WRITE, READ-AND-WRITE-WITH-LOCKOUT-OVERRIDE}\} \quad (27)$$

ADEPT permits simultaneous access to a file by many jobs if the quality of access is for READ only. However, only one job may access a file with WRITE, or READ-AND-WRITE quality. ADEPT automatically locks out access to a file being written to avoid simultaneous reading and writing conflicts. A special access quality, however, does permit lockout override. Equation (7) can now be extended as a set of pairs,

$$F_f = \{(u_0^q, q^0), (u_1^q, q^1), \dots, (u_\gamma^q, q^\gamma)\}; \quad (28)$$

where  $q^i$  are not necessarily distinct and are given by equation (27).

The implementation of equation (28) is dependent upon  $\gamma$ , the number of franchised users. When  $\gamma = 0$ , we have the ADEPT Private file, exclusive to the owner,  $u_0^q$ ; for  $\gamma = \max(U)$ , we have the Public file; values of  $\gamma$  between these extremes yield the Semi-Private file.  $\gamma$  is implicitly encoded as the ADEPT "privacy" item in the file's catalog control data, and takes the place of  $F_f$  for all cases except a Semi-Private file. For that case exclusively, equation (28) holds and an actual  $F_f$  list of *user:id*, *quality* pairs exists as a need-to-know list. The owner of a file specifies and controls the file's privacy, including the composition of the need-to-know list.

### Security control initialization: SYSLOG

SYSLOG is a component of the ADEPT initialization package responsible for arming the security controls. It operates as one of a number of system start-up options prior to the time when terminals are enabled. SYSLOG sets up the security profile data for *user:id* and *terminal:id*, i.e., the "given constants" of Table I.

SYSLOG creates or updates a highly sensitive system disc file, where each record corresponds to an authorized user. These records are constructed from a deck of cards consisting of separate data sets for *compartment* definitions, *terminal:id* classification, and *user:id* clearance. The dictionary of *compartment* definitions contains the less-than-9-character mnemonic for each member of the Category set. Data sets are formed from the card types shown in Table II. Use of *passwords* is described later in the LOGIN procedure.

An IDT card must exist for each authorized user; the PWD, DEV, SEC, and CAT card types are optional. Other card types are possible, but not germane to security control, e.g., ACT for accounting purposes. More than one PWD, DEV, and CAT card is acceptable up to the current maximum data limits (i.e., 64 *passwords*, 48 *terminal:ids*, and 16 *compartments*).

A variety of legality checks for proper data syntax, quantity, and order are provided. SYSLOG assumes the following default conditions when the corresponding card type is omitted from each data set:

PWD	No <i>password</i> required
DEV	All <i>terminal:ids</i> authorized
SEC	A = UNCLASSIFIED
CAT	C = null (all zero mask)

This gives the lowest user clearance as the default, while permitting convenient user access. Various options exist in SYSLOG to permit maintenance of the internal SYSLOG tables, including the replacement or deletion of existing data sets in total or in part.

The sensitivity of the information in the security control deck is obvious. Procedures have been developed at each installation that give the function of deck creation, control, and loading to specially cleared security personnel. The internal SYSLOG file itself is protected in a special manner described later.

### Access control

A fundamental security concern in multi-access systems is that many users with different clearances will be simultaneously using the system, thereby raising the

TABLE II—SYSLOG control cards

Card Type	Purpose
DICT <i>compartment</i> <sub>1</sub> ... <i>compartment</i> <sub>16</sub>	Identifies start of data set of <i>compartment</i> definitions. Defines up to 16 <i>compartment</i> s.
TERMINAL	Identifies start of data sets of terminal definitions.
UNIT <i>terminal:id</i>	Identifies start of a terminal data set.
IDT <i>user:id</i>	Identifies start of a user data set.
PWD <i>password</i> ... <i>password</i>	Defines legal <i>password</i> s for <i>user:id</i> up to 64.
DEV <i>terminal:id</i> <sub>1</sub> ... <i>terminal:id</i> <sub>48</sub>	Defines legal terminals for <i>user:id</i> up to 48.
SEC Authority	Defines <i>user:id</i> Authority.
CAT <i>compartment</i> <sub>1</sub> ... <i>compartment</i> <sub>16</sub>	Defines <i>user:id</i> Category set.

possibility of security compromise. Since programs are the "active agents" of the user, the system must maintain the integrity of each and of itself from accidental and/or deliberate intrusion. A multifile system must permit concurrent access by one or more jobs to one or more on-line, independently classified files.

ADEPT is all these things—multiuser, multiprogram, and multifile system. Thus, this section deals with access control over users, programs, and files.

User access control: LOGIN

To gain admittance to the system, a user must first satisfy the ADEPT LOGIN decision procedure. This procedure attempts to authenticate the user in a fashion analogous to challenge-response practices.

The syntax of the ADEPT LOGIN command, typed by a user on his terminal, is as follows:

*/LOGIN user:id password accounting*

Figure 1 pictorially displays the LOGIN decision procedure based upon the user-specified input parameters. *User:id* is the index into the SYSLOG file used to retrieve the user security profile. If no such record exists (i.e., equation (22) fails), the LOGIN is unsuccessful and system access is denied. If the security profile is found, LOGIN next retrieves the *terminal:id* for the keyboard in use from internal system tables, and searches for a match in the *terminal:id* list for which the *user:id* was franchised by SYSLOG. An unsuccessful search is an unsuccessful LOGIN.

If the terminal is franchised, then the current *password* is retrieved from the SYSLOG file for this *user:id* and matched against the *password* entered as a keyboard parameter to LOGIN. An unsuccessful match is again

an unsuccessful LOGIN. Furthermore, the terminal is ignored (will not honor input) for approximately 30 seconds to frustrate high-speed, computer-assisted, penetration attempts. If, however, the match is successful (equation (22) holds), the current *password* in the SYSLOG file for this *user:id* is discarded and LOGIN proceeds to create the job clearance.

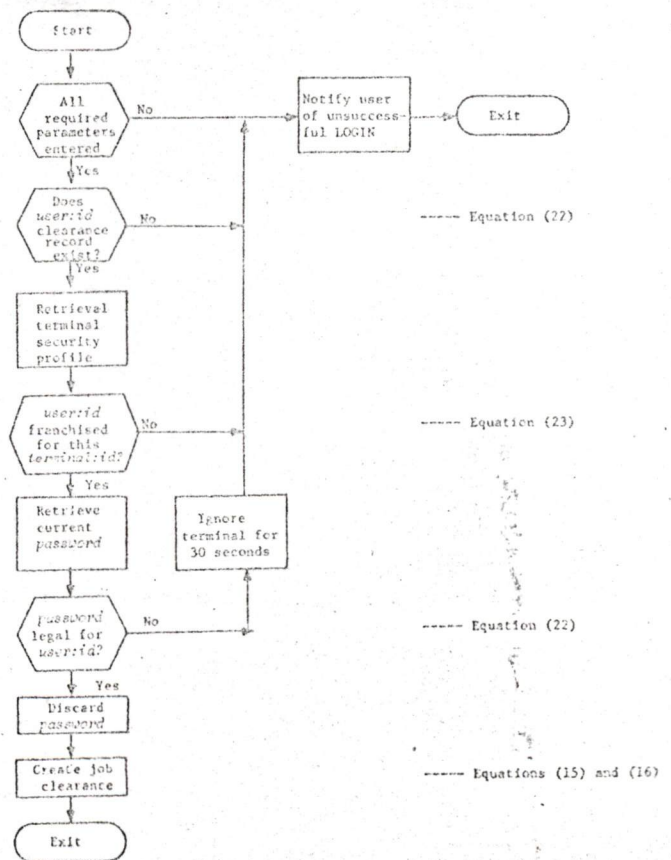


Figure 1—LOGIN decision procedure

*Passwords* in ADEPT obey the same syntax conventions as *user:id*. (See the earlier description of User Identification.) Although easily increased, currently SYSLOG permits up to 64 *passwords*. Each successful LOGIN throws away the user *password*; 64 successful LOGINS are possible before a new set of *passwords* need be established. If other than random, once-only *passwords* are desired, the 64 *passwords* may be encoded in some algorithmic manner, or replicated some number of times. Once-only *passwords* is an easily implemented technique for user authentication, which has been advocated by others.<sup>2,7</sup> It is a highly effective and secure technique because of the high permutability of 12-character-*passwords* and their time and order interdependence, known only to the user.

Once the authentication process is completely satisfied, LOGIN creates the job security profile according to equations (15) and (16) of our model. That is, the lower Authority of the user and the terminal becomes  $A_j$ , and the intersection (logical AND) of the user and terminal Category sets becomes the Category of the job,  $C_j$ . For example, a user with TOP SECRET Authority and a Category set (1001 1001 0000 1101) operating from a SECRET level terminal with a Category set (0000 0000 0000 0010) controls a job cleared to SECRET with an empty Category set.

#### Program access control: LOAD

As noted earlier, the ADEPT Executive consists of two parts: BASEX, the resident part, and EXEX, the swapped part. EXEX is a body of reentrant code shared by all users; however, it is treated as a distinct program in each user's job. Up to four programs can exist concurrently in the job. Each operates with the job clearance—the job clearance umbrella.

LOAD is the ADEPT component used to load the programs chosen by the user; it is part of EXEX and hence operates as part of the user's job with the job's clearance. Programs are cataloged files and as such may be classified with a given security profile. As is described in "File Access Control" below, LOAD can only load those programs for which the job clearance is sufficient. Once loaded, however, the new program operates with the job clearance.

In this manner, we see the power of the job umbrella in providing smooth, flexible user operation concurrent with necessary security control. Program files may be classified with a variety of security profiles and then operate with yet another, i.e., the job clearance. By this technique security is assured and programs of different classifications may be operated by a user as one job. It

permits, for example, an unclassified program file (e.g., a file editor) to be loaded into a highly classified job to process sensitive classified data files.

#### File access control: OPEN

Before input/output can be performed on a file, a program must first acquire the file by an OPEN call to the Cataloger. Each program must OPEN a file for itself before it can manipulate the file, even if the file is already OPENed for another program. A successful OPEN requires proper specification of the file's descriptors—some of which are in the OPEN call, others of which are picked up directly by the Cataloger from the job environment area (e.g., job clearance, *user:id*)—and satisfactory job clearance and *user:id* need-to-know qualifications according to equations (25) and (26) of our model. Equation (25) is implemented as (8) as a straightforward magnitude comparison between  $A_j$  and  $A_f$ . Equation (25) is implemented as (9) as an equality test between  $C_j$  and  $(C_j \wedge C_f)$ . We use  $(C_j \wedge C_f)$  to ensure that  $C_j$  is a subset of the job categories; i.e., the job umbrella. Lastly, equation (26) is a NOP if the file is Public; a simple equality test between  $u_j$  and  $u_f$  if the file is Private; and a table search of  $F_j$  for  $u_f$  if the file is Semi-Private. These tests do increase processing time for file access; however, the tests are performed only once at OPEN time, where the cost is insignificant relative to the I/O processing subsequently performed on the file.

The quality of access granted by a successful OPEN, and subsequently enforced for all I/O transfers, is that requested, even if the user has a greater Franchise. For example, during program debugging, the owner of a file may OPEN it for READ access only, even though READ-AND-WRITE access quality is permitted. He thereby protects his file from possible uncontrolled modification by an erroneous WRITE call.

Considerable controversy surrounds the issue of automatic classification of new files formed by subset or merger of existing files. The heart of the issue is the poor accuracy of many such classification techniques<sup>17</sup> and the fear of too many over-classified files (a fear of operations personnel) or of too many under-classified files (a fear of the security control officers). ADEPT finesses the problem with a clever heuristic—most new files are created from existing files, hence classify the new file as a private file with the composite Authority and Category of all files referenced. This is achieved in ADEPT by use of the "high-water mark."

Starting with the boundary conditions of equations (11) and (13), the Cataloger applies equations (12) and

(14) for each successful file OPEN, and hence maintains the composite classification history of all files referenced by the job. For each new and temporary file OPEN, the Cataloger applies equations (17), (18), and (19); they are reapplied for each CLOSE of a new file, to update the classification (due to changes in the high-water mark since the OPEN) when the file becomes an existing cataloged file in the inventory. The scheme rarely underclassifies, and tends to overclassify when the new file is created late in the job cycle, as shown by boundary equations (20) and (21).

#### *Trans-formal security features*

ADEPT contains a host of features that transcend the formalism presented earlier. They are described here because they are integral to the total security control system and form a body of experience from which new formalisms can draw.

#### **Computer hardware**

ADEPT operates on an IBM System 360/50 and is, therefore, limited to the hardware available. Studies by Bingham<sup>9</sup> suggest a variety of hardware features for security control, many of which are possessed by System 360.

IBM System 360 can operate in one of two states: the Supervisor state, or the Problem state. ADEPT executive programs operate in the Supervisor state; user programs operate in the Problem state.

A number of machine instructions are "privileged" to the Supervisor state only. An attempt to execute them in the Problem state is trapped by the hardware and control is returned to the executive program for remedial action. ADEPT disposes of these alarms by suspending the guilty job. (A suspended job may be resumed by the user.) Clearly, instructions that change the machine state are privileged to the executive only.

Another class of privileged instructions consists of those dealing with input/output. Problem state programs cannot directly access information files on secondary memory storage devices such as disc, tape, or drum. They must access these files indirectly by requests to the executive system. The requests are subjected to interpretive screening by the executive software.

Main memory is selectively protected against unauthorized change (write protected). We have also had the 360/50 modified to include fetch protection, which guards against unauthorized reading of—or executing from—protected memory. The memory protect instruc-

tions are also privileged only in the Supervisor state.

ADEPT software protects memory on a 4096-byte "page" basis (the hardware permits 2048-byte pages), allowing a non-contiguous mosaic of protected pages in memory for a given program. To satisfy multiprogramming, many different protection groups are needed. Through the use of programmable 4-bit hardware masks, up to 15 different protection groups can be accommodated in core concurrently. ADEPT executive programs operate with the all-zero "master key" mask, permitting universal access by all Basic and Extended Executive components.

There are five classes of interrupts processed by System/360 hardware: input/output, program, supervisor call, external, and machine check. Any interrupts that occur in the Problem state cause an automatic hardware switch to the Supervisor state, with CPU control flowing to the appropriate ADEPT executive interrupt controller. All security-vulnerable functions including hardware errors, external timer and keyboard actions, user program service requests, illegal instructions, memory protect violations, and input/output, are called to the attention of ADEPT by the System/360 interrupt system. The burden for security integrity is then one for ADEPT software.

#### **Monitor software**

Inducing the system to violate its own protection mechanisms is one of the most likely ways of breaking a multi-access system. Those system components that perform tasks in response to user or program requests are most susceptible to such seduction.

#### On-Line debugging

The debugging program provides an on-line capability for the professional programmer to dynamically look at and change selected portions of his program's memory. DEBUG can be directed to access sensitive core memory that would not be trapped by memory protection, since, as an EXEX component operating in the Supervisor state, DEBUG operates with the memory protection master key. To close this "trap door," DEBUG always performs interpretive checks on the legality of the debugging request. These checks are based upon address-out-of-bounds criteria, i.e., the requested debugging address must lie within the user's program area. If not, the request will be denied and the user warned, but he will not be terminated as has been suggested.<sup>7</sup>



### Input/output

Input/output in System/360 is handled by a number of special-purpose processors, called Selector Channels. To initiate any I/O, it is necessary for a channel program to be executed by the Selector Channel.

SPAM, the BASEX component that permits symbolic input/output calls from user programs, is really a special-purpose compiler that produces I/O channel programs from the SPAM calls. These channel programs are subsequently delivered and executed by the ADEPT Input/Output Supervisor, IOS.

SPAM permits a variety of calls to read, write, alter, search for, and position to records within cataloged files. To achieve these ends, SPAM depends upon a variety of control tables dynamically created by the Cataloger in the job environment.

The initiating and subsequent monitoring of channel program execution is the responsibility of the BASEX Input/Output Supervisor, IOS. IOS is called to execute a channel program (EXCP). System components, such as SPAM, branch to IOS at a known entry point that is fetch-protected against entry in the Problem state. IOS is off-limits to user programs attempting to access cataloged storage. For protection against unauthorized EXCP requests, IOS always performs legality checks before executing a channel program. These checks begin by examination of the device addressed by the channel program. If it is the device address for cataloged storage, further checks are made to determine the machine state of the calling program. That state must be Supervisor state for the call to be honored. A call in the Problem state would indicate an illegal EXCP call from a user program.

IOS makes other checks to guarantee the validity of an I/C request. It checks to see that the specified buffer areas for the transfer do not overlay the channel program itself, and lie within the user's program memory area, i.e., do not modify or access system or protected memory.

Covert I/O violations are also forestalled since I/O components take direction from information stored in the job environment—an area read- and write-protected from Problem state programs.

### Classified residue

Classified residue is classified information (either code or data) left behind in memory (i.e., core, drum, or disc) after the program that referenced it has been dismissed, swapped out, or quit from the system. The standard solution to the problem is to dynamically purge the contaminated memory (e.g., overwrite with

random numbers, or zeros). In a system supporting over  $\frac{1}{4}$  billion bytes of memory, that solution is unreasonable and in conflict with high performance goals. ADEPT's solution to the dilemma of denying access to classified residue while maintaining high performance depends upon techniques of controlled memory allocation.

#### 1. *Core Residue*

As noted earlier, all core storage is allocated as 4096-byte pages. These pages are always cleared to zero when allocated, thereby overwriting any potential residue.

Via the program's page map, the ADEPT executive system labels all code and data pages (they need not be contiguous) belonging to a given program with a single hardware memory protection key, thereby prohibiting unauthorized reading or writing by other, potentially co-resident user programs that may be in execution. Furthermore, BASEX keeps a running account of the status and disposition of all pages of core.

The Loader and Swapper components of ADEPT always work with full 4096-byte pages. Unfilled portions of pages at load time are kept cleared to zero as when they were allocated, and the full 4096 bytes are swapped into core, if not already resident, each scheduled time slice. Further, newly allocated pages are marked as "changed" pages, thus guaranteeing subsequent swap out to drum.

With these procedures, ADEPT denies access by a user or program to those pages of core not identified as part of his program, and clears core residue by over-writing accessible core at load and swap times.

#### 2. *Drum Residue*

ADEPT always clears a drum page to zero before it is allocated. The page may subsequently be cleared again to user-specified data. ADEPT also maintains a drum map that notes the disposition of all drum pages (800 pages for the IBM 2303 drum). Drum input/output, like all ADEPT I/O, is controlled by executive privileged instructions.

#### 3. *Disc Residue*

Disc files in ADEPT are maintained as "dirty" memory. That is, the large capacity of the file system makes it infeasible to consider automatic over-writing techniques for residue control; therefore, deleted disc tracks are returned to the available storage pool contaminated and unclean. It then becomes the burden of the

ADEPT file system to control any unauthorized file access, whether to cataloged files or uncataloged disc memory.

Team work between the Cataloger, SPAM and IOS components of ADEPT achieves this control via legality checking of all OPEN and I/O requests.

For example, all disc packs are labeled internally and externally with their *volume:id*, and this label is checked at the time of mounting by the Cataloger OPEN procedure to assure proper volume mounting. Tapes may also be labeled and checked as a user option.

Of particular note, SPAM always assumes that an end-of-file (EOF) immediately follows the last record written in a new file, and it prohibits reading beyond that EOF. Contaminated tracks allocated to new files cannot be read until they are first written. The act of writing advances the EOF and the user simultaneously over-writes the classified residue with his own data. The user cannot skip over the EOF, and the EOF location is itself protected in the job environment area.

#### 4. Tape Residue

No special features for tape residue control are implemented in ADEPT. Tape residue control is easily satisfied by manual, off-line tape degaussing prior to ADEPT use.

### System files

Equation (28) led us to examine Private, Semi-Private, and Public files. ADEPT possesses two additional file privacies that transcend our model; both are system files. Privacy-4 system files are the need-to-know lists created by the Cataloger itself for Semi-Private files. Privacy-5 system files are private system memory for the SYSLOG files and the catalogs themselves.

Access to these files is restricted to the system only. Special access checks are made that differ from those of equations (25) and (26). First, a special *userid* is required that is not a member of *U* (i.e., not in the SYSLOG file). Second, the program making the OPEN call must be in Supervisor state. Third, the program making the OPEN call must be a member of a short list of EXEX programs. The list is built into the Cataloger at the time of compilation. In this manner, access to system files is severely restricted, even to system programs.

### Security service commands

ADEPT provides a variety of service commands that involve security control. The commands are listed in Table III. Note that commands VARYON, VARYOFF, REPLACE, LISTU, AUDIT, AUDOFF, and WRAPUP are restricted to a particular terminal—the Security Officer's Station.

TABLE III—Security service commands

Command	Purpose
AUDIT*	Turns on security audit recording.
AUDOFF*	Turns off security audit recording.
CHANGE	Enables the owner of a file to change any of the access control information of the file.
CREATE	Enables a user to create a Semi-Private file and its need-to-know list.
LISTU*	Lists by <i>terminal:id</i> all the current logged in <i>user:ids</i> .
RECLASS	Enables a user to raise or lower his job clearance between the bounds of the original LOGIN and current high-water mark clearance.
RELOG	Like LOGIN, but reconnects a user to an already existing job, as when a remote terminal drops off the communications line.
REPLACE*	Enables a user to move his job to another terminal or to reclassify a given device.
SECURITY	Print on the user's terminal approximately every 100 lines (or only by request) the job high-water mark (or clearance by request) as a reminder to the user and as a classification stamp of the level of current security activity.
VARYON/VARYOFF*	Permits terminals to be varied on- and off-line for flexibility in system maintenance and configuration control.
WRAPUP*	Shuts down system after a specified elapsed time.

\* Restricted to Security Officer's Station only.

**Audit**

The AUDIT function records certain transactions relating to files, terminals, and users, and is the electronic equivalent of manual security accountability logs. Its purpose is to provide a record of user access in order to determine whether security violations have occurred and the extent to which secure data has been compromised. The AUDIT function may be initiated only at start-up time, but may be terminated at any time. All data are recorded on disc or tape in real time so the data is safe if the system malfunctions. An auxiliary utility program, AUDLIST, may be used to list the AUDIT file. The information recorded is shown in Table IV.

Implementation of AUDIT is quite straightforward, a product of general ADEPT recording and instrumentation.<sup>18,19</sup> AUDIT is an EXEX component that is called by, and at the completion of, each function to be recorded. The information to be recorded is passed to AUDIT in the general registers. Additional I/O overhead is the primary cost incurred in the operation of AUDIT, for swapping and file maintenance. This cost is nominal, however, amounting to less than one percent of the CPU time.

**SUMMARY**

In summary we may ask: How well have we met our goals? First, we believe we have developed and success-

TABLE IV—Security events and information audited by ADEPT-50

EVENT	TIME	STATUS	JOB SECURITY PROFILE	USER SECURITY PROFILE	ACCOUNT NUMBER	USER: ID	TERMINAL: ID	CPU TIME	NEW TERMINAL	TERMINAL SECURITY PROFILE	FILE NAME	FILE OWNER ID	FILE FORM PROFILE	FILE SECURITY PROFILE	FILE VOLUME NUMBER	PROSE CATEGORY NAMES
LOGIN		X	X	X	X	X	X	X	X							
LOGOUT		X	X							X						
OPEN FILE		X	X										X	X	X	X
REOPEN <sup>1</sup> FILE		X	X										X	X	X	X
CHANGE FILE		X	X										X	X	X	X
CLOSE FILE		X	X										X	X		X
DELETE FILE <sup>1</sup>		X	X										X	X		X
RECLASS		X	X	X												
REPLACE		X	X						X		X	X				
DEVICE LIST <sup>2</sup>		X										X				
CATEGORY DICTIONARY <sup>3</sup>		X														X
RESTART <sup>4</sup>		X														
WRAPUP <sup>5</sup>		X														

<sup>1</sup> This is the "OPEN existing file" command.  
<sup>2</sup> A list of all the terminal devices and their assigned security and categories is recorded at each system load.  
<sup>3</sup> A list of the prose category names is recorded at each system load.  
<sup>4</sup> Whenever the system is restarted on the same day (and AUDIT had been turned on earlier that day) the time of the restart is recorded.  
<sup>5</sup> The time that the AUDOFF action was taken, or the time that the WRAPUP function called AUDIT, to terminate the AUDIT function.

fully demonstrated a security control mechanism that more than adequately supports heterogeneous levels and types of classification. Of note in this regard is the LOGIN decision procedure, access control tests, job umbrella, high-water mark, and audit trails recording. The approach can be improved in the direction of more compartments (on the order of 1000 or more), extension of the model to include system files, and the implementation of a single Franchise test for all security objects. The implementation needs redundant encoding and error detection of security profile data to increase confidence in the system—though we have not ourselves experienced difficulty here. The increase in memory requirements to achieve these improvements may force numerical encoding of security data, particularly Category, as suggested by Peters.<sup>7</sup>

Second, SYSLOG has been highly successful in demonstrating the concept of "security arming" of the system at start-up time. Our greatest difficulty in this area has been with the human element—the computer operators—in preparing and handling the control deck. In opposition to Peters,<sup>7</sup> we believe the operator should not be "designed out of the operation as much as possible," but rather his capabilities should be upgraded to meet the greater levels of sophistication and responsibility required to operate a time-sharing system.<sup>20</sup> He should be considered part of line management. ADEPT is oriented in this direction and work now in progress is aimed at building a real-time security surveillance and operations station (SOS).

Third, we missed the target in our attempt to isolate and limit the amount of critical coding. Though much of the control mechanism is restricted to a few components—LOGIN, SYSLOG, CATALOGER, AUDIT—enough is sprinkled around in other areas to make it impossible to restrict the omnipotent capabilities of the monitor, e.g., to run EXEX in Problem state. Some additional design forethought could have avoided some of this dispersal, particularly the wide distribution in memory of system data and programs that set and use these data. The effect of this shortcoming is the need for considerably greater checkout time, and the lowered confidence in the system's integrity.

Lastly, on the brighter side, we were surprisingly frugal in the cost of implementing this security control mechanism. It took approximately five percent of our effort to design, code, and checkout the ADEPT security control features. The code represents about ten percent of the 50,000 instructions in the system. Though the code is widely distributed, SYSLOG, security commands, LOGIN, AUDIT, and the CATALOGER account for about 80 percent of it. The overhead cost of

operating these controls is difficult to measure, but it is quite low, in the order of one or two percent of total CPU time for normal operation, excluding SYSLOG. (SYSLOG, of course, runs at card reader speed.) The most significant area of overhead is in the checking of I/O channel programs, where some 5 to 10 msec are expended per call (on the average). Since this time is overlapped with other I/O, only CPU bound programs suffer degradation. AUDIT recording also contributes to service call overhead. In actuality, the net operating cost of our security controls may be zero or possibly negative, since AUDIT recordings showed us numerous trivial ways to measurably lower system overhead.

#### ACKNOWLEDGMENTS

I would like to acknowledge the considerable encouragement I received in the formative stages of the ADEPT security control design from Mr. Richard Cleaveland, of the Defense Communications Agency (DCA). I would like to thank Mrs. Martha Bleier, Mr. Peter Baker, and Mr. Arnold Karush for their patient care in designing and implementing much of the work I've described. Also, I wish to thank Mr. Marvin Schaefer for assisting me in set theory notation. Finally, I would like to applaud the ADEPT system project personnel for designing and building a time-sharing system so amenable to the ideas discussed herein.

#### REFERENCES

- 1 A HARRISON  
*The problem of privacy in the computer age: An annotated bibliography*  
RAND Corp Dec 1967 RM-5495-PR/RC
- 2 L J HOFFMAN  
*Computers and privacy: A survey*  
Stanford Linear Accelerator Center Stanford Univ Aug 1968 SLAC-PUB-479
- 3 H E PETERSEN R TURN  
*System implications of information privacy*  
Proc SJCC Vol 30 1967 291-300
- 4 W H WARE  
*Security and privacy in computer systems*  
Proc SJCC Vol 30 1967 279-282
- 5 W H WARE  
*Security and privacy: Similarities and differences*  
Proc SJCC Vol 30 1967 287-290
- 6 R LINDE C WEISSMAN C FOX  
*The ADEPT-50 time-sharing system*  
Proc FJCC Vol 35 1969 Also issued as SDC Doc SP-3344
- 7 B PETERS  
*Security considerations in a multi-programmed computer system*  
Proc SJCC Vol 30 1967 283-286
- 8 RYE CAPRI COINS OCTOPUS SADIE Systems

- NOC Workshop National Security Agency Oct 1968
- 9 H W BINGHAM  
*Security techniques for EDP of multi-level classified information*  
Rome Air Development Center Dec 1965 RADC-TR-65-415
- 10 R M GRAHAM  
*Protection in an information processing utility*  
ACM Symposium on Operating Systems Principles Oct 1967 Gatlinburg Tenn
- 11 L J HOFFMAN  
*Formularies--Program controlled privacy in large data bases*  
Stanford Univ Working Paper Feb 1969
- 12 D K HSIAO  
*A file system for a problem solving facility*  
Dissertation in Electrical Engineering Univ of Pa 1968
- 13 J I SCHWARTZ C WEISSMAN  
*The SDC time-sharing system revisited*  
Proc ACM Conf 1967 263-271
- 14 P BARAN  
*On distributed communications: IX, security, secrecy, and tamper-free considerations*
- RAND Corp Aug 1964 RM-3765-PR
- 15 C WEISSMAN  
*Programming protection: What do you want to pay?*  
SDC Mag Vol 10 No 8 Aug 1967
- 16 J P TITUS  
*Washington commentary--Security and privacy*  
CACM Vol 10 No 6 June 1967 379-380
- 17 I ENGER et al  
*Automatic security classification study*  
Rome Air Development Center Oct 1967 RADC-TR-67-172
- 18 A KARUSH  
*The computer system recording utility: Application and theory*  
System Development Corp March 1969 SP-3303
- 19 A KARUSH  
*Benchmark analysis of time-sharing systems: Methodology and results*  
System Development Corp April 1969 SP-3343
- 20 R R JINDE P E CHANEY  
*Operational management of time-sharing systems*  
Proc 21st Nat ACM Conf 1966 149-159

# The ADEPT-50 time-sharing system

by R. R. LINDE and C. WEISSMAN

*System Development Corporation*  
Santa Monica, California

and

C. E. FOX

*King Resources Company*  
Los Angeles, California

## INTRODUCTION

In the past decade, many computer systems intended for operational use by large military and governmental organizations have been "custom made" to meet the needs of the particular operational situation for which they were intended. In recent years, however, there has been a growing realization that this design approach is not the best method for long term system development. Rather, the development of general purpose systems has been promoted that provide a broad, general base on which to configure new systems. The concepts of time-sharing and general-purpose data management have been under development for several years, particularly in university or research settings.<sup>1,2,3</sup> These methods of computer usage have been tested, evaluated, and refined to the point where today they are ready to be exploited by a broad user community.

Work on the Advanced Development Prototype (ADP) contract was begun in January 1967 for the purpose of demonstrating—in an operational environment—the potential of automatic information-handling made possible by recent advances in computer technology, particularly advances in time-sharing executives and general-purpose data management techniques. The result of this work is a large-scale, multi-purpose system known as ADEPT, which

operates on IBM system 360 computers.\*

The entire ADEPT system is now being used at four field installations in the Washington, D. C. area, as well as at SDC in Santa Monica. The system was installed at the National Military Command System Support Center in May 1968, at the Air Force Command Post in August 1968, and at two other government agencies in January 1969. These four field sites collectively run ADEPT from 80 to 100 hours per week, providing a total of some 2000 terminal hours of time-sharing service monthly to their users.

The ADEPT system consists of three major components: a time-sharing executive; a data management system adapted from SDC's Time-Shared Data Management System (TDMS) described by Bleier,<sup>4</sup> and a programmer's package. This paper deals exclusively with the ADEPT Time-Sharing Executive, and particularly with the more novel aspects of its architecture and construction. Before examining these aspects it will be instructive if we review the basic design and hardware configuration of the system.

### *A general purpose operating system*

The ADEPT executive is a general-purpose time-

---

\* Development of ADEPT was supported in part by the Advanced Research Projects Agency of the Department of Defense.

sharing system. The system operates on a 360 Model 50 with approximately 260,000 bytes of core memory, 4 million bytes of drum memory, and over 250 million bytes of disc memory, shown graphically in Figure 1 and schematically in the appendix. With this machine configuration, ADEPT is designed to provide responsive on-line interactive service, as well as background service to approximately 10 concurrent user jobs. It handles a wide variety of different, independent application programs, and supports the use of large random-access data files. The design—basically a swapping system—provides for flexibility and expansion of system functions, and growth to more powerful models in the 360 family.

ADEPT functions both as a batch processor (whereby jobs are accumulated and fed to the CPU for operation one by one) and as an interactive, on-line system (in which the user controls his job directly in real time simply by typing console requests).

Viewed as a batch system, ADEPT allows jobs to be submitted to console operators or submitted from consoles via remote batch commands (remote job entry). In either case, jobs are "stacked" for execution by ADEPT in a first-in/first-out order. The stack is serviced by ADEPT as a background task, subject to the priorities of the installation and the demands of "foreground" interactive users. Viewed as an interactive system, ADEPT allows the user to work with a typewriter, allowing computer-user dialog in real time. Via ADEPT console commands, the user identifies himself, his programs, and his data files, and selectively controls the sequence and extent of operation of his job in an ad lib manner. A prime advantage of the interactive use of ADEPT is that the system provides an extendable library of service programs that permit the user to edit data files, compile or assemble programs, debug and eliminate program errors, and generally manage large databases in a responsive on-line manner.

#### System architecture

The architecture of the ADEPT executive is that of the "kernel and the shell". The "kernel," referred to as the Basic Executive (BASEX), handles the major problems of allocating and scheduling hardware resources. It is small enough to be permanently resident in low core memory, permitting rapid response to urgent tasks, e.g., interrupt control, memory allocation, and input/output traffic. The "shell," referred to as the Extended Executive (EXEX), provides the interface between the user's application program and the "kernel". It contains those non-urgent, large-

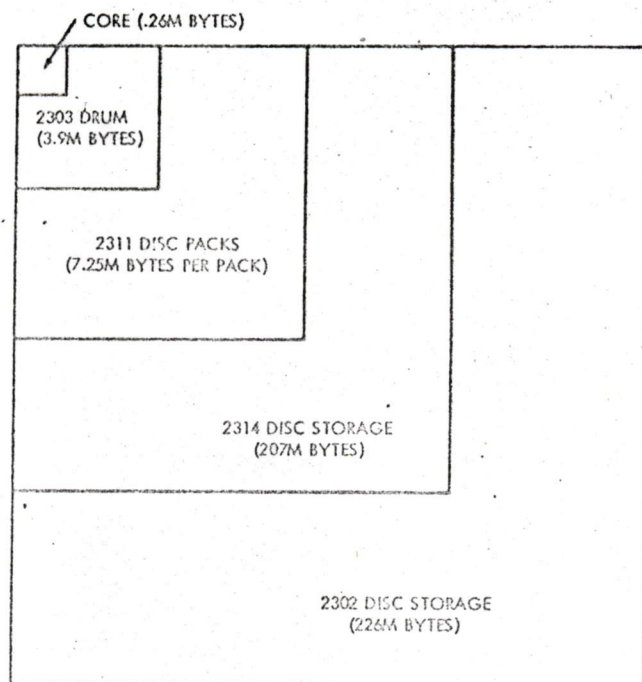


Figure 1—Relative capacity of various ADEPT direct-access storage media available in less than 0.2 seconds. The initial system that operates at SDC utilizes core, 2303 drum, 2311 and 2314 disc packs, and 2302 disc storage. The NMCSSC system utilizes 2314 disc storage in lieu of 2311 or 2302 discs. The architecture of the ADEPT executive is such that it permits any combination of the above types of disc storage in varying amounts.

task extensions of the basic "kernel" processes that are user-oriented rather than hardware-oriented; they may, therefore, be scheduled and swapped.

The version of the ADEPT time-sharing system, thus far developed has multiple levels of control beyond the two-level "kernel-shell" structure—i.e., it can be thought of figuratively as an "onion skin". Figure 2 shows these relationships graphically.

Beyond EXEX, "object systems" may exist as subsystems of ADEPT (developed by the user community without modification to EXEX or BASEX), thus further distributing and controlling the system resources for the object programs that form still another level of the system. The design ideas embodied in ADEPT parallel those of Dijkstra,<sup>5</sup> Corbato,<sup>6</sup> and Lampson,<sup>7</sup> but differ in techniques of implementation.

The ADEPT Basic Executive operates in the lower quarter of memory, thereby providing three quarters of memory for user programs. With the current H core configuration, ADEPT preempts the first 65,000 bytes of core memory, the bulk of which is dedicated to BASEX; EXEX must then operate in user memory

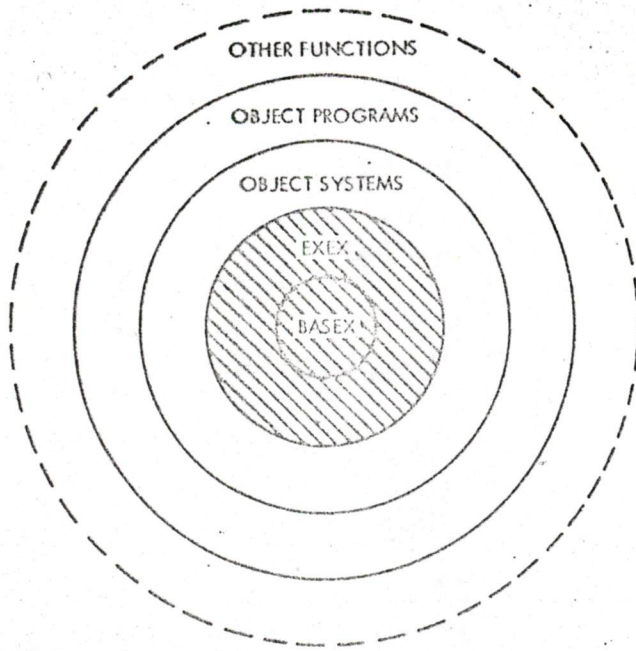


Figure 2—Multiple levels of control in ADEPT

in a fashion similar to user programs. ADEPT is designed to operate itself and user programs as a collection of 4096-byte pages. BASEX is identified as certain pages that are fixed in main storage and that cannot be overlaid or swapped. EXEX and other programs are identified as sets of pages that move dynamically between main storage and swap storage (i.e., drum). It is necessary to maintain considerably more descriptive information about these swappable programs than about BASEX. This descriptive information is carried in a set of system tables that, at any point in time, describe the current state of the system and each program.

ADEPT views the user as a job consisting of some number of programs (up to four for the 360/50H configuration) that were loaded at the user's request. These programs may be independent of one another or, with proper design, different segments of a larger task. Implicitly, EXEX is considered to be one of these programs. To simplify system scheduling, communication, and control, only one program in the user's set may be active (eligible to run) at a time. When ADEPT scheduling determines that a job may be serviced, the current job in core is saved on swap storage, and the active program of the next job is brought into core from swap storage and executed for a maximum period of time, called a quantum. The process then repeats for other jobs. Figures 3 and 4 schematically depict these relationships.

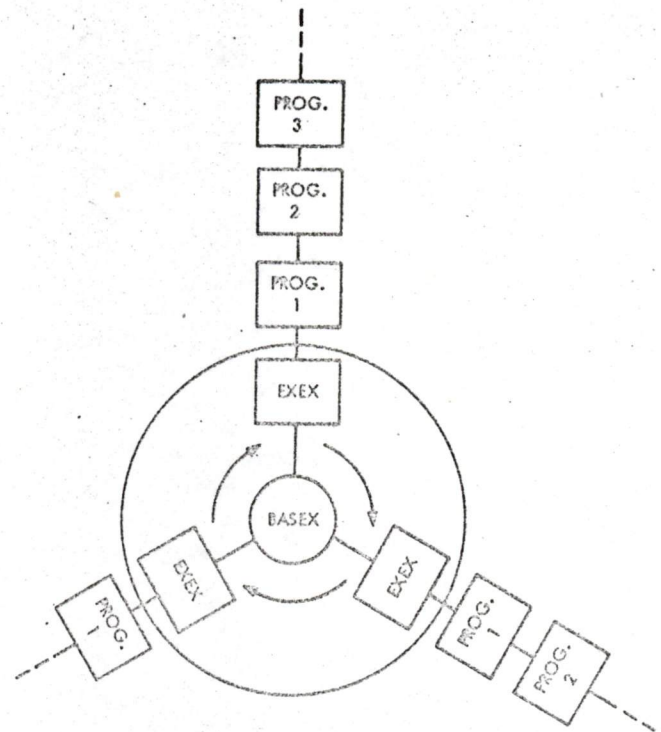


Figure 3—Simple commutation of users programs. This figure illustrates the relationship between users programs' EXEX and BASEX. Each spoke represents a user's job, with his EXEX providing the interface between BASEX and the hardware resources. The maximum number of interactive job the IBM 360/50H configuration is ten.

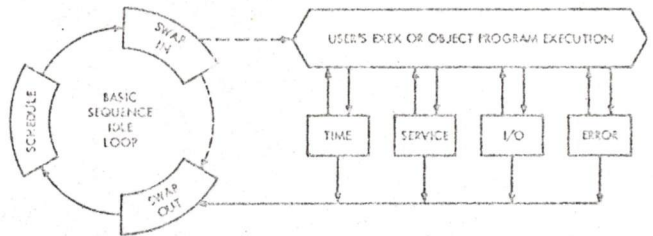


Figure 4—ADEPT's basic sequence of operation. This figure shows the basic operating system cycle: idle loop is interrupted by an external interrupt (an activity request); a program is scheduled, swapped into core from the drum, and executed. escape from the execution phase occurs when quantum termination condition (e.g., time expiration, service or I/O call, error condition) is met; the program is then swapped out and control is returned to the idle loop (if no other programs are eligible to be scheduled).

### Basic executive (BASEX)

Table I lists the BASEX components and their general functions as of the eighth and latest executive release. These basic system components form an integrated, non-reentrant, non-relocatable, perma-



nently-resident, core memory package 16 pages long (each page is 4096 bytes). They are invoked by hardware interrupts in response to service requests by users of terminals and their programs. Note the division of input/output control into cataloged (SPAM and IOS), terminal (TWRI), and drum (BEXEC) activities to permit local optimization for improved system performance.

TABLE I—Basic executive components

<i>Component</i>	<i>Function</i>
ALLOC	Drum and core memory allocation.
BXBUG	Debugger for executive programs.
BEXEC	Basic sequence and swap control.
BXECsvc	SVC handlers for WAIT, TIME, DEVICE, STOP AND DISMISS calls.
EXEX	Linkage routines for EXEX (BASEX/EXEX interfaces); also services commands DIALOFF, DIALON.
INTRUP	First-level interrupt control.
IOS	Channel-program level input/output supervisory control.
RECORD	Records SVC, interrupt activity in BASEX.
SKED	Scheduler.
SPAM	Input/output access methods to cataloged storage.
TWRI	Terminal input/output control.
System Tables	Resident system data areas for communication table (COMTAB), logged-in user's table (JOB), loaded programs table (PQU), drum and core status tables (DSTAT, CSTAT), and a variety of other tables.

#### Extended executive (EXEX)

Unlike the tight, closed package of integrated BASEX components, EXEX is a loose, open-ended collection of semiautonomous programs. Table II lists this collection of programs. EXEX is treated by BASEX as a user program, with certain privileges, and each user is given his own "copy" of the EXEX. It is transparent to the user that EXEX is reentrant

TABLE II—Extended executive components

<i>Component</i>	<i>Function</i>
AUDIT	Maintains a real-time recording of all security transactions as an accountability log.
BMON	Batch monitor for control of background job execution.
CAT	Cataloger for file storage access control; also services FORGET command.
DTD	Transfers recording information from drum to disc.
DBUG	Debugger for non-executive (user) programs.
LOGIN	User authentication and job creation.
SERVIS	Library of service commands that are reentrant, interruptible and scheduled: APPEND, CHANGE, CREATE, CYLS, DELETE, DRIVES, INIT, LISTF, LISTU, LOAD, LOADD, LOAD and GO, OVERLAY, REPLACE, RESTORE, RESTORED, SAVE, SEARCH, VARYOFF, VARYON.
RUN	Remote batch job submission control servicing commands RUN and CANCEL.
XXTOO	Library of small, fast, executive service commands: CPU, BGO, BQUIT, BSTOP, DIAL, DRUMS, GO, LOGOUT, QUIT, RESTART, SKED, SKEDOFF, STATUS, STOP, TIME, USERS.
SYSDEF	Defines input/output hardware configuration at time of system start up.
SYSLOG	Defines authorized user/terminal security profiles at time of system start up.
TEST	Initializes system tables at time of system start up.
SYSDATA	Non-resident, shared, system data table for dial messages and other common data, e.g., lists of all logged-in users; other non-resident, job-specific tables also exist, e.g., job environment page, push-down list data page.

and is being shared with other users, except for its data space. Each job has its own "machine state" tables saved in its unique set of environment pages. This structure permits flexible modification and orderly system expansion in a modular fashion. EXEX is always scheduled in the same way as other user programs.

Though EXEX components are, in large part, non-self-modifying reentrant routines and thus, could at small cost, be relocatable; neither user programs nor EXEX components are relocated between swaps. The lack of any mapping hardware on the IBM 360/50 and the design goal and knowledge that most user programs would be of maximum size made unnecessary a software provision to relocate programs dynamically. User programs may be relocated once at load time, however.

#### *Communication and control techniques used in ADEPT*

Communication is the generic term used to cover those services that permit two (or more) programs to inter-communicate, be they system program, user program, or both. From this communication vantage point we shall examine the connective mechanism used between the Basic and Extended Executives; the techniques that allow components within the EXEX to make use of one another; and the system design that permits an object program to control its own behavior as well as to communicate with the system and with other object programs.

#### *The ADEPT job or process*

Before we discuss the system mechanics, let us examine how the system treats each user logically. A user in the system is assigned a job number. Each job in the system may be viewed as a separate *process*, and each process is, by definition, independent of all other processes running on the machine. A process—or job—is not a program. It is the logical entity for the execution of a program on the physical processor, and it may contain as many as four separate programs. A program consists of the set of machine instructions swapped into the processor for execution, and the Extended Executive is one of these programs.

The ADEPT executive requires a large number of system tables to permit Basic and Extended Executive communication. Conceptually, the use of descriptive tables defining the condition of a user's process is analogous to the state vector (or state word) discussed by Lampson and Saltzer.<sup>5,9</sup> That is, the collection of information contained by these tables is

sufficient to define an inactive user's process state at any given moment. By resetting the central processor from the state vector, a user's job proceeds from an inactive to an active state as if no interruption had occurred. The state vector contains such items as the program counter, the processor's general registers, the core and drum map of all the programs in the job, and the peripheral storage file data. All of the collective data for each program or task in the process are contained in the state vector.

#### *Basic and extended executive communication*

Each ADEPT user (i.e., any person who initiates some activity within the system by typing in commands) is given a job number and assigned an entry in the JOB table. The JOB table contains the system's top-level bookkeeping on user activity. It contains the user's identification, his location, his security clearance, and a pointer to his program queue. Each user is assigned one entry, or JOB, in the table. Associated with each JOB are the one or more programs that the user is running.

Top-level bookkeeping on programs is contained in the Program Queue (PQU) table. Each PQU entry contains a program identification and some (but not all) information that describes that program in terms of its space requirements, its current activity, its scheduling conditions, and its relationship to other programs in the PQU that belong to the same JOB. The detailed descriptive information and the status of each JOB and its programs are carried in the swappable environment space.

The environment pages (there can be as many as four) comprise a number of separate tables that contain such information as the contents of the general registers, the swap storage page numbers where the balance of the program resides, the program map, and lists of all active data files. A single environment page (or pages) is shared by all programs that belong to the same JOB (user). The system design allows for environment page overflow at which time additional pages are assigned dynamically. The environment pages, PQU table, JOB table, and data pages comprise the state vector of the user's job.

To permit storage of "global" system variables, and to allow system components to reference system data that may be periodically relocated, there exists a system communication table, which resides in low core so that it can be referenced without loading a base register.

The IBM 360 supervisor call (SVC) is used exclu-

sively by EXEX components and object programs to request BASEX services. Though additional overhead is incurred in the handling of the attendant interrupt, the centralization of context switching provided is of considerable value in system design, fabrication, and checkout.

**Extended executive communication**

An EXEX may make use of another EXEX function by use of the SVC call mechanism. To support the recursive EXEX, an additional SVC processing routine is required to manage the different recursive contexts. This routine, called the SVC Dispatcher, processes calls from user and EXEX functions alike, manages a swappable data page, and switches to an interface linkage routine. The data page contains a system communication stack that consists of a program's general registers and the Program Status Word at the time of the SVC. This technique is analogous to the push-down logic of recursive procedure calls found in ALGOL or LISP language systems. The stack provides a convenient means of passing parameters between routines in the EXEX. Since each job has its own unique data page and environment page, EXEX is both recursive and reentrant.

The environment status table (ESTAT) contains the swap and core location for each component in the EXEX and for each program in the job. It resides in the job environment page. When an EXEX service is requested, only that particular EXEX program is brought in from swap storage, rather than the full service library. The interface linkage routine provides this management function; it lies as a link between the SVC Dispatcher and the particular EXEX function. The interface routine picks up necessary work pages for the EXEX component involved and branches to that component after it is brought into core. The interface routine maintains a separate push-down stack of return addresses providing the means for the EXEX component to properly exit and return control to its interface routine and then to the system.

The EXEX component called may make additional EXEX SVC calls before exiting. To provide correct work page allocation during recursive calls, the interface routine also saves the work page core and drum page addresses in the push-down stack. Upon completion of a call, the EXEX component returns to its interface routine; the interface routine releases all allocated work pages to the system and branches to a common unwind procedure.

The unwind procedure, like the SVC Dispatcher, is simply a switching mechanism. It determines, via

the stack, whether to return to a still higher level EXEX function, or to turn the EXEX off and exit to the Basic Sequence. This recursive/reentrant control is the most complex portion of ADEPT and is the "glue" that binds BASEX and EXEX together. Figure 5 illustrates the recursive process.

**Object program communication**

One of the more stringent services required of an operating system is the rapid interchange of large quantities of data between object programs. The interchange of even simple arrays, matrices, and tables via stack parameters or a common file suffers from the inadequacy of limited capacity or extensive I/O time. Many operating systems ignore this requirement, thereby restricting the general-purpose applications. Yet there are solutions to this problem, and one successful technique employed in the ADEPT system is that of "shared memory". Shared memory is achieved by using the basic mechanism for managing reentrancy, namely the program environment page map. Through the ADEPT SHARE Page call, an object program can request that designated pages of another program

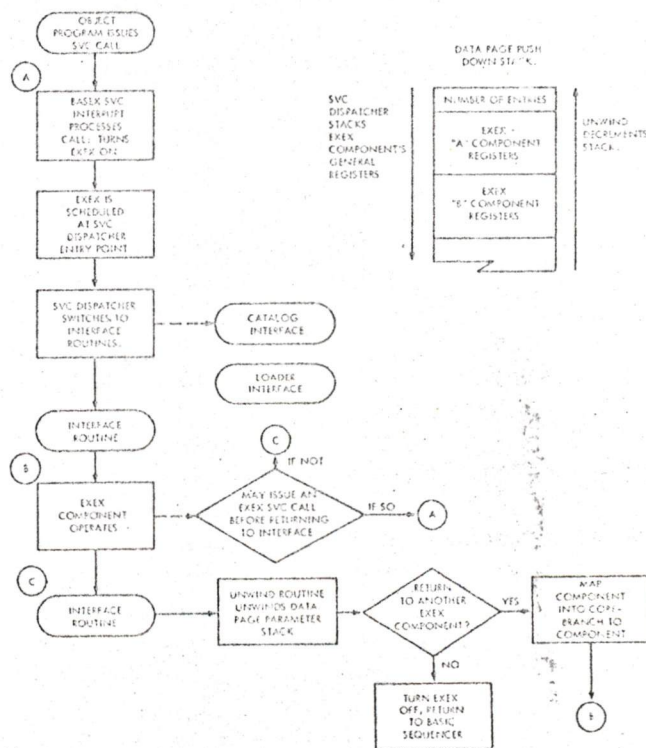


Figure 5—Block diagram of EXEX behavior and control

in the job be added to its map. If core page numbers are passed as parameters in various service calls, whole pages of data may be passed between programs. EXEX and many object programs operating under this system use this method for inter-program communication.

ADEPT operating on the IBM 360/50H restricts its user programs to 46 active core pages. However, by utilizing the GETPAGE call, an object program may acquire up to 128 drum pages and may subsequently activate and deactivate various page sets by utilizing another service call, ACTDEACT (activate/deactivate). This scheme permits bulk data from disc storage to be placed on drum and operated upon at "swap" speeds. Thus skilled system users can achieve efficient use of time and memory by managing their own "paging". We consider this the best alternative considering the questionable state of other, automatic paging algorithms.<sup>10,11,12,13</sup> Most EXEX components use these calls for just such purposes. For example, the interface routines mentioned above use activate calls to "turn on" called components of the EXEX.

The Allocator component of ADEPT manages the page map for each program. This software map reflects the correspondence between drum and core pages, established initially by the SERVIS (service) component at load time. The Allocator's function is to inventory available core and drum pages by maintaining two resident system tables: one for core, the other for drum. Whenever drum pages are released or obtained, the Allocator updates the page map in the job's environment page. The Allocator processes the SHARE (page), GETPAGE, FREEPAGE, and ACTDEACT calls from EXEX and object programs. SERVIS allows a program at run time to add data pages or to overlay program segments from disc or tape. In so doing, SERVIS makes use of the various Allocator calls.

### Simulating console commands

An important attribute of ADEPT time-sharing is that nearly all the functions and services that can be initiated at the user's console can also be called forth within a user's program. A program designer can, for example, build a system of programs, which can operate in batch mode under the control of a program by issuing internal commands in much the same manner as the user sitting at the console. With this approach, the ADEPT batch monitor controls background tasks by simulating user terminal requests. Batch requests can be enqueued by users from any

console and then processed in turn by this supervisor function.

### Armed interrupts and rescue function

The basic design of ADEPT conveniently provides for processing object program "armed" interrupt calls. This means that an object program is able to conditionally start (wakeup) and stop (sleep) the execution of its own programs, and others as well. The conditions for employing wakeup calls include too much elapsed time, or the occurrence of unpredictable but anticipated events, e.g., errors and other program calls. In "arming" these "software-interrupt" conditions by object program calls, the program entry point(s) for the various conditions are specified. When such conditions occur, the operating system transfers to the specified entry point and gives the appropriate condition code. (Note that if we take this call one step further, and permit one object program to arm the software and hardware interrupts of another object program, we have the basic control mechanism necessary to permit the operation of "object systems," i.e., subexecutives—another level in the "onion skin" of ADEPT control.)

User programs interface with the ADEPT system primarily via the supervisor call (SVC) instruction; a secondary interface is provided via the program check interrupt that protects the program and system after various error conditions. The executive design allows user programs to trap all such interfaces with the system via its rescue arming mechanism. This means that one program can trap and get first-level control of all occurrences of SVC's and program checks within a single job. This mechanism also means, then, that the responsibility and meaning for these interfaces can be redefined at the user program level.

As of this writing, this mechanism is being employed to construct object systems for an improved batch monitor, an interface for the proposed ARPA Network,<sup>14</sup> and to experiment with automatic translators for compatibility with other operating systems. Other uses include improvements in program recovery in a variety of user tools, e.g., compiler diagnostics.

### Resource allocation, access, and management

ADEPT system design, of course, includes a complete set of resource controls that monitor secondary storage devices.

### The cataloger

The Cataloger, an EXEX component, is functionally analogous to the core/drum Allocator, but is used for devices accessible by user programs. It maintains an inventory of all assignable storage devices, assigns unused storage on the devices, maintains descriptions of the files placed on these devices, controls access to these files, and—upon authorized request—deletes any file. Specifically, the Cataloger:

- Assigns storage on 2302, 2311 and 2314 discs.
- Assigns tape drives.
- Locates an inventoried file by its name and certain qualifiers that uniquely identify the file.
- Issues tape or disc pack mounting instructions to the operator when necessary.
- Verifies the mounting of labeled volumes.
- Passes descriptive information to the user program opening a file.
- Allows the user of a file to request more storage for the file.
- Denies unauthorized users access to files.
- Returns assigned storage to available storage whenever a file is deleted.
- Maintains a table of contents on each disc volume.

As the largest single component of the ADEPT Executive (65,000 bytes), the Cataloger was written in a new, experimental programming language called MOL-360 (Machine-Oriented Language for the 360).<sup>15</sup> It is a "higher-level machine language" developed under an ARPA-sponsored SDC research project on metacompilers. It resolved the dilemma involving our desire for higher-level source language and our need to achieve flexibility with machine code. The Cataloger design and checkout, enhanced by the use of MOL-360, showed simultaneously the validity of MOL compilers for difficult machine-dependent programming.

### The SPAM component

SPAM is a BASEX component that permits symbolic, user-oriented I/O. It can be viewed as a special-purpose compiler that compiles symbolic user program I/O calls into 360 channel programs, and delivers them to the Input/Output Supervisor (IOS) for execution via the EXCP (execute channel program) call. The

results of EXCP for the call are "interpreted" by SPAM and returned to the user program as status information. As such, SPAM represents a more symbolic I/O capability than the EXCP level. It provides a relatively simple method for executing the operations of reading, writing, altering, searching for, and positioning records within ADEPT cataloged and controlled disc-based and tape-based file structures.

### Resource management

As of this writing, the computer operator has a set of commands at his disposal that allow him to control the system resources. Various privileged on-line commands enable him to monitor the terminal activities of system users and to control assignment and availability of storage devices. However, there is an increasing need for a "manager" to be given more latitude in dynamically controlling the system resources and observing the status of system users, particularly because ADEPT was designed to handle sensitive information in classified government and military facilities. To meet these objectives, a design effort is under way that gives the computer operator system-manager status, with the ability to observe and control the actions of system users. The result will be a program that encompasses some of the management techniques reported by Linde and Chaney<sup>16</sup> tailored to present needs.

### Swapping and scheduling user programs

Most of the programs that run under ADEPT occupy all of the core memory that is not used by the resident Basic Executive (46 pages on the 360/50H). If the set of needed pages could be reduced considerable reduction in swap overhead could be expected. One way to achieve this is to mark for swap-out only those pages that were changed during program execution. The hardware needed to automatically mark changed pages is unavailable for the 360/50; however, through use of the store-protect feature on the Model 50, ADEPT software can simulate the effect and produce noteworthy savings in swap time.

### Page marking

Whenever a user program is swapped into core, its pages are set in a read-only condition. As the program executes, it periodically attempts to store data (write) in its write-protected pages. The resulting interrupt is fielded by the system. After satisfying itself that the store is legal for the program, the executive marks the target page as "written," turns off write-protect

for that page, and resumes the program's execution. The situation repeats for each additional page written. At the completion of the program's time slice, the swapper has a map of all the program pages that were changed (implied in the storage keys with no write protection). Only the changed pages are swapped out of core. Measurement of this scheme shows that about 20 percent of the pages are changed; hence, for every five pages swapped in, only one need be swapped out, for a total swap of six pages, rather than the full swap of ten pages (five in, five out). The scheme makes the drum appear to be 40 percent faster.

The use of the storage protection keys is based on the functional status of each page rather than on some user identity. User programs always run with a program status word key of one, and the bits in the storage key associated with the programs start out at zero. After a page has been initially changed, its key is set to one also. The other bits in the key are used to indicate: first, a page is transient, not yet completely moved to or from swap storage; second, a page is unavailable, i.e., it belongs to someone else; third, a page is locked and cannot be swapped or changed; and finally, a page is fetch-protected because it may contain sensitive information.

#### Scheduling algorithm

The scheduling algorithm provides for three levels of scheduling. Jobs that are in a "terminal I/O complete" state get first preference in the schedule. Jobs in the second level, or background queue, are run if there are no level-one jobs to run. A job is placed in level two when the two-second quantum clock alarm terminates its operation two consecutive times. Compute and I/O-bound programs are treated alike. A level-two job—when allowed to run—is given quantum interval equal to the basic quantum time multiplied by the scheduling level (i.e.,  $2 \text{ sec} \times 2 = 4 \text{ sec}$ ). However, a level-two background job may be preempted after two seconds for terminal I/O. Any operation a level-two job makes that terminates its quantum prematurely will return the job to a level-one status. The batch monitor job is run when the first two queues are empty. User programs may be written to overlap execution and I/O activity. Our choice of scheduling parameters for quantum size, and number of service levels was selected empirically and as a result of prior experience.<sup>17</sup>

A command SKED, which is limited to the operator's terminal, has the effect of forcing top priority for a job (the job stays at level one all the time). Only

one job may run in this privileged scheduling state at a time.

#### Pervasive security controls

Integrated throughout the ADEPT executive are software controls for safeguarding security-sensitive information. The conceptual framework is based upon four "security objects": user, terminal, file, and job. Each of these security objects is formally identified in the system and is also described by a security profile triplet: Authority (e.g., TOP SECRET, SECRET), Need-to-Know Franchise, and Special Category (e.g., EYES ONLY, CRYPTO). At system initialization time, user and terminal security profiles are established by security officers via the system component SYSLOG. SYSLOG also permits the association of up to 64 passwords with each user. At LOGIN time, a user identifies himself by his unique name, up to 12 characters, and enters his private password to authenticate his identity. The LOGIN component of ADEPT validates the user and dynamically derives the security profile for the user's job as a complex function of the user and terminal security profiles. The job security profile is used subsequently as a set of "keys," used when access is made to ADEPT files. The file security profile is the "lock" and is under control of the file subsystem.

File access Need-to-Know is permitted for Private, Sem-Private, and Public use. With the CREATE command, a list of authorized users and the extent of their access authorization (i.e., read-only, write-only, read and write) can be established easily for Semi-Private files. Newly created files are automatically classified with the job's "high water mark" security triplet—a cumulative security profile history of the security of files referenced by the job. Through judicious use of the CHANGE command, these properties may be altered by the owner of the file.

Security controls are also involved in the control of classified memory residue. Software and hardware memory protection is extensively used. Software memory protection is achieved by interpretive, legality checking of memory bounds for I/O buffer transfers, legality checking of device addresses for unauthorized hardware access, and checks of other user program attempts to seduce the operating system into violating security controls.

The hardware protection keys are used to fetch-protect all address space outside the user program and data area. Also, newly allocated space to user programs is zeroed out to avoid classified memory residue.

for that page, and resumes the program's execution. The situation repeats for each additional page written. At the completion of the program's time slice, the swapper has a map of all the program pages that were changed (implied in the storage keys with no write protection). Only the changed pages are swapped out of core. Measurement of this scheme shows that about 20 percent of the pages are changed; hence, for every five pages swapped in, only one need be swapped out, for a total swap of six pages, rather than the full swap of ten pages (five in, five out). The scheme makes the drum appear to be 40 percent faster.

The use of the storage protection keys is based on the functional status of each page rather than on some user identity. User programs always run with a program status word key of one, and the bits in the storage key associated with the programs start out at zero. After a page has been initially changed, its key is set to one also. The other bits in the key are used to indicate: first, a page is transient, not yet completely moved to or from swap storage; second, a page is unavailable, i.e., it belongs to someone else; third, a page is locked and cannot be swapped or changed; and finally, a page is fetch-protected because it may contain sensitive information.

#### Scheduling algorithm

The scheduling algorithm provides for three levels of scheduling. Jobs that are in a "terminal I/O complete" state get first preference in the schedule. Jobs in the second level, or background queue, are run if there are no level-one jobs to run. A job is placed in level two when the two-second quantum clock alarm terminates its operation two consecutive times. Compute and I/O-bound programs are treated alike. A level-two job—when allowed to run—is given quantum interval equal to the basic quantum time multiplied by the scheduling level (i.e.,  $2 \text{ sec} \times 2 = 4 \text{ sec}$ ). However, a level-two background job may be preempted after two seconds for terminal I/O. Any operation a level-two job makes that terminates its quantum prematurely will return the job to a level-one status. The batch monitor job is run when the first two queues are empty. User programs may be written to overlap execution and I/O activity. Our choice of scheduling parameters for quantum size, and number of service levels was selected empirically and as a result of prior experience.<sup>17</sup>

A command SKED, which is limited to the operator's terminal, has the effect of forcing top priority for a job (the job stays at level one all the time). Only

one job may run in this privileged scheduling state at a time.

#### Pervasive security controls

Integrated throughout the ADEPT executive are software controls for safeguarding security-sensitive information. The conceptual framework is based upon four "security objects": user, terminal, file, and job. Each of these security objects is formally identified in the system and is also described by a security profile triplet: Authority (e.g., TOP SECRET, SECRET), Need-to-Know Franchise, and Special Category (e.g., EYES ONLY, CRYPTO). At system initialization time, user and terminal security profiles are established by security officers via the system component SYSLOG. SYSLOG also permits the association of up to 64 passwords with each user. At LOGIN time, a user identifies himself by his unique name, up to 12 characters, and enters his private password to authenticate his identity. The LOGIN component of ADEPT validates the user and dynamically derives the security profile for the user's job as a complex function of the user and terminal security profiles. The job security profile is used subsequently as a set of "keys," used when access is made to ADEPT files. The file security profile is the "lock" and is under control of the file subsystem.

File access Need-to-Know is permitted for Private, Semi-Private, and Public use. With the CREATE command, a list of authorized users and the extent of their access authorization (i.e., read-only, write-only, read and write) can be established easily for Semi-Private files. Newly created files are automatically classified with the job's "high water mark" security triplet—a cumulative security profile history of the security of files referenced by the job. Through judicious use of the CHANGE command, these properties may be altered by the owner of the file.

Security controls are also involved in the control of classified memory residue. Software and hardware memory protection is extensively used. Software memory protection is achieved by interpretive, legality checking of memory bounds for I/O buffer transfers, legality checking of device addresses for unauthorized hardware access, and checks of other user program attempts to seduce the operating system into violating security controls.

The hardware protection keys are used to fetch-protect all address space outside the user program and data area. Also, newly allocated space to user programs is zeroed out to avoid classified memory residue.

Typically, the complete system reaches "on the air" status in less than a minute.

#### *System instrumentation*

Many of the parameters built into the scheduling and swapping of early ADEPT versions were based upon empirical knowledge. The latest versions of the Basic and Extended Executives include routines to record system performance, reliability, and security locks.

Built into the BASEX is a routine to measure the overall and the detailed system performance.<sup>20</sup> Such factors as the number of users, file usage, hardware and software errors, and page transaction response time are recorded on unused portions of the 2303 drum. These measurements provide a better understanding of the system under a variety of inputs and give the designers insight into how the hardware and software components of the system affect the performance of the human user.

An AUDIT program was made part of the EXEX to record the security interaction of terminals, users, and files. AUDIT records EXEX activity in the areas of LOGIN, LOGOUT, and File Manipulation. This routine strengthens the security safeguards of the executive. Specific items that are recorded involve: type of event, user identification, user account number, job security, device identification, time of event, file identification, file security and event success. In addition, this routine provides accounting information and is used as a means of debugging the security locks of new system releases.

In addition to the BASEX recording function, several object programs have been written that simulate various modes of user activity and provide controlled job distributions. These programs, called "benchmarks," run under controlled conditions and enhance the means of improving system performance and throughput, as described elsewhere by Karush.<sup>21</sup> The programs are designed to gather performance measures on the major routines of the executive and have been of considerable help in system "tuning," because they reflect the effect of coding and design changes to various system routines. The routines in the executive that are of primary concern are the swapper, the scheduler, the terminal read/write package, and the interrupt handling processes. Attempts are being made to design a set of benchmarks that represent a typical job mix. However, we are primarily interested in measuring the performance of our system against various modifications of itself and in measuring its behavior with respect to different job mixes.

#### SUMMARY

The ADEPT executive is a second-generation, general-purpose, time-sharing system designed for IBM 360 computers. Unlike the monolithic systems of the past,<sup>1,2</sup> it is structured in modular fashion, employing distributed executive design techniques that have permitted evolutionary development. This design has not only produced a flexible executive system but has given the user the same facilities used by the executive for controlling the behavior of his programs. ADEPT's security aspects are unique in the industry, and the testing and fabrication methods employ a number of novel approaches to system checkout that contribute to its operational reliability.

It is important to note that this system deals particularly well with size limitation problems of very large files and very large programs. The provisions made for multiple programs per job, active/inactive page status for programs larger than core size, page sharing between programs, common file access across programs within jobs, and the commitment of considerable space to active file environment tables (up to four pages worth) contribute to this success. Nevertheless, all these capabilities are designed to handle the smaller entities as well. We feel ADEPT-50 is a significant contribution to the technology of general-purpose time-sharing.

#### ACKNOWLEDGMENTS

We would like to express our appreciation for the dedicated efforts of some very *adept* individuals who participated in the design and building of this time-sharing system. Our thanks go to Mr. Salvador Aranda, Mr. Peter Baker, Mrs. Martha Bleier, Mr. Arnold Karush, Mrs. Patricia Kribs, Mr. Reginald Martin, Mr. Alexander Tschekaloff and all the others who have followed their lead.

#### REFERENCES

- 1 P CRISMAN editor  
*The compatible time-sharing system: A programmer's guide*  
MIT Press Cambridge Mass 1965
- 2 J SCHWARTZ et al  
*A general-purpose time-sharing system*  
Proc SJCC Vol 25 1964 397-411 Spartan Books Baltimore
- 3 E W FRANKS  
*A data management system for time-shared file-processing using a cross-index file and self-defining entries*  
AFIPS Proc Vol 28 1966 79-86 Also available as SDC document SP-2248 21 April 1966



4 R E BLEIER  
*Treating hierarchical data structures in the SDC time-shared data management system (TDMS)*  
 Proc 22nd Nat ACM Conf Thompson Book Co 1967 41-49

5 E W DIJKSTRA  
*The structure of T.H.E. multi-programming system*  
 C A C M Vol 11 No 5 May 1968

6 F J CORBATO V A VYSSOTSKY  
*Introduction and overview of the multics system*  
 Proc FJCC Nov 30 1965 Las Vegas Nevada

7 B W LAMPSON  
*Time-sharing system reference manual*  
 Working Doc Univ of Calif Doc No 30.1030  
 Sept 1965 Dec 1965

8 B W LAMPSON  
*A scheduling philosophy for multi-processing systems*  
 C A C M Vol 11 No 5 May 1968

9 J H SALTZER  
*Traffic control in a multiplexed computer system*  
 MAC-TR-30 thesis MIT Press July 1966

10 G H FINE et al  
*Dynamic program behavior under paging*  
 Proc ACM 1966 223-228 Thompson Book Co Wash D C

11 E G COFFMAN L C VARIAN  
*Further experimental data on the behavior of programs in a paging environment*  
 C A C M Vol 11 No 7 July 1968 471-474

12 I A BELADY  
*A study of replacement algorithms for a virtual storage computer*  
 IBM Systems Journal Vol 5 No 2 1966

13 R W O'NEIL  
*Experience using a time-shared multi-programming system*

with dynamic address relocation hardware  
 Proc SJCC 1967 Vol 30 611-627 Thompson Book Co Washington D C

14 J G ROBERTS  
*Multiple computer networks and intercomputer networks and intercomputer communication*  
 ACM Symposium on Operating System Principles  
 Oct 1-4 1967 Gatlinburg Tenn

15 E BOOK D C SCHORRE S J SHERMAN  
*Users manual for MOI-360*  
 SCC Doc TM-3086/003/01

16 R R LINDE P E CHANEY  
*Operational management of time-sharing systems*  
 Proc ACM 1966 149-159

17 P V McISSAC  
*Job descriptions and scheduling in the SDC Q-32 time-sharing system*  
 SDC Doc TM-2996 June 1966 28

18 C WEISSMAN  
*Security controls in the ADEPT-50 time-sharing system*  
 AFIPS Proc FJCC Vol 35 1969

19 W A BERNSTEIN J T OWENS  
*Debugging in a time-sharing environment*  
 AFIPS Proc FJCC Vol 33 1968 7-14

20 A D KARUSH  
*The computer system recording utility: application and theory*  
 SDC Doc SP-3303 Feb 1969

21 A D KARUSH  
*Benchmark analysis of time-sharing system*  
 SDC Doc SP-3343 April 1969

APPENDIX A: Advanced development prototype system block diagram.

