TECHNICAL REPORT

NATICK/TR-80/035

✓ 10/18

AUTOMATED HEADCOUNT SYSTEMS - A STATE-OF-THE-ART SURVEY

by

L. R. Birnbaum

D. P. Leitch

June 1980

APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED.

UNITED STATES ARMY
NATICK RESEARCH and DEVELOPMENT LABORATORIES
NATICK, MASSACHUSETTS 01760

Operations Research/Systems Analysis Office

Citation of trade names in this report does not constitute an official indorsement or approval of the use of such items.

Destroy this report when no longer needed. Do not return it to the originator.

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
NATICK/TR-80/035

2. GOVT ACCESSION NO.

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
AUTOMATED HEADCOUNT SYSTEMS - A STATE OF THE ART SURVEY

5. TYPE OF REPORT & PERIOD COVERED

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)

Linda R. Birnbaum
D. Paul Leitch

8. CONTRACT OR GRANT NUMBER(s)

9. PERFORMING ORGANIZATION NAME AND ADDRESS
US Army Natick Research & Development Laboratories
Operations Research and Systems Analysis Office
Natick, MA 01760

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
OMA, P728012.19

11. CONTROLLING OFFICE NAME AND ADDRESS
US Army Natick Research & Development Laboratories
Operations Research and Systems Analysis Office
Natick, MA 01760

12. REPORT DATE
June 1980

13. NUMBER OF PAGES
231

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)

15. SECURITY CLASS. (of this report)
Unclassifed

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
N/A

16. DISTRIBUTION STATEMENT (of this Report)
Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES
Service Requirement Identification: USN 7-6, Procurement of Enlisted Dining Facility Patron Identification and Recording System

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

SIGNATURE HEADCOUNT SYSTEM
MEAL CARD
RATION ACCOUNTABILITY
AUDIT TRAIL
AUTOMATED HEADCOUNT
FOODSERVICE SYSTEMS

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The signature headcount system, established to control the entry of authorized personnel into military enlisted dining facilities, has received recent and severe criticism by DAA auditors as being unreliable, time consuming, and difficult to audit. In an effort to address these problems, the Navy Food Service Systems Office tasked the NLABS OR/SA Office to investigate the potential of an automated system for Navy foodservice.

A state-of-the-art survey of commercially available automated headcount systems was conducted. Results reported herein include a description of the operational capabilities of each of the eight systems identified and an evaluation of their potential for military usage. A comparison of system costs is also included.

It is concluded that the advantages offered by these systems are the capabilities to produce legible audit trails, potentially useful management reports, and to provide for controls on excess meal card usage. It is also noted that automated headcount systems will not solve meal card and headcount station control problems. Automated systems only provide better information upon which management can act upon -- or ignore. Due to the advantages of automated card reading systems and DoD interest in the conversion to a la carte foodservice, it is recommended that the Navy acquire an automated headcount system and evaluate it in conjunction with their pending test of an a la carte system. Furthermore, it is recommended that headcount practices will have to change if a valid test is to be achieved.

PREFACE

This survey was conducted as part of the Department of Defense (DoD) Food RDT&Eng Program under Project No. 728012.19, DoD Production Engineering in Support of Stock Fund Food and Food Service Items. The Service Requirement was identified as USN 7-6, "Procurement of Enlisted Dining Facility Patron Identification and Recording System" and sponsored by the Navy Food Service Systems Office (NAVFSSO).

The following individuals assisted on numerous occasions and deserve special credit. These include Dr. Robert J. Byrne, Chief, Operations Research and Systems Analysis Office, for his overall technical guidance and his encouragement and support; Mr. Philip Brandler for his helpful suggestions and special assistance, and Mrs. Patricia A. Yow and Mrs. Maryellen Jennings who provided secretarial support for the project.

In order to make this report as informative as possible, we have included in the appendices reproduced copies of all the relevant brochures and articles that we received when we were conducting the survey. Permission has been granted by each of the companies whose literature appears in this report to reproduce their material for informative and educational purposes only.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT'D)

TABLE OF CONTENTS (CONT'D)

LIST OF FIGURES

LIST OF TABLES

AUTOMATED HEADCOUNT SYSTEMS - A STATE OF THE ART SURVEY

SECTION I

INTRODUCTION

The Signature Headcount system was established by the Annual Military Appropriations Act, DoD Directive 1338.10-M and a Memorandum added to DoD Directive 1338.10-M, dated 10 May 1968, to control the entry of authorized personnel into military enlisted dining facilities, to insure proper payment for meals consumed by personnel not authorized Subsistence-In-Kind and to provide an appropriate audit trail. Recent criticism of the system includes claims that it is unreliable, cumbersome, and time consuming. In addition, headcount sheets are difficult to audit and the requirement to sign for a meal is considered to be demeaning and a source of irritation to patrons.

In an effort to address these inadequacies in the present system the Navy Food Service Systems (NAVFSSO) tasked the Operations Research and Systems Analysis Office (OR/SAO) of the US Army Natick Research and Development Laboratories (NLABS) to provide technical assistance in assessing commercially available automated headcount systems for application to Navy foodservice. To accomplish this task, OR/SA conducted a survey of off-the-shelf automated headcount systems. This report presents the results of the survey. These results include a description of the operational capabilities of each of the systems identified in the survey and an evaluation of their potential for military usage. A comparison of system costs is also included. In addition, this report discussess prior military experience with automated headcount systems, government audit results of the existing signature headcount system, and some general problem areas associated with the signature system. Conclusions and recommendations are also presented.

PRIOR RESEARCH

The Navy is not the first DoD Agency to have expressed an active interest in improving the existing headcount system. In 1972, during a test of the Centralized Army Feeding (CAFE) concept at Fort Lewis, Washington, a form of automated headcount was utilized.[1] Terminals in the dining facilities recorded card information on computer tape through a central polling device and key tape units. The results showed that an Automated Headcount System was feasible and that the concept should be refined and tested further.[2]

[1] R. Bustead, "The CAFe System Experiment at Fort Lewis, Washington", Technical Report, TR-73/20-OR/SA, December, 1972, (AD 759284).

[2] D. P. Leitch, and Hertweck, G., "An Automated Headcount System", Technical Report, Natick/TR-73/11-OR/SA, November, 1972, (AD 752118).

In 1973, authority was granted to the Troop Support Agency (TSA) at Fort Lee, Virginia to conduct an Automated Headcount test in Fort Lee, Virginia.[3] The test as operated showed two types of results: first, the problems encountered in a system of this design, and second, the advantages of an automated system. The problems encountered included:

1. the off-the-shelf equipment was not specially designed for the function it was to perform and as a result hampered test operations,

2. it took too long to validate transactions (at best, an average of 7 seconds),

3. because the equipment was obtained from seven different manufacturers, there were problems in communications between components and in isolating machine malfunctions,

4. approximately 40% of the people lost their meal cards during the test period,* and

5. the damage rate to cards was high, causing the cost of card preparation to be high.

Furthermore, the voice grade telephone lines that were used to connect the system were viewed as a possible cause for the slow response times and many of the error responses experienced during the test. It was concluded that the concept of automating the headcount requirement was viable, but that the automation package as tested at Fort Lee should not be proliferated.

However, the automated system showed some definite advantages over the signature headcount system. These included: (1) the automated system was highly accurate when compared to the signature system and was difficult to "pad" and (2) the system provided an improved method of accounting for meals, report preparations, and auditing dining facility transactions.

[3] J. W. Marker, "Automated Headcount System Test", Final Report, US Army Troop Support Agency, November, 1974, (CS-SD-7601).

*Fort Lee annually experiences a 20% loss rate of military ID cards, which are infrequently removed from individuals' wallets. The meal card, on the other had, was removed as many as three times per day, seven days per week, which would explain the 40% loss rate during the short duration of the test.

There were, however, (and still are as per current audit reports) two major problems in existence that were not solved by either of the two automated systems tested and that can not be solved by automation. These problems include inadequate meal card and headcount station control practices. An automated headcount system will not significantly improve record keeping in regards to ration status and card issuance and control. Nor will an automated badge reader have the capability to stop unauthorized people from getting free meals if the headcount attendant lets them go through. Any good access control system, including an automated system, depends upon good and exacting record keeping practices on who is authorized and "GO - NO GO" enforcement practices at the point of access control.

FUNCTIONAL REQUIREMENTS

NAVFSSO provided NLABS with a statement of functional requirements for the selected system(s) and to a large extent, these requirements guided this survey's search for alternative systems. The specific requirements were:

1. Validation of eligibility of personnel to insure that only persons entitled to subsistence-in-kind are permitted to eat at government expense.

2. Prevention of unauthorized personnel from using a valid entitlement instrument.

3. Providing daily and monthly auditable headcount totals by meal periods and category of personnel, e.g., subsistence-in-kind, cash sales, and meals consumed by patrons from other services.

4. Facilitate the verification of meal counts for audit purposes.

5. Substantiate ration credits and monetary allowances claimed by Navy enlisted dining facilities.

It should be noted that the requirement to validate personnel eligibility was the driving force behind the decision to narrow the scope of this survey to automated alternatives. It should also be noted that when the requirement to provide auditable headcount totals is satisfied, the requirements for verifying meal counts and substantiating ration credits are also partially satisfied. Therefore, from both the Navy's and from the surveyors' perspective, the requirement to provide auditable headcount totals was considered the most important.

SURVEY METHODOLOGY

There were three major stages involved in conducting the survey. First, a list of potential vendors was generated. Second, each vendor was contacted and asked to respond to the specially designed questionnaire given in Appendix A. Finally, where time and resources allowed, actual users were interviewed either in person or by telephone.

The search for potential vendors was designed to be as extensive as possible. Trade journals such as "Security World" and Datamation" and the Sandia Handbook[4] on Entry-Control Systems were reviewed, and all relevant articles, advertisements and system descriptions contained therein were extracted for further investigation. User interviews provided another means for identifying potential vendors. Interviews were conducted with personnel involved in either foodservice or security access applications. During the course of each interview, users were asked to identify other systems, if any, which were considered prior to making the decision to purchase or lease the actual system in use. This particular approach proved to be the most valuable one, because some of the vendors included in this report were not listed in either the trade journals or in the Sandia Handbook. Other questions that were posed to users provided information on system reliability and performance, vendor service and training policies, and user satisfaction.

As can be seen in Appendix A, the vendor questionnaire was divided into three categories: Hardware, Cards, and Other. The Hardware section addressed itself to issues of system cost and operating capabilities. The Card Section was concerned solely with card costs and characteristics, and the last category dealt with issues considered important but not falling into either of the other two categories, such as the number of current foodservice applications and the nature of applications other than foodservice.

ANALYTICAL ASSUMPTIONS

The actual costs of any particular system are determined by its size and the special requirements it must satisfy. Systems provided by each vendor therefore must be configured to provide the functions required for a particular site. In order to present a meaningful cost comparison of the systems included in this report, however, certain assumptions which would represent appropriated fund foodservice on Navy ashore bases were made. These were:

1. 2000 authorized patrons (i.e., cardholders) would be enrolled in the system.

2. A 40% yearly card turnover/replacement rate would be experienced.

3. Where applicable, only one card encoder would be required.

4. Two dining facilities located less than three miles apart would be the only two locations requiring card readers.

[4] Entry-Control Systems Handbook, (Sand-77-1033), Sandia Laboratories, Albuquerque, New Mexico, September 1977, Revised September 1978.

Note that only two cost components (hardware and card stock/preparation costs) were evaluated in this survey. Other cost elements such as installation, operating, maintenance, labor, and energy were not considered germaine since these factors would be evaluated in a field test, should any of the available systems be selected for further consideration.

The costs of the various systems presented herein should be considered as budgetary estimates rather than firm fixed prices. These prices were obtained over the latter months of Fiscal Year 1979 and may not currently reflect a unique market position for any one item. Funds cited in this report were checked for reasonableness, but were considered as budgetary estimates which could be effectively used for comparison purposes. Therefore, the costs associated with each of the systems is essentially correct relative to each of the other systems.

It should be noted that some companies failed to respond to our repeated requests for information (Burroughs) while others provided incomplete information (Rusco). These companies are nonetheless mentioned in this survey because it was apparent through user interviews that they are capable of satisfying Navy requirements. (The detailed description in Appendix B of a Burroughs user's application shows how this company's hardware could function in an automated headcount system capacity.) Another company, Entrec Corporation, replied long after the survey deadline expired, and time constraints did not allow discussion of their system in this report. However, it was apparent from the company's literature that they are probably capable of satisfying the Navy's functional requirements; hence, all the literature that Entrec provided the survey team is included in Appendix C.

DOD A LA CARTE POLICY

A memorandum, dated 12 January 1974, by the Deputy Assistant Secretary of Defense (Supply Maintenance and Services) requested all services including the Navy to test the Basic Allowance for Subsistence (BAS) A La Carte concept (all enlisted personnel are paid BAS, and dining facilities are operated like civilian cafeterias where food items are priced individually) at one or more of its installations. In view of the above directive and subsequent tests,[5] the DoD Food Planning Board recommended on 24 January 1979 that an A La Carte feeding system for appropriated funded dining facilities be adopted where feasible.

It should be noted that this recommendation impacts on any future implementation of an automated headcount system because the cash register equipment utilized in an a la carte pricing system can be adopted to produce an automated audit trail of headcounts. Hence, in an a la carte environment,

[5] P. Brandler, et al., "An Evaluation of an All Commuted Rations Ashore/ A La Carte System for the Navy", Technical Report, TR-77/011, January, 1977 (AD A043439).

an automated headcount system would be impractical, as it would be redundant to capture headcount information at the headcount station and at the end of the serving line on cash register tape. In fact, at Marine Corps Base, 29 Palms, California, where an a la carte test is currently in progress, the headcount station at the front of the line was abolished for this very reason. Headcount data is now captured by a cash register, located at the end of the serving line, and is entered through the register's keyboard by a cashier.

Due to the potential keying errors (e.g., entering meal card number 0634 as opposed to meal card number 0635) that might occur in such a system as 29 Palm's, a more reliable approach to capturing headcount data at the end of the serving line might be to attach a card reader to the cash register. The upcoming Navy a la carte test at Little Creek Naval Station, Norfolk, Virginia will provide an opportunity to test this concept.

Where a la carte is not feasible, however, an automated headcount system could be located at the beginning of the serving line. In this situation, then, the systems identified in this report remain viable candidates.

SECTION II

AUDIT REQUIREMENTS AND RESULTS

Since the most important requirement guiding this survey of automated systems was that involving an audit trail, four recent Navy audit reports were obtained and reviewed. In each of the four reports obtained, the following problems were cited:

(1) Meal Signature Records contain illegible signatures, meal pass numbers, and duty station designations.

(2) Blank passes are not positively secured until used nor are they handled in a manner which fosters strict accountability.

(3) Meal passes are not serially numbered or issued in numerical sequence.

(4) Personnel are lending their meal passes to others, or using invalid meal passes.

Further, an estimate of the potential annual cost incurred as a result of these problems was provided in one of the aforementioned reports. This report stated the results of a comparison made between Meal Signature Records and the meal-pass log for the week ending 30 September 1978. Numerous unmatched names, signatures, and meal pass numbers were found. Because similar conditions were noted for this base's tenant commands, the auditors believed that the percentages encountered were representative of the total unauthorized meals served at this base during Fiscal Year (FY) 1978. Of the 380,000 actual meals served by the enlisted dining facility in FY 1978, an estimated 43,000 were unauthorized, as shown in Table 1. In addition, 6,266 potentially unauthorized night meals costing $7,200 ($1.15 x 6,266) were also served during FY 1978. Thus, the audit board estimated that during FY 1978, on the base under review, meals costing $55,000 could have been served to unauthorized persons.

It is important to emphasize that audit reports identify potentially unauthorized meals. Some illegible signatures -- countered by auditors as unauthorized meals -- may be, in reality, from authorized customers. In a similar vein, a meal pass that was not issued in proper numerical sequence may still have been issued to an authorized patron. To the extent that these cases occur, audit reports are inflated estimates of unauthorized meals. On the other hand, audit reports may be an underestimate of fraudulent meals served because auditors may not detect those unauthorized individuals who intentionally bypass the headcount station and, more importantly, auditors would not be able to detect personnel on BAS who use borrowed SIK cards and sign the headcount sheet with SIK*cardholders' names.

*Subsistence-In-Kind.

TABLE 1

Projected Annual Cost of Unauthorized Meals

Meal (Unit/Cost)[a]	Number of Meals Reviewed			Number of Meals Annually[b]		
	Served	Unauthorized	Percent	Served	Unauthorized	Cost
Breakfast (55¢)	221	28	12.7%	58,286	7,402	$ 4,071
Lunch ($1.15)	426	44	10.3	116,373	11,986	13,784
Dinner ($1.15)	429	45	10.5	119,115	12,507	14,383
Brunch ($1.30)[c]	156	17	10.9	50,724	5,529	7,188
Dinner ($1.55)[c]	110	16	14.5	35,884	5,203	8,065
TOTAL	1,342	150	11.1%	380,382	42,627	$47,491

[a] Unit cost as of 7 October 1977.

[b] Projected number of meals for the representative base.

[c] Weekends only.

These considerations lead the authors to conclude that while audit results provide an indication of the magnitude of monetary losses under the present system, they lack sufficient precision to serve as exact estimates of tangible reductions in unauthorized meals under manual or automated headcount alternatives. An automated system would, however, have some impact on problems identified in audit reports:

An automated system would produce computer generated audit trails, thus greatly reducing* if not eliminating illegible signature on meal records. In addition, it seems fairly clear that the problem of "lost" blank uncoded meal cards would be alleviated in automating the headcount system since blank cards would be rejected by the dining hall card reader. It must be noted, however, that this probable benefit would depend upon the extent to which access to meal card encoder(s) is strictly limited to authorized personnel.

From the prior experience with automated systems at Fort Lewis and Fort Lee, there appears to be some deterrent value associated with an automated headcount system since customers realize that misuse cannot be covered over by an illegible signature. The reduction in the extent to which meal cards are loaned to and used by someone other than the authorized individual seems to be one of the clearer benefits of an automated system.

Considering prior tests of automated headcount systems and accountability problems detailed in audit reports, the best conclusion at this point seems to be that the cost-benefit equation is still unclear. While automated systems have shown some effect in improving audit trails and ration accountability, the probable savings have not equaled auditors' estimates of dollar losses from unauthorized meals. Nor is it entirely clear at this time that the introduction of automated equipment is a clearly superior alternative to strict enforcement of existing manual procedures in controlling access to the enlisted dining facilities. What is clear, however, is that the procurement and installation of an automated system will offer an opportunity to upgrade record keeping and headcount station control to the levels which should exist in the present signature headcount system.

*A back-up manual sign-in system may have to be used if the automated system is down temporarily. Under this condition illegible signatures could still occur.

SECTION III

SYSTEMS OVERVIEW

There are two building blocks in the alternative systems to be described in this report. The first is a machine readable card. The second is the data collection equipment (i.e., system hardware) utilized in capturing the information that is encoded on the cards. System cards can either have the owner's photograph on them or they can be blank. The choice of having photo cards or not is entirely up to the user, and for that reason, the system discussions and corresponding cost estimates in the following sections address both these options.

Software is for some applications, a significant third building block. Only two systems included in this report required a software package. Since it is a highly variable factor and is not a significant contributor to costs of access-control systems, software costs are not considered except in the cases of Validine and IBM.

CARDS

Card Encoding Processes. Four processes used to encode data onto cards were identified. These are:

1. Magnetic-Stripe: Magnetic-stripe encoding is widely used in commercial credit card systems, and several vendors manufacture equipment which is compatible with the American National Standard Institute (ANSI) for this technique. With the magnetic-stripe-coded badge, a stripe of magnetic material located along one edge of the badge is encoded with alphanumeric data. Two types of encoding are specified in the ANSI standard for magnetic-stripe encoding. One type, the American Bankers Association (ABA) standard allows up to 40 numeric characters. The other, the International Air Traffic Assocation (IATA) standard, has up to 90 alphanumeric characters. The use of alphanumeric IATA coding allows the badge holder's name to be included in addition to a badge number. One disadvantage of the 90-character data encoding, however, is that more accurate reader spacing and alignment are required. These data are then read as the magnetic stripe is moved past a magnetic read head. Credential forgery is relatively easy since data from the magnetic stripe can be decoded and duplicate badges encoded by the use of parts from a common magentic tape recorder. Certain of these types of cards are also easily erased by even weak magnetic fields such as might be encountered in a Navy degaussing station.

2. Magnetic: This badge contains a sheet of flexible magnetic material on which an array of spots has been magnetized. (The number of usable information bits, or spots, typically ranges from 23 to 36.) The code is determined by the polarity of the magnetized spots. The badge reader contains either magnetic sensors which are interrogated electrically or magnetic read switches which are mechanically actuated when a magnetic spot with the proper polarity is located adjacent to the read. The magentic spots can be accidently erased if the badge is placed in a sufficiently strong magnetic field. However, field experience has shown that this is not a significant problem. Since it is possible to build equipment to recode or duplicate the pattern of magnetic spots, fabrication of a false credential is possible. It is more difficult, however, to falsify this type of credential than to fabricate a magnetic-stripe-coded badge.

3. Optical: The optical coded badge contains a geometric array of spots printed on an insert laminated into the badge. Photo detectors in the badge reader detect the relative optical transmission of the spots and hence the code. To make this coded badge more tamper resistant, the pattern of spots can be concealed by making the badge opaque to visible light but transparent to infrared light. The spots are printed with ink which is opaque to infrared light. This technique offers good tamper protection, and badges are reasonably difficult to counterfeit.

4. Passive-Electronic: A passive-electronic coded badge is a badge onto which electrically tuned circuits are laminated. In order for the code to be read, a swept-frequency, radio frequency (RF) field is generated and then the frequencies at which significant energy is absorbed are deflected. These frequencies correspond to the resonant frequencies of the tuned circuits and are decoded to give a unique badge number or code. An advantage of this technique is that the badge does not need to be inserted into a reader mechanism but can simply be placed near the antenna which serves as the read station. The disadvantages are (1) badges can be decoded with common RF test instruments, allowing counterfeit badges to be fabricated, and (2) the number of unique code combinations is limited to a few thousand.

Resistance to Decoding and Counterfeiting. Any type of coded badge can be decoded and duplicated if sufficient time, money, and talent are devoted to the attempt. The following list ranks the coding techniques described previously from the easiest to the most difficult to duplicate:

1. Magnetic-stripe code
2. Magnetic code
3. Optical code
4. Passive-electronic code

A 1973 Business Week article described just how easy it is to duplicate a magnetic stripe code:[6] " ... use heat from a household iron to duplicate the magnetic pattern of the "good" card on an ordinary, blank piece of cassette tape ... after five minutes of work, a second tape that can be pasted on to another card is created ... there are still other methods ... (in fact) Cal. Tech students came up with 22 different ways ...."

In general, it is not necessary to decode a badge to duplicate it. However, the degree of difficulty in decoding the badges listed does parallel the degree of difficulty in duplicating them. Sometimes the code data are crytographically encoded or contain other internal checks. When these internal checks are used in the encoding process, counterfeiting a new badge then requires both decoding and understanding the check algorithm; which makes counterfeiting much more difficult.

Resistance to decoding and counterfeiting is not as important if the badge is used in conjunction with a separate personnel identification system. In this type of system, the badge number simply indexes a file, called the reference file, where personnel identifier data are stored. Access is allowed only if the personnel identifier algorithm is satisfied. In this case, counterfeiting a badge will not, in itself, guarantee access.

Card and Card Program Costs. In general, the more resistant a particular encoding process is to duplication, the more expensive a card that utilizes that process will be. The prices quoted for magnetic-striped cards ranged from $0.30 to $1.17 a card, magnetic card costs were quoted as being between $1.02 and $1.95 a card, and the prices quoted for an optical or passive-electronic coded card were $2.00 or $3.25 a card, respectively. It must be noted that these prices are for cards that do not accommodate photographs. On average, vendors charge an additional $0.45 per card for a photo card. (Basically, a photo card is nothing more than a "regular" card with an attached plastic laminate flap or photograph embedded in the card itself).

It is important to note that the quoted prices mentioned above are not directly comparable because some vendors include the cost of card encoding in their prices and others do not. In particular, two of the vendors whose systems utilize magnetic-striped cards do not pre-encode their cards; instead, they sell blank cards and a system encoder to their users and require them to encode their own cards. Therefore, where applicable, the cost of a card encoder must be included in that system's total cost. Further, if a photo card program is desired, then not only should card encoders be included in the total system cost, but cameras, laminators, die cutters, and film should be included as well.

[6] "Beating the New Credit Cards", Business Week, August 11, 1973.

Appendix D contains a detailed breakdown of the specific costs associated with each system's blank and photo card program. Card costs are based on 2,000 authorized patrons (i.e., cardholders) and a 40% card turnover/replacement rate for those 2,000 patrons. The number of cards required would thus be 2,800 during the first year of operation and 800 per year thereafter. A 40% turnover rate seems reasonable in view of the results of the Fort Lee headcount test.

Card-Size. Several card sizes are in common use; selection of a particular size is usually a compromise between a smaller, easily handled card and a larger card with more room for a photograph, color-code indicators, and necessary printed information. Most commercially available coded-credential systems utilize the standard credit card size, 54 by 86 mm (2-1/8 by 3-3/8 inches). This size, however, is too small or, at best, marginally acceptable for a picture badge. A slightly larger common card size is 60 by 83 mm (2-3/8 by 3/¼ inches). Although the latter badge is not much larger than the standard credit card, its slightly smaller aspect ratio provides significantly more usable badge area when the badge is laid out with the longer dimension oriented vertically.

DEFINITIONS

To facilitate the discussion of the alternative systems described in this report, the following definitions of specific system features and of general security-access terms are provided:

Access Control - Any system or method which automatically controls the passage of people into or out of an area or structure.

Access Levels - In a facility containing several material-access or vital areas, personnel can be authorized to enter one or more of the areas; thus, multilevel access may be required. The control processor maintains a record of the access authorization for each individual badge and checks it each time an access request occurs. Because this authorization checking is automated, a detailed set of access levels can be readily implemented.

Anti-passback - The control processor can check the occupant list and indicate when a badge is being used for two successive entries or exits. Thus, for example, an employee cannot use his badge to gain entry through a portal then pass it back (for instance, over a fence or out of a window) to another person to use.

Card Reader - A device for reading information represented by punched holes, magnetic spots, magnetic stripe or other encoding methods and converting it into another form for processing by a central controller.

Central Controller - A microprocessor designed to simultaneously monitor and control the activities of all other units in the system. It collects data, analyzes or inteprets events based on stored instructions retrieved from memory, and initiates the appropriate operations required such as opening a door, or sounding an alarm and recording all transactions in real time as they occur.

Facility Code - A code, unique to each user, which assures that only those cards belonging to a particular system will activate the system's readers.

Instant-Access Change - Several entry-control points can be controlled from one centrally located control processor. As a result, when access authorizations are added or deleted at the control processor, this revised information can be immediately utilized at all entry-control points throughout the facility. Also, when a coded credential is lost or stolen or when an individual's access authority has ended, it is not necessary to recover the badge in order to make it void.

Interface - The channels or parallel paths and associated control circuitry which provide the connection between a central processor and its peripheral units. It is the connection that allows two separate items to be tied together.

Modem - An acronym for modulator/demodulator, it permits data to be transmitted over long distances. A device which is used to convert digital input signals from a central controller Reader Terminal to frequency shift keying (tonal) form for telephone transmissions, and to reconvert signals from telephone circuits back to digital form.

Multiplexer - A device which substantially reduces the amount of hard wiring required to link a number of on-line card readers to the central controller. It also expands the allowable distance between remote data collection terminals (i.e., card readers) and the central controller.

Multiplexing - The transmission of messages from multiple sources at high speed and in digital form over the same communication channel.

Status Levels - A code to indicate whether a card is "in" or "out" of the area wherein the reader is located.

Time Zones - Time zone control restricts access to specified times of the day or night.

SYSTEM CAPABILITIES

In specific details, each manufacturer offers a unique system. In evaluating the alternative systems, however, a pattern of common capabilities emerged. Characteristics that are shared by all of the identified systems are:

1. Capability to read and record by automated devices unique authorization code numbers encoded on pass (meal) cards.

2. Provides the user with capability to deny access to an individual or group of individuals by telling the central console which existing card codes are no longer valid thus making it unnecessary to collect old cards.

3. Provision for several levels of access authorization, such as access only at certain times during the day (time zones), or only at selected entry-control points (access levels).

4. Provision of built-in standby power in the event of a power failure.

5. Provision for an automatic capability to identify patrons attempting to use a card given them by someone ahead of them in line (anti-passback).

6. Provision of indicator lights on the Card Reader to inform the Head-count Station Monitor whether or not a patron is clear to eat.

7. Accommodation of 1500 or more cards.

8. Accommodation for at least eight reader stations.

9. Maximum response times (time/required to read a card entered into the reader) of six seconds or less, and

10. Capability to operate at temperatures normally encountered in enlisted dining facilities (50°F or above).

Furthermore, all but one system identified can generate computer compatible output directly and/or interface directly into a mainframe computer. It must be mentioned, however, that even though one of the identified systems does not have this capability, the manufacturer does market a larger version which includes this characteristic.

Another characteristic shared by many of the alternative systems is that, up to the specific distance limit (i.e., the maximum distance that a card reader can be located from the central console without line compensation) established by each manufacturer, the user has a choice of either hardwiring or using telephone lines. The advantage of using phone lines is that it is less costly to connect a system via phone lines than it is to hardwire. However, the tradeoff is that data transmission over telephone lines is less reliable and slower than over hardwires. Fort Lee's experience with voice grade telephone lines, as discussed previously, substantiates the fact that data transmission over phone lines is indeed slow and unreliable. It appears, therefore, that for an access-control type of application, telephone wiring would be better suited for off-line validation of transactions since speed and reliability of data transmission would not be an issue in an off-line validation mode.

PRINCIPLES OF OPERATION

Coded badge numbers are enrolled in the memory of the control processor. Badge numbers are programmed into memory with their operating parameters (i.e., authorized time zones and access levels) by means of a keyboard located either on the central console or on a separate data entry device. All parameters are displayed for verification before being stored in memory. The display indicates whether parameters being programmed have been stored in memory or rejected as unacceptable.

Badges may be group-loaded into memory when access levels and time zones are the same. Groups of cards with the same access parameters can be voided out of the system just as quickly. To program or invalidate a larger number of cards, the console operator simply types in the first and last serial numbers on the block -- a "from-to" instruction and presses appropriate keyboard controls for access status or cancellation.

There is a problem associated with the cancellation of lost or stolen cards in many central controllers, however. When cards are group-loaded, information is programmed into the controller memory for departments of any group in which personnel have similar access characteristics. The cards are numbered sequentially, in numerical order. If a block programmed card is subsequentially lost or stolen, the serial number on the card that replaces it will not be in the same numerical order. For example, if cards numbered 1 through 100, all with the same access parameters are programmed into a system at one time and card number 43 is lost, it might be replaced by card number 208. Consequently, whenever a program change for the entire group of cards is desired, card number 208 and other cards replaced since the card group was first programmed, are out of numerical order, and must be reprogrammed separately, one at a time. The provision of multiple issue levels for each card number eliminates this problem. Only one of the identified central controllers has this provision.

Once a card has been encoded and enrolled in a system's controller unit, the card is ready for use. Then, when the card is inserted in a card reader at an access point, the coded information is transmitted back to the central controller. The card data are received by the central controller, checked for transmission errors, and the access decision process begins. First, the controller begins scanning its memory in an attempt to find the cardholder's ID number. If the number is located, indicating that the card is valid, its assigned "access level" is then examined. If the cardholder's status level specifies access at the reader location at the current time of day and day of the week, the controller issues a "go command" to the reader (otherwise a "no go" command is issued). At the same time, a transaction record is formatted and transmitted to a printing device.

MAINTENANCE

Coded-credential systems are generally complex electronic systems, and, as such, require competent electronic technicians to perform maintenance. At the time of purchase therefore, a maintenance contract should be placed with either the manufacturer or an established contractor authorized by the manufacturer. The maintenance contract should include operational spares so that system downtime can be minimized.

SECTION IV

CARDKEY

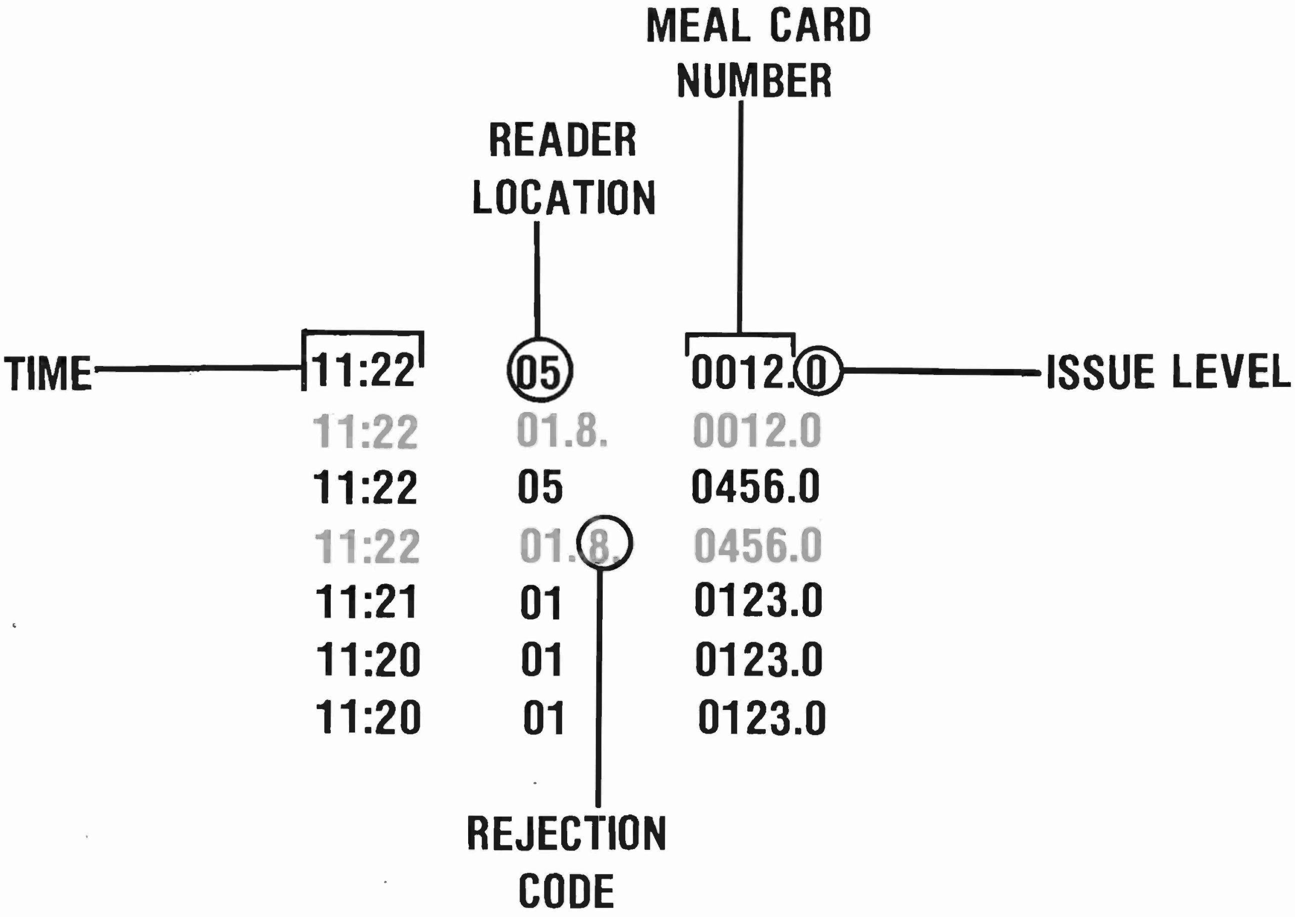
Source: Cardkey Systems
Division of VSI Inc.
20339 Nordhoff Street
Chatsworth, CA 91311

SYSTEM OVERVIEW

The Interrogator 790 Model is a microprocessor controlled system that is capable of controlling up to 16 Reader/Terminals and 2,500 patron accounts. The basic Interrogator 790 system includes 32 Access Levels, a hard copy printer installed in the Central Controller, an internal Audible Alarm, 8 Time Zones, and the ability to interface with a main frame computer via either an electronic interface panel or a magnetic tape interface. Reader/Terminals may be connected to the Central Controller directly up to a distance of 1.5 miles without line compensation. Modems, operating at a speed of 1200BAUD, may be connected to provide unlimited operating distances over telephone circuits. The Cardkey reader is the only one on the market that has its electronics separated from the reader head. This feature prohibits tampering with the reader's electronics and minimizes malicious damage to the system.

All programming is performed by means of a single keyboard on the front panel of the Central Controller. A special key-operated switch on the panel restricts programming operations to authorized personnel only. A built-in card reader is available for reading "Securiti-Cards" (trade name) and further restricting the programming of the system to authorized personnel. Both the key-operated switch and an authorized card would then be required before programming operations could be initiated. Therefore, unauthorized personnel could not change the functional parameters programmed into the Controller.

Programmed data controls a person's access authorization -- when and where he can enter or exit -- according to time period, access authorization, or in/out status. If an authorized person attempts to use a card at the wrong door -- or the right door at the wrong time -- his or her presence and location would be immediately detected at the central console, and the attempted intrusion would be simultaneously documented on the system's hard copy printer. The format of this documented record is similar to the format shown in Figure 1. Valid entries are shown in black indicating card number, time, and terminal number. Invalid entries are given in red and show, in addition to the same transaction data as valid entries, a code that signifies why access was not granted.



```
11:22    05    0012.0
11:22    01.8. 0012.0
11:22    05    0456.0
11:22    01.8. 0456.0
11:21    01    0123.0
11:20    01    0123.0
11:20    01    0123.0
```

FIGURE 1. Sample Audit Trail

Vendor supplied specifications are given in Appendix E and a photograph of the 790 Console is shown in Figure 2.

PRINCIPLES OF OPERATION

When a badge is inserted into a reader, its invisible code triggers the card reading device. The card reader can make individual access decisions based on the code or can signal the microprocessor based central controller to check the corresponding access information that has been programmed into its memory. If access is not granted for any reason, a blinking red light flashes on the card reader. A blinking green light signals that access should be granted. Continuous electronic communication between readers and the central terminal will indicate malfunctions by audio and visual means when the terminal does not respond.

SYSTEM COSTS

The purchase price of this system is as follows:

Hardware	Cost	Cards	Cost
System 790 Control Unit With Printer and Data Entry Device	$ 7,755	2,800 Non Photo 2,800 Photo	$ 2,856 $ 3,836
2 Card Readers	$ 1,950		
Interfaces	$ 3,920		
Total Hardware	$13,625		

Thus, the first year cost of a Cardkey 790 system with a non-photo program would be $16,481: $13,625 for the system hardware and interfaces and $2,856 for the 2800 meal cards that would be required under the specific card-related assumptions of this survey. The first year cost for the Cardkey system with a photo meal card program would be $17,161: $13,625 for the hardware and $3,836 for 2800 photo cards. The only additional costs that would be incurred in the second and subsequent years with the Cardkey system would be the cost for 800 newly issued cards a year, $816 for non-photo cards and $1,106 for photo cards.

USER INTERVIEW

A Cardkey 790 system used solely for access control was seen in a New York engineering firm. The central polling unit was kept in a locked closet and a continuous tape was kept of all persons entering and leaving the controlled access points. The Director of Security at this firm reported that the system functioned according to specifications and that after some initial installation problems were remedied, the system was also completely reliable. It seems that even though the locked closet's internal temperature was in the specified interval, the central polling device repeatedly overheated. Cardkey recommended that a duct be built in the closet and after this was accomplished, no further problems were encountered.

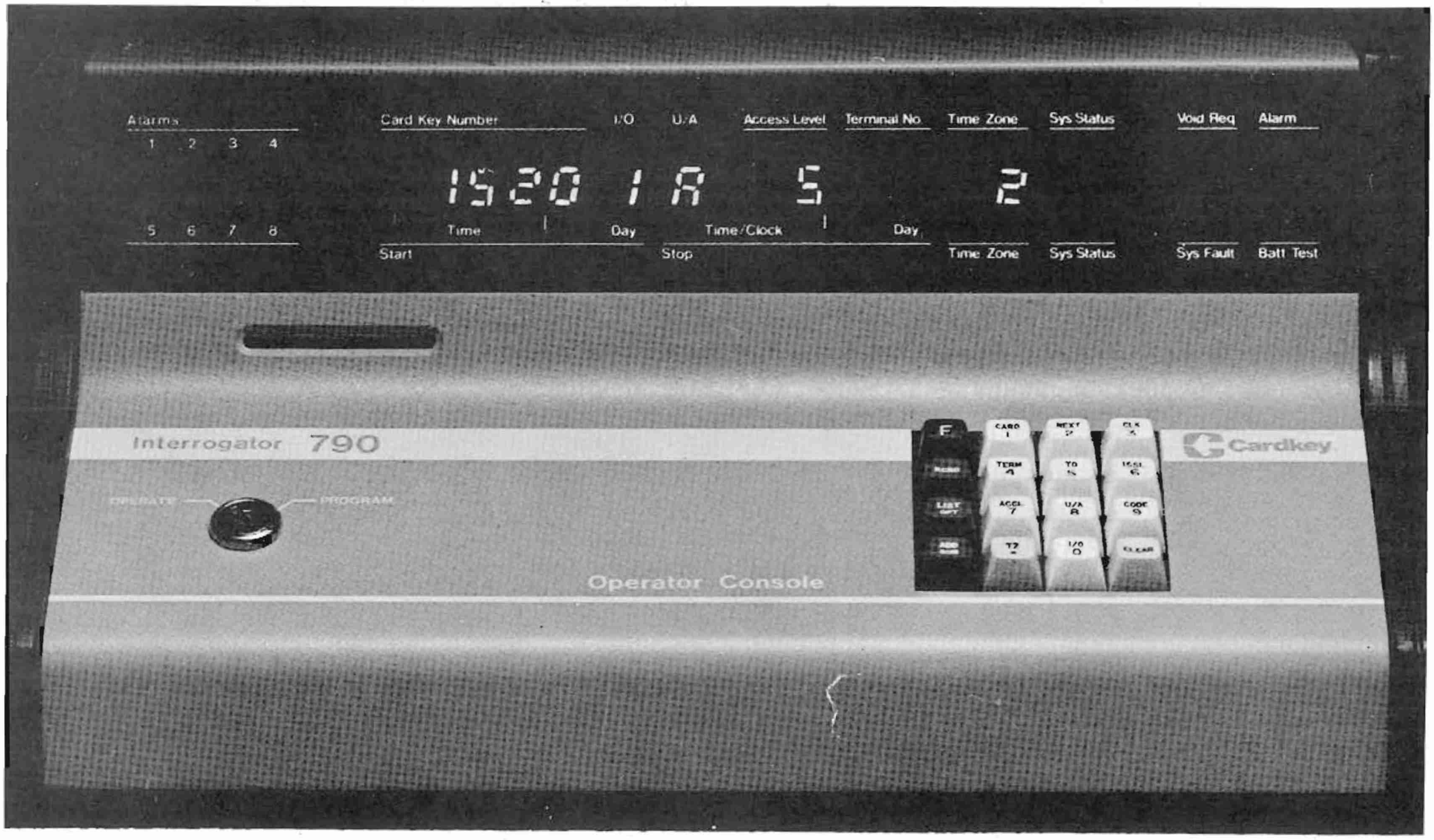


FIGURE 2. Cardkey 790 Console

EVALUATION FOR MILITARY APPLICATION

On those military installations that have a limited number of dining facilities as well as customer populations in the range of 2000 to 2500 personnel, the Cardkey 790 system offers several potential benefits. The Cardkey system is unique in that provisions are included to allow reissuing the same card number to replace lost or stolen cards by changing the card issue level. Only the card with the latest issue level will operate the system, and since the serial number is unchanged, recordkeeping in not affected. In other systems, once a card is lost or stolen, a new card with a new serial number must be issued.

Cardkey's magnetically encoded "Securiti-Card" is less easily erased or duplicated than other system's cards that are simply encoded with a magnetic-stripe. This feature is due to the fact that the "Securiti-Card" contains an embedded layer of berrium ferrite upon which the encoded information is stored. In addition to making the card less easily erased, the embedded ferrite material porbably makes the card more durable than the usually thinner magnetic-striped cards.

Although not a unique feature of the Cardkey system, the fact that its card readers are designed to actuate turnstiles and locks makes it possible for management to place these readers in areas where access control might be important in the food service operation. Rather than padlock refrigerator doors to keep unauthorized personnel from pilfering food after hours, management might, for example, place a Cardkey reader on doors into refrigerated or dry storage areas. Looking beyond a foodservice application, readers could also be placed at other areas on the installation where security access is an important concern such as the Post Exchange (PX).

Based on NLAB'S observations of the 790 in a user environment, it appears that the readers and interrogator (i.e., central polling device) constitute a relatively "sailor-proof" system. Furthermore, given the fact that the card reader can be separated from the terminal interface unit, the opportunity for intentional tampering with the reader's electronics is minimized.

On the negative side of the ledger, the Cardkey system is an expensive configuration to simply replace the existing headcount sheet approach to accountability. Another limitation of the Cardkey system is that being designed for a specific purpose, there is a very severe limit placed on the system's capability to meet the broad range of functions required for ration accountability. For example, the Cardkey system as described in this report could not be programmed to provide a signal if a meal card appeared at a midrats meal if it also appeared at the breakfast, dinner, and supper meals during that day.

And finally, the interrogator 790 model and associated card reader does not have the capability to provide a total headcount by meal period. Some kind of counter could undoubtedly be added to the card reader. This feature, however, is not part of the manufacturer's off-the-shelf system.

SECTION V

IDENTIMAT

Source: Stellar Systems, Inc.
231 Charcot Avenue
San Jose, CA 95131

INTRODUCTION

Identimat, using biometric data, electronically records an individual's hand geometry on to magentic stripped cards. Hand geometry, which is a measurement of relative finger length, has been found to be a "unique" characteristic of individuals.[7] In 1969, Stanford Research Insitute performed computerized statistical analysis of finger-length data (excluding the thumb) and concluded that hand geometry is a distinct human characteristic that can be related to individuals.

SYSTEM OVERVIEW

The Identimat system can be configured in either one of two ways. A separate printer may be used with each hand reader or, several readers may be connected to a Central Station (multiplexer) permitting the use of only one printer for the entire system. That is, the system can be operated in either a stand-alone or an on-line mode. In its stand-alone configuration, the Identimat system can support 10,000 patron accounts and an unlimited number of reader terminals. In its on-line mode, the system can carry 10,000 accounts and 63 reader stations which can either be hardwired to the central station via a three-twisted-pair cable or linked via dedicated telephone lines.

Due to the nature of Identimat's unique approach to patron identification, system cards are encoded on site. The Identimat Encoder plugs into any hand reader in the system. In addition to encoding hand geometry onto the cards, the Encoder can also encode the card with area access and account number information. The Encoder for each system is unique (i.e., a card made on one customer's system cannot be used in another system). The typical time to encode a card is less than 30 seconds. However, for individuals with arthritic problems, or for persons who fail to firmly place their fingers in the reading slots, encoding time can be longer than 30 seconds.

Reader terminals measure 19" high by 13" wide by 19" deep with a weight of 32 pounds. They are small enough to sit on a desk or small table, but should be positioned so that users may comfortably position their hands.

[7] Personnel Identification by Hand Geometry Parameters, Stanford Research Institute Report, July 15, 1969.

Manufacturer supplied specifications on the hand readers used in either the stand alone or on-line mode, encoder, and central station are included in Appendix F.

PRINCIPLES OF OPERATION

To encode an individual, a blank magnetic-stripe card is inserted into the Encoder's card slot and the individual places his/her hand on the card reader. The encoder automatically computes the measurements M_1 through M_4 shown in Figure 3 and encodes those readings on the card along with any area access and/or employee number data manually entered into the encoder. The measurements are made by photodetector devices located beneath a top-lighted plate on which the hand is positioned. As can be seen in Figure 4, the hand is positioned on the plate by means of a peg which projects between the middle and ring fingers. The hand-positioning is not critical; however, the fingers must be placed firmly in each slot to block the light entering the photodetector that scans each slot. A capacitive-switch must sense the presence of a hand to initialize a scan.

After an individual has been encoded and wants to gain access to a controlled area, he inserts his identity card into the reader terminal, places one hand on the top plate and presses down gently. Verification is accomplished when the individual's hand geometry characteristics are measured and compared against the data previously encoded on the user's card. (Read and response times are typically one second). Terminals respond after verification with either an ACCESS or NO ACCESS message. An ACCESS signal indicates verification of the user's identity and authorization for that area. A NO ACCESS signal indicates wrong hand geometry, wrong area and/or wrong system.

At the same time that the reader signals its message, a printed record is made of the verification attempt. The printer gives the date, time, card number, reader location, and the reason for a rejection if it occurs. All rejects are printed in red. To negate the task of physically counting the number of entries on the printer tape, the use of a mechanical counter at each reader station is recommended.

If the stand-alone version of the Identimat system is used, then the printed record is formed on a printer located next to the reader station thus providing a separate audit trail for each reader station location. When the on-line system is employed, the printed record is provided by the Central Console which can be located anywhere. In the on-line mode, dining facilities would not be able to receive their own audit trails as the system is only capable of printing the transactions as they occur (i.e., sequentially).

Another difference between the stand-alone and on-line modes of operation is that the on-line capability allows you to list and delist patron numbers in memory. That is, the Central Console functions partially as a data entry device, and cards can be invalidated without the necessity of recalling them. With a stand-alone system, cards could not be invalidated unless they were physically removed from their owner's possession. Both versions of the Identimat system can be expanded to interface with a mainframe computer.

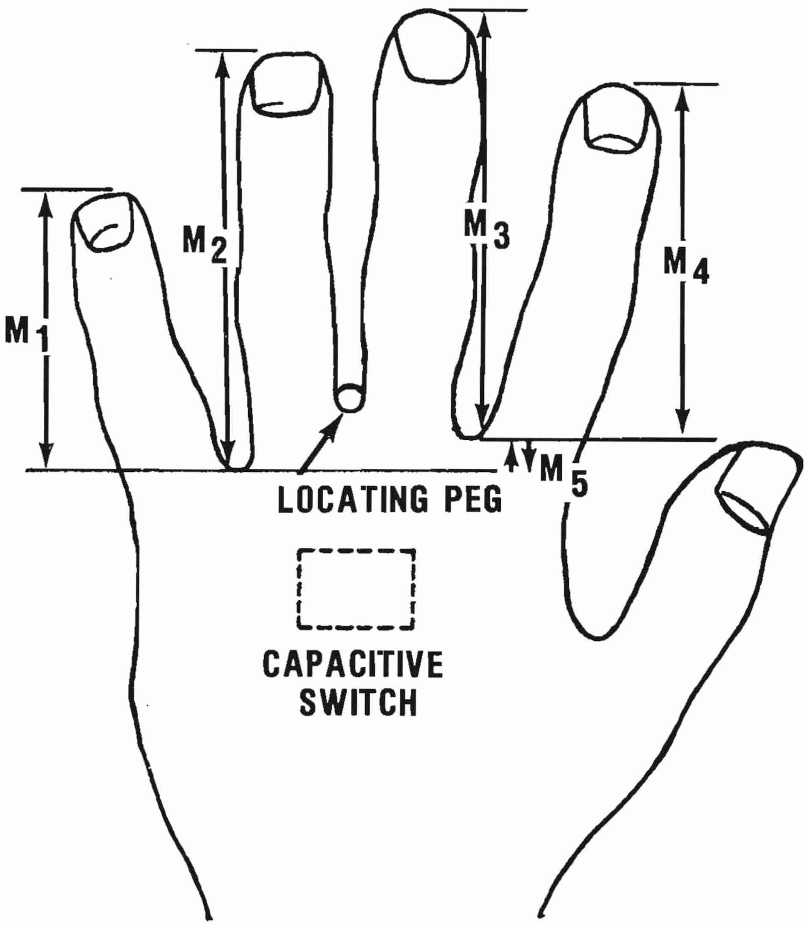


FIGURE 3. Measurements Used By Identimat

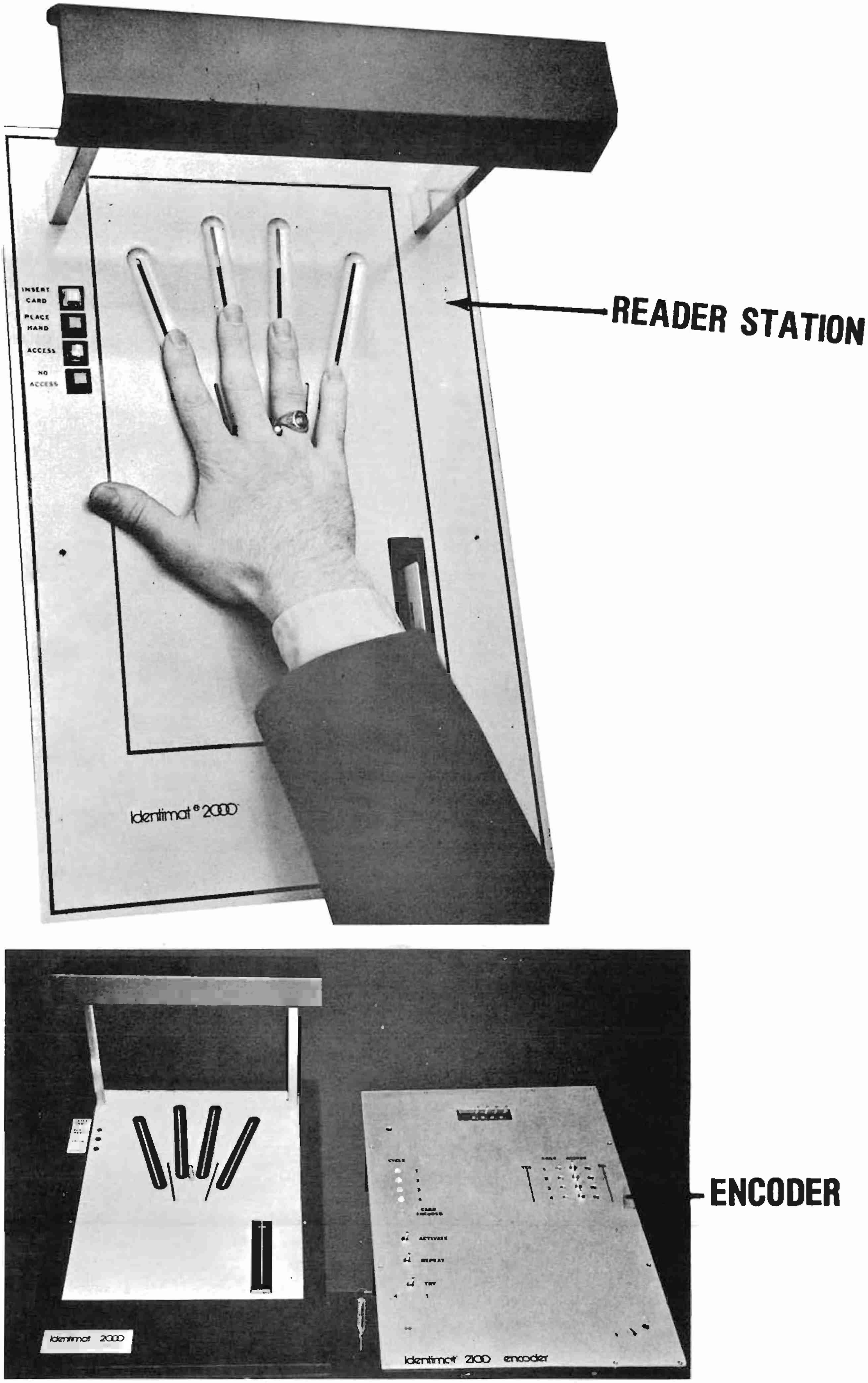


FIGURE 4. Identimat Reader Station and Encoder

SYSTEM COSTS

Hardware and card costs are presented on the following page for both the stand-alone and on-line systems. For each system, the cost for the basic equipment represents a fixed charge and the cost for the station equipment represents a variable charge (i.e., station costs are provided on a per-station basis). This method of presentation was selected so that the reader could compute for himself, using his own size inputs, the total system cost for each alternative configuration.

Thus, the purchase price of a stand-alone system with 2 Reader Stations, 2000 current patrons, and 800 patron turnover and replacement accounts is $17,605--$4,275 for the basic equipment, $12,490 for the 2 Reader Stations, and $840 for the magnetic-stripped cards. An on-line system of the same size would cost $22,700: $12,910 for the basic equipment, $8,950 for the 2 Reader Stations, and $840 for the magnetic-stripped cards. For either configuration, the only charge that would be incurred in the second and subsequent years would be $240 for the 800 new cards that would be issued each year.

USER INTERVIEW

An interview was held with the Manager of Food Service at the University of Tennessee where an Identimat system was installed six years ago. The University chose Identimat because prior experience with picture I.D. cards proved them to be an inadequate control. Student appearances (beard on picture shaved off later, etc.) changed often enough to render pictures deceiving. Problems such as loaning meal cards to a friend for his/her unauthorized use have been dramatically reduced in the transition from "Picture I.D." to the Identimat system.

EVALUATION FOR MILITARY APPLICATION

The uniquely attractive feature of the Identimat system is that verification of the cardholder's identity is performed by the headcount equipment rather than by visual comparison of pictures and faces. Thus, with an Identimat system, a photo card program would not be needed to determine card transfers or "loans" among patrons, as an encoded Identimat card could not be transferred without detection due to the encoding of the cardholder's handprint on the card.

To prevent counterfeiting of the system's card, half of the bits on the card's magnetic stripe are invalid - randomly thrown in by a "garbage hit generator". Copying an Identimat card is thus made ineffective in two ways: it would be difficult if not impossible to tell which field to use and, if somehow one could, the hand geometry would not match anyhow. However, even though an Identimat card would be difficult to duplicate, it is still highly susceptible to erasure.

STAND-ALONE SYSTEM HARDWARE

Basic Equipment	Cost	
1 - Encoder	$ 4,250	
1 - Degausser	25	
Cost for Basic Equipment		$ 4,275

Station Equipment (1 Station)	Cost	
1 - Hand Reader	$ 3,775	
1 - Printer	385	
1 - Printer	1,785	
1 - Mechanical Counter	300	
Cost per Station		$ 6,245

USING CENTRAL STATION

Basic Equipment	Cost	
1 - Encoder	$ 4,250	
1 - Degausser	25	
1 - Central Station w/capacity for 2000 accounts*	6,850	
1 - Printer Option	1,785	
Cost for Basic Equipment		$12,910

Station Equipment (1 Station)	Cost	
1 - Hand Reader	$ 3,775	
1 - Transmit Board	400	
1 - Mechanical Counter	300	
Cost per Station		$ 4,475

CARDS - BOTH SYSTEMS

2800 - Magnetic Stripped Cards ($0.30/card)	$ 840

*The basic Central Station includes a capacity for 1,000 valid identification numbers. The valid memory list may be expanded up to a total of 10,000 at a cost of $430 for the second thousand and $215 for each additional thousand.

Another potential disadvantage of the Identimat system is that initially, dining facility patrons might possibly view the system as a "fingerprinting" operation and develop a high degree of resentment towards it. However, if the University of Tennessee's experience is any indication of how military patrons will react to the Identimat system, then the period of customer resistance and resentment will be relatively short. What the University did in response to initial customer complaints was to educate them about the Identimat system and prove to them that it was not a "fingerprinting" operation. Their educational campaign was quite successful and, therefore, it is recommended that a similar campaign should be conducted on any base where an Identimat system is to be installed.

SECTION VI

VALI-DINE

Source: R. D. Products, Inc.
6132 Route 96
P. O. Box E
Victor, NY 14564

INTRODUCTION

R. D. Products markets an electronic meal card control system, trademarked VALI-DINE, that was originally designed specifically for use in college foodservice. First introduced in 1974, the VALI-DINE System has now been adopted by over 200 colleges and universities across the country. Several variations of the VALI-DINE System are commercially available, but only one of these, the Series/4, is capable of producing hard copy participation data. Figure 5 contains a sample equipment configuration for the Series/4. Specifications provided by the manufacturer on the Series/4 are contained in Appendix G.

For the reader's general information, two Vali-Dine system descriptions are contained in Appendix H. The first describes how a New York State college gained computerized control over its a la carte operation with Vali-Dine and the second discusses how effective Vali-Dine has been in computerizing the library checking-out function at Penn State College.

SYSTEM OVERVIEW

The Series/4 Computer is a 64K microprocessor based mini-computer. In its normal configuration, the Central Processing Unit (CPU) will support an unlimited number of patron accounts, 24 Card Readers, two Interactive Terminals, one Data Storage Terminal, one Dine Printer, and one port to link to another computer.

Card Readers are designed to operate in an on-line, and if necessary in an off-line mode. In the off-line mode, however, the Card Readers can not validate transactions; they are only capable of recording the fact that a transaction occurred via mechanical counters. Readers can either be hardwired to the CPU via a 3002 dedicated data line, or linked via a dedicated phone line.

The data storage terminal is linked directly to the CPU. The function of this terminal is to dump on tape daily all memory stored in the CPU. In case of a CPU malfunction or scramble, as can occur during a severe lightening storm, if lightening hits close by, then a simple load of the previous tape brings all files back to their original condition. The dump is accomplished daily via a time schedule; all that is required of the operator is to put in the tape at the end of the day and take it out the next morning. It takes approximately 20 minutes to totally restore the memory.

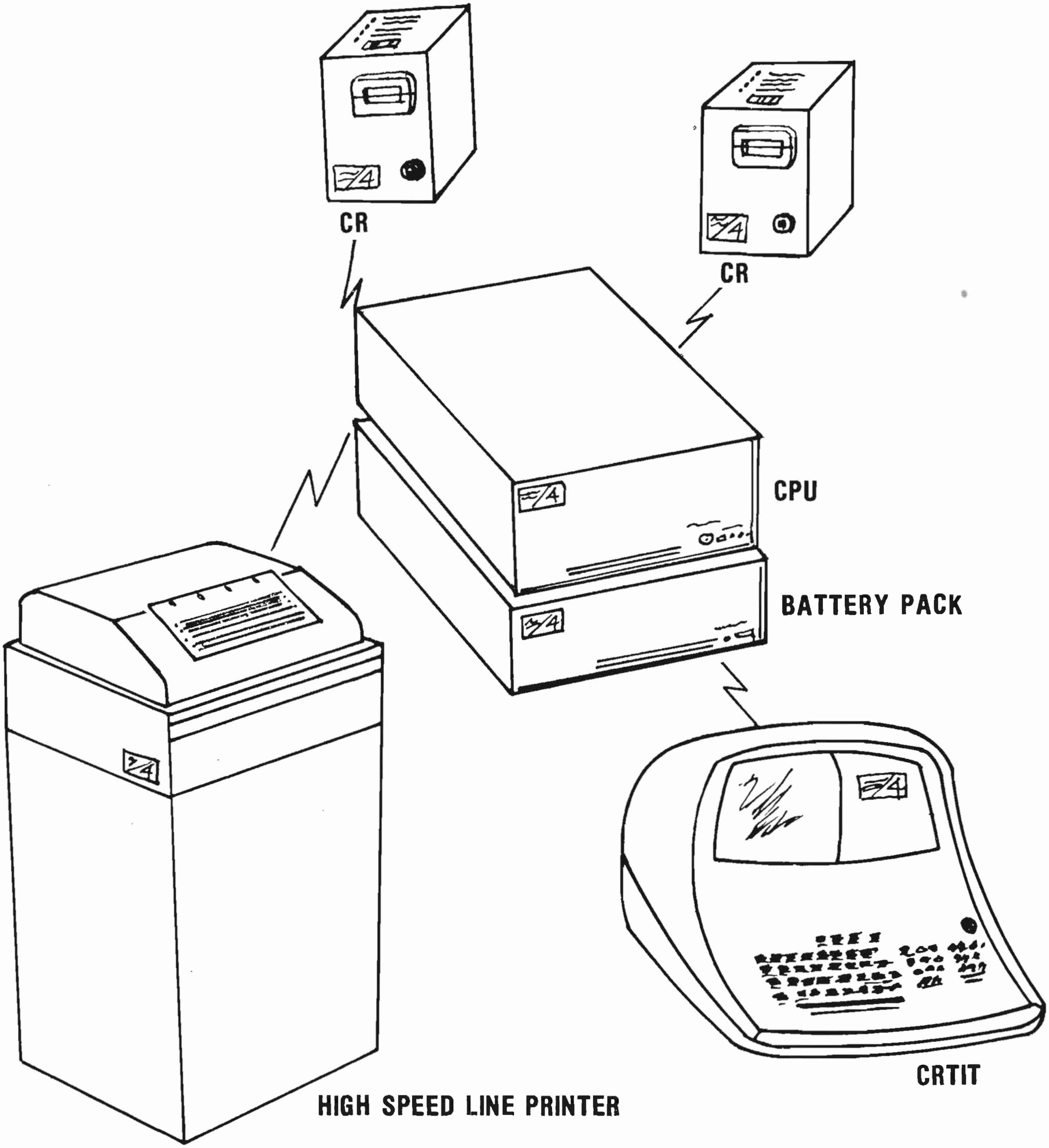


FIGURE 5. Vali-Dine Series/4 Equipment Configuration

The Cathode Ray Interactive Terminal (CRTIT) is used to check patron files, make changes in the files or, in general, instruct the computer to set up time schedules, produce reports, etc. In other words the unit gains access to the memory of the CPU and gives one the opportunity to manipulate the memory in any way required. All this can be accomplished rapidly since this unit operates at 9600 baud.

The line printer operates at 300 lines per minute and is contained in a soundproof enclosure. Reports that are on a daily time schedule are linked to the printer in order to produce a hard copy of daily transactions. To maximize the efficiency of the printer, a specialized serial transmission technique is used which operates at 56K bits per second. This enables the CPU to continue on-line terminal transactions while the printer is in operation. This is to say, while the printer is producing a report, all the readers remain on-line and operate normally.

A major software system controls the operations of the Series/4 computer. It consists of a real time operating system which coordinates the actions of a command line interpreter, a transaction processor, an Input/Output processor and a time activated command (time schedule). A special purpose language has been designed for the Series/4 System. It allows the operators of the system to maintain the data base through the use of words and phrases that are common to the areas of university food service. The language also serves a management information system which will produce summary information about the data base and student activity on a per meal and daily re-cap basis.

The Vali-Dine meal card contains a strip of imbedded magentic tape. The tape is imbedded under several layers of plastic and thus is less susceptible to erasure than other magnetic stripe cards. Vali-Dine's photo meal card program does not permit the user to prepare the actual meal card. The user photographs and gathers information on each patron but then must forward the pictures and data to R. D. Headquarters for the final stages of card preparation. Estimates obtained from users in industry indicate that R. D. Products returns the finished cards within two weeks of receipt.

PRINCIPLES OF OPERATION

When a meal card is inserted into a card reader, the system reads the patron's meal plan type and account status to determine if he/she is clear to eat, then informs the headcount monitor via indicator lights on the card reader. The responses of the card reader are:

- PASS
- MEAL EATEN
- MAX. MEALS EATEN
- INVALID
- MESSAGE

The MESSAGE light indicates that someone is trying to locate this patron and that he/she should contact the proper authority for further information. All the other responses are self-explanatory.

As presently programmed, the Series/4 generates only two types of management reports. Samples of these reports are contained in Figures 6 and 7. The Individual Status Report shown in Figure 6 portrays the current status (i.e., as of 3:37 PM on February 27, 1979) of patron account number 10004. This patron is on meal plan #1 which means (in this example) that this person is authorized to eat at all meals, on all days, as many times as desired until such time as his 25,600 points are used up (with the Vali-Dine System you have the option of simulating a cash program by defining the point value as $0.01 per point and charging customers a flat rate per meal).

It can also be seen from this report that this patron has 192.34 points remaining of the original 25,600 and that this account is still valid. The term "Activity" in this report refers to functions other than foodservice that the student might be allowed to participate in. For example, ACTIVITY #2 could signify library rights and a "yes" after this activity signifies that this student's account at the library is up to date and he/she is allowed to enter the library. A "no" after this activity would signify that the student's account is delinquent and he/she would not be granted access to the library.

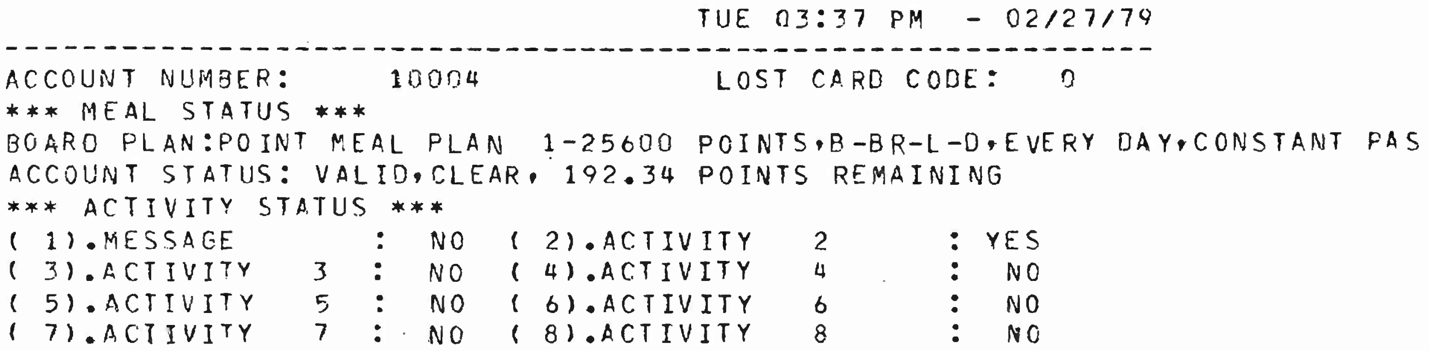
The Recapitulation Report formatted in Figure 7 gives, by reader location (LOC), and type of meal plan, (i.e., meal plan 2: any 10 meals) the total number of meals eaten, total number of points used, and the average value of meals sold (in points). It should be noted that if a simulated cash program is not desired, then the total number of points used and the average check value columns in this report would not be included.

SYSTEM COSTS

Under the constraints defined in this survey, the Vali-Dine system is available on a lease-only basis. As the pricing schedules in Tables 2 through 4 indicate, Vali-Dine equipment is reduced to 35% of the first year rental prices in effect at the time of renewal for the third and subsequent years. The second year equipment use charge is 35% of the first year charge.

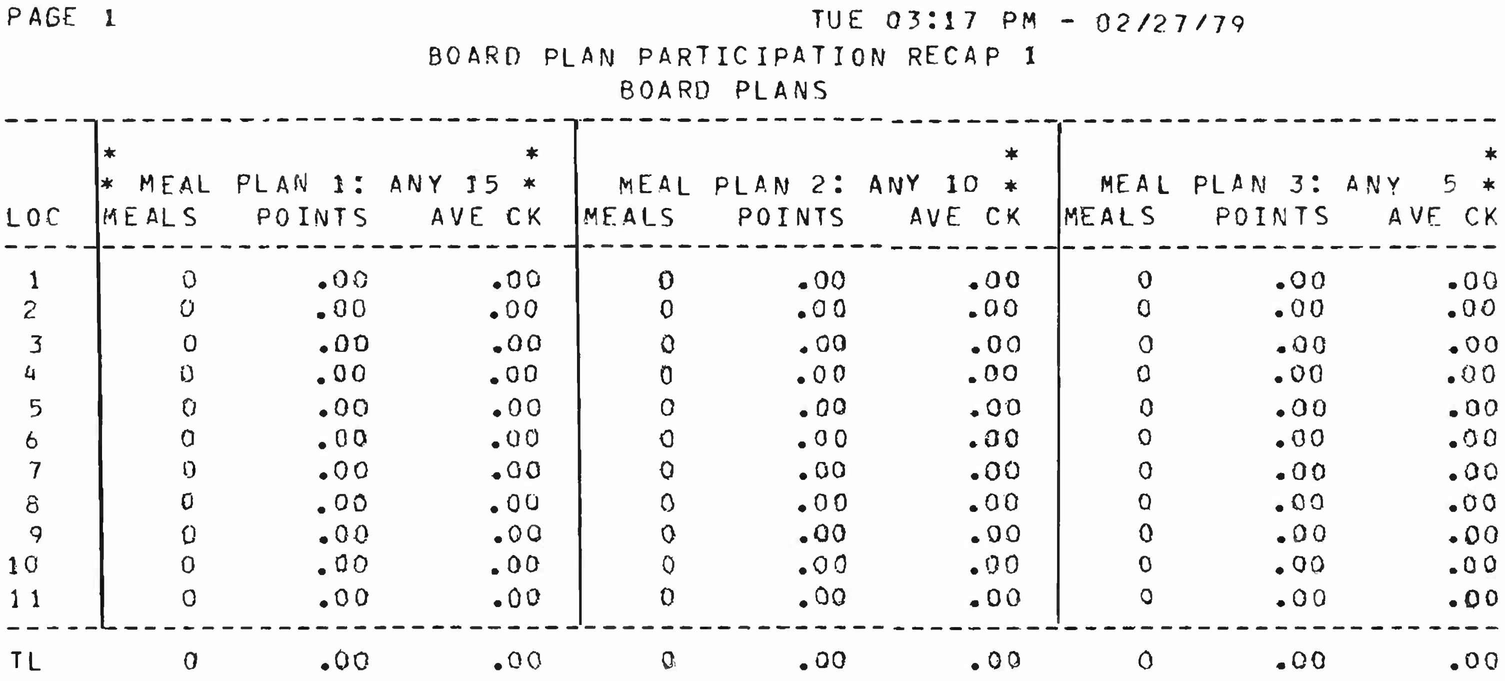
Table 2 contains the 1979 pricing schedule for the Series/4 hardware which includes a central processing unit, two card readers, an interactive terminal, and a printer. Total first year charges for this equipment would be $18,860. The estimated second year charge for this same equipment configuration would be $6,601.

The pricing schedule for Vali-Dine's meal card program is presented in Table 3. Depending on whether or not a photo meal card program is desired, not all of the supplies listed would be applicable. Specifically the Permanent I-D Camera and photo meal cards would not be required in a non-photo meal card program but the transparencies (containing the desired logo), non-photo cards, permanent information cards (for office record keeping purposes), an artwork and engraving plate, and an econder/verifier would be required.



```
                                           TUE 03:37 PM   - 02/27/79
-------------------------------------------------------------------
ACCOUNT NUMBER:      10004              LOST CARD CODE:    0
*** MEAL STATUS ***
BOARD PLAN:POINT MEAL PLAN  1-25600 POINTS,B-BR-L-D,EVERY DAY,CONSTANT PAS
ACCOUNT STATUS: VALID,CLEAR, 192.34 POINTS REMAINING
*** ACTIVITY STATUS ***
( 1).MESSAGE            :  NO  ( 2).ACTIVITY    2       : YES
( 3).ACTIVITY      3    :  NO  ( 4).ACTIVITY    4       :  NO
( 5).ACTIVITY      5    :  NO  ( 6).ACTIVITY    6       :  NO
( 7).ACTIVITY      7    :  NO  ( 8).ACTIVITY    8       :  NO
```

FIGURE 6. Vali-Dine Individual Account Status Report



```
PAGE  1                                           TUE 03:17 PM - 02/27/79
                            BOARD PLAN PARTICIPATION RECAP 1
                                      BOARD PLANS
-----------------------------------------------------------------------------------------
     |*                          *|                          *|                          *
     |* MEAL PLAN 1: ANY 15 *     |  MEAL PLAN 2: ANY 10 *    |  MEAL PLAN 3: ANY  5 *
LOC  |MEALS    POINTS     AVE CK  |MEALS    POINTS     AVE CK |MEALS    POINTS     AVE CK
-----------------------------------------------------------------------------------------
 1   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
 2   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
 3   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
 4   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
 5   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
 6   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
 7   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
 8   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
 9   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
10   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
11   |    0       .00        .00  |    0       .00        .00 |    0       .00        .00
-----------------------------------------------------------------------------------------
TL        0       .00        .00       0       .00        .00      0       .00        .00
```

FIGURE 7. Vali-Dine Recapitulation Report

TABLE 2

Vali-Dine System Hardware Proposal Pricing Schedule - January 1, 1979

Description	Quantity	Unit Price	Total
R. D. Series/4 CPU (est.)	1	$ 12,400.00	$ 12,400.00
Series/4 Card Reader (1:8 backup ratio) (quantity 1-3)	2	$ 1,100.00 ea.	$ 2,200.00
Series/4 CRTIT	1	$ 1,675.00 ea.	$ 1,675.00
Series/4 Line Printer (LP-300) with sound proof enclosure	1	$ 2,585.00 ea.	$ 2,585.00

TOTAL FIRST YEAR SERIES/4 SYSTEM HARDWARE USE CHARGE...(est.)$ 18,860.00

Estimated Second Year Series/4 Equipment Use Charge
is 35% of first year use charge........................... $ 6,601.00

TABLE 3

Vali-Dine Meal Card Program

Estimated Quantity	Supplies	Unit Price	Total
1	Permanent I-D Camera (includes any additional cameras required for mass photographing)	$ 450.00	$ 450.00
2800	Transparencies	$ .10 ea.	$ 280.00
2800	Non-Photo Cards	$ .75 ea.	$2,100.00
2800	Vali-Dine Photo Meal Cards	$ 1.50 ea.	$4,200.00
2800	Permanent Information Cards	$ .02 ea.	$ 56.00
1	R. D. Encoder/Verifier	$1,875.00	$1,875.00
1	Artwork & Engraving Plate	$ 150.00	$ 150.00

Note 1: Vali-Dine equipment is reduced to 35% of the first year rental prices in effect at time of renewal for the third and subsequent years.

Note 2: Proper Data Line Installation is the responsibility of the customer.

TABLE 4

Vali-Dine Series/4 System Summary Cost Proposal

	1979
Vali-Dine Series/4 Equipment Configuration Rental............$	18,860.00
Non-Photo Card Program.......................................$	4,461.00
Photo Card Program...$	7,011.00
TOTAL FIRST YEAR ESTIMATED COST WITH NON-PHOTO CARDS......$	23,321.00
TOTAL FIRST YEAR ESTIMATED COST WITH PHOTO CARDS..........$	25,871.00

Estimated Subsequent Year Cost	1980
Val-Dine Series/4 Equipment Rental...........................$	6,601.00
Non-Photo Card Program.......................................$	1,352.00
Photo Card Program...$	2,402.00
TOTAL SECOND YEAR ESTIMATED COST WITH NON-PHOTO CARDS.....$	7,953.00
TOTAL SECOND YEAR ESTIMATED COST WITH PHOTO CARDS.........$	9,003.00

The required supplies for a photo card program are: the Permanent I-D Camera, transparencies, photo meal cards, permanent information cards, an artwork and engraving plate, and an encoder/verifier. For the specific assumptions of this survey, the first year cost for a Vali-Dine non-photo meal card program would be $4,461, and the first year cost for a photo card program would be $7,011.

Subsequent year costs for Vali-Dine's meal card programs reflect the following four factors: (1) 800 new cards, with associated transpariencies and permanent information cards, would be issued per year, (2) the equipment use charge for the encoder/verifier would be 35% of the first year charge, (3) the equipment use charge for the I-D camera would be 100% of the first year charge (i.e., the unit price for the camera represents an annual charge), and (4) the price for the artwork and engraving plate is a one-time charge and is therefore not figured into the subsequent year cost estimates. Thus, estimated subsequent year costs for the non-photo program would be $1,352 and $2,402 for the photo card program.

A summary cost proposal is contained in Table 4. As this table indicates, the total first year estimated cost with non-photo cards is $23,321, and the first year estimated cost with photo cards is $25,871. Second year total costs for the equipment and non-photo and photo card programs are $7,953 and $9,003, respectively.

USER INTERVIEW

An interview was held with the Dining Service Manager at the University of New Hampshire where a Vali-Dine Series/4 System had been installed more than two years ago. In the manager's eyes, the Series/4 was cost effective and the system operators (e.g., the card clerk and headcount monitor) also praised the system. The central polling station, printer and data entry console are located in the University's computer facility thus benefitting from a controlled environment. Human error in forgetting to reset the equipment's internal time clock caused the loss of data from one breakfast meal. The two standard management reports provided with the Vali-Dine system have proven adequate for this university application.

EVALUATION FOR MILITARY APPLICATION

Of all the system reviewed in this report, the Vali-Dine system is, by far, the most prevalent in foodservice applications. The fact that it is currently used in over 200 foodservice facilities is a distinct advantage of the Vali-Dine system. Some of the other systems included in this report are not, at this time, involved at all in any type of foodservice operation and thus, Vali-Dine's widespread use indicates that R. D. Products' management possesses a level of foodservice expertise that is unmatched by its competitors. Another advantage of the Vali-Dine system is that it produces management-type reports which provide detailed information on individual patrons and on dining facility participation rates. Although these two particular reports do not currently conform to an acceptable audit trail definition, R. D. Products has assured NARADCOM that specific user designed formats could be provided, at an additional expense, should the system be procured.

A major drawback of the Vali-Dine system is that it is currently available only on a lease basis. And as shown in the cost analysis chapter of this report, this constraint has caused Vali-Dine's uniform annual costs to be extremely high. This policy, however, might be relaxed if the company were responding to a DoD-wide bid for automated headcount equipment. A more serious concern with respect to Vali-Dine's equipment is that, of all the systems reviewed, it appears to be the most sophisticated and, thus, perhaps the least "sailor-proof". For example, the equipment requires that the time clock be reset after any kind of power outage. If the time clock is not reset, the data collection and corresponding analyses are simply not performed. In fact this actually did occur at the University of New Hampshire (UNH) and they "lost" their breakfast-meal headcounts the day after they experienced a power outage.

Although the company literature does not indicate that a temperature-controlled environment is required for the reliable operation of the central processing equipment, UNH has located its equipment in its computing center. It was the feeling of the users at New Hampshire that the equipment was sensitive enough so that if located in any other place, reliability could be adversely affected.

Finally, as was mentioned previously, R. D. Products does not allow its users to assemble their own photo meal cards. The primary reason that R. D. Products has adopted this policy is that their technique for incorporating photographs onto plastic meal cards is a proprietary process. It should be noted that this constraint in a military environment would probably result in intolerable delays, administrative overhead, and reduced security. Should the Vali-Dine system satisfy other requirements, however, the system can be operated with non-photo meal cards and military ID cards as is presently done.

SECTION VII

RUSCO ELECTRONICS

Source: Rusco Electronic System
P. O. Box 5005
1840 Victory Blvd.
Glendale, CA 91201

SYSTEM OVERVIEW

The Rusco Model 540 is a microprocessor central controller capable of controlling up to 20,000 patron accounts and 256 Reader/Terminals. The Rusco 550 is a micro-auxiliary controller that interfaces directly with the 540. The function of the 550 is to maintain and update the transaction data from the 540. The basic 540/550 system includes 256 access levels and 127 time zones. Reader/Terminals may be connected directly up to a distance of 2 miles. Telephone modems may be connected to provide unlimited operating distances over telephone circuits.

Thr Rusco coded badge (entitled "Ruscard") employs a 25-mm by 55-mm strip of flexible magnetic material laminated inside a credit-card-size badge. The coding for the badge consists of magnetized spots permanently encoded at the factory. The Rusco card reader senses the magnetized spots using a 5 by 8 element array of magnetic sensors. The card reader can make individual access decisions based on the code or can signal the controller to check the corresponding access information that has been programmed into its memory. If access is denied, a red light flashes on the reader. A green light indicates that access should be granted.

Vendor supplied specifications are included in Appendix I and a photograph of the 540 Controller is shown in Figure 8.

PRINCIPLES OF OPERATION

Insertion of a Ruscard in a system reader activates the reader's built in microprocessor, which senses the digital code stored in the card's embedded memory core. If the Ruscard does in fact belong with this specific system, the reader will unscramble the card code bits into a system code and a cardholder ID number. If the card does not belong with the system, the reader's output will be "garbage".

The reader then transmits the system code and cardholder ID number of the 540. (For distancesup to two miles, communication may be over 2 wire pairs; longer distance transmission requires a dedicated full-duplex voice channel (such as a leased phone line) with a System 500 modem at each end). The card data are received by the central controller, checked for transmission errors, and the access decision process begins.

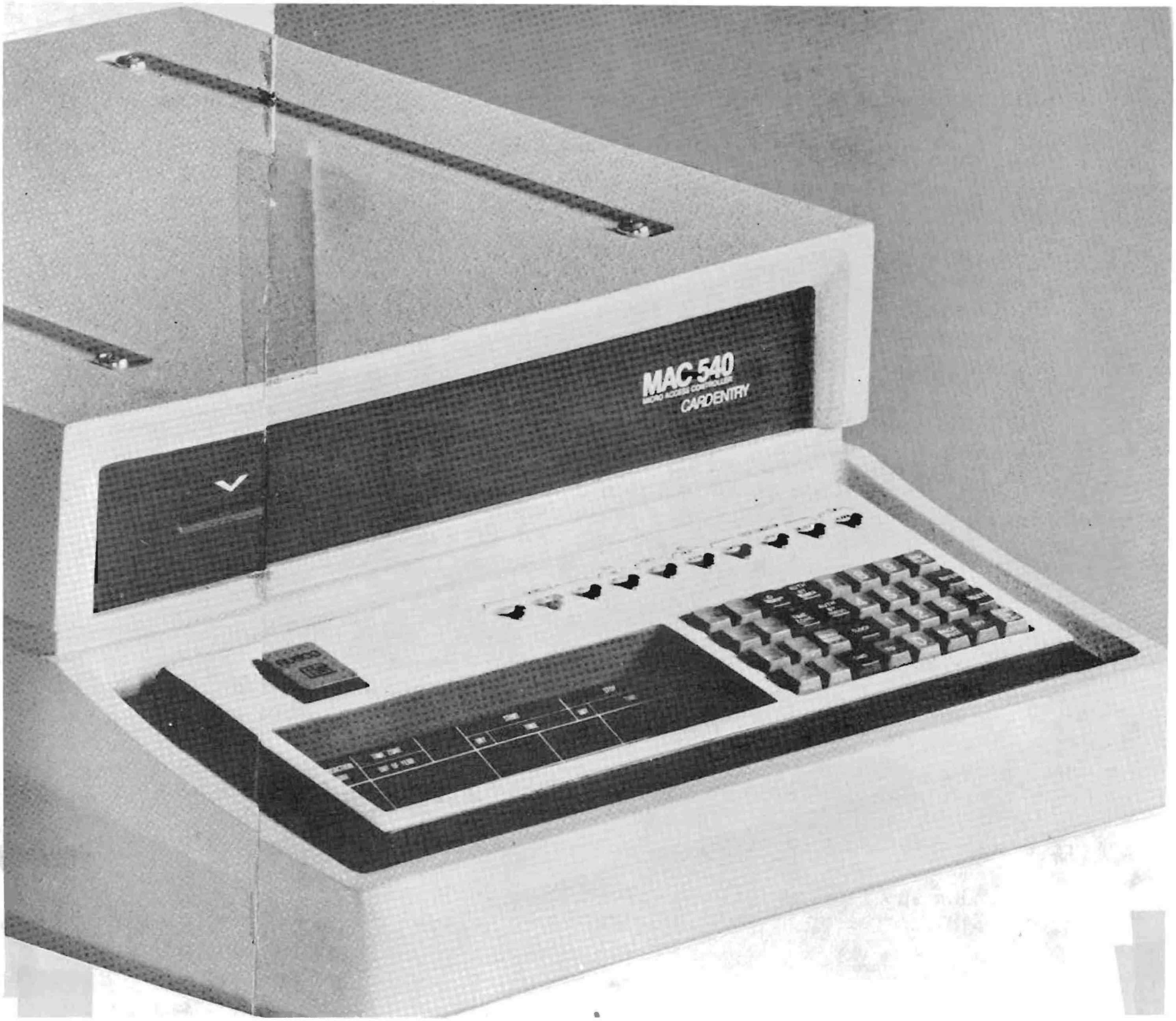


FIGURE 8. MAC 540 Controller

First the system code is verified as a double-check on the validity of the card. Then, the central controller begins scanning its memory in an attempt to find the cardholder ID number. If the number is located, indicating that the card is valid, its assigned status level, if any, is then examined. (A status level is a collection of cardholders with the same access privileges. It is defined by a list of instructions keyed into the controller specifying when access is permitted at each reader location in the system. Any cardholder's status level may be assigned or changed via the 540 keyboard). If the cardholder's status level specifies access at the reader location at the current time of day and day of week, the processor issues a "GO" command to the reader; otherwise, a "NO GO" command is issued. When the reader receives the access command, if the command is "GO" a green "GO" light on the reader faceplate lights.

At the same time that the processor is issuing an access command to the reader, a transaction record is formatted and sent to a system logging device (printer, magentic tape, etc.). The transaction record contains the reader location, time of day, cardholder ID number, cardholder status level, and a transaction code indicating the type of transaction.

Note that the controller makes four separate tests before granting access: correct system code, valid cardholder ID number, valid status level, and authorized time zone. Failure of any of these tests will cause denial of access, and will generate a transaction record in red ink on the printer logger, identifying the time, location, and cardholder ID number, and specifying the reason for denial of access. The format of this transaction record is similar to the format shown in Figure 1.

SYSTEM COSTS

An initial price quotation was received from Rusco Electronics in July 1979. At that time, it was explained that the proposal was incomplete and that another proposal which would address iteself to the 550, custom software, and Ruscards would be forthcoming. The follow-up information has not as yet been provided despite repeated requests by the authors. For cost comparison purposes, all known Rusco prices are included in this report.

Specifically, the following quotes were received:

1. Model 540 with Multiple Use Option:	$ 14,872
2. System Printer:	$ 1,720
3. 2 Card Readers w/Tamper Switches and No-Go Output:	$ 2,992
4. Interfaces and Modems:	$ 2,400

Thus, it is known that Rusco 540/550 System hardware would cost at least $21,984. Further, it can be assumed that the additional cost of the controller and customized software would significantly raise the total system cost.

In the absence of data from Rusco concerning their card costs, Ruscards were assumed to be between those of Vikonics and Cardkey since all three companies' readers utilize a magnetic-coded card. Thus, a Rusco card program for 2000 users who experience a 40% turnover and loss rate would cost (for the first year) approximately $4,158 for a non-photo application and approximately $7,348 for a photo application ($5,348 for the cards and $2,000 for the photographic equipment).

USER INTERVIEW

The Rusco installation at Walter Reed consists of a central polling device wired to badge readers in the cafeteria and other limited access areas. The foodservice division has not been able to use the Rusco equipment for its intended purpose, which was to eliminate the need for an individual assigned to the headcount/cashier function. The equipment was down at the time the site was visited.

EVALUATION FOR MILITARY APPLICATION

One advantage of the Rusco system is that there appears to be an in-place military expertise with respect to Rusco operations since this system is currently in operation at Walter Reed Army Medical Hospital. Although the Rusco system at Walter Reed is not specifically utilized in the foodservice function, the expertise currently being gained can be easily expanded to include headcount operations. Another advantage of the Rusco equipment is that its card readers accept magentic as opposed to magentic-striped cards. Magnetic cards, as was stated previously, are less susceptible then magnetic-striped cards to erasure and duplication.

On the negative side of the ledger, Rusco, in comparison to Cardkey, is a much more expensive alternative to produce a time-sequenced audit trail. It is the authors' opinion that these two systems are almost identical in terms of their capabilities and outputs. Both systems could be expanded to produce management reports the costs of which are unknown at this time. (Cardkey through their PASS system or through interfacing; Rusco with its 550). Furthermore, there is some evidence, based on the authors' experiences at Walter Reed, that implies that Rusco's maintenance policies might not be as rapid as would be desirable in a foodservice environment where failure to capture headcount data on meals would represent a serious accountability problem.

SECTION VIII

VIKONICS

Source: Vikonics, Inc.
23-25 East 26th Street
New York, NY 10010

SYSTEM OVERVIEW

The TAC-1000^{TM} microcomputer controller can accommodate up to 128 magnetic card readers and up to 4000 patron accounts. The Controller features a front panel Cathode-Ray-Terminal (CRT) display which interacts with the operator, and an 80-character hard copy printout which provides a numerical documentation of all transactions accompanied by a limited narrative. Reader/Terminals may be connected directly up to a distance of 1.5 miles without line compensation. For remote locations up to three miles from the Controller, a multiplexer can be used. Each multiplexer can handle up to 16 readers. For distances greater than three miles, telephone lines driven by modems must be used. TAC-1000 offers up to 128 access levels and up to eight time zones per day.

The TAC system has a floppy diskette capability. Up to 12,000 transactions or three day's worth of system activity (assuming 2,000 cards (representing either authorized or unauthorized patrons) are presented at two meal periods per day), can be stored on the diskettes. These stored transactions can be referenced through the keyboard on the Controller, and stored either by card number or by dining facility location. The system will print the sorted data thus providing separate audit trails for each dining facility or individual patron activity reports. The floppy diskette capability included in this system (at no additional charge) facilitates data transfer between the TAC and a mainframe computer so that any desired management reports could be obtained given the requisite programming.

Vendor supplied specifications are given in Appendix J and photographs of the TAC Controller and card reader are shown in Figures 9 and 10, respectively.

PRINCIPLES OF OPERATION

The TAC system operates with a magnetically encoded, plastic encased, credit-card-sized badge. Each card that is to be used with the system is programmed at the Controller with identification number, access level, and time zone. A card may only be inserted into a reader when the INSERT card light is flashing. Once inserted, the reader indicates via flashing lights with ENTRY GRANTED or ENTRY DENIED and a simultaneous hardcopy record is printed. A sample Vikonics output is shown in Figure 11.

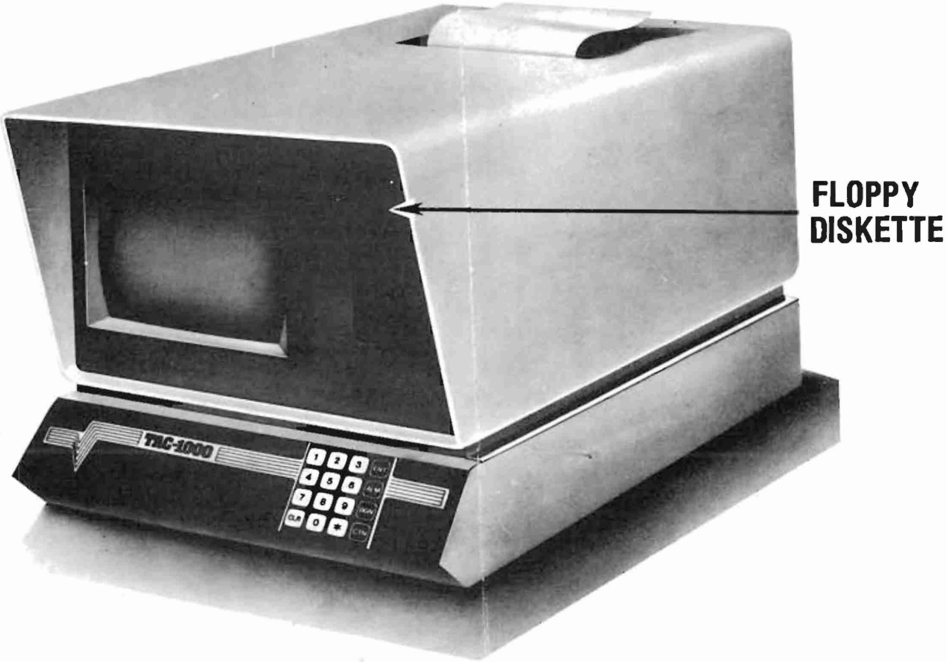


FIGURE 9. TAC 1000 Controller

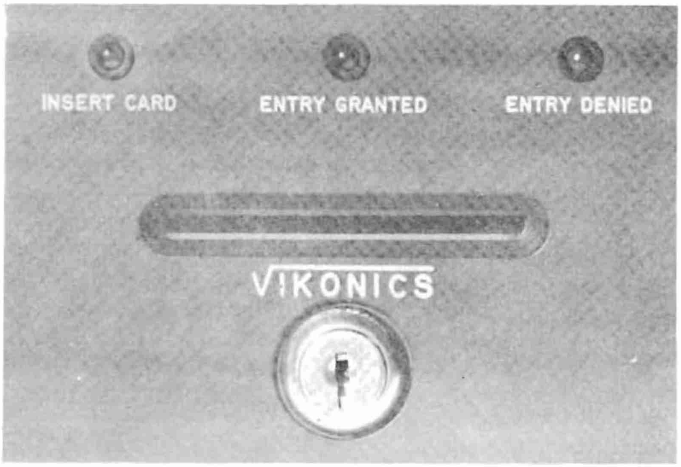
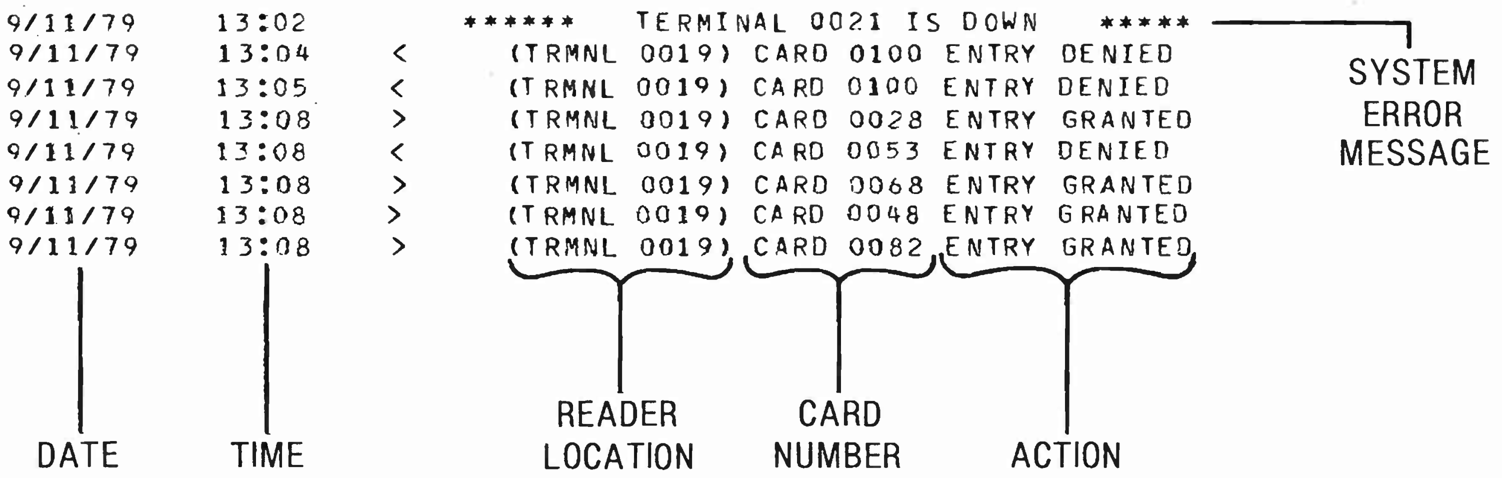


FIGURE 10. Vikonics Card Reader



```
9/11/79    13:02          ******   TERMINAL 0021 IS DOWN    *****
9/11/79    13:04    <       (TRMNL 0019) CARD 0100 ENTRY DENIED
9/11/79    13:05    <       (TRMNL 0019) CARD 0100 ENTRY DENIED
9/11/79    13:08    >       (TRMNL 0019) CARD 0028 ENTRY GRANTED
9/11/79    13:08    <       (TRMNL 0019) CARD 0053 ENTRY DENIED
9/11/79    13:08    >       (TRMNL 0019) CARD 0068 ENTRY GRANTED
9/11/79    13:08    >       (TRMNL 0019) CARD 0048 ENTRY GRANTED
9/11/79    13:08    >       (TRMNL 0019) CARD 0082 ENTRY GRANTED
```

SYSTEM ERROR MESSAGE
DATE
TIME
READER LOCATION
CARD NUMBER
ACTION

FIGURE 11 SAMPLE VIKONICS OUTPUT

SYSTEM COSTS

The following price quotations were received by NLABS in September 1979 from a Vikonics sales representative.

HARDWARE	COST	CARDS	COST
Central Console and Data Entry Device	$ 11,200	2,800 Non Photo	$ 5,460
		2,800 Photo	$ 6,860
Printer	2,250		
2 Card Readers	2,000		
Interfaces	No Charge		
Total Hardware:	$ 15,450		

The purchase price, given the assumptions of this survey, for a TAC 1000 system with non-photo meal cards would, therefore, be $20,910: $15,450 for the system hardware and $5,460 for the meal cards. The TAC system with photo meals can be purchased for $22,310: $15,450 for the hardware and $6,860 for the cards. In the second and subsequent years, 800 new non-photo cards costing $1,560 or 800 new photo cards costing $1,960 would be issued. Besides the film costs for the photo cards, the cost of the 800 new cards that would be issued each year is the only other cost that would be incurred in the second and outyears of operation. The cost analysis chapter of this report incorporates film and photographic equipment costs into the calculation of this system's uniform annual cost.

EVALUATION FOR MILITARY APPLICATION

An advantage of the Vikonics system is that it provides system error messages. NLAB's past experiences with automated headcount system (Fort Lewis and Travis) have shown that it is helpful to have a system's error messages recorded so that a dining facility manager's claims that manual headcounts were obtained because a reader was down can be verified. A second advantage of the Vikonics equipment is that it provides floppy diskette capability and can sort and print out the data base by dining facility location or meal card number. If a "grow-to" capability is an important selection criterion for an automated headcount system, then the Vikonics system is one which will allow an easy transition to higher ration accountability functions. While the TAC-1000 is significantly more expensive than some of the other access control systems described in this report, it must be emphasized that its cost includes its diskette which allows greater storage and sorting capabilities.

The only apparent cause for concern with the TAC system is that, like Vali-Dine, the central processor might require a temperature-controlled environment. It should be noted that since NLABS was not able to interview users of this equipment, this is offered as a precautionary remark rather than an authoritative statement.

SECTION IX

SCHLAGE ELECTRONICS

Source: Schlage Electronics
3260 Scott Boulevard
Santa Clara, CA 95051

SYSTEM OVERVIEW

The Schlage System employs a standard credit card sized, passive-electronic coded vinyl badge and a proximity badge reader technique. That is, when a badge is positioned within 10 cm of a badge reader, it is automatically interrogated and the badge code is transmitted to the control processor for validation. This system is less vulnerable than other readers to tampering and direct physical attack because the badge reader can be housed inside a wall or desk and hence, have no exposed parts.

Model 414 can control up to eight badge readers located up to 2,000 feet from the control processor. (Expanding capabilities for additional distance are not available). The standard 414 system also has a memory capacity for 1,500 individual patron accounts, 8 time zones, and 255 access levels. The system can not be interfaced into a mainframe computer to produce management reports, nor can it do any data processing to sort transactional data by dining facility location or meal card number. Company representatives have indicated, however, that larger scale versions of the 414, capable of operating at longer distances, performing data processing activities, and interfacing with a host computer, are available and that 414 can be expanded to handle 2000 patron accounts.

Vendor supplied specifications are given in Appendix K and a sample equipment configuration is shown in Figure 12.

PRINCIPLES OF OPERATION

The Schlage system's card-reader operates by proximity. A hidden sensor reads the credit-card-sized command card and transmits signals to a control unit, which regulates access, and to a printer, which records access and attempts. Access is gained by placing an authorized command key within 4 inches of the sensor that is located near the access point. If the user is authorized for that door, at that time, a green light flashes on the sensor. At the same time, the system prints the date, time, key number and the access location. Unauthorized attempts cause a red light to flash and are recorded and printed in red ink with an additional code indicating the reason for rejection. A sample Schlage report is shown in Figure 13.

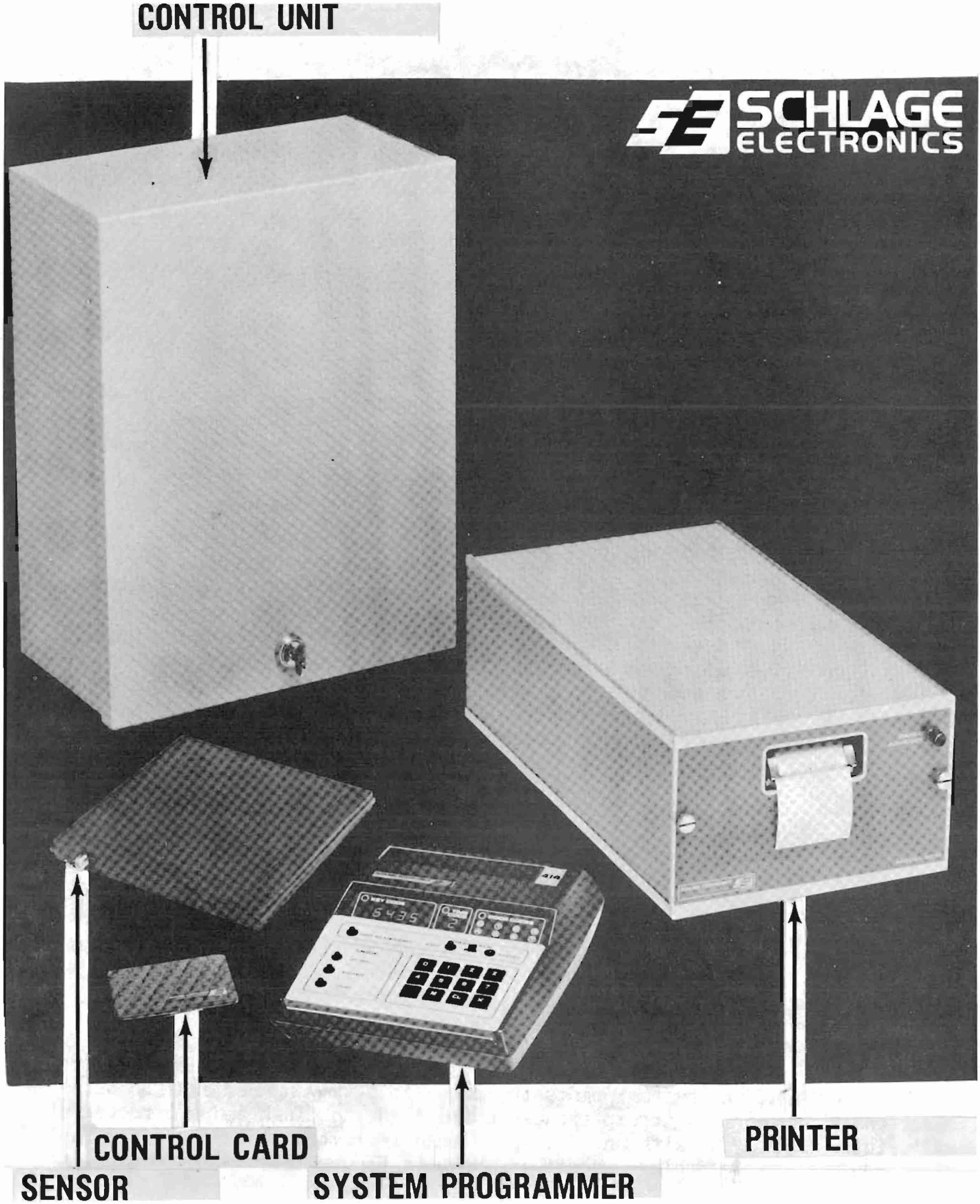
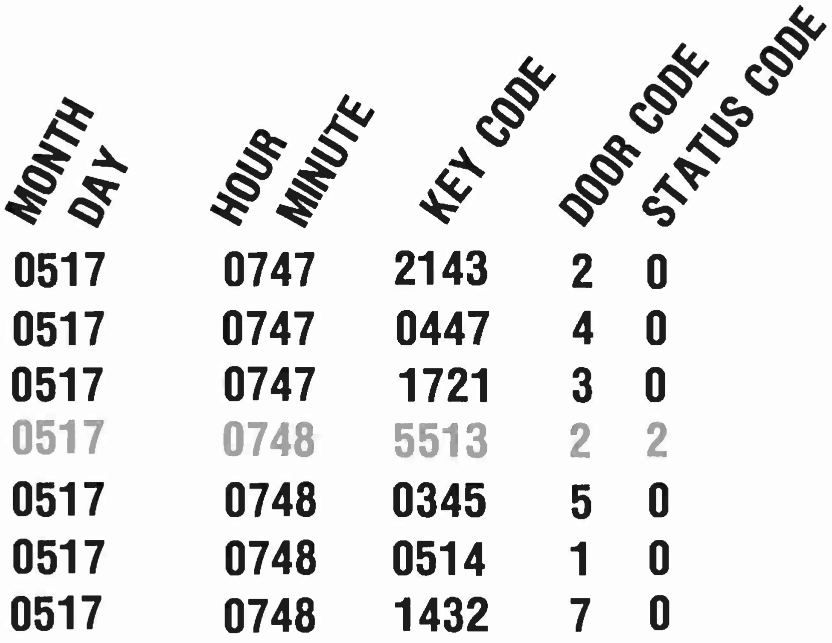


FIGURE 12. Schlage 414 Equipment Configuration



```
MONTH  HOUR    KEY   DOOR  STATUS
DAY    MINUTE  CODE  CODE  CODE
0517   0747    2143  2     0
0517   0747    0447  4     0
0517   0747    1721  3     0
0517   0748    5513  2     2
0517   0748    0345  5     0
0517   0748    0514  1     0
0517   0748    1432  7     0
```

FIGURE 13. Sample Schlage Output

System programming is performed on a small desk-sized unit which plugs into the control unit. Three modes of operation are available. The scan mode is used to display the contents of memory. The enter mode is used to enter or update key codes, time zones, or door authorizations. The void mode is used to void or "rule out" a key code. When not in use, the programmer can be easily removed for safe-secure storage.

SYSTEM COSTS

In September 1979, the following price quotations were received by NLABS from a Schlage sales representative:

HARDWARE	COST	CARDS	COST
System 414 Control Unit	$ 5,000	2,800 Non-Photo	$ 9,100
2 Sensors (Card Readers)	500	2,800 Photo	$11,200
System Programmer (Data Entry Device)	1,200		
Printer	1,000		
Interfaces	2,400		
Total Hardware	$10,100		

It should be noted that under the assumptions guiding this survey, the cost of just the required amount of Schlage photo cards excees the costs of the system hardware. A photographic system (i.e., camera, laminator, and die cutter) would also have to porcured if a photo meal card program is desired. An estimate obtained from a Polaroid representative for such a system is $2,000. Thus, the total system procurement cost for a Schlage 414 system with photo meal cards would be $10,100 for hardware plus $11,200 for photo cards and $2,000 for a photographic system, or $23,300. The same system without a photo meal card program would cost $19,200. Under the assumptions of this survey, in the second and subsequent years, a cost of $2,600 for 800 non-photo cards or $3,200 for 800 photo cards would be incurred.

EVALUATION FOR MILITARY APPLICATION

The passive-electronic card utilized in the Schlage system is the most durable card identified in this survey. It is also the card that is most difficult to decode or destroy. The durability of Schlage's card is this system's primary advantage. Another advantage of the Schalge system is that it would allow the fastest throughput of patrons at the headcount station because unlike other systems, patrons do not have to wait while their cards are inserted in and out of a reader.

On the negative side of the picture, the Schlage 414 system is costly. The system's cost is primarily due to the high cost of the cards employed (In fact, 2,800 photo-Schlage cards cost more than the hardware that is needed to support those cards). Furthermore, the 414 can neither interface with a mainframe computer nor perform any data processing activities so that dining facilities could receive their own audit trails. And again, as with other access control systems, Schlage's readers do not contain counters as integral parts. Such counters would be an additional item of expense.

SECTION X

INTERNATIONAL BUSINESS MACHINES (IBM)

Source: IBM
General Systems Division
Northside Parkway
Post Office Box 2150
Atlanta, GA 30301

SYSTEM OVERVIEW

The IBM controlled access system utilizes a magnetic-stripe credit card encoded with a 10-digit credential number. The control element for the system is an IBM Series/1 mini computer. The Series/1 could be used for other tasks in addition to access control as the use of a computer allows a great deal of flexibility in the operation of the access-control functions.

The system is designed to permit entry only to personnel who are currently authorized to enter a specific area. Access to as many as 63 points may be controlled by this system. Each of these points to which a badge reader is connected may be assigned to one of fifteen access control classes or groups. The basic system allows each of 1,000 individual magnetically encoded badges to be assigned to one or more of these access levels. Up to 4,000 badges may be assigned, without program modification, by expanding the system storage capacity.

The IBM magnetic-stripe card readers can be mounted on a door,wall or pedestal. They sense the coded data from the magnetic-stripe and transmit the signal by telephone-type wires to the Series/1. All data transmitted by the card reader and all control signals received by the card reader are over four wires. The maximum direct wire separation from a card reader to the Series/1 is five wire miles. For installations with more remote requirements, translators or modems allow distances greater than five wire miles over voice grade communications facilities. (A wire mile is defined as the amount of wire that would be required to link two points that are located a mile apart together. That is, a wire mile is the minimum length of wire required to cover the distance of one mile).

The IBM Controlled Access System uses the IBM 4974 Bidirectional Printer for recording system activity, including: access data, invalid entry attempts, with time and date indicated. Operation of the system is provided through the use of the IBM 4979 Display Section as a keyboard console. The console operation is designed to guide the operator through each procedure with simple step-by-step instructions. Minimal training would, therefore, be required in order to become confortable in operating the system.

Vendor supplied specifications on the Series/1 are provided in Appendix L and a sample equipment configuration is shown in Figure 14.

PRINCIPLES OF OPERATION

The person desiring entrance to a controlled area inserts his/her card into the slot provided in the reader. If the Series/1 allows access, the door control mechanism or other device (i.e., a flashing light) is activated and allows entry. If access is denied, the light will not flash and the person attempting to gain entrance can insert the card again. Each time the card is inserted, the data is read and transmitted to the Series/1 for a decision and is automatically logged on the system's printer. The printed log contains a record of all system activity including: access data, invalid entry attempts, time of day, date, door, and badge number.

The IBM system can be programmed by the user or by the manufacturer for a minimal fee to provide anti-passback capabilities, individual audit trails for each dining facility, and management type reports. No additional hardware would be required as a floppy diskette is already included in the cost proposal presented in Table 5.

SYSTEM COSTS

The minimum Series/1 equipment configuration for 2,000 badges and 2 doors is comprised of 14 individual hardware components. The associated purchase prices and mandatory monthly maintenance fees for these components are listed in Tables 5 and 6.

Thus, the cost of an IBM Series/1 configuration for 2,000 patrons and 2 doors includes a purchase price for the hardware elements, a monthly maintenance fee for those components, and a monthly software charge. First year expenditures for the Series/1 equipment configuration would, therefore, be $26,664: $22,662 for the hardware, $2,262 for the yearly maintenance fee, and $1,740 for the yearly software charge. In the second and each year thereafter a charge of $4,002 would be incurred: $1,740 for the use of IBM's software package and $2,262 for the mandatory yearly maintenance fee.

For the specific card-related assumptions of this survey, the first year cost of a non-photo program would be $3,417: $100 for the one-time layout charge, $3,248 for the card stock, and $67 for the setup charge. For the second and subsequent years, the cost of a non-photo card program would be $997: $928 for the card stock plus $67 for the order setup charge. A photo card program would cost $4,061 in the first year: $3,892 for the cards, $100 for the layout, and $67 for the order's setup. For the second and subsequent years, a photo card program would cost $1,181: $1,112 for the cards and $67 for the setup charge.

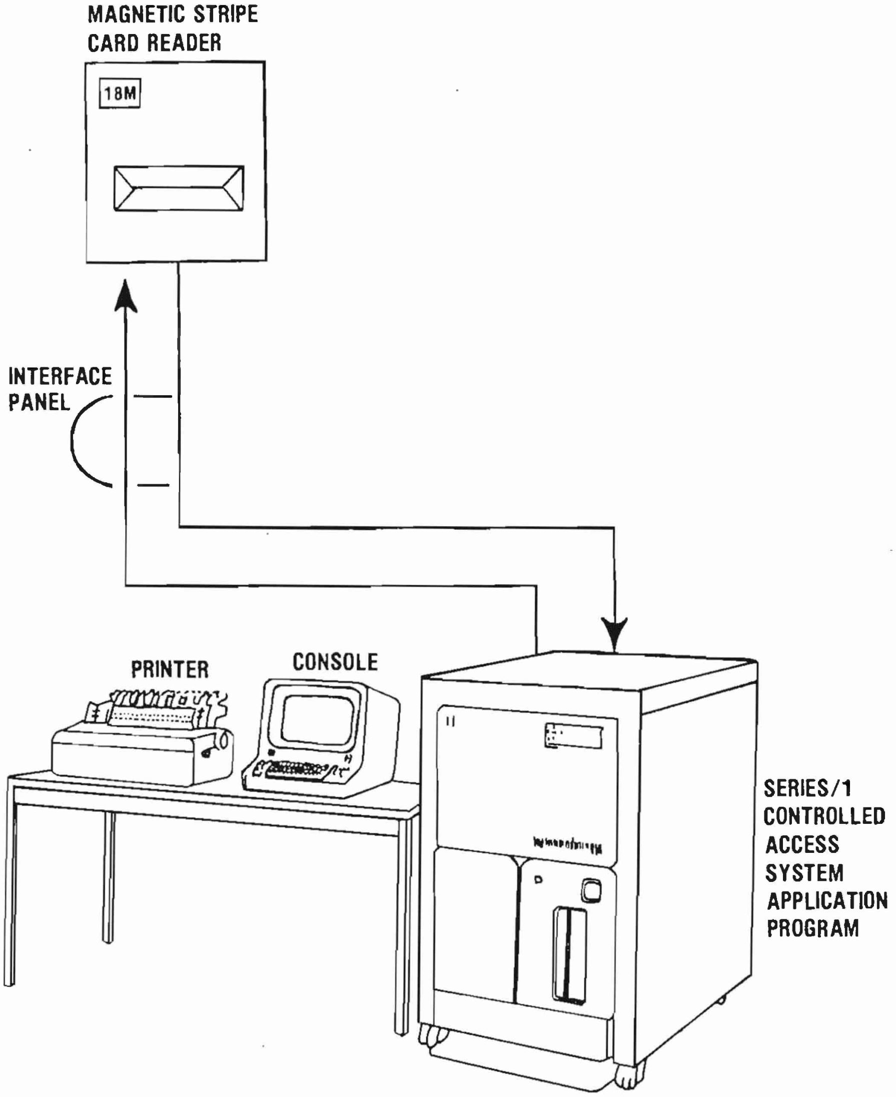


FIGURE 14. IBM Series/1 Controlled Access System Configuration

TABLE 5

IBM Series/1 Summary Cost Proposal

Hardware Component	Purchase Price	Monthly Maintenance
32K Processor	$ 7,400	$ 83.00
Diskette Attachment	730	6.00
Display Station Attachment	955	7.00
Printer Attachment	930	3.50
Timer	570	4.00
Integrated Digital Input/Output	825	12.00
Rack Mounting	55	N/C
Additional Storage-16K	1,750	6.00
Diskette	2,410	17.00
Printer	2,790	32.00
Display Station	1,735	16.00
Metre Rack	870	2.00
2-Card Readers	544	N/C
Interface Panel	1,098	N/C
Total	$ 22,662	$ 188.50
Software Charge	Purchase Price	Monthly Maintenance
Series/1 Software	N/C	$ 145.00

TABLE 6

Detailed Card Costs For IBM Series/1 System

Item	Cost	Set-Up Charge/Order
Layout Charge	$ 100.00[a]	
Basic Plastic Card	.12[b]	$ 40.50
Magnetic Stripe	.12[b]	
Signature Panel	.01[b]	
Printing	.52[b]	28.00
Arrow for Proper Insertion	.02[b]	
Encoding Charge	.37[b]	
Total Cost of a Blank Card	$ 1.16[b]	
Total Set-up per Order		$ 68.50
+ Polaroid Flap	+ .23[b]	
Total Cost of a Photo Card	$ 1.39[b]	

[a] One Time Only

[b] Each Card

In summary, the first year cost of an IBM Series/1 with a non-photo program would be $30,081. The second and subsequent years' cost for the Series/1 with a non-photo card program would be $4,999. The Series/1 with a photo-card program would cost $30,725 in the first year and $5,183 in the second and subsequent years.

EVALUATION FOR MILITARY APPLICATION

The advantages and disadvantages of an IBM Series/1 system in a military environment are very much similar to those already enumerated for the Cardkey and Vikonics systems. In each case, however, IBM represents a more expensive alternative to achieving roughtly the same results as Cardkey and Vikonics can accomplish. It should be noted, however, that the field service force in IBM is a large and experienced one. An IBM customer can feel confident that, in years to come, his system will be serviced in a timely manner. The field organizations of those companies whose primary business is in the access control idustry are not as yet as developed as IBM's due to the fact that these companies are still relatively new. On those military installations which currently employ IBM mainframe computers, an additional advantage would accrue in that the Series/1 would, of course, be directly compatible with existing computation facilities. This becomes particularly important in any grow-to kind of application.

SECTION XI

APD SECURITY SYSTEMS

Source: APD Security Systems
Division of Automatic Parking Devices, Inc.
24700 Crestview Court
Farmington Hills, MI 48018

INTRODUCTION

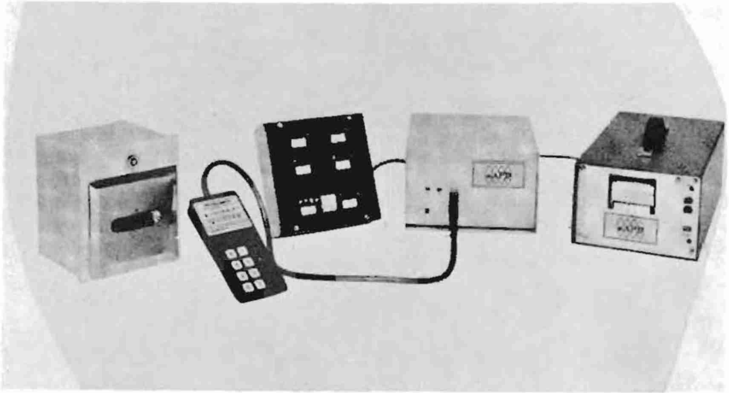
APD offers two configuration methods for its access control system. It can either be operated as a stand-alone or an on-line system. The discussion of APD's systems, however, will be limited to its stand-alone system because it was determined that the on-line system would cost over three times as much as the stand-alone system and would not offer any recognizable advantages over the stand-alone system. The main reason why the on-line system is so much more expensive is that its distance limit is 4,000 feet*, and as a result, two separate and complete systems would be required to satisfy the assumptions of this survey. For the sake of completeness, however, the system cost and all manufacturer supplied literature on the on-line system are given in Appendix M. Sample equipment configurations for both systems are shown in Figure 15.

PRINCIPLES OF OPERATION

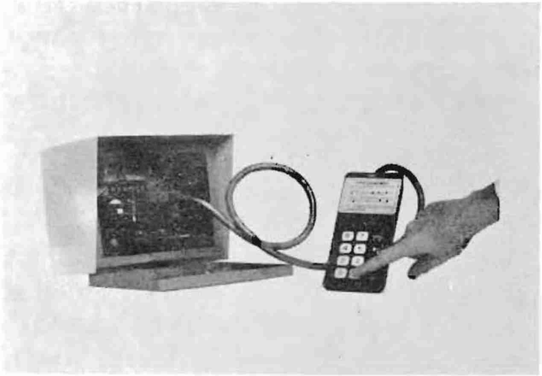
The 740 Series Programmable Off-Line Reader is a stand-alone programmable unit capable of accepting up to 4,000 individually coded cards. The cards used are the APD "Optic Kards" which may be programmed in or out of memory by a hand-held programmer. Coding is accomplished with optical filters which can only be decoded by the reader. Having access to the precise optical filter in the card would not benefit a counterfeiter since the card contains a plurality of different filters all separately assigned to an analog value in the reader. The filters are inaccessible, invisible, and part of the plastic itself. Cards are factory encoded upon order.

The 740 Series is an off-line unit which does not require any wiring back to a central unit. Voiding or validating cards from the system is accomplished by simply opening the front panel door of the reader, plugging in the hand-held programmer, and entering the card number on the programmer's keyboard. A bright four-digit display shows the number and its status. The card status can be changed by pressing just two buttons. An optical unauthorized card alarm is available that will signal when a voided card has been inserted into the reader. This feature facilitates recovery of lost or stolen cards.

*Information was furnished by a company representative in a telephone conversation.



On-Line Central Memory System



Programmable Off-Line Reader

FIGURE 15. Sample APD Equipment Configurations

Many options are available including anti-passback, time zones, and printer interface. The APD printer unit offers an eighteen column capacity with black printing for all valid entries and red printing for all invalid attempts. The unit prints out month and day, twenty-four hour time, location or station number, and card number.

SYSTEM COSTS

Hardware and card costs are presented below for both the stand-alone and on-line systems.

STAND-ALONE SYSTEM HARDWARE	COST
Station Equipment (1 station)	
Card Reader	$ 2,150
Printer	1,400
Power Supplies	90
Reader Enclosure	100
Mounting Enclosure	100
Printer Interface	150
Hand-held Programmer	750
Cost Per Station	$ 4,740

ON-LINE SYSTEM HARDWARE	COST
Equipment	
2 Memory Centrals	$ 5,990
2 Printers	2,800
2 Expanders	1,500
2 Card Readers	1,730
4 Power Supplies	180
2 Printer Interfaces	300
2 Hand-held Programmers	1,500
Total Hardware Cost	$ 5,600

CARDS - BOTH SYSTEMS	COST
2800 Non-Photo Optic Kards ($2.00/card)	$ 5,600
2800 Photo Optic Kards ($3.50/card)	$ 9,800

A stand-alone system with 2 reader stations, 2000 current patrons, 800 patron turnover and replacement accounts, and a non-photo card program would cost $15,080 in the first year: $9,480 for two reader stations and $5,600 for the non-photo card program. In the second and subsequent years, under the assumptions of this survey, this configuration requires that a $1600 cost be incurred in each year so that 800 new cards can be issued.

The same configuration as above with the exception of having a photo-card program instead of a non-photo program would cost $19,280 in the first year. To replace 800 cards per year in the second and subsequent years would cost $2,800 per year. It should be noted that the cost of the photographic equipment and film is not considered here but is given extensive treatment in the Cost Analysis Section of this report.

EVALUATION FOR MILITARY APPLICATION

The principle feature of APD that offers a competitive edge is its stand-alone capability. For application in the Navy or for remote feeding sites with one enlisted dining facility and few patrons, the stand-alone mode could be very useful. Furthermore, in a stand-alone mode, one printer would be located in each facility and therefore separate audit trails could be generated for each location. It does, however, require that each reader be programmed individually. On large installations, of course, this requirement is impractical. The optical card used in APD's system is also an attractive feature. It is more difficult to duplicate or destroy the optically encoded information on APD's cards than it is to do so on a magnetic or magnetic stripe card. The APD system appears to have no unique problems that are not shared with other types of access control equipment.

SECTION XII

ECONOMIC ANALYSIS OF ALTERNATIVE SYSTEMS

INTRODUCTION

A uniform annual cost method was used as a basis to compare the cost of each system. Annual costs have the advantage of incorporating into a single figure the investment and recurring costs with each alternative.

We have chosen to include meal card costs in this economic analysis even though there is a high probability that a magnetic striped military ID card will be used in future automated headcount systems. When such a card has been officially adopted, there will be no need for separate machine-readable meal passes. In the interim, the only viable alternative to automated access control at the dining facility entrance entails separate cards. Hence we have included these costs in our analysis.

ASSUMPTIONS

The following assumptions were made in performing this analysis:

1. The discount rate is 10%.*

2. The economic life of each system is 8 years.**

3. The total number of patron accounts will remain a constant 2,000 over the period of analysis.

4. Each year 800 new cards will be issued due to an assumed 40% turnover and replacement rate.

5. The various system configurations and associated interfaces etc., recommended by each vendor are adequate to satisfy the specified functional requirements and size and distance constraints established for this survey.

It is expected that film costs will be the only incremental costs incurred as a result of automating the headcount function as it was also assumed that:

*This rate was established by DODI 7041.3. It is the rate that is used in all economic analyses of proposed Defense investments.

**The DoD Economic Analysis Handbook, 2nd Edition, ALM 61-3517-H6, has established the economic life of automated data processing equipment to be 8 years.

6. The manpower and staffing levels currently required to operate a signature headcount system are sufficient to man the automated systems presented here, and

7. The amount expended on paper supplies in these systems would remain unchanged from the manual system because the expense for signature sign-in sheets would, to a large degree, be replaced by the expense for computer paper or paper tapes.

COST ELEMENTS

The following elements were identified as major costs areas in this analysis: hardware, plastic cards, software, and photographic film and equipment.

Hardware and software costs were based on the particular equipment configurations recommended by each of the alternative manufacturers, and the cost proposals or catalogs sent by those manufacturers. Annual costs for the hardware and associated software were calculated by taking into account the specified lease or purchase price, economic life, and the discount rate of investment dollars.

Card costs were analyzed in two categories: non-photo cards and photo cards. As stated previously, the choice of having photo cards or not is entirely up to the user, hence, both types of card options were considered in this analysis. Annual costs for the cards were calculated by taking into account the manufacturers' costs quotes and the number of cards that would be required in each year.

Photographic equipment and supplies were analyzed in conjunction with photo cards. Annual costs for the photographic systems were based on either a manufacturer specified lease price or on a cost quotation received from Polaroid Corporation for their ID System 3. (The Vali-Dine System was the only system identified that utilizes its own photographic equipment; the other seven systems are all compatible with the ID System 3). Film costs were estimated at $0.2906 per picture and were based on discussions with Polaroid.

OPERATIONAL SYSTEM CAPABILITIES

In addition to the costs, other system parameters are important in deciding which system is best suited for a particular application. In particular, such considerations as rate of card reader response, operating environmental temperature tolerance, or distance required between terminals and readers might make a particular system more suitable for small bases than for larger installations. Table 7 presents a summary of each system's characteristics.

TABLE 7

SUMMARY OF SYSTEM CAPABILITIES

SYSTEM	TECHNIQUE	MAXIMUM BADGE CAPACITY	MAXIMUM NO. OF READERS	DISTANCE LIMITS	MAXIMUM RESPONSE TIME	RECOMMENDED OPERATING TEMPERATURE
IBM Series 1	Magnetic-Stripe	Unlimited	31	5 wire miles[b]	5 Sec.	50° to 125°F
Rusco Model 540/550	Magnetic	20,000	256	2 miles[b]	5 Sec.	32° to 120°F
Vali-Dine[a] Series 4	Magnetic-Stripe	Unlimited	24	Unlimited	4.5 Sec.	65° to 70°F
Vikonics TAC 1000	Magnetic	4,000	128	1.5 miles[b]	1.5 Sec.	32° to 130°F
Cardkey Model 790	Magnetic	2,500	16	1.5 miles[b]	2.3 Sec.	38° to 85°F
Identimat Stand-Alone	Magnetic-Stripe	10,000	Unlimited	Unlimited	1 Sec.	50° to 100°F
Schlage Model 414	Passive-Electronic	1,500[c]	8	1000 ft.	1.4 Sec.	20° to 120°F
APD Offline	Optical	4,000	Unlimited	4000 ft.	4 Sec.	10° to 125°F

[a] Central mini-processor must be in a controlled environment.

[b] Without telephone modems which enable operation over telephone lines to any distance.

[c] For more capacity, contact factory.

RESULTS

Table 8 presents the first year and uniform annual cost for each of the alternative systems. This analysis shows that:

1. The Cardkey and Identimat systems represent the two least costly options in terms of both first year outlays and uniform annual costs.

2. The uniform annual cost rankings (i.e., least expensive to most expensive) differ between the photo and non-photo card programs. These differences are completely attributed to the incremental amounts that manufacturers charge for their photocards.

As noted in the earlier discussion of audit findings, the costs for even the most expensive system are less than half of the probable monetary losses from unauthorized meals on the audited Navy installation. There appears to be, therefore, some basis for expecting an automated headcount system to be cost-effective.

CONCLUSIONS AND RECOMMENDATIONS

Although this effort and survey were directed towards cataloging and reporting on available automated card-reading systems, it was difficult to ignore previous research, recent audit reports, and some misconceptions which are associated with automated card-reading systems. Therefore, it was important to insure that the conclusions and recommendations that follow consider all of these factors.

Current and past audit activities and reports establish a need for improving the performance of the signature headcount system in military dining facilities by instituting better meal card and headcount station control practices. However, even if present practices were improved, the existing system would not provide a legible audit trail. Because of this deficiency the current system cannot be used to accurately audit individual meal card usage across a number of different meals or among different dining facilities within a meal. The individuals responsible for the control and issuance of meal cards and responsible for the control of the headcount station are usually aware that the system is extremely difficult to audit. Therefore, their motivation to improve existing practices remains low.

Previous investigations and tests of automated headcount systems have demonstrated that this type of system could provide better access control to military dining halls by providing legible and auditable headcount records, a capability to control excess multiple use of meal cards at any one meal or over any predetermined number of meals or days among multiple dining facilities, and a capability to provide management with useful headcount analysis reports. However, the accuracy of these systems depends, as does

TABLE 8

UNIFORM ANNUAL COST SUMMARY TABLE NON-PHOTO AND PHOTO CARD PROGRAMS

VENDOR	NON-PHOTO CARD PROGRAM		PHOTO CARD PROGRAM[a]	
	FIRST YEAR COST	UNIFORM ANNUAL COST	FIRST YEAR COST	UNIFORM ANNUAL COST
Identimat	$ 17,605	$ 3,200	$ 21,679[b]	$ 4,386[b]
Cardkey	$ 16,481	$ 3,486	$ 20,275	$ 4,557
ADP	$ 15,080	$ 3,897	$ 22,094	$ 6,281
Vikonics	$ 20,910	$ 4,858	$ 25,124	$ 6,101
Schlage	$ 19,200	$ 5,429	$ 24,114	$ 6,957
Rusco[c]	$ 26,142	$ 5,441	$ 30,146	$ 6,599
IBM	$ 30,081	$ 9,247	$ 33,539	$10,132
Vali-Dine	$ 23,321	$10,572	$ 26,685	$12,209

[a] Includes photographic equipment and film cost estimates.

[b] Under normal circumstances, a photograph is not required for identification in the Identimat system. However, if the situation ever arose where the Military ID card would be used with Identimat encoding, then a photo card program for Identimat would be necessary. Identimat's photo card program was estimated by using a charge of $0.75 a card ($0.45 more than the cost of a "regular" Identimat card - $0.45 was used as it was determined that this is the amount, on average, that other vendors charge for their photo cards) the cost of a Polaroid ID-3 System, and Polaroid film.

[c] In the absence of data from Rusco, their card costs have been estimated to be between those of Vikonics and Cardkey since all three companies' readers use the same type of card. Furthermore, the Rusco system hardware, as portrayed in this analysis, represents a minimum charge as costs for the 550 Controller and customized software were not available.

the current signature system, upon good meal card and headcount station control practices. For example, if the file of valid authorized numbers that is entered into the automated system is as inaccurate as the file of valid authorized number kept by the existing system (meal-pass-log), a new automated system will be degraded to the same level of inaccuracy as the old system. Also, if headcount station control does not include accurate personnel identification and rejection of unauthorized personnel, little will be achieved with automation.

This survey identified eight specific automated systems which would more than satisfy the Navy's basic requirement for a legible audit trail. Furthermore, most of the alternative systems can be expanded to interface with a main frame computer so that any desired management reports could be obtained given the requisite programming. All systems are commercially available and can be leased and/or procured from a single manufacturer. For the specific analytical assumptions of this survey, approximate system first-year expenditure costs range from $15,000 to over $30,000.

Automated headcount systems are and will be expensive to implement in the military. The decision to implement these systems should be based upon the need to acquire the advantages offered by these systems. Major advantages include legible audit trails, control of excess meal card usage, and potentially useful management reports. However, automated systems will not solve meal card and headcount station control problems.

The implementation of A La Carte food service in the Air Force and as now recommended by the DoD food planning board for all the services can and will provide increased headcount control capabilities. The point-of-sale devices necessary to this system can produce an auditable headcount trail by having the cashier enter patron meal card numbers into the register. These numbers can be later printed out in hard copy after the meal. It appears possible to connect the point-of-sale device to a card reader and a computer so that meal card numbers can be automatically recorded and useful headcount summary reports produced. If hardware can be so configured, then A La Carte systems may be able to implement improved auditable headcount systems at minimal additional cost.

Based upon the potential advantages of the automated card reading systems, it is recommended that such a system be acquired and evaluated within the military. Because of DoD interest in the conversion to garrison A La Carte food service, the acquired system should have the capability to operate behind the line with a point-of-sale device as well as in front of the line as a separate headcount control system. The automated system should also have sufficient capabilities so that the evaluation can be conducted at both the lowest level of system capability (by simply providing a legible audit trail) and at the highest level (by providing an audit trail as well as useful headcount analysis reports).

It is more specificly recommended that the Navy acquire an automated headcount system and evaluate it in conjunction with their pending test of an A La Carte system. The system acquired should have the capability to interface satisfactorily with the point-of-sale device planned for the A La Carte test. This system should also have the capability to operate independently as a headcount control device and should be evaluated in this mode of operation.

Based upon prior experience in testing automated headcount systems, it is recommended that the military service conducting the test, the military base selected for the test and the foodservice personnel at that base be made aware, prior to the test, that existing headcount practices will have to change if a valid test is to be achieved. Command attention in the correction of current inadequacies in meal card record keeping and control at the headcount station is an essential ingredient in achieving a satisfactory test of an automated headcount system. It makes little sense to acquire an expensive test system or to expend the personnel and other scarce resources to conduct the test if command interest and necessary corrective actions are lacking.

LIST OF REFERENCES

Brandler, P., et al., "An Evaluation of an All Commuted Ration Ashore A La Carte System for the Navy", NATICK/TR-77/011, January 1977. (AD A043439).

"Beating the New Credit Cards", Business Week, August 11, 1973.

Bustead, R., "The CAFe System Experiment at Fort Lewis, Washington", Technical Report, TR-73/20-ORSA, December, 1972. (AD 759284).

ALM 61-3517-H6, The DoD Economic Analysis Handbook, 2nd Edition, Department of Defense.

Leitch, D. P. and G. Hertweck, "An Automated Headcount System", Technical Report, TR-73/11-ORSA, November, 1972. (AD 752118).

Marker, J. W., "An Automated Headcount System Test", Final Report, US Army Troop Support Agency, November, 1974. (CS-SD-7601).

"Entry-Control Systems Handbook", Sandia Laboratories, September, 1977, Revised September, 1978. (SAND-77-1033).

"Personnel Identification by Hand Geometry Parameters", Stanford Research Institute, July, 1969.

DISTRIBUTION LIST

Copies

Commanding Officer
Navy Food Service Systems Office
Bldg. 166, Washington Navy Yard
Washington, DC 20374 3

Commandant of the Marine Corps
ATTN: Code RDS
Headquarters, US Marine Corps
Washington, DC 20380 1

Commander
US Army Test and Evaluation Command
ATTN: AMSTE-TO-P
Aberdeen Proving Ground, MD 21005 1

Commander
US Army Aberdeen Proving Ground
ATTN: STEAP-MT (Mr. Resch)
Aberdeen Proving Ground, MD 21005 1

Commander
US Army Cold Regions Test Center
ATTN: STECR-TA (Mr. Haslem)
APO Seattle 98733 1

Commander
US Army Electronic Proving Ground
ATTN: STEEP-CO (Mr. Banister)
Fort Huachuca, AZ 85613 1

Commander
US Army Aviation Development Test Activity
ATTN: STEBG-CO (Dr. Kishi)
Fort Rucker, AL 36362 1

Commander
US Army Dugway Proving Ground
ATTN: STEDP-CO (Dr. Rothenberg)
Dugway, UT 84022 1

Commander
US Army Jefferson Proving Ground
ATTN: STEJP-TD (Mr. Petersen)
Madison, IN 47250 1

DISTRIBUTION LIST (CONT'D)

Copies

Commander
US Army Tropic Test Center
ATTN: STETC-CO (Mr. Mendez)
APO Miami 34004 1

Commander
US Army White Sands Missile Range
ATTN: STEWS-CG (Dr. Duncan)
White Sands Missile Range, NM 88002 1

Commander
US Army Yuma Proving Ground
ATTN: STEJP-TD (Mr. Miller)
Yuma, AZ 85364 1

Commander
US Army Test and Evaluation Command
ATTN: DRSTE-TO-P
Aberdeen Proving Ground, MD 21005 1

CMDT
USAADS
ATTN: ATSA-CD-A
Ft. Bliss, TX 79916 1

Commanding General
26th Infantry Division
Mass Army National Guard
925 Commonwealth Avenue
Boston, MA 02215 1

HQ, US Air Force/LEEES
ATTN: Mr. Earl
Bldg. 516
Bolling AFB
Washington, DC 20332 1

Commandant
US Army Quartermaster School
ATTN: ATSM-CD
Ft. Lee, VA 23801 1

Supt, USAAHS
ATTN: HSA-CDM
Fort Sam Houston, TX 78234 1

Commandant of the Marine Corps
ATTN: Code LFS-4
Headquarters, US Marine Corps
Washington, DC 20380 2

DISTRIBUTION LIST (CONT'D)

	Copies
Dr. Eileen Matthews Professor Foodservice Administration University of Wisconsin - Madison Department of Food Science Babcock Hall 1605 Linden Drive Madison, WI 53706	1
Secretary of Defense for Research and Engineering ATTN: Director, Environmental and Life Sciences The Pentagon, Room 3D129 Washington, DC 20301	1
AUL/LSE 76-77-256 Maxwell AFB, Alabama 36112	1
HQ USAF/LEEHC Room 5D427, Pentagon Washington, DC 20330	1
LCDR A. W. Frost, MSC, USN Director, Food Management Service National Naval Medical Center Bethesada, MD 20014	1
Office of the Surgeon General Chief, Dietician Section, AMSC ATTN: DASG-DBD Room 3E477, Pentagon Washington, DC 20310	2
HQDA ATTN: DAMA-CSS-D Washington, DC 20310	1
Director US Naval Research Laboratory ATTN: Code 6180 Washington, DC 20390	1
HQ, AFESC/DEHF Tyndall AFB, FL 32403	3
Commander HQ, Air Force Logistics Command ATTN: AFLC/DEHS Wright-Patterson AFB, OH 45433	1

DISTRIBUTION LIST (CONT'D)

	Copies
HQDA Office of the Deputy Chief of Staff for Logistics ATTN: DALO-TST Washington, DC 20310	1
Commandant of the Marine Corps ATTN: Code LME Headquarters, US Marine Corps Washington, DC 20380	4
US Army Research Office ATTN: B. Mann, Library P. O. Box 12211 Research Triangle Park, NC 27709	2
Commander US Army Troop Support Agency ATTN: DALO-TAF Ft. Lee, VA 23801	1
Mass Army National Guard 114 Med Bn, National Guard Armory ATTN: Commanding Officer 925 Commonwealth Avenue Boston, MA 02215	1
Mass Army National Guard 101 Eng Bn, Nat. Guard Armory ATTN: Maj Encarnacao Haverill Street Reading, MA 01867	2
Defense Logistics Studies Information Exchange US Army Logistics Mgmt Center Ft. Lee, VA 23801	2
Chief, Standardization Section Catalog Branch (TTFS) Directorate of Technical Operations Defense Personnel Support Center 2800 South 20th Street Philadelphia, PA 19145	5

DISTRIBUTION LIST (CONT'D)

	Copies
Commander US Army Troop Support Agency ATTN: DALO-TAD Ft. Lee, VA 23801	3
Chief USA Logistics Assistance Office FORSCOM (DARCOM) ATTN: DRXLA-FO, Bldg. 210 Ft. McPherson, GA 30330	12
Commandant ATTN: ATZA-CDC US Army Engineer School Ft. Belvoir, VA 22060	1
Library Russell Research Center, USDA-SEA P. O. Box 5677 Athens, GA 30613	1
Mr. Robert J. Moore Staff Director, Material Mgt Sys Div OASD (MRA&L), Pentagon Room 3B724 Washington, DC 20301	1
Commander Letterman Army Institute of Research Presidio of San Francisco, CA 94129	2
HQ, AMD-RDX Brooks Air Force Base San Antonio, TX 78235	1
HQ AFMSC/SGB (Col Jackson) Brooks AFB, TX 78235	1
HQDA DCSLOG ATTN: DALO-TST-F Washington, DC 20310	2

DISTRIBUTION LIST (CONT'D)

Copies

Larry Rosenthal
ARA Services, Iec.
Operations Services - 4th Floor
Independence Square, West
Philadelphia, PA 19106 1

Mr. Allen J. Wyllie
Project Manager
Defense Audit Service
1300 Wilson Boulevard
Arlington, VA 22209 1

Lt. Col. Roger Olson, USAF
OASD (MRA&L)
The Pentagon, Room 3B737
Washington, DC 20301 1

Lt. Gen. John D. McLaughlin
US Army, Retired
President
L. J. Minor Corporation
3235 Boulevard
Colonial Heights, VA 23834 1

Dr. Frank D. Borsenik
Professor
College of Hotel Administration
University of Nevada
Las Vegas, NV 89154 1

Dr. Fergus M. Clydesdale
Professor
Department of Food Science and Nutrition
University of Massachusetts
Amherst, MA 01003 1

Miss Mary Elisabeth Crimmins
Vice President-School Services
ARA Services, Inc.
Independence Square West
Philadelphia, PA 19106 1

Dt. Stevenson W. Fletcher
Department Head
Hotel, Restaurant, and Travel Administration
University of Massachusetts
Amherst, MA 01003 1

DISTRIBUTION LIST (CONT'D)

Copies

Ms. Marsha W. Lilly, R.D.
Food Service Director
North Carolina Department
of Correction
831 West Morgan Street
Raleigh, NC 27603 1

Mr. Normand L. Peckenpaugh
Assistant Dean for Administration
School of Hotel Administration
104 Statler Hall
Cornell University
Ithaca, NY 14853 1

Mr. C. K. Litman
6728 Lost Dutchman Drive
Phoenix, AZ 85253 1

Mr. Robert Altmar
Eastern Zone Manager
Cardkey Systems
1730 N. Lynn
Suite 400
Arlington, VA 22209 1

Mr. John R. Sczepanski
Vice President/Sales
Stellar Systems
231 Charcot Avenue
San Jose, CA 95131 1

Mr. Kent M. Sterling
Manager - Sales Department
Schlage Electronics
3260 Scott Boulevard
Santa Clara, CA 95051 1

Mr. Dave Hornak
Regional Sales Manager
APD Security Systems, Inc.
24710 Crestview Court
Farmington Hills, MI 48018 1

Mr. Ronald H. Schmoll
Marketing Services Manager
Rusco Electronic Systems
1840 Victory Boulevard
P. O. Box 5005
Glendale, CA 91201 1

DISTRIBUTION LIST (CONT'D)

Copies

Mr. Donn R. Heath
Senior Account Executive
Rusco Electronic Systems
38 Mechanic Street, Suite 5
Foxboro, MA 02035 1

Mr. William A. Lee
Marketing Manager
Vikonics, Inc.
23 East 26th Street
New York, NY 10010 1

Mr. Robert W. Reedy
Branch Manager
IBM Corporation
400 Wyman Street
Waltham, MA 02154 1

Mr. Gene F. Olsen
Applications Engineer
Harco Industries, Inc.
10802 N. 21st Avenue
Phoenix, AZ 85029 1

Mr. Arthur C. Brent
V.P. & General Manager, Systems Division
R.D. Products, Inc.
6132 Route 96
P. O. Box E
Victor, NY 14564 1

Mr. Neil Jackson
Burroughs Corporation
1 Burroughs Place
Detroit, MI 48202 1

Ms. Florence Cowden
Manager, Sales Administration
Cardkey Systems
20339 Nordhoff Street
Chatsworth, CA 91311 1

DISTRIBUTION LIST (CONT'D)

	Copies
Commander	1
Technical Director	1
Deputy Technical Director, Food Service Systems Program	1
Deputy Technical Director, Clothing & Equipment Systems Program	1
Commaner, US Army Institute of Environmental Medicine	1
Special Assistant for DOD Food Program	2
Director, Aero-Mechanical Laboratory	1
Director, Clothing Equipment & Materials Engineering Laboratory	1
Director, Food Engineering Laboratory	3
Director, Food Sciences Laboratory	3
US Army Representative, Joint Technical Staff, for DOD Food RDT&Eng Program	2
US Air Force Representative, Joint Technical Staff, for DOD Food RDT&Eng Program	2
US Marine Corps Representative, Joint Technical Staff, for DOD Food RDT&Eng Program	2
US Navy Representative, Joint Technical Staff, for DOD Food RDT&Eng Program	2
US Air Force Liaison Officer	3
Chief, Engineering Programs Management Office	2
Chief, Technical Library	2
Chief, Operations Research and Systems Analysis Office	20
Chief, Behavioral Sciences Division, Food Sciences Laboratory	2
RDT&E Advisor, Food Service Facility and Equipment Planning Board, Food Engineering Laboratory	1

APPENDIX A

Survey Questionnaire

APPENDIX A

Survey Questionnaire

I. HARDWARE

A. COSTS

- Central Processing Unit (CPU)
- Data Entry Device
- Installation
- Card Reader (Each)
- Printer
- Software
- Interfaces

B. How much core storage?

C. Response time?

D. How is system connected? Cost/ft?

E. What are the responses of the card reader?

F. How are those responses displayed?

G. Characteristics and composition of output files?

H. With additional programming, what is the system's output?

I. How many readers can the CPU support?

J. What is the recommended temperature control for the CPU?

II. CARDS

A. How are they encoded?

B. Decimal digit capacity?

C. Cost per card with picture?

D. Cost per card without picture?

E. Are they recodable?

F. Will a card reader read a bent card?

G. Hardware cost of card preparation equipment?

H. How long does it take to encode a card?

III. OTHER

A. How long to install the system?

B. Estimated length of response time after receiving a purchase order?

C. Is the company on the GSA schedule?

D. Number of food service applications (Names and Locations).

E. Nature of applications other than food service.

F. Does the company train users? If yes, at what cost?

G. Does the system have the capability to print transactions locally?

H. If a reader goes down, does the CPU get notified? If yes, how? Does the headcount monitor get notified? How?

APPENDIX B

Burroughs Application at Cornell University Food Service

APPENDIX B

Burroughs Application at Cornell University Food Service

Source: Burroughs Corporation
1 Burroughs Place
Detroit, MI 48232

INTRODUCTION

In 1977 Burroughs Corporation installed automated headcount equipment at Cornell University, Ithaca, New York. System software was developed by the university. The system used at the university consists of a Burroughs B-80 microcomputer and twelve remote Burroughs TT602 terminals. Terminals are located in each dining facility with an additional terminal located in the dining department's administrative section. This is the only terminal that allows for add, change or delete actions to the student information contained in the CPU. A reader screen is also provided at this terminal for verification of information. Cornell's system is connected through telephone lines using a modem at each terminal. It can handle up to 1800 students per hour at each terminal and provides a two second response time. Manufacturer literature on the B-80 and TT602 terminals are contained in this Appendix.

MEAL CARD PROGRAM

Meal cards are supplied by Polaroid and prepared by the university. Each card contains a photo of the student and a magnetic strip encoded with student I.D. number and type of meal plan. During FY 79, Polaroid charged Cornell approximately one dollar per card. Cornell issues the cards free. When a student loses his card, a line checker sells him a "lost card voucher" for $5. This voucher remains valid until the dining office flags it as inactive, usually one business day following the creation of the voucher to allow the student time to get a new card.

ACTIVITIES AT THE TERMINAL

When a student arrives at the entrance to a dining facility, he/she must have in his/her possession either a meal card, a lost voucher card, or five dollars. The line checker follows a different procedure in each circumstance.

Meal Card Entry. If a student brings a meal card, the checker "reads" the card into the terminal. This is done by passing the card through the scanning/reading device that is attached to the rear of the terminal. If the card is not read properly due to the mechanical method of reading the card or some failure in the data communication system, the invalid red light will flash on the terminal. When this occurs, the checker either re-reads the card or enters the information through the keyboard at the terminal. Once the information is actually transmitted, the terminal will respond via flashing indicator lights.

If the terminal flashes light 1 (green), it means that this is a valid meal card and the student should be admitted. The system tallies an entrance for the unit.

If the terminal flashes light 2 (orange), it means that this is a valid meal card but the plan does not allow eating at this particular time period. The student is turned away.

If the terminal flashes light 3 (yellow), it means that this card has previously been used to gain entry to a dining facility during the present time period (i.e., a repeat entry). The checker must verify the identity of the student. This is done by looking more closely at the picture on the card or demanding some other form of identification, preferably a university I.D. card.

If the terminal flashes light 4 (blue), it means that this student is a possible violator of the dining system (i.e., he may be allowing another student to use his/her card as this student has accumulated a large number of repeat entries). The checker must once again verify the student's identity.

If the terminal flashes light 5 (red), it means that this card has been reported lost or stolen. The checker confiscates the card and does not allow the student to enter.

Lost Card Entry. The checker inputs the student's I.D. number through the keyboard using the lost card transaction. The terminal will again flash the appropriate light to indicate the status of the card. If the number is valid, the checker issues a lost card voucher and tells the student when the voucher expires.

Lost Card Voucher Entry. When a student enters with a lost card voucher, the checker asks for additional identification. The checker inputs the I.D. number of the student through the keyboard using the lost card voucher input transaction. Once again, the terminal lights will flash according to the status of the student's record.

SYSTEM OUTPUTS

The system produces a daily report of the total number of students admitted to each dining facility during each meal period (time zone). The following is a list of the totals that are accumulated for each terminal and time zone:

1. The number of valid first entries (green lights).
2. The number of repeat entries (yellow lights).
3. The number of invalid students found (red lights).
4. The number of possible violators encountered (blue lights).
5. The number of lost card vouchers processed.

BURROUGHS B 80
COMPUTER SYSTEM

Compatible with the future

BURROUGHS B 80

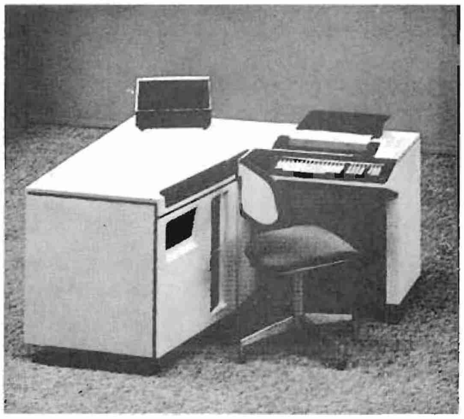
A Very Small But Powerful Fully Featured General Purpose Computer System For:

- The business considering a computer for the first time.
- The business upgrading from a less advanced computer.
- The larger organization with branches, warehouses, plants or other facilities seeking better business management by placing computer power at the locations where transactions occur and where management information is required.

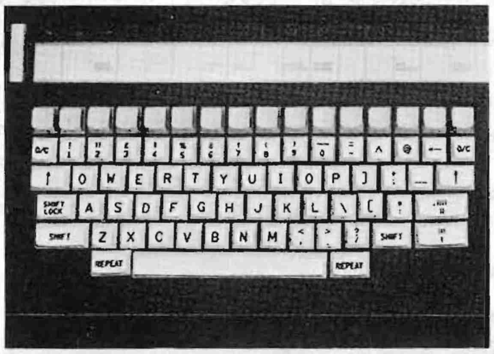
The Burroughs B 80, because it incorporates a unique integrated system of operating and application software called the Computer Management System (CMS), is the one small computer which meets the data processing and management reporting needs of organizations of all sizes. Combined with the advanced hardware design of the B 80, CMS provides ease of use, powerful performance, and growth capacity not available in any other computer of similar size and cost.

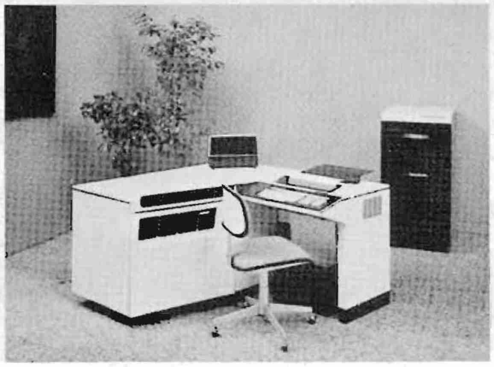
Included in the CMS software is the operating system of the B 80 called the Master Control Program (MCP), first developed by Burroughs for its larger computers. Burroughs now offers this advanced MCP technology in a very small computer system — the B 80. Combined with powerful new microprocessors, new disk technology, and Burroughs worldwide support, CMS — including BMS® application programs — makes the B 80 unique in its price range: the system designed for ease of use and ease of growth, both now . . . and later, to future, larger Burroughs systems, without changing your programs or data files.

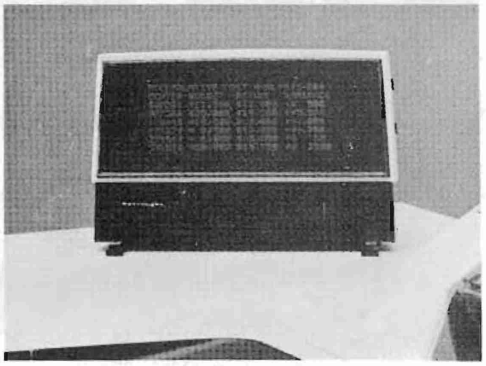
The system designed to be compatible with the future.



Burroughs


Q/C
Q W E R T Y U I O P
SHIFT LOCK
A S D F G H J K L
SHIFT
Z X C V B N M
SHIFT
REPEAT
REPEAT





BURROUGHS B 80
A Flexible Response To Data Processing Requirements

For the business considering a computer for the first time, or upgrading from a less advanced computer.

The B 80 is within the means of many businesses which could not previously afford a computer of this capability. The B 80 is available in a wide range of configurations, so the user can obtain the system which best meets his needs.

Installation of the B 80 is simple, and it's probable that space currently occupied by accounting machines or less advanced electronic equipment will accommodate the B 80.

For the business already using electronic equipment, Burroughs can provide assistance to make the change to the B 80 with a minimum of expense and delay. Burroughs Data Base Bridging System, part of the Computer Management System, permits users of Burroughs Series L business minicomputers or other manufacturer's systems to transfer existing data bases to B 80 systems utilizing magnetic tape cassettes with minimum effort.

Once installed, the B 80 becomes a compact information center, streamlining daily work and providing immediate access to records for better business management. Because it is easy to use, employees can be quickly trained by Burroughs to operate the B 80.

Most importantly, the B 80 brings electronic efficiency within your business — and under your organizational control. Your records are stored on removable Burroughs super mini-disks or removable disk cartridges. The Burroughs super mini-disk has a storage capacity up to four times that of other generally available mini-disks. The two super-mini-disks used on a minimum B 80 (up to six can be used) can store system software, application programs, and approximately 5500 account records. Information can be retrieved from a Burroughs super mini-disk in one-fourth of a second: significantly faster than other mini-disks.

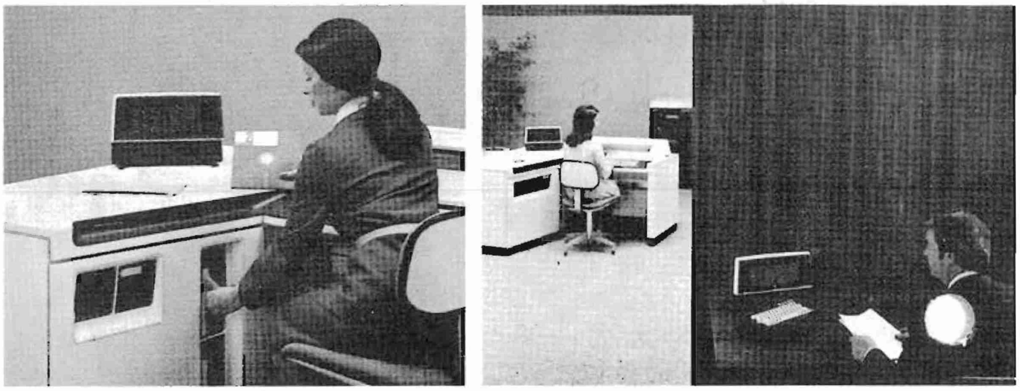
Disk cartridges offer even greater storage capacity and access speed. The B 80 can use up to six disk cartridges simultaneously: the equivalent of approximately 150,000 account records on-line at one time. Information can be retrieved in an average of one-tenth of a second.

All disks are removable, so storage capacity is virtually unlimited.

Business records and information stored on magnetic disks are immediately available, either through the B 80 printer, the system's display panel, or management information display terminals strategically located within your company. Records are protected simply by copying them on another disk which may be stored in a secure area, safe from damage or misuse.

Within the CMS software, Burroughs offers Business Management System program products for the B 80, designed for the requirements of your particular business. These BMS programs are of special value to the organization which does not normally employ a professional data processing staff and are available at a fraction of the cost of custom program development.

Because it is easy to use, employees can be quickly trained by Burroughs to operate the B 80.



Business records and information stored on magnetic disks are immediately available, either through the B 80 printer, the system's display panel, or management information display terminals strategically located within your company.

BURROUGHS B 80

Convenient And Economical Growth Through Advanced Technology

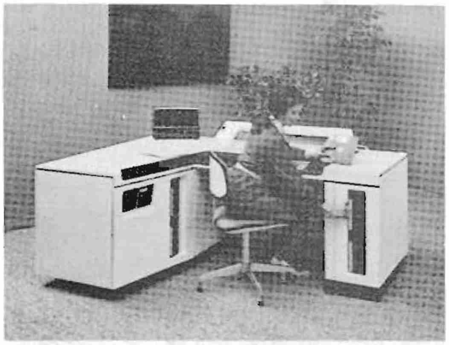
Burroughs B 80: The Right System Now... And For The Future

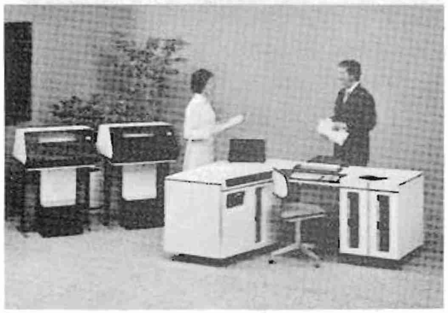
Burroughs will recommend and provide the B 80 system that best satisfies your current requirements. As these requirements expand, the MCP technology allows B 80 growth without reprogramming for system power improvement. Expand memory, peripheral units, BMS application programs, and data communications capability: whatever the expansion, through MCP the B 80 will automatically accept the increased system power. No need to rewrite current programs. No need to retrain personnel. No need to alter operating procedures.

That's convenient growth. Economical growth.

The B 80 system may be configured using:

- Burroughs super mini-disks for the ultimate in compact, convenient information storage.
- Disk cartridges for even larger file capacity. The file capacity of the B 80 may be increased over 13 times through the addition of more mini-disk or disk cartridge units to the basic B 80. And because all disks are removable and interchangeable, multiple B 80 installations are a practical way to grow.
- A system display to confirm B 80 input and output, including immediate management information provided by Burroughs BMS programs.
- Magnetic tape cassette stations and industry-compatible mini-disks.
- Line printers to complement the advanced matrix system printer. The print capability of the B 80 can be increased 23 times through the addition of such line printers.
- Burroughs Audit Entry Systems for local or remote preparation of audited input. Audit Entry Systems may also be connected to the B 80 for batch transmission of data.
- Burroughs visual display terminals for immediate management access to information, providing data entry as well as inquiry capability. Terminals may be located locally or remotely.





BURROUGHS BUSINESS MANAGEMENT SYSTEMS

Complete Application Programs For The B 80

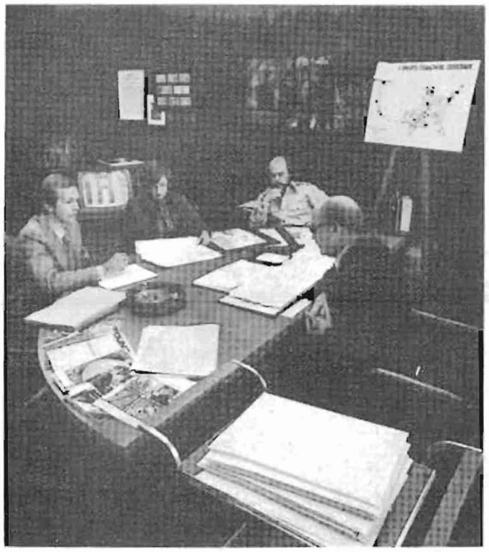
Burroughs application program products for the B 80 can eliminate custom program preparation and are much more economical. Called Business Management Systems, these BMS program products have been designed, written, tested, and perfected by Burroughs programmers and applications experts on a worldwide basis. BMS programs satisfy the requirements of a wide range of organizations, including manufacturers, hospitals, government, and finance. In the commercial / industrial area, there are Business Management Systems of particular interest to a wide range of wholesalers and distributors.

BMS programs provide dynamic management reporting to furnish, in addition to routine accounting documents, the information needed to manage successfully. This key management information is available in printed or display form, locally or remotely, periodically or on demand. Such immediate access to information provides the B 80 user with management control not available from less advanced systems.

Because BMS programs are available either as complete packages or modularly, the B 80 user may obtain a total Business Management System immediately, or just those applications presently required. As applicational needs increase, the MCP technology of the B 80 allows subsequent modules to be added conveniently — without reprogramming — and integrates these automatically with existing programs.

Information input and retrieval to and from the BMS programs is made easy by Burroughs Data Control System (DCS), another element in the comprehensive Computer Management System (CMS).

The Data Control System makes the handling of B 80 data simple by allowing acceptance of Audit Entry media, whether cassette, industry-compatible mini-disk, or Burroughs super mini-disk; by reducing the programming effort required for file creation and maintenance; and by providing basic reporting and inquiry capability without the creation of separate report programs. DCS permits data retrieval and display without detailed operator or programmer knowledge of the data or report formatting techniques.



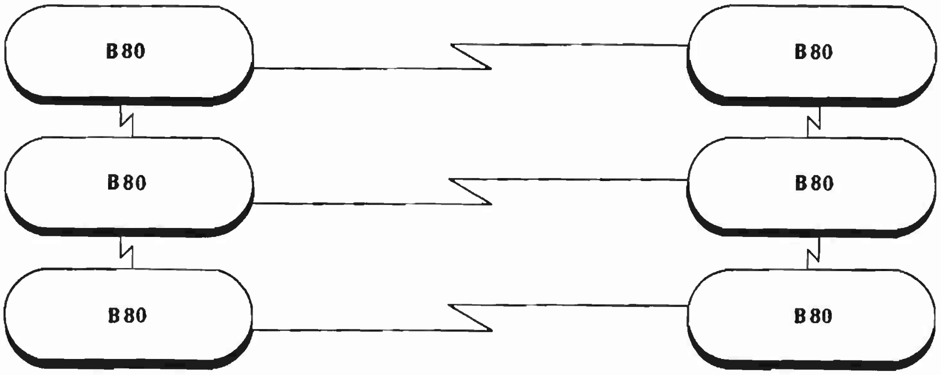
For the larger organization seeking better business management by placing computer power where transactions occur and where management information is required.

The moderate cost of the B 80 makes multiple installations economically feasible, while its ease of use and power assure the capability to process work on-site at decentralized locations.

For the larger organization, the B 80 puts data processing capability where it is needed. Local business records and information are under local control; and, through the B 80's data communications capabilities, remote records and summary reports are available to management at central locations.

Burroughs Business Management System program products are available to the larger organizations with decentralized, diversified, or multinational computer operations. These BMS program products, written in the higher level languages of COBOL and RPG, are designed for the requirements of local business offices. A full range of procedural capabilities and the network languages of NDL (Network Definition Language) and MPL (Message Processing Language) simplify the use of B 80 systems in data communications networks. Implementation of the Computer Management System (CMS) on future, larger Burroughs systems will allow users of these systems and B 80 users to use the same programs and data files without reprogramming or recompiling.

Of special importance is Burroughs worldwide support capability for the B 80. No matter where your network extends, professional training, support, and maintenance can be provided.



Maximum flexibility in establishing decentralized data processing is possible because the B 80 can effectively operate in a stand-alone environment; as a host to its own terminal network; as a terminal computer system connected to a larger host system; or, as illustrated here, in a network of several B 80's connected to each other. These various networks may be connected utilizing local direct connect facilities or remotely utilizing Burroughs data communications procedures.

BURROUGHS B 80
Simplified Operation Through Advanced Technology

The B 80 operates under a complete Master Control Program with the capabilities of the Master Control Programs used on Burroughs larger computer systems. The Master Control Program (MCP) makes possible much of the superiority of the B 80, functioning independently on the user's behalf with no special effort required by the operator. The MCP assumes responsibilities, exercises control, and monitors jobs which would otherwise require operator attention. Because the MCP does so much automatically, the B 80 is easy to operate — especially important to the first time user.

System-To-Operator Communication

Through the MCP, the B 80 communicates with the operator in simple language statements. No matter how the B 80 is configured or what applications are being used, these statements are universal: consequently, personnel may use other B 80 systems with no loss of efficiency.

As part of system-to-operator communication, the MCP will advise the operator:

- Whether the system and peripherals are operational.
- Whether proper files are available.
- Whether necessary peripherals are ready for use.

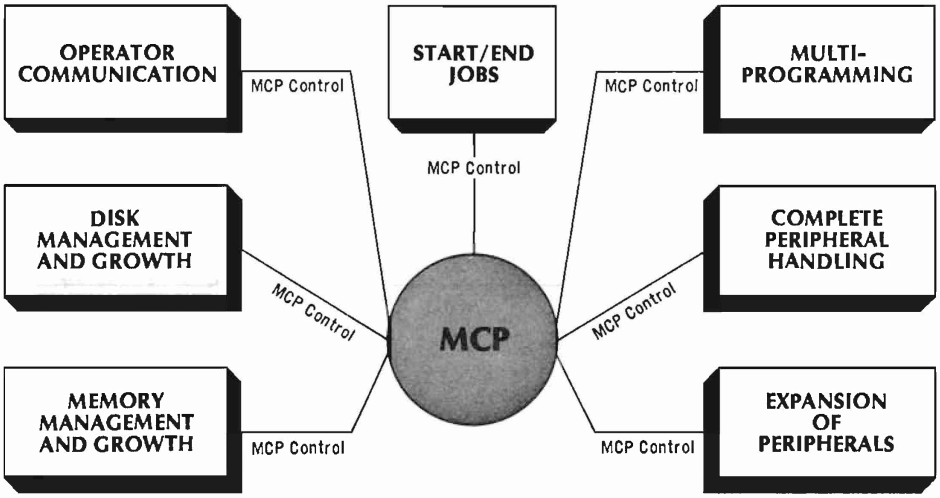
Because the MCP does this checking automatically, operator efficiency is greatly increased.

Dynamic Resource Allocation

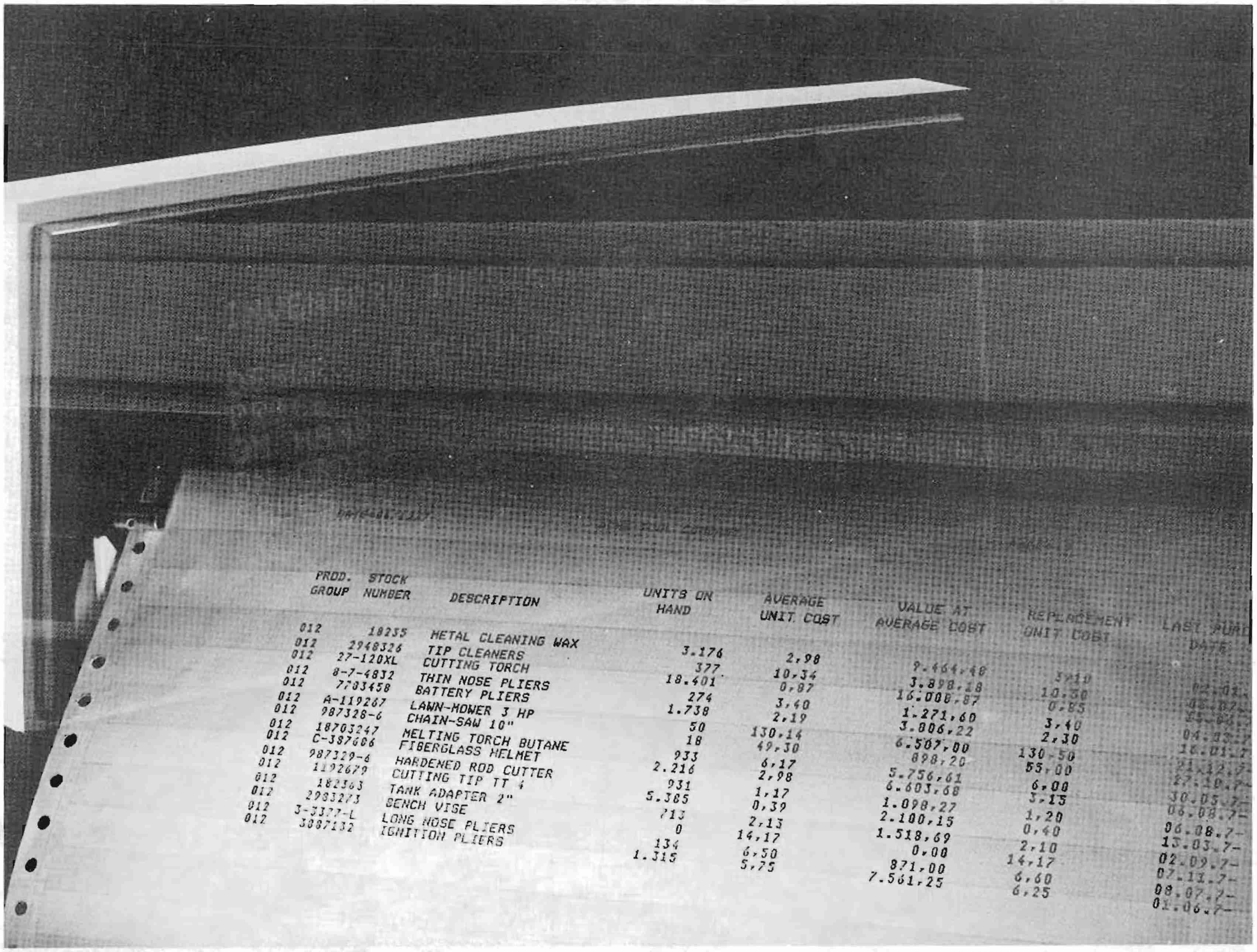
The MCP manages the B 80, simplifying operation. Utilizing Dynamic Resource Allocation, the MCP will:

- Automatically select the peripherals necessary to execute a job in the most efficient way.
- Automatically utilize available memory in the most efficient way.
- Automatically assign system components as they are required by application programs.
- Automatically allow several programs to run simultaneously (the number depends on the size of the B 80 used and the applications processed), and allow application program combinations to vary from one time to another.
- Automatically execute jobs by priority levels previously established. The jobs most important to the user become those most important to the B 80: MCP sees to it they get done fast.
- Automatically control the assignment of files and data components (i.e., memory locations and specific disks) without operator intervention.

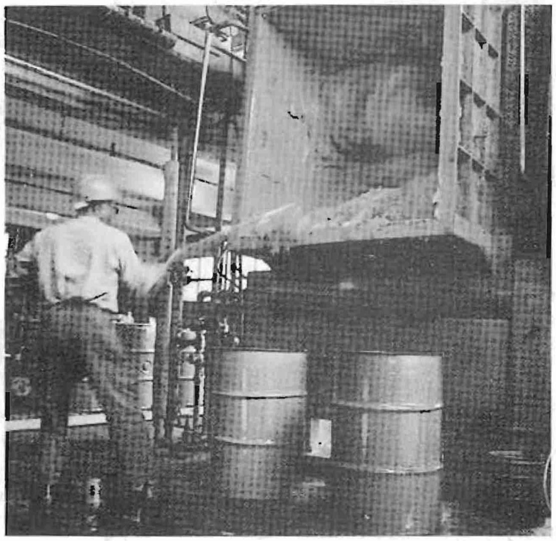
The B 80 Master Control Program: automatic communication, management, selection, multi-programming, and job priority execution. All in one small computer which combines unprecedented power with ease of use: the B 80.



MCP Means Simplified B 80 Operation



PROD. GROUP	STOCK NUMBER	DESCRIPTION	UNITS ON HAND	AVERAGE UNIT COST	VALUE AT AVERAGE COST	REPLACEMENT UNIT COST	LAST PURC DATE
012	18235	METAL CLEANING WAX	3.176	2,98	9.464,48	3,10	02.01.[illegible]
012	2948326	TIP CLEANERS	377	10,34	3.898,18	10,30	[illegible]
012	27-120XL	CUTTING TORCH	18.401	0,87	16.000,87	0,85	[illegible]
012	8-7-4832	THIN NOSE PLIERS	274	3,40	1.271,60	3,40	04.03.7
012	7703458	BATTERY PLIERS	1.738	2,19	3.806,22	2,30	16.01.7
012	A-119267	LAWN-MOWER 3 HP	50	130,14	6.507,00	130,50	21.12.7-
012	987328-6	CHAIN-SAW 10"	18	49,30	898,20	55,00	27.10.7-
012	18703247	MELTING TORCH BUTANE	933	6,17	5.756,61	6,00	30.05.7-
012	C-387606	FIBERGLASS HELMET	2.216	2,98	6.603,68	3,15	06.08.7-
012	987329-6	HARDENED ROD CUTTER	931	1,17	1.098,27	1,20	06.08.7-
012	1192679	CUTTING TIP TT 4	5.385	0,39	2.100,15	0,40	13.03.7-
012	182363	TANK ADAPTER 2"	713	2,13	1.518,69	2,10	02.09.7-
012	2983273	BENCH VISE	0	14,17	0,00	14,17	07.11.7-
012	3-3377-L	LONG NOSE PLIERS	134	6,50	871,00	6,60	08.07.7-
012	3887132	IGNITION PLIERS	1.315	5,75	7.561,25	6,25	01.06.7-

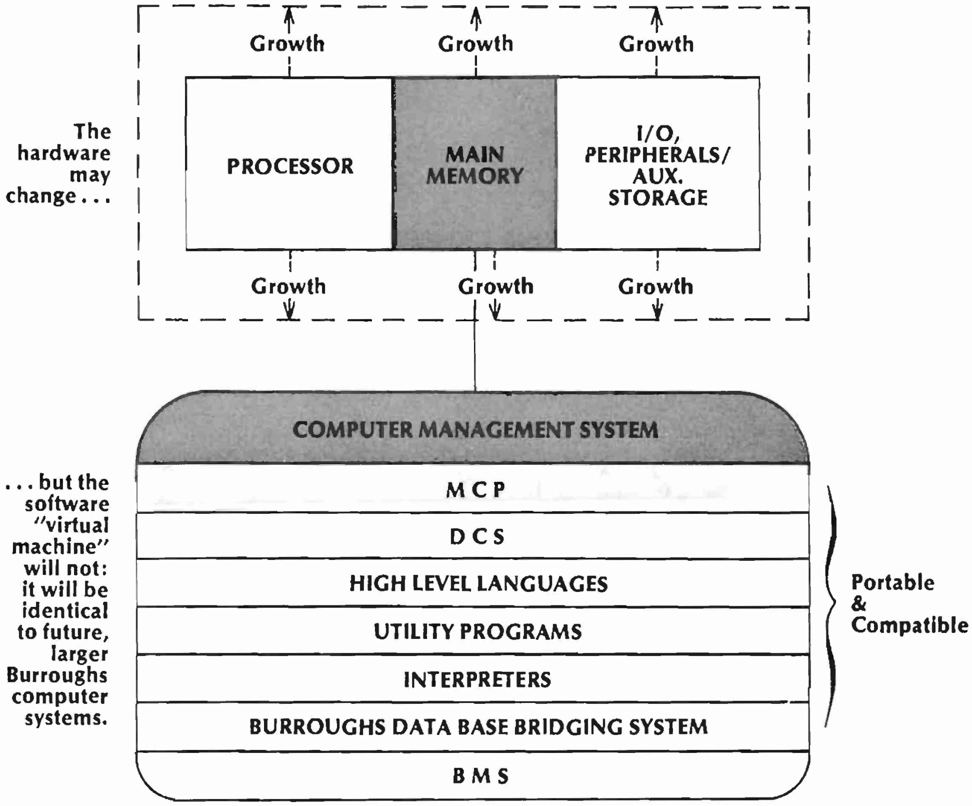


BURROUGHS
Provides And Supports Everything The B 80 User Requires

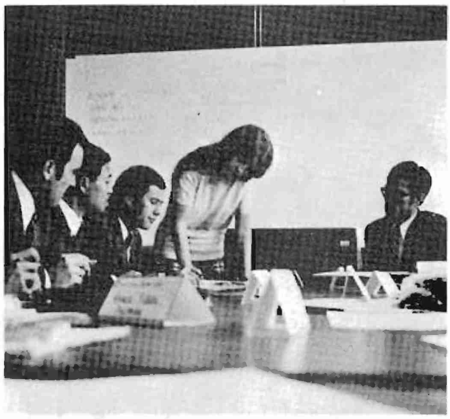
- All hardware, including peripherals.
- All Computer Management System software, including the Master Control Program, the Data Control System, High Level Languages, Utility Programs, Interpreters, Burroughs Data Base Bridging System, and Business Management Systems. Together, B 80 hardware and CMS are the B 80 system: easy to use; easy to expand across the broad range of B 80 models; and easy to upgrade to larger Burroughs systems without reprogramming and to future, larger Burroughs systems without reprogramming or recompiling.

The compatible operating environment design provided by the Computer Management System means that application programs, data files, and operating methods and procedures are portable to other Burroughs systems without change. This B 80 compatibility with both future user requirements and future computer technology is unique in very small computer systems.

- All necessary pre-installation guidance.
- All customer training.
- All forms and supplies.
- All necessary product maintenance, from field engineers located throughout the world.


Growth
Growth
Growth
The hardware may change . . .
PROCESSOR
MAIN MEMORY
I/O, PERIPHERALS/ AUX. STORAGE
Growth
Growth
Growth
COMPUTER MANAGEMENT SYSTEM
. . . but the software "virtual machine" will not: it will be identical to future, larger Burroughs computer systems.
M C P
D C S
HIGH LEVEL LANGUAGES
UTILITY PROGRAMS
INTERPRETERS
BURROUGHS DATA BASE BRIDGING SYSTEM
B M S
Portable & Compatible

All necessary pre-installation guidance.



All customer training.

All necessary product maintenance.

BURROUGHS B 80

Advanced Technology For System Power And Operational Simplicity

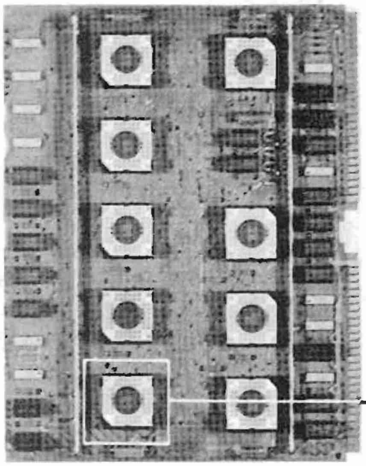
The B 80's are microprogrammed systems. At program execution time, an organized group of micro-instructions, called the interpreter, is brought into memory by the MCP to monitor and direct system functions and to execute application programs.

The B 80 processor is implemented using nine advanced large scale integrated circuits contained on a single printed circuit board. The circuits include a nano memory, a micro stack, input/output logic and system registers, and utilize microprocessor technology.

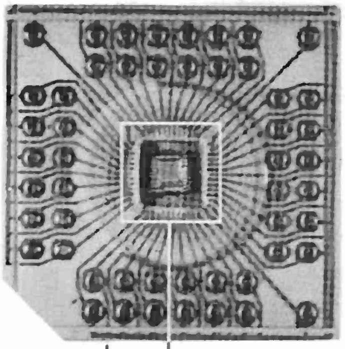
The B 80 processor operates at one MHz. The system's main memory has an access time of 500 nanoseconds, and utilizes metal oxide silicon (MOS) LSIC. Read/write main memory is expandable from the basic 32,768 bytes capacity to 61,440 bytes in 4KB increments.

Processor throughput is significantly increased by an "overlap" feature which allows the processor, during the execution of a micro-instruction, to "look ahead" at the next micro-instruction to be executed.

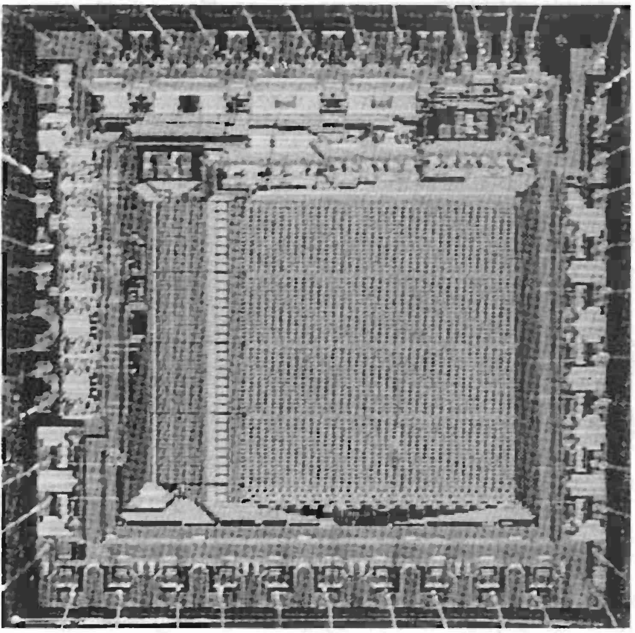
The B 80 system has up to 11 individual buffered controls for handling input/output devices. System efficiency is increased by an automatic hardware "interrupt" system. With this system, each input/output channel notifies the processor when data is ready for processing or transmission. This feature eliminates the need for the processor to scan channels continuously and is accomplished without programmer intervention.



The B 80 processor is implemented using nine advanced large scale integrated circuits contained on a single printed circuit board.



The circuits include a nano memory (shown), a micro stack, input/output logic and system registers, and utilize microprocessor technology.



Detail of nano random access memory large scale integrated circuit.

NO MATTER WHAT YOUR LINE OF BUSINESS . . . NO MATTER WHAT ITS SIZE . . .
NO MATTER WHAT SPECIAL NEEDS YOU MAY HAVE . . .
NO MATTER WHAT EQUIPMENT YOU PRESENTLY USE . . .

Contact your Burroughs representative for a B 80 demonstration.
See for yourself why the B 80 is compatible with the future . . .
with your future.

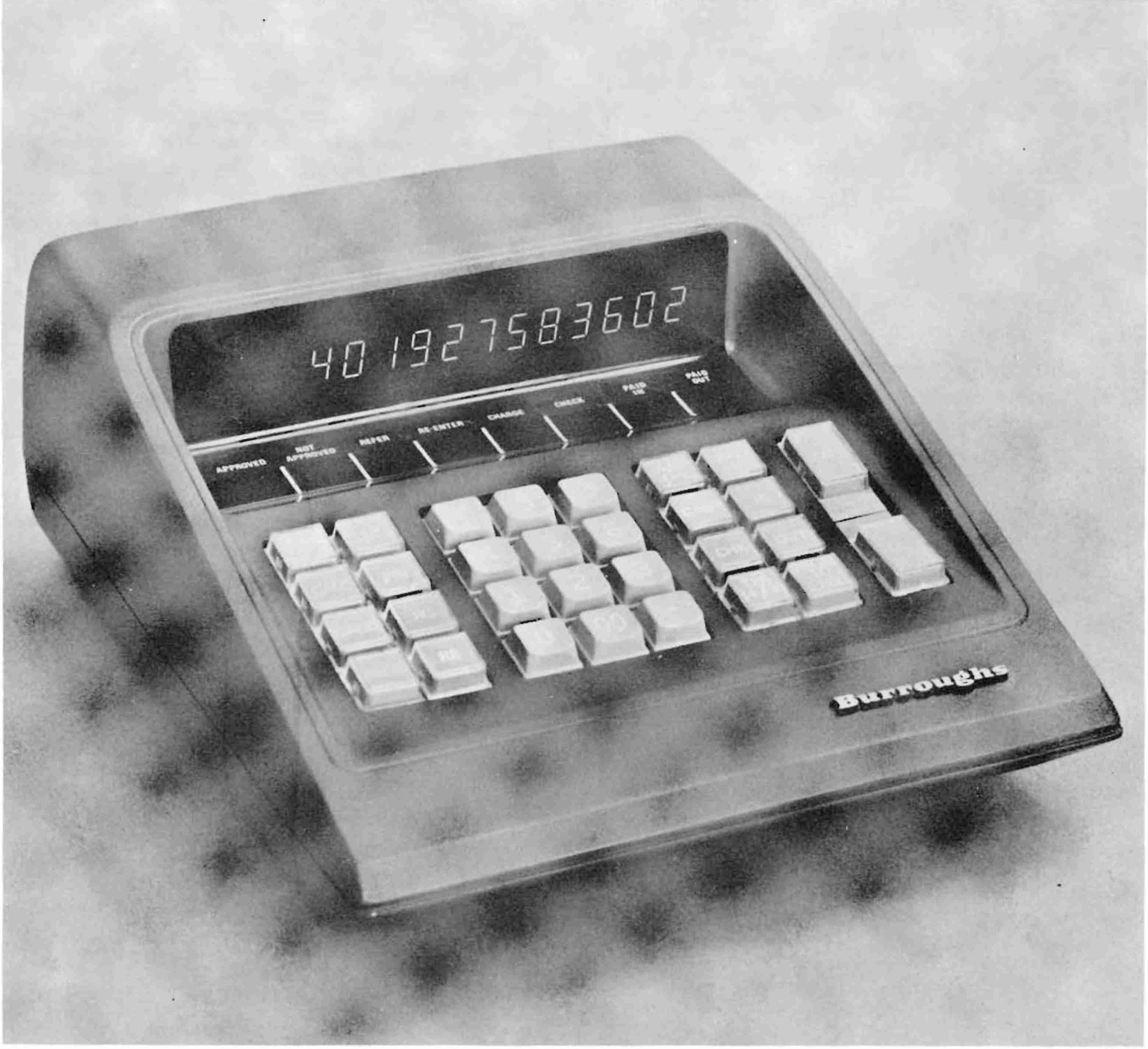
BURROUGHS B 80 COMPUTER SYSTEM

Compatible with the future

Burroughs

Burroughs TT 602

Transaction Control Terminal Systems



Burroughs TT 602 is an interactive transaction control terminal for numeric data entry, display and communications with a central system or system and communications processor. It is a modular, low-cost, compact and extremely flexible terminal having a wide variety of applications.

The basic TT 602 System is comprised of a keyboard/display module and a power supply/logic module. Optional components include a Magnetic Striped Card Reader, Magnetic Striped Card Reader/Writer and a Personal Identification Number (PIN) Keyboard.

Financial institutions, which are expanding into Electronic Funds Transfer Systems (EFTS), will find the TT 602 particularly appealing. Within the financial institution, it may be used by tellers, loan officers or even customers. In retail point-of-transaction locations, financial uses may include credit authorization, check verification, check guarantee, deposits, withdrawals and direct transfers of funds between accounts.

Because of the TT 602's extreme flexibility, it may be used in many non-financial environments. Sales and inventory data might be input through the TT 602. Hotels, motels and restaurants may enter and verify guest charges. Hospitals may use it in a "mini" nursing station environment for data entry or inquiry regarding patient accounting or medical care data. Wholesalers and manufacturers may utilize the TT 602 to collect data on shipments, receipts or production jobs.

Any industry requiring collection of numeric data or numeric inquiry into central files in an on-line, real-time environment may use the Burroughs TT 602.

Keyboard/Display Module Characteristics

■ Input

12-key numeric keyboard (including double zero and decimal point keys)

4 basic function keys

CLEAR – clears data communications buffer and enforces previous transaction data to be cleared before proceeding with a new transaction.

CLEAR DISPLAY – allows data to be corrected as it is being entered and permits selective correction of previously entered fields prior to transmission.

PAGE – allows sequential display of data fields in the buffer for verification of input or display of multiple fields received from the central site.

TRANSMIT – transmits data entered through the keyboard, magnetic striped card reader and Personal Identification Number (PIN) keyboard to the central site.

6 to 14 field identification keys – legends may be customized to applicational requirements.

■ Display

16-digit Panaplex® display panel may display 0 through 9, A, C, E, F, –, and blank. ("F" may only be displayed in the least significant position.)

8 optional status indicator lights refer to a removable legend strip and are activated by codes sent from the central site.

■ Operator Communication

Terminal controlled messages on the display panel identify the status of a transaction at all times:

F – is displayed when the operator depresses a field identifier key or upon successful reading of a magnetic striped card.

CC – indicates a magnetic striped card is to be read.

EOF – indicates the operator has depressed the PAGE key a sufficient number of times to reach the "End-Of-Fields". Depression of the PAGE key again causes the contents of the buffer to be redisplayed a field at a time.

C – shows that the operator has entered "calculator mode" (optional).

A – indicates the transmit key has been depressed and the TT 602 is "awaiting" a response.

O – indicates the terminal is in an idle state with a clear buffer, awaiting entry of data.

E – indicates an operator error or improper reading of a magnetic striped card.

E-A — indicates "entry accepted" upon completion of entry from the Personal Identification Number (PIN) keyboard.

Power Supply/Logic Module Characteristics

- Self-contained unit which satisfies the power, memory and logic requirements of the TT 602 terminal, including:

  Keyboard/display module

  Data communications processor

  Optional magnetic striped card reader

  Optional magnetic striped card reader/writer

  Optional Personal Identification Number (PIN) keyboard

- The power supply/logic module may be used as a stand for the keyboard/display module or may be located up to eight (8) feet away.

  8-foot (243.8 cm) cable may be easily disconnected at the keyboard/display module for quick substitution of a replacement keyboard/display module.

  Cable and plug attachment, when installed through a counter top, requires a hole measuring .9-inches (2.3 cm) x 1.4-inches (3.5 cm).

- Data communications line activity light

  Located on power supply/logic module

  Blinks when there is activity on the line and the terminal is responding.

- On/Off switch

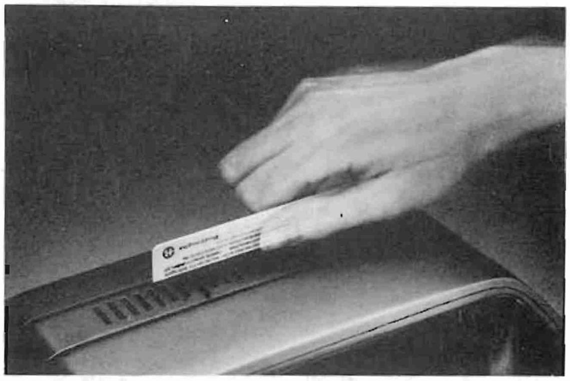
- Self-diagnostic capability

  Whenever the TT 602 is turned on, an in-built Maintenance Test Routine (MTR) checks all the terminal circuitry.

  If these tests indicate that all logic is functional, a facsimile of the word "GO" is displayed to the operator on the keyboard/display module.

  If certain types of failure are found, a numeric representation of the failure is displayed on the keyboard/display module to allow repair to be more readily effected.

Magnetic Striped Card Reader (Optional) Characteristics



- Attaches to rear of keyboard/display module.
- Pass-through reader.
- Reads Track II (75 BPI density) or Track III (210 BPI density).
- Compatible with cards read by other Burroughs terminals.

Magnetic Striped Card Reader/Writer (Optional) Characteristics

- Attaches to rear of keyboard/display module.
- Card lock-in security mechanism assures that the card which is read is the card which is written.
- Track III read/write (210 BPI density) and/or Track II read (75 BPI density).

Personal Identification Number (PIN) Keyboard (Optional) Characteristics

- 12-key pad.
- Available with magnetic striped card reader or reader/writer options.
- Allows customer entry of secret Personal Identification Number (PIN).
- May be hand-held or cradle-mounted.
- Attaches to keyboard/display module by a 14-foot (420 cm) cable.

  Cable has a 4-foot (120 cm) straight section and a 10-foot (300 cm) coiled section when extended.

Data Communications

- Free-standing terminal – requires no shared controller.
- 150-digit or 256-digit transmit/receive buffer.
- Interface

  Asynchronous

  Mode of operation – half-duplex.

  Transmission speeds – 75, 100, 150, 300, 600, 1200 and 1800 BPS.

  Data code – USASCII X 3.4 - 1968.

  Character length – 7 data bits and one even parity bit, plus one start and one stop bit.

  Bit sequence – least significant bit first.

  Data set interface – E.I.A. RS232C.

  Longitudinal message parity check.

  Network environment – 2-wire manua' dial-up lines, 4-wire leased lines, 4-wire leased with 2-wire dial-up back-up capability, or direct connect (BDI).
- Procedures

  Multipoint poll/select.

  Group polling.

  Fast select.

  Modified contention.

Additional Features (available on some styles)

- Supervisor key switch

  Located on power supply/logic module.

  Allows entry of uniquely identified constants which are transmitted with each message sent from the TT 602.

  Also allows temporary override of normal terminal address.
- Back-up rate switch

  Allows switching from a normal leased-line operation to a dial-up line for back-up should data communications problems develop.
- Calculator

  Allows the TT 602 to be used as a four-function electronic calculator in addition to normal on-line operations.

  May calculate up to four decimal places and round off to either two, three or no decimal places for entry as a data field in the message.
- Internal data sets

  1200 or 1800 BPS internal data sets are available on the TT 602.

Physical Characteristics

- Keyboard/display module

Width:	8.9" – (22.6 cm)
Height:	4.2" – (10.7 cm)
Depth:	10.7" – (27.2 cm)
Weight:	5.0 lbs. – (2.3 kg)

Power supply/logic module

Width: 9.8" – (24.9 cm)

Height: 9.1" – (23.1 cm)

Depth: 14.3" – (36.3 cm)

Weight: 28.6 lbs. – (13.0 kg)

Magnetic striped card reader (optional) (attaches to rear of keyboard/display module)

Width: 8.9" – (22.6 cm)

Height: 4.2" – (10.7 cm)

Depth: 3.3" – (8.3 cm)

Weight: 1.2 lbs. – (.6 kg)

Magnetic striped card reader/writer (optional) (attaches to rear of keyboard/display module)

Width: 8.9" – (22.6 cm)

Height: 4.2" – (10.7 cm)

Depth: 4.2" – (10.7 cm)

Weight: 3.3 lbs. – (1.5 kg)

Personal Identification Number (PIN) keyboard (optional) (cable-connected to magnetic striped card reader or reader/writer)

Width: 2.7" – (6.9 cm)

Height: 1.7" – (4.2 cm)

Depth: 6.4" – (16.2 cm)

Weight: .8 lbs. – (.4kg)

U.S. standard – 120 volts, 60 Hz.

Other – 100, 110, 115, 127, 200, 208, 220, 230 or 240 volts, 50 or 60 Hz.

Three-wire, non-detachable power cord connected to power supply/logic module.

Type 5-15P NEMA wall plug.

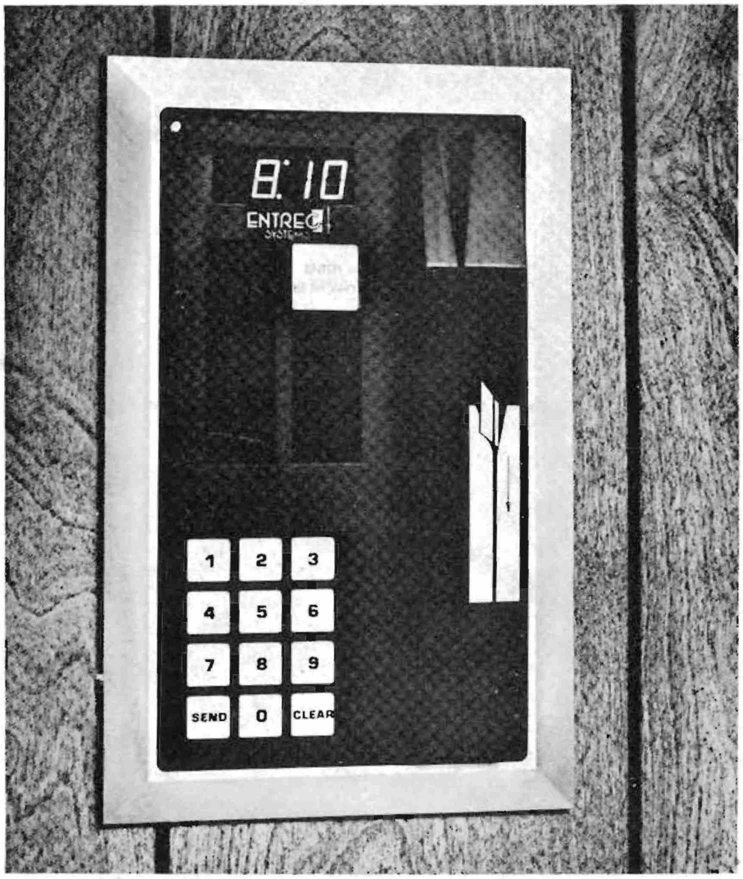
Length: 102 inches (260 cm).

APPENDIX C

Entrec Systems

Systematic
peace of mind.
1
2
3
4
5
6
7
8
9
END
0
LEAR
INSERT BADGE
ENTREC SYSTEMS
UNIVERSITY OF SOUTH FLORIDA

Entrec Systems eases your mind



It's no secret that the world today is not the same one we knew as youngsters. Times are different. People are different. Your employees are different too. Chances are, they're better educated than the workforce of a generation ago. More independent and less apt to accept rules without question.

Changes like these have created problems in business and on campus. Access problems. Security problems. Timekeeping problems. Attendance problems. Inventory control problems. Managers and administrators began to feel that they were losing control.

But you don't have to feel that way.

Now, Entrec Systems eases your mind by placing control where it belongs — in your hands. With state-of-the-art electronics, using rugged, reliable microprocessors and a powerful minicomputer, the Entrec Controlled Access System provides you with a firm grip on your operations.

The system and how It works

With an Entrec System, you get a complete, turnkey package that can be expanded easily to meet your future needs. Included are these components:

- Entrec magnetic stripe card reader terminals, the heart of the control system. Each compact terminal features an easy-to-use, wipe-through reader that eliminates jamming due to bent cards. Entrec's unique reader design gives you a terminal that will read a badge with a clip attached. It actually straightens out bent cards and reads them — insuring error-free operation. Users are guided by six lighted, easy-to-read message panels.

- A nationally known and serviced minicomputer.

- An Entrec software operating package designed for applications like yours. Operation is simplicity itself. You don't need a degree in computer programming to use an Entrec System, which is engineered to respond to human English requests and commands. Because of modular construction, the software packages can be modified at reasonable cost to provide the control you need and the information you want — when you want it.

- A compact printer and keyboard provides a control center which gives you system use information in easy-to-read, printout form. It allows you to enter changes and other information quickly and efficiently.

- All the equipment needed to enable you to make and encode photo identification cards is available with your Entrec System. If you wish, Entrec Systems will produce the initial cards for your installation. You can purchase encoders, cameras, laminators, die cutters and all the supplies to make cards on site.

- Entrec System components don't require air-conditioned rooms or extensive modifications to your facilities. They can be installed easily. Carefully engineered and matched, they provide you with long, troublefree service in applications almost as wide as your imagination. Here are a few fields in which Entrec Systems are at work.

Security

Key to the Entrec System is a high-quality, laminated photo identification card. Each card has its own individual identification number. Reliability results from a magnetic stripe material that becomes a permanent part of the card and which virtually cannot be erased.

The cards themselves are rugged. They've been proven in high security laboratory installations. And they've been tested by the toughest users of all — college students. They've been bent, folded, twisted, mutilated. Some have had holes punched in them. Still, they continue to work. Completely. Accurately. At one prominent university, the Entrec System has been operating without failure for two years. During that time, students have passed cards through the readers

about security and control.

21,000 times each day with an average read and response time of less than one second each.

As an Entrec System owner, you can make and encode cards with up to 40 characters of information each on the magnetic stripe. Your system can be programmed to control access to sensitive production, engineering, research and development, office and EDP areas. You can be assured that proprietary information and restricted areas are kept secure from unauthorized use or from attempts at industrial espionage.

Time and attendance

Available with an optional LED clock readout, the Entrec Card Reader eliminates the need for old fashioned time clocks. As entering and departing employees pass their cards through the readers, you can control access to work areas at the same time you improve the speed of processing. Entrec card readers are faster than conventional time clocks. And your printer provides you with all the information you need for payroll processing. The keyboard permits rapid updating of the system. When an employee leaves, he is removed from the system and can no longer gain entry even though he may keep his card.

Entrec magnetic card reader terminals are now available in handy, economical, stand-alone form. Stand-alone units have a built-in memory for up to 999 persons. And they'll control access in up to four time zones.

Entrec stand-alone card readers are easily programmed from any keyboard-printer. And they can be used in dial-up mode.

Access control

With an Entrec System, you can regulate access to, and control the use of, virtually any area or equipment.

For instance, colleges and universities can regulate entry to eating facilities, dormitories, research areas and special events. Libraries can use the system to check books in and out.

Businesses can restrict use of company vehicles and monitor the use of increasingly valuable fuel, as well as access to parking lots, reserved parking and executive areas, work areas, warehouses, copy machines, elevators.

Your Entrec System will give you the information you need to keep track of what your costs are. And you'll be able to control them.

In a world where inflation, security problems, stolen ideas, pilferage and improper use of equipment all can spell red ink, you'll have the ability to slash losses and move your operating statement more solidly onto the plus side.

That's what control and peace of mind are all about.
And those are what Entrec Systems give you.

For further information, call or write: **Harco Industries, Inc.**
10802 N. 21st Avenue • Phoenix, AZ 85029 • Phone: (602) 944-1565.

ENTREC
SYSTEMS
HARCO INDUSTRIES, INC.

Builders of photo identification systems for more than 30 years.

Specifications

Entrec Card Reader Terminal

- Available in wall mount or tabletop models.
- Microprocessor based (Intel 8085).
- EPROM programmable memory.
- Internal on-board regulated power supply.
- Modular circuit board design.
- Internal solid state relay for external switching.
- Standard RS 232c interface.
- Six lighted, variable message indicator panels.
- 115V AC, 60Hz, 250ma.
- Options: LCD time clock display. 12- or 16-position keypad. Internal counter.

Central Minicomputer

- National service contract available.
- Up to 64K bytes memory.
- Additional disc and tape support available.
- Diagnostic software and bootstrap loader standard.
- Real time clock.
- Power fail auto restart standard.
- Multiple communication lines (four minimum).
- Complete line of expansion equipment.

Control Console

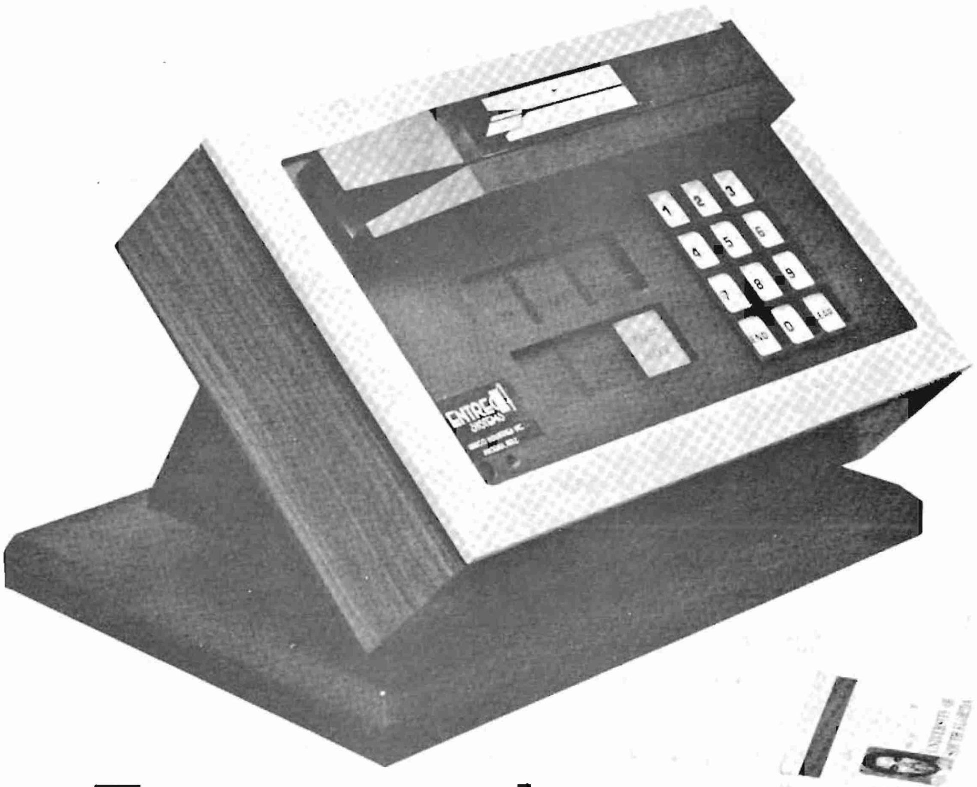
- Lightweight, silent printer.
- CRT optional.
- Multiple units available.

ENTREC
SYSTEMS

HARCO INDUSTRIES, INC.

Builders of photo identification systems for more than 30 years.

10802 N. 21st Avenue • Phoenix, AZ 85029 • Phone: (602) 944-1565.



Easy reader

Entrec Magnetic Stripe Card Reader Terminals

Reliable, trouble-free, easy to install and use, Entrec Magnetic Stripe Card Reader Terminals are designed and built with proven technology and state-of-the-art components.

Easy to use

With a wipe-through reader that eliminates jamming due to bent cards, each Entrec terminal straightens bent or deformed cards. It's designed to read a card with a clip attached and to provide error-free operation. Life of the reading head is more than a half-million reads.

Easy to understand

Six lighted message indicator panels clearly indicate to the cardholder the results of the read. Pleasant or unpleasant audible tones reinforce the messages. An optional, 12-position keypad permits the entering of personal identification numbers. Audio signals verify proper keystroke. An optional four-digit LED. indicator may be used as a time clock or for other digital messages.

Easy to Install

Entrec Card readers connect to standard, 115V AC wall outlets. Output for computer interface is the standard EIA RS232c with switch selectable baud rates of from 300 to 9600. Wiring is simply two twisted pairs between the computer and reader. You can wire as many as 15 readers in multi-drop form on one line.

Entrec magnetic card reader terminals are now available in handy, economical, stand-alone form. Stand-alone units have a built-in memory for up to 999 persons. And they'll control access in up to four time zones.

Entrec stand-alone card readers are easily programmed from any keyboard-printer. And they can be used in dial-up mode.

Easy to service

Entrec card readers almost never require service. That's because they're microprocessor based, using the reliable Intel 8085 integrated circuit. With modular construction, circuit boards can be removed quickly if repairs are necessary.

Easy to program

Programmable memory in each unit permits us to make fast and easy program changes to meet the needs of specific installations. The internal microprocessor reads the card, verifies that it was read correctly and stores the data until the central minicomputer requests it. If a card must be re-read, an indicator light requests that the card be entered again.

Easy card production

Almost impossible to erase, the magnetic stripe material used in Entrec System cards will carry up to 40 digits of information. Readers erase all normal encoding, eliminating false cards or experimental entries. With available equipment and supplies, you can make and encode cards on site.

Easy system

With other components, it's easy to build a complete Entrec Controlled Access System. Included are the readers, a nationally known and serviced minicomputer, a keyboard printer-console, controlled access software, card producing and encoding equipment. Attach floppy discs, CRTs or other standard peripherals as options. With the tape cartridge option, you can have transaction logging, data reloading and program reloading.

Easy to get

Just write or call **Harco Industries, Inc.**, 10802 N. 21st Avenue, Phoenix, AZ 85029. Phone: (602) 944-1565.

Specifications

Entrec Card Reader Terminal

- Available in wall mount or tabletop models.
- Microprocessor based (Intel 8085).
- EPROM programmable memory.
- Internal on-board regulated power supply.
- Modular circuit board design.
- Internal solid state relay for external switching.
- Standard RS 232c interface.
- Six lighted, variable message indicator panels.
- 115V AC, 60Hz, 250ma.
- Options: LCD time clock display. 12- or 16-position keypad. Internal counter.

ENTREC
SYSTEMS

HARCO INDUSTRIES, INC.

Builders of photo identification systems for more than 30 years.

10802 N. 21st Avenue • Phoenix, AZ 85029 • Phone: (602) 944-1565

APPENDIX D

Derivation of System Card Costs

TABLE D-1

Costs Associated With a Non-Photo Meal Card Program

Vendor	Price/Card	Encoding Equipment	Total First Year Cost	Outyear Cost
IBM	$ 1.16	Not Required	$ 3,417[a]	$ 997[b]
Rusco[c]	$ 1.49[d]	Not Required	$ 4,158	$ 1,188
Vali-Dine	$ 0.87	$ 1,875	$ 4,461[e]	$ 1,352[f]
Vikonics	$ 1.95	Not Required	$ 5,460	$ 1,560
Cardkey	$ 1.02	Not Required	$ 2,856	$ 816
Identimat	$ 0.30	$ 4,275	$ 5,115	$ 240
Schlage	$ 3.25	Not Required	$ 9,100	$ 2,600
APD	$ 2.00	Not Required	$ 5,600	$ 1,600

[a] Includes a one-time layout charge of $100 and a $67 setup charge.

[b] Includes a $67 setup charge.

[c] In the absence of data from Rusco, their card costs have been estimated to be between those of Vikonics and Cardkey since all these companies' readers use the same type of card.

[d] Rounded up from $1.485 which was used in the cost calculations.

[e] Includes a one-time layout charge of $150.

[f] Includes a rental fee of $656 for the encoding equipment.

TABLE D-2

Cost Associated With a Photo Meal Card Program

Vendor	Price/ Card	Encoding Equipment	Photographic Equipment	Total First Year Cost[a]	Outyear Cost[b]
IBM	$ 1.39	Not Required	$ 2,000	$ 6,873[c]	$ 1,411[d]
Rusco[e]	$ 1.91	Not Required	$ 2,000	$ 8,162	$ 1,760
Vali-Dine	$ 1.62	$ 1,875	$ 450	$ 7,825[f]	$ 2,634[g]
Vikonics	$ 2.45	Not Required	$ 2,000	$ 9,674	$ 2,192
Cardkey	$ 1.37	Not Required	$ 2,000	$ 6,650	$ 1,328
Identimat	$ 0.75[h]	$ 4,275	$ 2,000	$ 4,914	$ 832
Schlage	$ 4.00	Not Required	$ 2,0Q0	$14,014	$ 3,432
APD	$ 3.50	Not Required	$ 2,000	$12,614	$ 3,032

[a] Includes a film cost estimate of $814 (2800 cards x $0.2906/card).

[b] Includes a film cost estimate of $232 (800 cards x $0.2906/card).

[c] Includes a $100 layout charge and a $67 setup charge.

[d] Includes a $67 setup charge.

[e] In the absence of data from Rusco, their card costs have been estimated to be between those of Vikonics and Cardkey since all these companies' readers use the same type of card.

[f] Includes a $150 layout charge.

[g] Includes a rental fee of $656 for the encoding equipment and $450 for the photographic equipment.

[h] Although photo cards are not necessary with the Identimat system, an estimated photo card program was included for the reader's information. The price per card was estimated by adding $0.45 to the cost of Identimat's "regular" card. $0.45 more per card was used as the estimate because it was determined in this report that, on average, this is what other vendors charge for their photo cards.

APPENDIX E

Cardkey Specifications

An Access Control System that does more and costs less

INTRODUCING

the Cardkey Interrogator 790 Security Access Control System

Cardkey™

control
at your fingertips

Total security control and monitoring is now available in a neat, compact desk top unit. The Cardkey Interrogator 790 puts this full control at your fingertips, quietly, unobtrusively.

The Interrogator 790 is a COMPLETE system. No hidden extras or options are necessary for total security control. Connection of the cardreaders to the system processor and console results in an instantly active installation.

Modern electronic engineering and Cardkey's nearly forty years of experience in the security business have come together to produce this simple-to-operate, compact yet complete system at a remarkably low cost.

The digital display indicates activity, which is also recorded on a printout. Personnel changes, variations of access levels and time zones can all be made from the convenient keyboard without retrieving the card or alerting the cardholder.

Backed by nationwide service the Interrogator 790 is built for **your** security needs.

Access Control

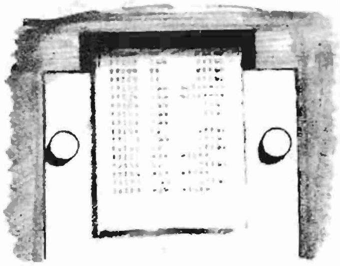
Controlling **who** goes **where** and, as importantly, **when,** is a principal function of the Interrogator 790 system. The invisibly coded card keys contain data which, when inserted into the cardreader, is interrogated by the system and will grant or deny access according to authorization predetermined by management. This predetermination includes both periods of time (time zones) and areas for which access is granted (access level), providing absolute control.

Parking

The Interrogator 790 monitors parking lots, recording who arrives and leaves, preventing overcrowding and providing space for those who have paid for it in advance, or, are otherwise authorized. The same card key that admits to the parking area can also contain the access status for the areas in the facility for which the cardholder is authorized. The Interrogator 790 also has the capability to alert the console operator in the event of the parking arm malfunction. Single use and anti-pass back options are also available.

Equipment/Machine Control

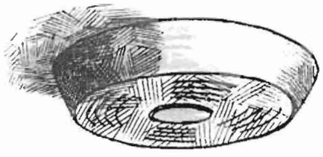
As part of the Interrogator 790 system, various office machines or plant equipment may be made operational only through the use of an authorized card key. All transactions on controlled equipment will be monitored and recorded for later analysis.

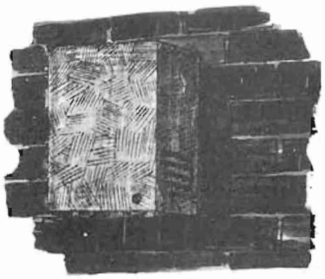


Printed Record

All activity is recorded automatically. Valid entries are indicated in black, showing card number, time and date. Denied entries are printed in red, indicating the card number, time, date and reason for invalidity. Alarms and environmental records indicate which monitor is reporting. The time, date, and reason for activity are printed out in red. Audio warning occurs simultaneously, directing the console operator's attention to the alarm and enabling swift remedial action to be taken.

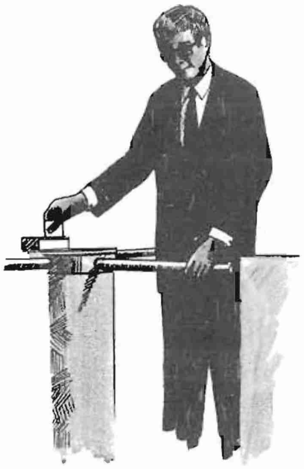
The Interrogator 790 performs many functions, some of them are illustrated below. Its cost effectiveness is indisputable. Constantly monitoring, controlling and recording all activities simultaneously, it eliminates the emotions and inherent problems of human guards. It cannot be coerced, will not get sick or suddenly leave your employ. Physical attack on the cardreaders at the secure location will not result in entry. Whether you see your security problem illustrated or not, call Cardkey Systems, we will be happy to discuss your specific needs and advise how the versatile, low cost Interogator 790 system will help you.





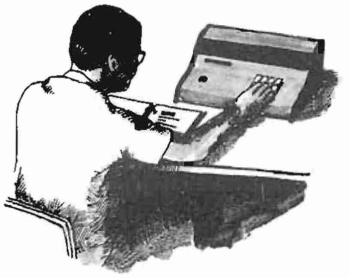
Alarms

In addition to controlling and recording access activity, an important function of the Interrogator 790 is the ability to monitor many alarms. All this is done simultaneously but alarms are given first priority. Air-conditioning, smoke, noise level, intrusion and other environmental and security alarms are constantly reviewed by the Interrogator 790 system and deviations beyond predetermined parameters result in audio warning and immediate printout of the problem. This instant warning permits appropriate action to be taken swiftly, limiting potential liability.



Turnstyles/Mantraps

Cardkey's Interrogator 790 can also be used in conjunction with turnstyles and mantraps. As with any door, a Cardkey Securiti-Card® is used to gain entry. The optional In-X-It™ function requires the use of the card to exit. This provides the capability to obtain a printout of all personnel on the premises at any given time.



Central Control

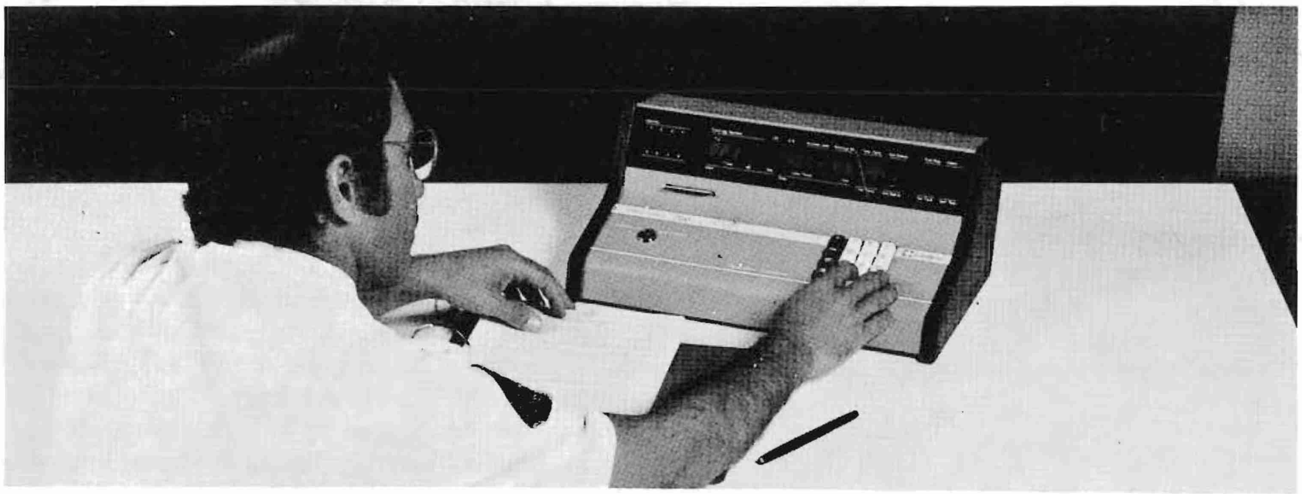
One person can easily monitor the total security system covered by the Interrogator 790. All operations are conducted at the neat, compact console. The parameters of access levels and time zones can be changed using the console. Individuals or groups may be changed instantly without recalling the card itself or alerting the cardholder. A warning sound occurs with alarm activity and the printout indicates to the operator the nature of the problem.
The clear digital display indicates the time and date and is used for programming, controlling and testing the daily operations of the system.

Guard Tours/ Housekeeping Control

Guard tours can also be monitored and recorded by the Interrogator 790. Janitorial staff are strictly controlled by limiting the access time to any particular area. The Interrogator 790 will also monitor when emergency exits are opened and closed.

Cardkey™

The name that started an industry



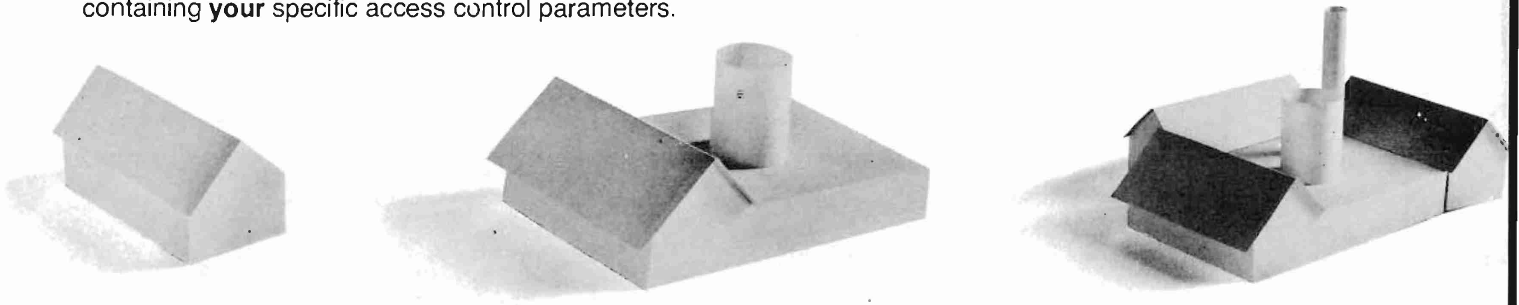
The new look in security systems.

The Interrogator 790 is a **complete package system** designed to perform multiple security control and environmental monitoring functions. The low cost makes it eminently suitable for most businesses.

A small credit card size Securiti-Card® is issued to each person, which contains their invisibly coded access privileges.

Cardreaders, located at the security entrances and alarm monitoring terminals, relay information to the micro-computer built into the Interrogator 790 containing **your** specific access control parameters. As this data is received the computer is interrogated and instantaneously grants or denies access.
The use of invalid card keys with incorrect access levels or time zones results in an alarm condition, which is both signalled audibly and printed out. Abnormal environmental conditions also result in an alarm mode.

The clear digital display indicates all activity as it occurs and enables rapid changes in card authorization to be made accurately.



Cardkey Systems expand as you do.

The problems of security compound with growth. Cardkey Systems grow with you providing control and monitoring for thousands of personnel, vehicles entrances and alarm points.

Cardkey Systems — for total concept access control and environmental monitoring.

Cardkey™

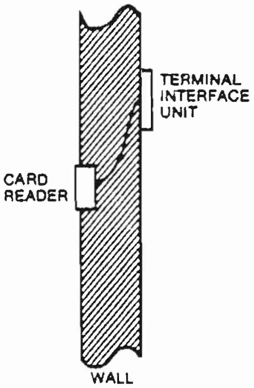
The name that started an Industry

CARDKEY SYSTEMS
20660 BAHAMA STREET
CHATSWORTH, CALIFORNIA 91311
(213) 998-7560/TELEX: 651-375
EUROPEAN MANUFACTURING AND SALES OFFICE
CARDKEY SYSTEMS LTD
23 STADIUM WAY
READING BERKSHIRE RG3 6ER ENGLAND
0734 415 211
TELEX 847733
REGIONAL OFFICES WORLD WIDE

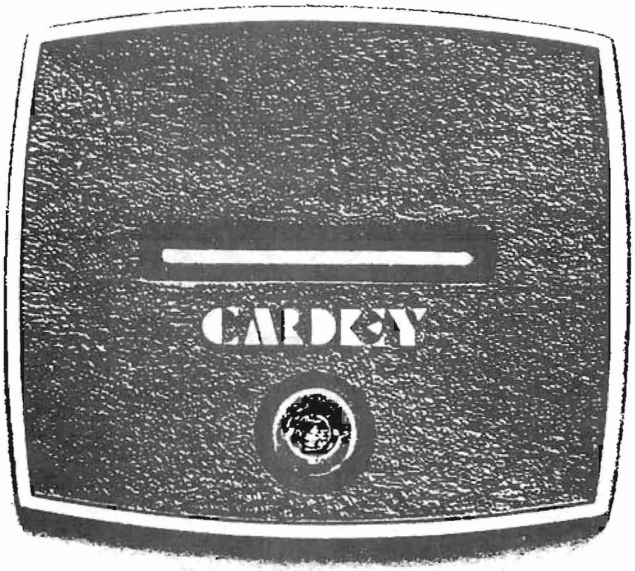
VSI A VSI COMPANY

Cardkey Serial Reader

Cardkey's Serial Reader is a combination of two units — a Card Reader, and a Terminal Interface Unit. The Card Reader is mounted on a wall surface **outside** the restricted area and near the door, and the Terminal Interface is installed inside the restricted area. The two units are connected electrically via cable harness.



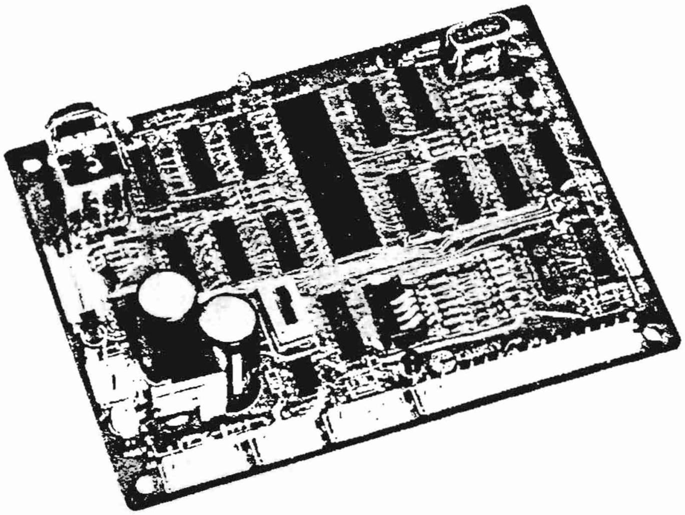
The Card Reader is used with the Securiti-Cards™ furnished by Cardkey. It utilizes a magnetic lock which prevents an improperly coded or false card from fully entering the Reader. Only a correctly coded card, matching the coding of the Matrix Card in the lock, can fully enter, and actuate the Card Key switch. The closing of this switch enables the Serial Reader to provide a card identification number when polled by the Interrogator 880™ Central Controller through its interconnection system. The Card Key contains a magnetically-encoded identification number, which is "read" by the Reader when the card is fully inserted.



The Terminal Interface converts the parallel data received from the Card Reader into a serial form, for use with the Interrogator 880. It both receives information from and transmits information to the Controller. It monitors the status of four alarm functions associated with the Reader, and provides this information to the Central Controller when required. An Access Relay in the Terminal Interface is actuated to enable door strike operation when the appropriate signal is received from the Controller. Door access time is adjustable within the Terminal Interface from one to more than 10 seconds.

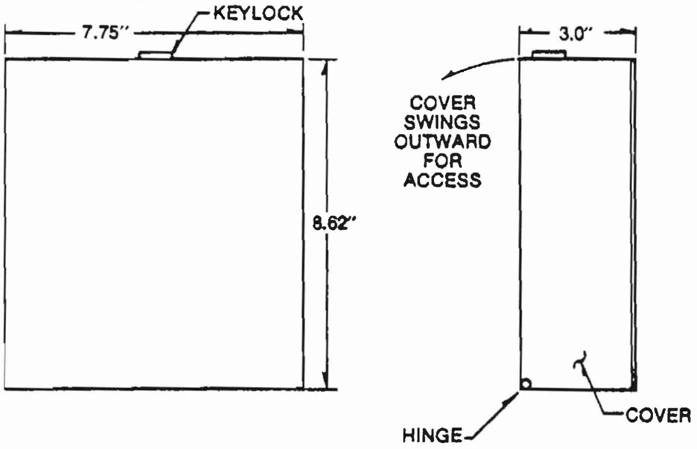
A separate Emergency Battery and Charger Unit is an accessory which may be used to provide standby power in the event of a power failure. All critical circuitry is contained within the Terminal Interface located in the secured area, and tampering with the Card Reader cannot result in access being granted.

By taking advantage of the Reader's dual code capabilities, each Reader in the system may be operated off-line, independent of the Central Controller. The built-in mode of operation is easily selected by a switch located within the Terminal Interface.

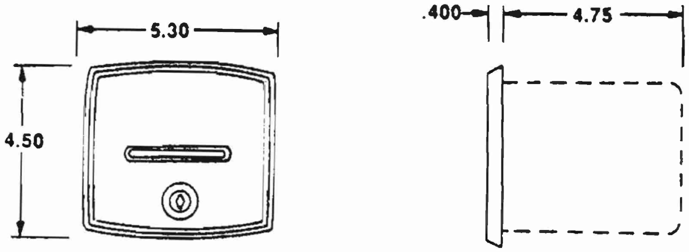


Two twisted pairs of wires are required for the connections between the Terminal Interface and the Central Controller. Connections may be made in any of several methods. Direct connections may be made up to a maximum of 1.5 miles. Connections may also be made (1.5 miles maximum) to a Terminal Expander which, in turn, may be up to 1.5 miles from the Central Controller. Connections may also be made through Modems and telephone circuits for unlimited distances.

Enclosure Dimensions



Card Reader (flush mount)



Procurement Specifications

The Serial Reader/Terminal shall be ol solid state design. It shall include a Card Reader mounted within (specify one: flush mount, surface mount, weather-resistant surface mount, etc.) and a serial Terminal Interface unit manufactured by Cardkey Systems as the Serial Reader/Terminal. No system compromise shall be possible from circuitry located within the Card Reader unit. All critical circuitry will be located within the independent Terminal Interface unit in the secure area and the Central Controller to which the Serial Reader/Terminal connects. The Terminal Interface unit shall be tamper-proof (Tamper switch) and equipped with a keylock.

The Serial Reader/Terminal shall be capable of operation with the Cardkey Systems' Interrogator 880 Central Controller and shall require no more than two twisted pairs of 22 gauge unshielded wire for the interconnection. The Reader/Terminal shall be capable of operating up to 1.5 miles from the Central Controller, with no special termination being required for different distances. The Reader/Terminal shall also be capable of operation with the Cardkey Systems' Terminal Expander and Modem units to provide maximum installation flexibility, communications efficiency, and cabling economy.

The Card Reader shall have two levels of operational security. The first level shall be a magnetically operated mechanical locking section programmed by means of a Program card inserted into the secured side of the Reader and having a unique facility code. The second level shall be an electronic reading section capable of reading an invisibly coded identification number with the Securiti-Card™.

The access output shall be a relay contact closure, located within the Terminal Interface unit, capable cf ac/dc operation. Access time shall be adjustable from 1 to 10 seconds. The Terminal Interface shall include capability to monitor four dry-contact closure type alarm detectors and provisions to transmit alarm status information each time the unit is polled by the Central Controller. A switch located within the Terminal Interface shall be capable of converting the operation of the Serial Reader/Terminal from an on-line mode to an off-line mode of operation. Provisions shall also be included for the connection of an Emergency Battery and Charger accessory to provide standby power in the event of power failure.

OPERATION

The System shall operate through the insertion of a properly encoded Securiti-Card. The Serial Reader/Terminal is polled by the Central Controller and the card identification number is transmitted to the Central Controller where it is checked for validity, Time Zone status, and Access Level status. If the identification number is found to meet all entrance criteria, a signal from the Central Controller enables the Terminal Interface unit to grant access. When the identification number is invalid for any reason, access is not granted, and an alarm condition is generated at the Central Controller.

CARDKEY
TOTAL CONCEPT ACCESS CONTROL
CARDKEY SYSTEMS
A DIVISION OF GREER HYDRAULICS, INC.
20339 NORDHOFF STREET
CHATSWORTH, CALIFORNIA 91311
(213) 882-8111/TELEX: 651-375

Procurement Specification for
INTERROGATOR 790 ACCESS CONTROL SYSTEM

1.0 GENERAL

The access control system shall be as manufactured by Cardkey Systems as the Interrogator 790 Access Control System and shall include an Operator Console and Central Controller console; (specify quantity) remote access control Reader/ Terminals; (specify quantity) Cardkey Securityi-Cards; (optional: specify quantity) Terminal Expanders; (optional: specify quantity) Alarm Monitors; and (optional: specify quantity) Modems.

2.0 OPERATOR CONSOLE AND CENTRAL CONTROLLER

The centrally located Operator Console and Central Controller console shall be of all solid state design. The system shall include the functions of Contact Alarm Reporting, Alarm Print Select, Calendar Clock, and bulk loading of Securiti-Cards from any single or multiple parameter. The system shall be capable of controlling (specify quantity from one group below) Reader/Terminals and shall have a memory bank capable of storing data for (specify quantity from same group) Securiti-Cards.

	Reader/Terminals	Memory
(Group A)	4	500
(Group B)	8	500
(Group C)	16	1500
(Group D)	8	2500
(Group E)	16	2500

The system shall provide 32 Access Levels and 32 Transaction buffer. The system shall contain the functions and features contained in Option Package (specify: 1, 2, 3, or 4) which includes (specify contents of selected option package):

(Option Package 1) a hard copy Printer installed in the Central Controller, an internal Audible Alarm and 8 Time Zones

(Option Package 2) a hard copy Printer installed in the Central Controller, and internal Audible Alarm, 8 Time Zones, Entry-Exit, Programmable Lock-out, and Print Select.

(Option Package 3) a hard copy Printer installed in the Central Controller, an internal Audible Alarm, 8 Time Zones, and Manual and Automatic Terminal Override.

(Option Package 4) a hard copy Printer installed in the Central Controller, an internal Audible Alarm, 8 Time Zones, Entry-Exit, Programmable Lockout, Print Select, Manual and Automatic Terminal Override, Listing Capability, and Test Card Reader and Program Enable.

All controls shall be on the Operator Console front panel. A single keyboard shall be provided to enter functional and digital information. Large, easy-to-read, .43-inch high displays shall be provided for use during keyboard entries, and to present all parameters for Reader/Terminals and Securiti-Cards. The display shall include time information from an internal clock which controls all time-related functions. The time display includes Time of Day, Day of Year, and Day of Week. Time Zone control shall be accurate to the minute of time displayed. In the event of power failure the Controller shall maintain vital memory parameters and continue to update the system clock so that Time Zone Control will still be operational for a minimum of 16 hours for a 500 card system on emergencey batteries. A battery condition indicator shall be provided. It shall be possible to enable access at any terminal location by means of keyboard entries at the Controller. The following optional accessories and functions shall be included in the Controller (Specify): EIA Interface-Output Only, EIA Interface-Output/Input, and Magnetic Tape Interface. (Specify: A Remote Printer shall be supplied for hard copy printouts and the associated EIA RS-232-C interface shall be included in the Controller.)

2.2 PROGRAMMING

The program mode shall be controlled by a keyswitch (and by cards assigned to a preselected Access Level when Test Reader/Program Enable option is included). Terminals and cards are programmed into memory with their operating parameters by means of simple keyboard entries. All parameters are displayed for verification before being stored in memory. The display shall indicate whether parameters being programmed have been stored in memory, or rejected as unacceptable. Cards or terminals may be group-loaded into memory when Access Levels and Time Zones are the same. After keying in card data, group loading speed to load card shall be included to allow reissuing the same card number to replace lost or stolen cards by changing the card issue level.

2.3 OPERATION

The Controller shall control Securiti -Cards by comparing the time and location of any attempted usage with information stored in memory. When a card is used, access will be granted only when it has a valid number, it is valid for the current time period and for the terminal where it is used, and when the terminal is operational in the current time period.

When all conditions have been satisfied, a signal to the terminal shall instantly enable access at that location and the display shall show the card number, time, and terminal number. If access is not granted for any reason, an alarm indicator shall illuminate and the display shall show the same transaction data plus a code signifying the reason access was not granted.

The Controller constantly polls all terminals and all terminals always respond. If a terminal is disabled (cut cable, etc.) an alarm indicator shall illuminate and the display shall show the terminal number, time, and code indicating that the terminal is disabled. Any alarm condition (from 4 alarm inputs to each Reader/Terminal or from 8 alarm inputs to each Alarm Monitor) is instantly displayed. Any alarm shall be provided at a rear panel connector for optional use with an external alarm. All valid transactions can be printed in black and all invalid transactions can be printed in red.

2.4 DISPLAY

Once entered into memory, parameters may be recalled for display without risk to the stored information. The Controller shall be capable of recalling from memory and displaying the next item in sequence for: card number; terminal number, Access Level for terminal number entered; and day of Time Zone entered. All entries for card data are made using the card identification number; no separate addresses or tables are used. The time periods for each Time Zone for each day of the week can be displayed. The Controller shall be capable of storing the last 32 transactions for recall to display, showing all data pertinent to the type of transaction.

2.5 SEARCH AND LISTING CAPABILITY (Option)

The Controller shall be capable of searching for and displaying sets of parameters. For Securiti-Cards: All cards entered into memory; next higher card number having the displayed Time Zone, Access Level, Void/Valid status, Entry/Exit status, or any combination of these parameters. For Reader/Terminals: Next higher terminal number having the displayed Time Zone, Void/Valid status, or both.

The Controller shall be capable of searching for and providing a hard copy printout of the following. For Time Zones: List all Time Zones with all parameters for each. For Securiti-Cards: Sequential blocks of card numbers with parameters for each; valid cards in a block of card numbers with parameters for each; cards having specified Time Zone; cards having specified Access Level; all cards in system; (with Entry/Exit feature: Cards currently in plant; cards currently out of plant). For Reader/Terminals: Sequential group of terminals and parameters for each; for a group of terminals, list terminals having specified Time Zone, Void/Valid status, or both;

list all Access Levels for terminal specified; list all terminals for specified Access Level: list all terminals for specified group of Access Levels. The Controller shall include buffering so that system speed is not limited by printer speed.

2.6 PERIPHERAL EQUIPMENT

The Controller shall be capable of having Reader/Terminals, Terminal Expanders, and Alarm Monitors connected directly up to a distance of 1.5 miles; no line compensation shall be required. Modems, operating at a speed of 1200 BAUD, may be connected to provide unlimited operating distances over telephone circuits. Alarm Monitors may be substituted in place of Reader/Terminals; 16 Alarm Monitors will enable the use of 128 alarm detectors. The addition of Modems or other peripheral equipment shall not reduce system capabilities. The system may be expanded in the field to achieve maximum Reader/Terminal capacity and memory capacity. Interfaces may be added for operation with magnetic tape and other computer peripherals.

3.0 SERIAL READER/TERMINAL

3.1 GENERAL

The Serial Reader/Terminal shall be of solid state design. It shall include a Card Reader mounted within (specify one: flush mount, surface mount, weather-resistant surface mount,etc.) and a serial Terminal Interface unit manufactured by Cardkey Systems as the Serial Reader/Terminal. No system compromise shall be possible from circuity located within the card reader unit. All critical circuitry will be located within the independent Terminal Interface unit in the secure area and the Central Controller to which the Serial Reader/Terminal connects. The Terminal Interface unit shall be tamper-proof (Tamper switch) and equipped with a keylock.

The serial Reader/Terminal shall be capable of operation with the Cardkey Systems' Interrogator 790 Controller and shall require no more than two twisted pairs of 22 gauge unshielded wire for the inter-connection. The Reader/Terminal shall be capable of operating up to 1.5 miles from the central controller, with no special termination being required for different distances. The Reader/Terminal shall also be capable of operation with the Cardkey Systems' Terminal Expander and Modem units to provide maximum installation flexibility, communications efficienty, and cabling economy.

The Card Reader shall have two levels of operational security. The first level shall be magnetically operated mechanical locking section programmed by means of a Program Card inserted into the secured side of the Reader and having a unique facility code. The second level shall be an electronic reading section capable of reading an invisibly coded identification number within the Securiti-Card.

The access output shall be a dry relay contact closure located within the Terminal Interface unit, capable of ac/dc operation. Access time shall be adjustable from 1 to 10 seconds. The Terminal Interface shall include the capability to monitor four dry-contact closure type alarm detectors and provisions to transmit alarm status information each time the unit is polled by the Central Controller.

A switch located within the Terminal Interface shall be capable of converting the operation of the Serial Reader/Terminal from an on-line mode to an off-line mode of operation. Provisions shall also be included for the connection of an Emergency Battery and Charger accessory to provide standby power in the event of power failure.

3.2 OPERATION

The system shall operate through the insertion of a properly encoded Securiti-Card. The Serial Reader/Terminal is polled by the Central Controller and the card identification number is transmitted to the Central Controller where it is checked for validity, Time Zone status, and Access Level status. If the identification number is found to meet all entrance criteria, a signal from the Central Controller enables the Terminal Interface unit to grant access. When the identification number is invalid for any reason, access is not granted, and an alarm condition is generated at the Central Controller.

4.0 TERMINAL EXPANDER

The Terminal Expander shall be of solid state design. It shall include isolated interface ciruitry for (specify: 8, 16) Serial Reader/ Cardkey Systems' Interrogator 790 Central Controller and shall be capable of operation up to 1.5 miles from the Controller. Connections to the Controller may be made directly via two twisted pairs of unshielded wires, or through Cardkey Systems' Modems and telephone circuits for greater distances. The isolated inputs shall be capable of operating with either Serial Reader/Terminals or Alarm Monitors. Reader/Terminals may be located up to 1.5 miles from the Terminal Expander.

5.0 ALARM MONITOR

The Alarm Monitor shall be of solid state design. It shall include inputs for eight, dry-contact type alarm detectors. The Alarm Monitor shall be capable of operation with the Cardkey Systems Interrogator 790 Central Controller, and shall require no more than two twisted pairs of unshielded wires for the interconnection. The Alarm Monitor shall also be capable of operation with the Cardkey Systems Terminal Expander and Modem units to provide maximum system flexibility.

The Alarm Monitor shall continually monitor the status of the alarm detectors. When polled by the Central Controller, the Alarm Monitor shall respond with a signal which identifies each of the eight alarm detectors by address and number, and provides the status of each. A change in status of any alarm detector will generate an alarm condition at the Central Controller.

6.0 MODEM

The Modem shall be of solid state design. It shall be capable of interfacing with Cardkey Systems' Interrogator 790 Central Controller, Serial Reader/Terminal, or Alarm Monitor. The Modem shall convert digital input signals from such equipment to FSK form telephone transmissions. Upon receiving FSK signals from a telephone circuit the Modem shall convert these signals to digital form for interfacing with the Central Controller, Serial Reader/Terminals, or Alarm Monitors. FSK signals shall be comprised of 1200 Hz and 2200 Hz frequencies. Telephone operation shall be over 3002 service, 4-wire full duplex telephone circuits. Data rate shall be 1200 BAUD.

The Modem shall include isolated interface circuitry for at least 16 Serial Reader/Terminals, or Alarm Monitor Terminals.

7.0 CARD KEYS

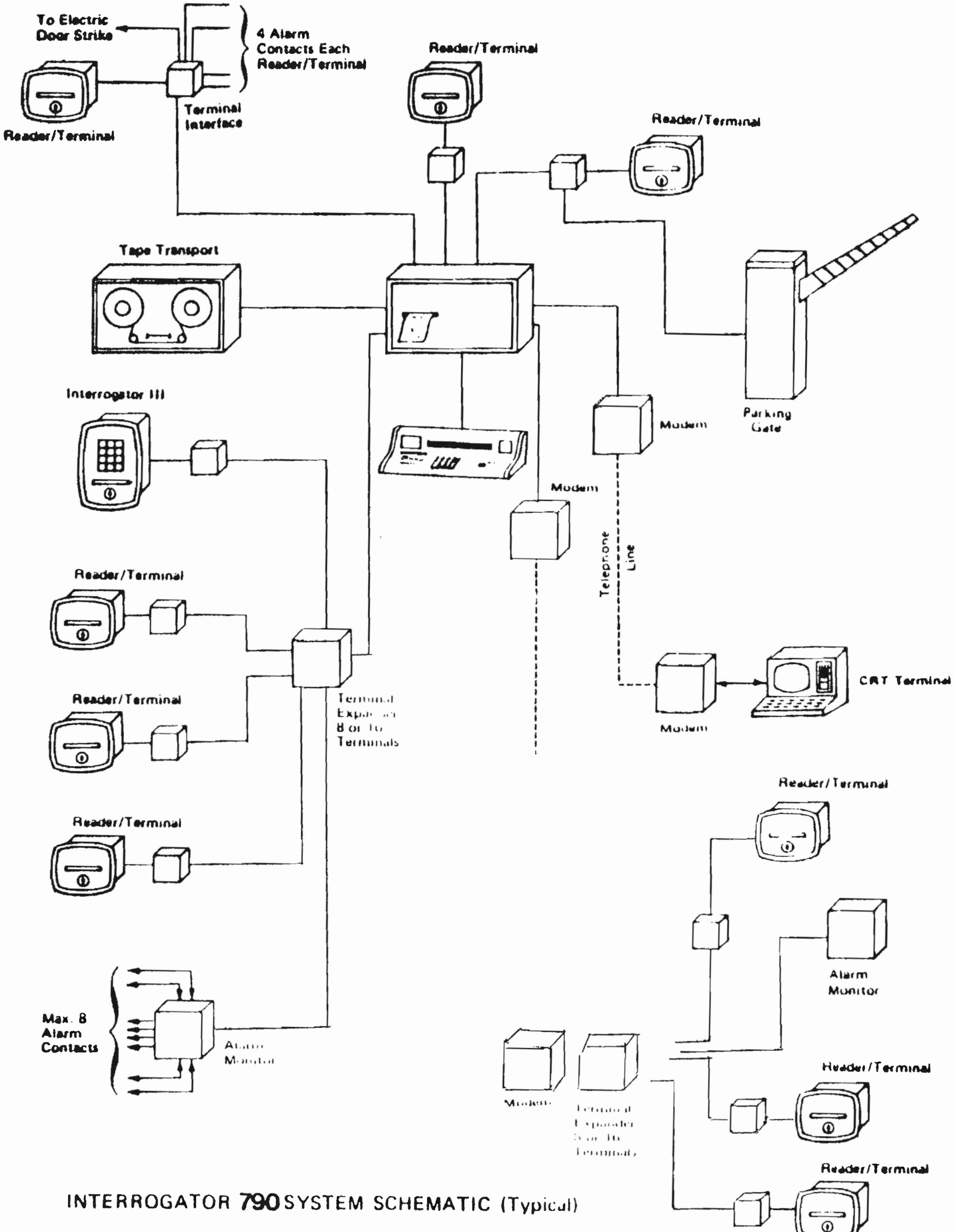
Each invisible encoded Securiti-Card contains two separate codes necessary to obtain access to a facility. The first code is a unique facility code consisting of a minimum of five (5) bits. The second code is a personalized five (5) digit code. The cards are capable of accepting coded bits in a scrambled pattern as a unique identification code stored within the cards. The cards are capable of operating the Reader Terminal Units. The card keys are highly resistant to wear and environmental deterioration. Cards are capable of being printed on any area of the card, front and back, and of being produced as a pressure and heat laminated photo I.D. card. The access level of each card is programmable to permit access to specific areas of the facility.
The cards have an issue level feature permitting the same basic identification number to be retained by an employee when a replacement card is issued.

Interrogator 790

OPERATING SPECIFICATIONS

				Access
Model	Ambient Temp.	*Humidity	Power Req.	Outputs
Operator Console	32°F - 115°F	0 - 95%	---	---
Central Controller	"	"	115vac, 2A, 50/60Hz 230vac, 1A, 50/60Hz	---
Reader/Terminal	32°F - 130°F	0 - 95%	8vac, 10VA,50/60Hz	Dry Contacts 5A res. at 24 vdc, or 3A res. at 115 vac.
Alarm Monitor	"	"	"	---
Terminal Expander	"	"	8vac, 20VA,50/60Hz	---
Modem	"	"	8vac, 10VA,50/60Hz 16vac, 10VA,50/60Hz	---

*Non-condensing



INTERROGATOR 790 SYSTEM SCHEMATIC (Typical)

Copyright 1979 – Cardkey Systems

APPENDIX F

Identimat Specifications

IDENTIMAT CORP.
135 WEST 50th STREET
NEW YORK, N.Y. 10020 (212) TEL. 371-3300

IDENTIMAT® 2000D

TRANSMITTING IDENTIFIER

D

FUNCTION

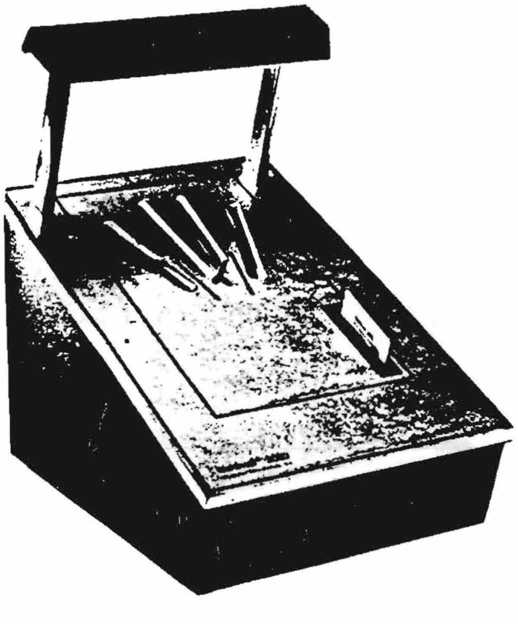
The IDENTIMAT 2000D is an on-line unit that quickly, automatically, and positively verifies the identity of a person, and not just their card. This verification is accomplished when an individual's hand geometry characteristics are quickly, precisely and automatically measured and compared against data previously encoded on the user's card. The employee number is then transmitted to the IDENTIMAT 3000 Central Console for validation. Upon final verification the IDENTIMAT provides an "access" signal which could release an electronic door turnstile, allow a time clock to punch, permit access to a computer, etc. A printed record of each transaction including time, date, station number, and employee number can be provided by the IDENTIMAT 3000 Central Console.

OPERATION

The user inserts the identity card into the machine, places one hand on the top plate and presses down gently. An "access" signal indicates verification of the user's identity and authorization for that area. A reject signal indicates wrong hand geometry, wrong area, wrong system, and/or invalid employee number.

FEATURES

- Automatically rejects lost, stolen or transferred cards even when not reported. Programmable to accept only those persons valid for that area or activity.
- One second cycle time; the time needed for the system to measure hand, read card and verify identity.
- An IDENTIMAT 2100 Encodes enables new employees hand geometry characteristics to be encoded onto card in less than 30 seconds.
- Uses magnetic stripe cards (standard credit card size) meeting American Bankers Association standards
- Unique coding for each customer.
- Solid-state integrated-circuit logic.
- Adjustable lock control timer.
- Usable in a stand-alone mode.



IDENTIMAT 2000D SPECIFICATIONS

Number of areas programmable: 12

Identification cycle time: 1 second

Switch Selectable Operating Modes: On-Line
Stand-Alone

User Instructional Lights: Insert Card
Place Hand
Access
No Access

Outputs: Accept Signal: 24 Volts A.C. (1 Amp.)
and/or contact closure

Overall Dimensions: 13" wide x 21" deep x 19½" high
Recommended shelf height: 30"-33"
above floor

Operating Temperature: 50°F to 100°F

Weight: 45 lbs.

Door Lock Timer Limits: 0.5 - 15 seconds

IDENTIMAT CORP.
135 WEST 50th STREET
NEW YORK, N.Y. 10020 TEL. (212) 371-3300

IDENTIMAT® 3000
CENTRAL CONSOLE

CC

FUNCTION

The IDENTIMAT 3000 CENTRAL CONSOLE provides employee number (up to 10,000) validation data for up to 63 Identimat stations. It also provides a printed record (using Central Console Printer option) of all Identimat station transactions. New employee numbers can be listed as valid in the Central Console Memory and terminated employee numbers can be delisted as invalid.

The Central Console is compatible with either the IDENTIMAT 2000D Identifier or the IDENTIMAT 200 Card Reader.

OPERATION

The IDENTIMAT 3000 CENTRAL CONSOLE is completely automatic and does not require an operator except for listing and delisting employee numbers in the memory.

A permanent printed record of employee number, time, date, Identimat station number and "access" indication or reason for "no access" can be obtained for each transaction using the central console printer option.

Alarm Point Station Monitor option enables automatic monitoring of alarm points (Doors, Windows, etc.). An alarm condition will give an audible as well as visual display and printed record.

CENTRAL CONSOLE FEATURES

- Automatic polling of up to 63 Identimat Stations.
- Can be used with any combination of IDENTIMAT 2000 or IDENTIMAT 200 units.
- Up to 10,000 employee numbers can be contained in memory.
- Automatic battery backup for memory in case of power failure.
- Printer option enables printing a record of all Identimat uses.
- Alarm Point Station Monitor option available.
- Solid State Integrated Circuit Logic.

SPECIFICATIONS

Voltage: 115V 50/60 Hz.
Maximum Number of Employees: 10,000
Maximum Number of Stations: 63
(Identimat and/or Alarm Point)
Visual Indicators: Employee Listed
Employee Delisted
Station Number

CENTRAL CONSOLE OPTIONS

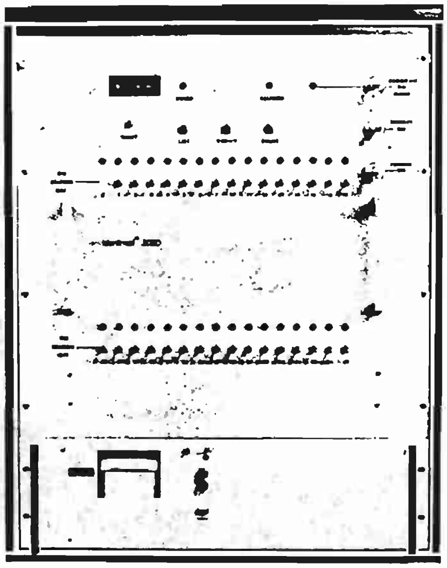
Central Console Printer CCP1: The Central Console Printer provides a permanent printed record of all transactions taking place within the Identimat system. The printed record includes: Time, Date, Station Number, Employee Number, Reason for Reject (if reject occurs). All rejects are printed in red.

Memory Expansion: The basic Central Console contains memory for 1,000 employees. This may be expanded in 1,000 increments to a maximum of 10,000. Order option MXK where X=capacity in thousands. (e.g. M7K=7,000 capacity).

Station Expansion: The basic Central Console can be used with up to 15 Identimat Stations. This may be expanded to a maximum of 63 increments of 16 stations.

For 31 Stations Order Option S31
For 47 Stations Order Option S47
For 63 Stations Order Option S63

Alarm Point Station Monitor AP1: This option provides an audible, visual and permanent printed record (using option CCP1) of alarm conditions. The alarm Point Station Monitor can detect unauthorized opening of doors, windows, etc. Available in 16 Station increments.



IDENTIMAT CORP.
135 WEST 50th STREET
NEW YORK, N.Y. 10020

(212)
TEL. 371-3300

IDENTIMAT® 2100
ENCODER

E

FUNCTION

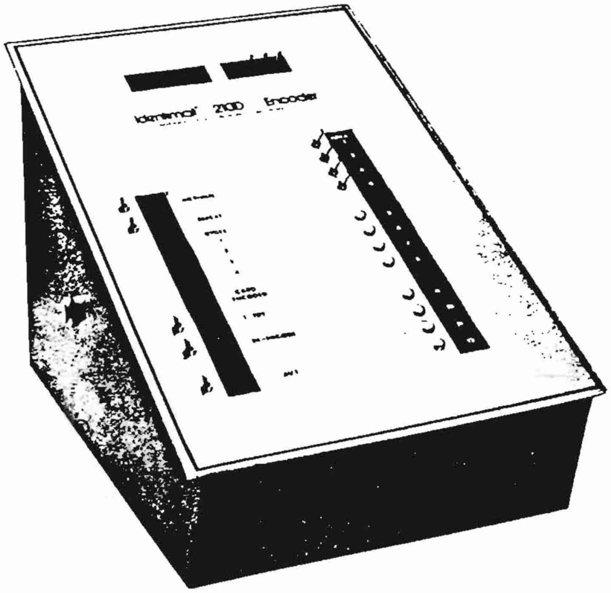
The IDENTIMAT 2100 Encoder plugs into any IDENTIMAT 2000 within its system and enables magnetic stripe cards to be encoded. In addition to encoding hand geometry on cards, the encoder can also encode the card with area access and employee number information. The encoder for each customer is unique. A card made on one customer's system cannot be used in another customer's system. The typical time to encode a card is less than 30 seconds.

OPERATION

The IDENTIMAT 2100 encoder is plugged into the IDENTIMAT 2000 and a blank card is inserted into the IDENTIMAT 2000 card slot. The user places one hand on the IDENTIMAT 2000 and the IDENTIMAT 2100 encoder automatically computes the hand geometry readings for that individual and encodes those readings on the card along with any area access and/or employee number data. The card is now invisibly encoded and ready to use.

IDENTIMAT 2100 ENCODER FEATURES

- Quickly converts any IDENTIMAT 2000 within a system into an encoding IDENTIMAT without installation.
- Cards can also be used with the IDENTIMAT 200 Card Reader.
- Unique coding for each customer.
- Solid state integrated circuit logic.
- Completely automatic encoding of Hand Geometry.
- Automatic encoding of any combination of up to 12 area access zones.
- Automatic programming of up to eight digit employee numbers.
- Less than 30 seconds to make a card.
- Automatic duplication of cards, if desired.



IDENTIMAT 2100 ENCODER SPECIFICATIONS

Voltage: 115 VAC 50/50 Hz.

Operating Temperature: 50°F to 100°F

Area Access Zones: Any combination of up to .
12 areas may be set. (optional)

Employee Number: Up to 8 numerals (optional)

Visual Status Indicators: Encoded cycle
Card Encoded
Area (with access option)

Dimensions: 13" wide x 19" deep x 12" high

Weight: 22 lbs.

ENCODER OPTIONS

Areas: Order option A4 for 4 areas
Order option A8 for 8 areas
Order option A12 for 12 areas

Numerical Digits: Order option Dx
x is the number of Numerical Digits required (up to 8)

Example order for IDENTIMAT 2100 Encoder with 4 Areas and 5 Digits:

IDENTIMAT 2100-A4-D5 Encoder

IDENTIMAT CORP.
135 WEST 50th STREET
NEW YORK, N.Y. 10020

(212)
TEL. 371-3300

IDENTIMAT® 2000S

STAND-ALONE IDENTIFIER

S

FUNCTION

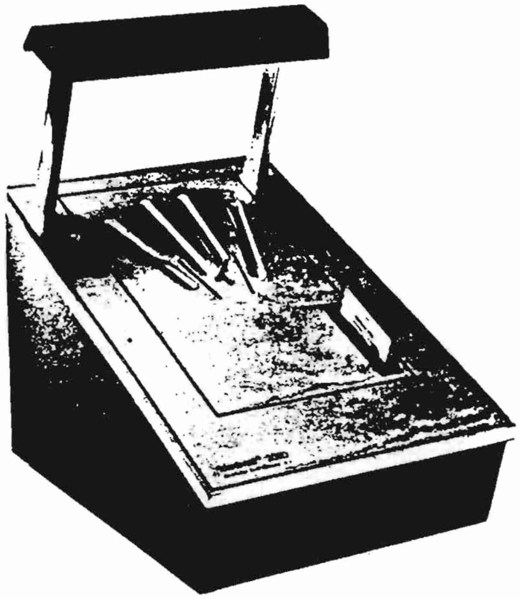
The IDENTIMAT 2000S is a stand-alone unit that quickly, automatically, and positively verifies the identity of a person, and not just their card. This verification is accomplished when an individual's hand geometry characteristics are quickly, precisely and automatically measured and compared against data previously encoded on the user's card. Upon verification the IDENTIMAT provides an "access"signal which could release an electronic door turnstile, allow a time clock to punch, permit access to a computer, etc.

OPERATION

The user inserts the identity card into the machine, places one hand on the top plate and presses down gently. An "access" signal indicates verification of the user's identity and authorization for that area. A reject signal indicates wrong hand geometry, wrong area, and/or wrong system.

FEATURES

- A completely self-contained unit that automatically rejects lost, stolen or transferred cards even when not reported. Programmable to accept only those persons authorized for a particular area or activity.
- One second cycle time; the time needed for the system to measure hand, read card and verify identity.
- An IDENTIMAT 2100 Encoder enables new employees hand geometry characteristics to be encoded onto card in less than 30 seconds.
- Uses magnetic stripe cards (standard credit card size) meeting American Bankers Association standards.
- Unique coding for each customer.
- Solid-state integrated-circuit logic.
- Adjustable lock control timer.



IDENTIMAT 2000S SPECIFICATIONS

Number of areas programmable: 12

Identification cycle time: 1 second

User Instructional Lights: Insert Card
Place Hand
Access
No Access

Outputs: Accept Signal: 24 Volts A.C. (1 Amp.)
and/or contact closure

Overall Dimensions: 12" wide x 21" deep x 19½" high.
Recommended shelf height: 30" - 33" above floor.

Operating Temperature: 50°F to 100°F

Weight: 45 lbs.

Door Lock Timer Limits: 0.5 - 15 seconds

APPENDIX G

Vali-Dine Specifications

VALI-DINE SYSTEM

FOR COLLEGE AND UNIVERSITY FOOD SERVICE

OBJECTIVES OF A VALI-DINE SYSTEM INSTALLATION {S/4}

LOWER FOOD COSTS

INCREASE FOOD SERVICE REVENUE

PROVIDE 1 ANNUAL MEAL CARD PER STUDENT

CONTROL MISSED MEAL FACTOR/PARTICIPATION

ELIMINATE UNAUTHORIZED USE OF "LOST" CARDS

INCREASE PREDICTABILITY OF COSTS AND INVENTORY

PREVENT TRANSFER OF MEAL CARDS BETWEEN STUDENTS

ALLOW FOR AND CONTROL VARIETY OF BOARD PLAN OPTIONS

RECONCILE BOARD REVENUE BETWEEN RESIDENCE/DINING HALLS

ALLOW FOR AND CONTROL NON-RESTRICTIVE DINING PRIVILEGES

PROVIDE FOR HARD COPY PARTICIPATION DATA FOR MORE EFFECTIVE MANAGEMENT

DATA COLLECTION: HEAD COUNTS BY BOARD PLAN, BY DINING HALL, BY MEAL PERIOD

R. D. PRODUCTS, INC. is a specialist supplier for the College and University market. A major portion of our company's business is to design, implement and service administrative and electronic control programs for College and University Food Service Departments.

The Vali-Dine Systems have become synonymous with meal card Food Service Control.

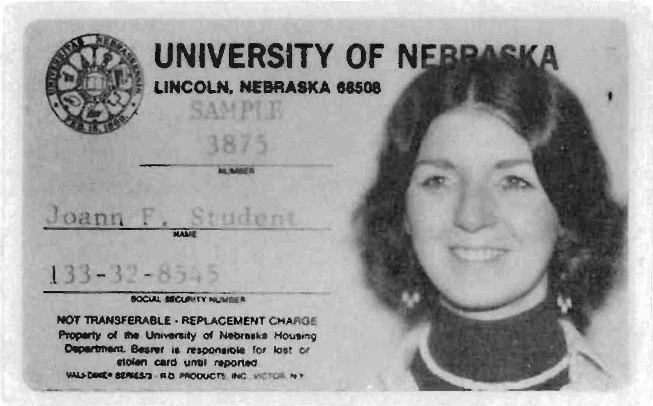
The following Vali-Dine presentation will explain how the System may serve your many Food Service Departmental needs. The implementation of a Vali-Dine program for contract Food Service control consists of the following:

The analysis of an account's needs and program requirements for the development of an integrated electronic system which will satisfy these needs

This analysis takes into account:

- The control problems which may exist with systems currently in use.
- Number of board plan options available or anticipated.
- Number of board plan or contract members.
- Number of dining halls and entrances.
- Statistical Data Collection and necessary statistical output required by Food Service Administration.
- Income allocation requirements of the department.

Vali-Dine Card:



UNIVERSITY OF NEBRASKA
LINCOLN, NEBRASKA 68508

SAMPLE
3875
NUMBER

Joann F. Student
NAME

133-32-8545
SOCIAL SECURITY NUMBER

NOT TRANSFERABLE · REPLACEMENT CHARGE
Property of the University of Nebraska Housing Department. Bearer is responsible for lost or stolen card until reported
VALI-DINE® SERIES/3 · R.D. PRODUCTS, INC. VICTOR, N.Y.

The continued growth of R. D. Products, Inc. and the rapid acceptance of our products and systems in the College and University Food Service market can be attributed to our responsiveness to changing needs, innovations in solving new problems and constant improvement in the products and services available to our customers.

Whether the College is managing its own food service operation or it is handled by an outside firm, there is a critical need for positive administrative control of the board plan participation. The Vali-Dine System offers you a sophisticated and professional means of controlling your meal card program.

In addition to the component description below, also included in the presentation are BASIC system hardware component speciifcation sheets for your interest.

SYSTEM COMPONENTS

The Vali-Dine System is a self contained, economical electronic board plan control system consisting of electronic hardware and photo meal cards. Students are issued portrait photo cards which are magnetically encoded with their individual account number.

CARD READER

When the line checker inserts the student's meal card into the "Card Reader" at the entrance to the cafeteria, the System reads the student's meal plan type and account status to determine if he is clear to eat, then informs the checker via indicator lights on the Card Reader.

The Card Reader responses will be one of the following:

- PASS
- MEAL EATEN
- MAX MEALS EATEN
- INVALID
- MESSAGE

ANY CARD MAY BE PRESENTED AT ANY READER, since all Card Readers are connected into the Central Processor {memory unit}. {See Sample Schematic}. As a general rule, a student will only be allowed to eat one meal during that specific meal period. If a second entrance is attempted anywhere on campus where there is a Card Reader, the response will be "meal eaten". On the other hand, a student may be allowed continuous entrance to the dining halls in a program where, for example, points are used. This is all a function of the system programming and can be accomplished with the Vali-Dine System.

CENTRAL PROCESSING UNIT

The Vali-Dine System {S/4} CPU is a 64K microprocessor based mini-computer which is capable of simultaneously handling virtually any board plan combination; as well as keeping a constant watch for lost and invalid cards. You can invalidate any meal card number at any time. In addition, the System CPU, High Speed Line Printer and CRT Interactive Terminal located in the main office enable you at the end of the day to obtain statistical data and participation counts in basically any configuration you may need. This data will generally include such factors as total number of meals served by dining hall, by board plan type, by meal period, guest counts, cash counts, etc. The Vali-Dine System CPU also is equipped with a Data Storage Terminal which allows you to obtain a cassette magnetic tape dump of the program contents in the event of a power outage or malfunction. The CPU contains all necessary program software required for total control of the Food Service board plan operation.

VARIABLE BOARD PLANS

Board plan feeding has become increasingly difficult to monitor since the advent of the variable type 'any 10 meals/week', 'any 15 meals/week', 'any 2 meals/day', etc., board plan programs currently gaining popularity on campus. In this type of board plan a student is allowed to eat 'X' number {any 10, any 2, etc.} of the total meals served weekly or daily. The Vali-Dine System remembers when a student has eaten his total allotted number of meals and it prevents additional participation after that number of meals has been reached.

In addition to its simplicity, economy and effectiveness, the Vali-Dine Card Readers {CR} are so compact they will easily fit on existing shelf space presently used by your checker.

The System has the capacity to handle up to 800 students per hour at each terminal unit and it can control any program with an unlimited number of students on board plan. The CR units and the memory unit {Central Processing Unit} are connected by simple dedicated data lines and involve a minimum installation cost.

The Vali-Dine System is economically, administratively and operationally justified simply because of its ability to "close the loopholes" in all other traditional meal control systems as well as providing a new dimension to the management of your department.

An individual with no photographic or past computer technical knowledge can be easily instructed to operate the entire System. The tamper-proof Vali-Dine photo card gives you a head and shoulder portrait of the individual, not the typical square "mug shot" that is found on all other photo identification cards. This large photo makes for easier recognition by the line checkers and in addition, is well accepted by the student body, not only as a meal card, but it also has the potential for expanded campus use as the needs may arise.

In effect, what has traditionally been known as the student I-D card is now taking on a more comprehensive meaning and that card is becoming a Data Input Device, not just an I-D card.

For years Food Service Departments have wanted and needed the control the Vali-Dine Systems offer -- now it is available on a cost effective basis and its use is growing rapidly in College and University Food Service Departments of all sizes across the nation.

The enclosed customer list will testify to the rapid acceptance of the Vali-Dine System on College and University Campuses.

To properly discuss our Vali-Dine System benefits as they specifically relate to your departmental needs, R. D. Products, Inc. has at your disposal, Regional Managers who will be pleased to meet with you and your associates on campus to review our Systems in more detail.

Regional Sales Offices:

Philadelphia, PA; Atlanta, GA; Columbus, OH; Kansas City, MO; Dallas, TX; Portland, OR

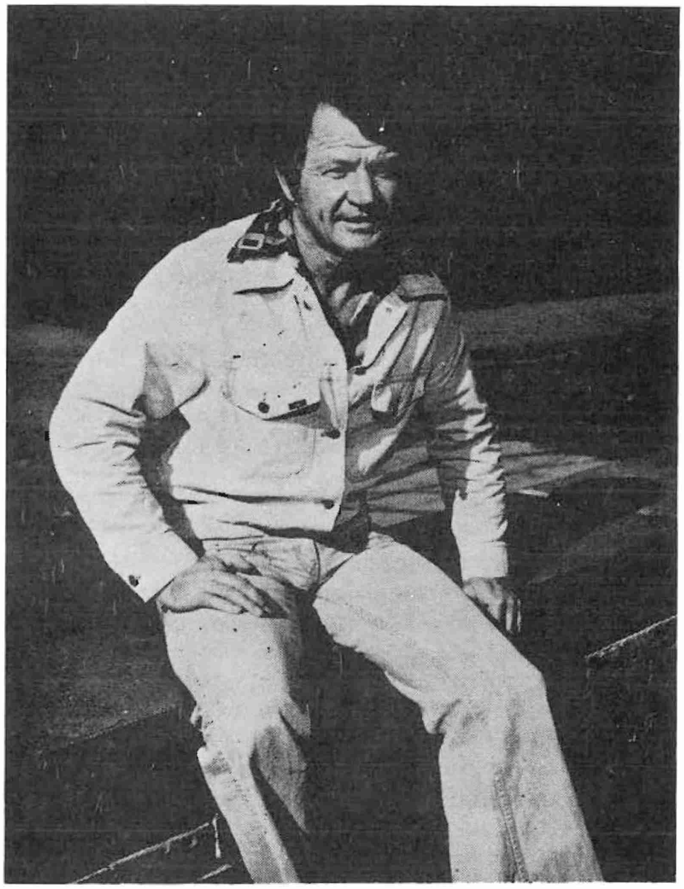
APPENDIX H

Technical Reference Articles on Vali-Dine

Computerized Control of A La Carte Dining

by Ross Cordell

How SUNY AT Oneonta, New York Evolved From The Traditional 21-Meal Plan To A La Carte With Complete Computerized Control



Ross Cordell
General Manager
Faculty Student Association
State University of New York
Oneonta, New York

Until the early 1970's, most colleges throughout the country had what is now called the "Traditional (21 meal) Board Plan" on their campuses. State University at Oneonta, New York was no exception.

In the early 1970's, students began to pressure for liberalization of the Traditional Board Plan, contending that they were paying for meals that were not being consumed. Attempts were made to explain to students the missed meal factor existing within the Traditional Board Plan to no avail, and in the early 1970's, college campuses across the country began to get away from the one board plan.

At Oneonta, we attempted to meet students' requests by first offering, in addition to the Traditional Meal Plan, a Fifteen Meal Plan and later a Fourteen Meal Plan. It became apparent in early 1973 that students in Oneonta wanted an even more liberalized selection of board plans than what was being offered.

A study was made of all types of board plans being offered around the country, ranging from a multi-choice system such as 19, 15, 14, 12, 10 then being used at the State University at Albany, New York, the Point Plan System then being used at the University of Wisconsin, to the A La Carte Coupon System then being used at Bowling Green University.

Under the Traditional Board Plan, students were admitted to the dining hall through the use of a meal card and number system. Once past the checker, students were provided food on an unlimited basis.

Under the Point System, students were issued books of points which they surrendered in various amounts depending on the meal such as one point for break-fast, two points for lunch and three points for dinner. Again once surrendering points and entering the feeding area, students were permitted unlimited food. However, under both systems some campuses placed restrictions on certain entree items.

The A La Carte Coupon System at use at Bowling Green University, functioned in a similar manner to a commercial cafeteria with the exception that the student surrendered coupons for payment of items purchased rather than cash. All items on the line were priced on a point basis (one point equal to five cents).

Of all the plans studied, the multi-choice board plan offered the least amount of flexibility and inherent within the plan was the major problem of waste and pilferage. The Point Plan System gave students considerably more flexibility than under the multi-choice plan since points were given a cash value and could be used in snackbars. However, under this plan remains the problem of waste and pilferage.

After all plans were studied and considered, the A La Carte Coupon Plan was selected at Oneonta, because the plan provided:

1. Wider choice of menu items — Under the A La Carte System, we are able to offer an almost unlimited selection of menu items because the student pays for each item on an A La Carte basis. For instance, we can offer steak each day and such items as lobster tails, chicken cardon bleu and prime rib. The Plan provides complete freedom in the offering of dessert and salad selections.

2. Minimized waste — We have found that since changing to the A La Carte System, there is little or no waste by the students in that the students only select those items which will be consumed. They are not inclined to sample as under the Traditional Board Plan.

3. Flexibility and diet, hours of service and eating locations — We have found that with the use of the A La Carte System, we can satisfy almost every diet because of the wide variety of menu items offered under the plan. The choice of students' diet need only be limited by price. Therefore, if a student wishes to eat steak every day, he or she may do so. Students may use the A La Carte Plan in all dining halls and all snack-bars and therefore at Oneonta students may eat on the board plan from 7:00 a.m. until 1:00 a.m. the following day.

4. Board rates — With the increasing cost of a college education, more and more pressure is being applied by parents and students to hold down board rates. We have found with the use of the A La Carte Plan and its elimination of waste, we have been able to maintain a relatively low board rate at Oneonta. A minimum board plan is set for all students and we have found that the light eaters (and their numbers are considerable) have been able to eat quite comfortably on the minimum amount. The plan therefore minimizes subsidization of one student by another. If a student chooses to eat a large amount of food, that student and only that student pays for it. Additional units in lots of $5.00 may be purchased over and above the minimum board plan.

A La Carte Feeding and Its Manual Control

When the A La Carte System was first introduced to Oneonta, food was distributed through the use of a coupon system. Students were issued books of coupons in denominations of 5 to $1.00. Menu items were priced in points — one point being equal to five cents. Students would enter the cafeteria, select the items they wish to eat and pay the cashier at the end of the line with the use of their coupons. The system worked fairly well, however, we found counting procedures very cumbersome. It was necessary to remove the coupons from the book by the cashier, seperate them at the end of the day and count them through the use of a ticket counter. We later corrected the counting problem by weighing the tickets rather than counting with the use of a gram scale. Students were forever losing their books and there was a considerable amount of theft. There was little or no chance of controlling the use of the coupons; therefore, if a student lost his or her book through displacement or theft, it was a considerable financial loss because it could not be replaced. To handle the coupon system entailed a considerable amount of additional labor in the area of accounting. Books were expensive since card-stock paper was used in printing coupons; even so, we found that they readily became shop-worn.

Automation of A La Carte Dining Via the Vali-Dine System

In the fall of 1975, we contacted R.D. Products Inc. presenting them with all of the problems we were having with the coupon system at Oneonta and asked them to make a study of the problems and present a proposal with the use of the Vali-Dine card.

R.D. presented their proposal of an automated system of control and the system was purchased in the Spring of 1976 for implementation in the Fall of 1976.

We experienced a great deal of benefit by the automation of our A La Carte System. One of the greatest areas of benefit is related to the financial impact of our dining services. To begin with, a prepaid board plan operation still allowed us the benefit of prepayment while at the same time maintained the concept of allowing students to participate in meals on a regular board plan basis. This cash flow benefit obviously allowed the University to work with meal plan funds to cover its general operating expenses, regarding labor, food costs and overhead. In addition, there are a great many budgetary benefits associated with the standard prepayment.

The automation of our A La Carte Dining System allowed for a higher degree of accurate data collection which in turn had an impact on our pricing structure which can now be more accurately addressed. The Vali-Dine System allowed us to determine an equitable pricing structure for our board plans based on the statistical data obtained from the system. This data also assisted us with our inventory control in the sense that we were able to determine the number of points or dollars left in every student's account and our board plan enrollment in general towards the end of a semester.

This allowed us to anticipate whether or not we should offer low or high priced items on our menu, to either use up excess points or to allow students to conserve points while still maintaining a proper dietary mix; as well as determine whether or not prepackaged foods will be purchased in greater quantity so the students will be able to use up their points before semester's end. One of the greatest benefits of the Vali-Dine System allowed our department to save on a least $30,000.00 a year in personnel expenditures. Most of these savings accrued from the elimination of checkers which were manditory to control the A La Carte System manually, but were no longer necessary with the Vali-Dine System.

General Description of the System

The Central Processing Unit (CPU) maintains the student data base. It contains each student's account number and their point balance. Here at Oneonta, the system is programmed to allow for a penny a point. Whereas each point in a student's program has the equivalent of a penny value. It is important to note that when we initially installed the system, we defined a point as having a nickel value. After the first year of operation we found it to be much more logical and valuable from our benefit at the student's benefit to work with a penny a point, therefore eliminating the mental conversion a student would have to go through to determine how many points were being used for each meal or remaining in his or her account. A penny a point system also allowed us a higher degree of accuracy in our pricing structure, whereby all of our items would not have to be rounded off to the closest nickel. The data that we received out of the CPU was presented via hard copy printout in recap form. A recap as we defined it was merely a printout of the accumulation of all our daily participation, at each location by individual point plan program. It allowed us to determine for income allocation purposes how many points were being used by each individual dining location during each meal period. These recaps also allowed us to determine on a daily basis the point usage as well as the number of cash customers that were served at each location.

Other useful information the system allows us to obtain is the number of valid accounts in the system at any given time, the number of points either totally or individually that the students have to spend, how many invalid accounts that are in the system and also the number of students that have purchased additional points over and above their initial purchase of the minimum point plan structure.

In addition to the Central Processing Unit and the hard copy printout, an intregal part of the system is the Data Storage Terminal which allows office personnel to obtain on tape or to record on tape, the current program contained in the CPU at any given time. This system capability provided us with an important backup system should we ever have had a malfunction with the Central Processor. It allows us to completely update our data base at any given time.

Vali-Dine System
is Speedy and Accurate.

In the event of power failure or power fluctuation, the battery pack will maintain memory in the CPU for up to twenty hours. With the resumption of the electrical service, the battery pack will be automatically recharged to an estimated life (maximum efficiency) for three years.

The Card Reader Terminals which are located at each checker location, also have data cassette tapes so that when the system is working on off-line basis all transactions can be recorded on tape for later updating in the CPU to maintain the credibility of the data base. It is important to note that with our system we were easily able to replace our cash registers which were up to this point, used only for cash patrons. By the addition of the cash drawer connected to the Logging Card Reader or LCR's as they are known, allowed us to collect cash for casual meals at the same time recording the cash totals in the Central Processor as well as maintain control of all point plan student participation.

Using Vali-Dine At The Snack Bar.

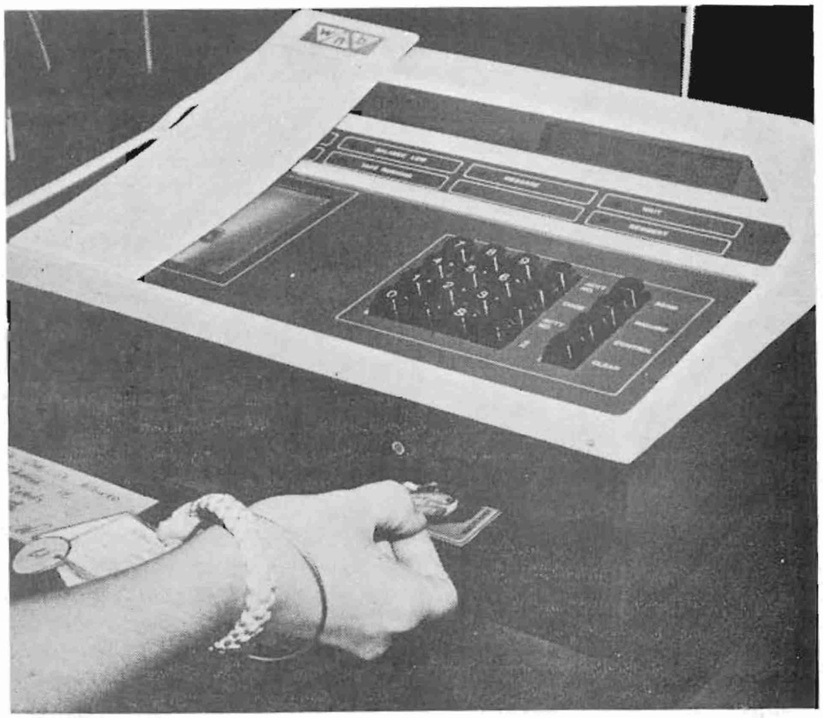


Photo I.D. Card Being Used.

Operationally, as the student approaches the checker, the checker simply keys in the total amount of food being purchased, reads the meal card in the Card Reader and the transaction is automatically deducted from the student's point balance maintained in the CPU. The transaction total as well as the remaining point balance is displayed on both the front and rear of the Card Reader for both the student and checker to equally observe. Should the student not possess sufficient funds to cover the transaction, the transaction will not be completed. Should a lost or invalid card be presented to the checker, the system alerts the checker accordingly. . . as it would do in any Vali-Dine System. A lost or stolen card or a card in possession of a student who dropped off the board plan is no longer usable in the system.

This subtle competitive aspect of our operation allows for and demands creativity and managerial expertise in our dining hall managers. We have found that it has assisted in instilling a merchandising approach to food service rather than a negative approach whereby we previously were working with the missed meal factor. With the A La Carte System the more points the students use the more profitable the dining services department can become.

Because of the fact that the student has the option to purchase or not to purchase from a variety of entrees, there exists the opportunity for the director to experiment with "exotic foods" which can be sold optionally and not forced on the students.

The Vali-Dine System because of its flexibility and comprehensiveness, allows us to easily control in a simple and effective way our A La Carte System which allows us to present many benefits to the student body. Without the benefit of an automatic electronic control system, much of the advantages we offer the students would not be possible on a manual control basis.

Regarding **student benefits,** there are many which have accrued to the students since the installation of the automated meal card system.

To begin with, the student need only carry a card, not cash or coupon books. Obviously for simplicity this is much easier than a two card system or a coupon book system which may not only be cumbersome, but is easier stolen or lost.

With the Vali-Dine System, the students can not lose their purchasing power since the point balance is maintained electronically in the central processing unit. Should a student lose his original card, a second or third card is issued using the same account number. Everytime a duplicate card is issued the system is programed to accept only that card issued. If circumstances warrant, a student's remaining point balance can be transfered to a new account number and a new card issued. The old account number is invalidated, therefore, making it unusable by anybody else.

In this sense, the Vali-Dine System has allowed us to issue what are in effect, credit cards used in reverse whereby the students are working from a diminishing balance. In the event no points are left in the student's account they have the option of either paying cash or purchasing additional points. The Vali-Dine System has also eliminated the possibility of theft of coupon books we used previously. A reported lost or stolen card is not transferrable nor valid in the Vali-Dine System.

The card itself carrys with it a large high quality color portrait of the student which serves as a positive ID for not only the dining service checkers, but also for use in the Rathskellar and other establishments which serve alcoholic beverages. This is possible since our department controls the student birthdate information which is contained on the card.

Employee Benefits

There are many advantages of the system as seen through the eyes of the employees. For instance, the student can now monitor the cashiers. Whereas before, the student/checker confrontation existed as to the number of coupons which may have been torn out of the book, etc. With the Vali-Dine System both the checker and the student are fully aware at the time of purchase how many points have been used at a given transaction and the remaining balance left in the student's account.

It is exceptionally important to us in New York State because the state law requires that we, the vendor, must control the use of the point plan. However, with the present system, the student now monitors the use of this system.

One of the motivating factors for us to automate the A La Carte Dining System is that the New York State tax law prohibited transferability of points from one student to another. This was difficult to control, but with the Vali-Dine System, this transferability is not possible, therefore taking the burden off our department to insure non-transferability and tax liability.

Another long range benefit of the system which is to be employed yet at Oneonta, is the fact that the Vali-Dine card has the capacity to be used as the general student ID card. In discussions with R.D. Products, the supplier of the Vali-Dine System, it appears should we desire, the meal card can be embossed, imprinted with OCR labels, bar code labels or any other means of data collection to be used in various types of terminals across campus.

Flexibility of Menu Operation

With proper and accurate income allocation figures now available with the Computerized A La Carte System, each dining hall is viewed as its own profit center. Subsequently, there exists a positive incentive for each individual dining hall manager to become more creative and market his services to the students. With our current system, should one dining hall manager market his product well and serve the type of food that is popular to the students, he invariably will attract a greater percentage of the student body to use their points in his dining hall. Should he continue to serve unpopular entrees, they obviously will not be purchased and therefore would be reflected in his participation figures.

Currently, the meal card is used only by the dining services area. However, the capacity to be used as an all campus card is obviously available and has many areas of efficiency connected with it.

One aspect of the system which is currently in our program is a general purpose paging signal which allows us to activate a message indicator on any account at any given time. Should a message indicator be activated in a student's account a message light will illuminate upon insertion of his card in the system anywhere on campus so he can be informed by the checker to contact the office because someone is trying to get in touch with him for one reason or another.

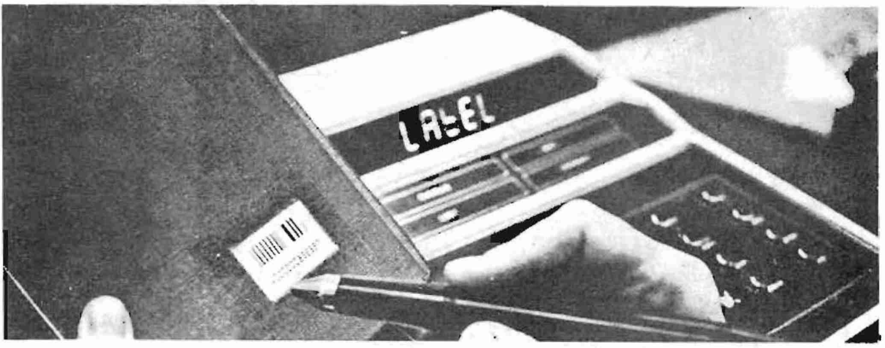
It is our understanding that the Vali-Dine System has the capacity to be expanded to other areas of use on campus, such as check cashing verification, library book charge out eligibility, student activities fee payment, etc.

In addition, an important point to remember is that although we at SUNY Oneonta offer an A La Carte Plan to our student body for dining services, the Vali-Dine System can be used very effectively in other types of plans, such as the traditional board plans currently found on most campuses across the nation.

The concept of control in all Vali-Dine Systems is basically the same. It allows you to offer dining privileges only to those students who are entitled and in no greater frequency than you statistically expect them to participate. Regardless of the type of Vali-Dine System used, regardless of the types of board plans offered, regardless of the number of dining halls that you have available for participation, the Vali-Dine System offers a great many of the above advantages concerning student and administrative control. The approach we have taken to our University Food Service has offered our students a great deal of flexibility and advantages.

The Vali-Dine System is simply an administrative tool which allows us to offer these advantages, while at the same time control the administrative burden normally associated with a manual meal card system.

A DISK PACK is being placed into the disk drive by Gordon Rawlins, chairman of Library Systems Development at the University. Part of a computer system in use at Pattee Library, the disk contains information for access by computer terminals at various locations in the library.



A LIGHT WAND on the circulation control terminal reads the bar code on a book as part of the automated procedure for charging a book out of the University's Pattee Library.

Computer Checkout: Groceries, Stores, and Now Library Books

By ANNE KELLER
Times Staff Writer

The time-saving aspects of computer technology have filtered down to the daily lives of most people Grocery and department store check-out times have been shortened by the use of computer systems. Banks run credit checks in a matter of seconds with the use of computers.

These time-saving techniques are about to be applied to the borrowing of books at Pattee Library on the University campus. On Monday a circulation control system will be instituted at Pattee and charging out a book will take a matter of mere seconds.

Each book will have a designated bar code, similar to those used on grocery items in the supermarket. Every borrower will have a registration card. The circulation control terminal (CCT) will read these, process the transaction and generate a date-due slip similar to a cash register receipt with the identification of the item, name of the borrower and date due on it. This slip will be paper-clipped inside the back of the book and the transaction completed.

The borrower hasn't even had to write his or her name and the process will take only about six seconds, estimates Gordon Rawlins, director of library computer services.

A small tape recorder is incorporated in the CCT to record all transactions. In the event the computer is unable to process the transaction immediately, it can pick it up from the tape at a later time.

Approximately 60 percent of the circulating materials have the bar codes already, according to Murray Martin, associate dean of University libraries, and about 3,000 registration cards have been issued.

If a book without a bar code is brought to the desk to be borrowed, the bar code will be put on immediately. If a borrower doesn't have a registration card, he will be issued one. Consequently, there may be some delays when the system is first implemented, Mr. Martin cautions, but he doesn't feel the delays will take any more time than the manual borrowing process took.

Registration cards are being issued at the main circulation desk in Pattee on weekdays from 8 a.m. to noon and 1 to 5 p.m. and on Saturdays from 1 to 5 p.m. Indentification bearing an address and signature, such as a student or faculty ID or driver's license, is required.

Another type of terminal will also be used at the main circulation desk. Nicknamed the CRT (for cathode ray tube), it will be used to search the status of a book which a borrower is unable to find in the stacks. With the punch of several buttons, a library staff member will be able to tell if that particular book has been charged out and, if so, when it's due; whether it is lost, or whether it is being held for someone who had previously requested it. In other words, it will perform a thorough records search in a matter of a very short time without the staff member ever leaving the desk.

The system has security measures incorporated into it to protect the privacy of the borrower and to prevent use of invalid registration cards, according to library officials. Access to the records is limited to authorized staff personnel.

Length of borrowing time has been standardized under the new system—all books will be charged out for four weeks, whether the borrower is a student, faculty member or "other." One renewal will be permitted, but at the end of that time, all materials must be returned to the library. Materials which do not normally circulate will be circulated, if at all, under a "special permission" status for a shorter period of time.

Standard fees will be charged for overdue books to recover the costs of sending recall notices. If there are persistent violations, borrowing privileges will be suspended until the borrower returns the material or re-charges it and pays the fine due

These measures are designed to provide a more effective way of ensuring better and more equitable access to library materials than was avilable under the manual system, according to library officials.

The computerized circulation system is just one part of a total system being implemented in the University libraries. Begun in 1974 with the installation of a computer in Pattee, the system includes having all bibliographic records stored in the computer. Automating circulation was moved ahead in the time schedule, according to library officials, because of increased use of library materials, which was causing the manual system to break down.

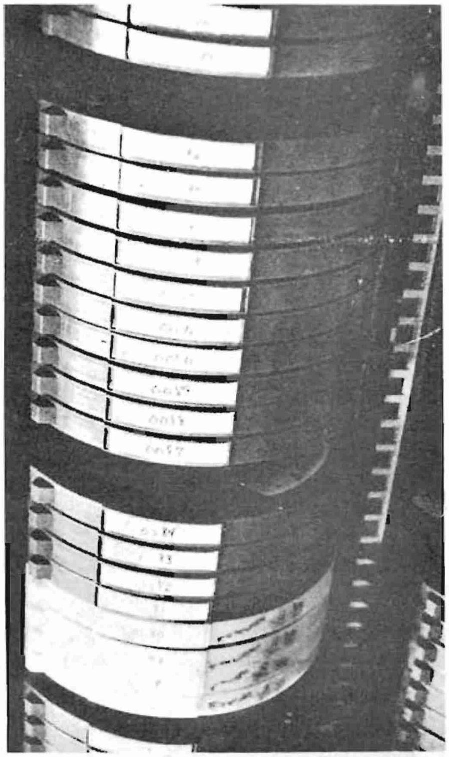
In addition to storing and analysing records, the computer will generate fine notices and personal reserve notices, similar to the sealed W-2 forms the federal government mails to employers. A "personal reserve" is a method whereby a patron becomes next in line to borrow a book when he finds the book already has been charged out.

The time and manpower saved in these procedures will be significant, according to library officials. However, increased use and a faster return time will probably result in increased stack activity, according to Charles Ness, assistant dean of University libraries. Any decreases in staff will come through normal attrition, he adds.

With automation beginning at Pattee, Mr. Martin says it is hoped to have the five branch libraries on campus incorporated into the system by the end of this academic year.

Because there was nothing available in the industry with the library's requirements, according to Mr Rawlins, he and Eric Ferrin, a colleague in Library Systems Development, designed their own terminal in cooperation with R D Products Inc. of Victor, N.Y.

It's a cost effective system, according to Mr. Rawlins, who says, "Hopefully other libraries will benefit from Pattee's front work. We were looking for improved performance within certain cost constraints." The CCT is designed, he adds, so that libraries much smaller than Pattee will also be able to use it—libraries as small as Schlow Library in State College, for instance. The terminals will be rented from R D Products, which will be in charge of maintenanee.



MAGNETIC TAPES contain library information in sequential order and are part of the security backup system. Not part of the circulation control system, these tapes are an additional record of library information.

CENTRE DAILY TIMES

SECOND SECTION Friday, Jan. 19, 1979 PAGE 15

TERMINALS ARE USED to feed information into the computer system about each book after it has been given a bar code to ensure proper inventory control.

A REGISTRATION CARD belonging to a borrower is read by the circulation control terminal. After the bar code on the book and the registration card are read, the transaction is processed by the terminal and a date-due slip generated. The complete charge-out process takes only seconds with the new computerized system.

APPENDIX I

Rusco Specifications

RES | RUSCO ELECTRONIC SYSTEMS
A DIVISION OF ATO

1840 VICTORY BLVD. • P.O. BOX 5005
GLENDALE, CALIFORNIA 91201
TELEX 696318 • (213) 240-2540

PRODUCT DESCRIPTION

MAC550 MICRO AUXILIARY CONTROLLER

The MAC550 Micro Auxiliary Controller is a highly sophisticated Data Processing System designed to enhance the operating, control and reporting features of the RES Series 500 Product Line. The RES Micro Auxiliary Controller is modular in design and expandable to accommodate a wide variety of optional capabilities. The basic hardware consists of a state-of-the-art processor and disk controller, one or more disk drives, CRT terminals and printers. The MAC550 interfaces directly with a MAC530 or MAC540 Micro Access Controller.

Basic features include English text display and printout of the MAC530/540 system activities and generation of reports. Operator guidance and prompting are provided on the CRT screen.

PRIMARY FILES

The files and records of the MAC550 are maintained and updated by transaction data from the MAC530/540 and by operator input.

The Personnel File is made up of data specific to each individual in the system. It contains, as a minimum, the following data.

- ID Number
- Name
- IN/OUT Status
- Last Reader Used
- Time Last Reader Used
- Date Last Reader Used
- Status

Several additional fields are available for storing other information such as Social Security Number, employee number, telephone number, start and stop times, department number, pay grade, etc. Such data as time, date and last reader used is sensed and automatically updated by the MAC550 based upon transactions received from the host controller.

The Reader/CCM File is a list of reader and CCM (Contact Condition Monitor) locations. Each reader/CCM in the system is described in English text, as to its status and location.

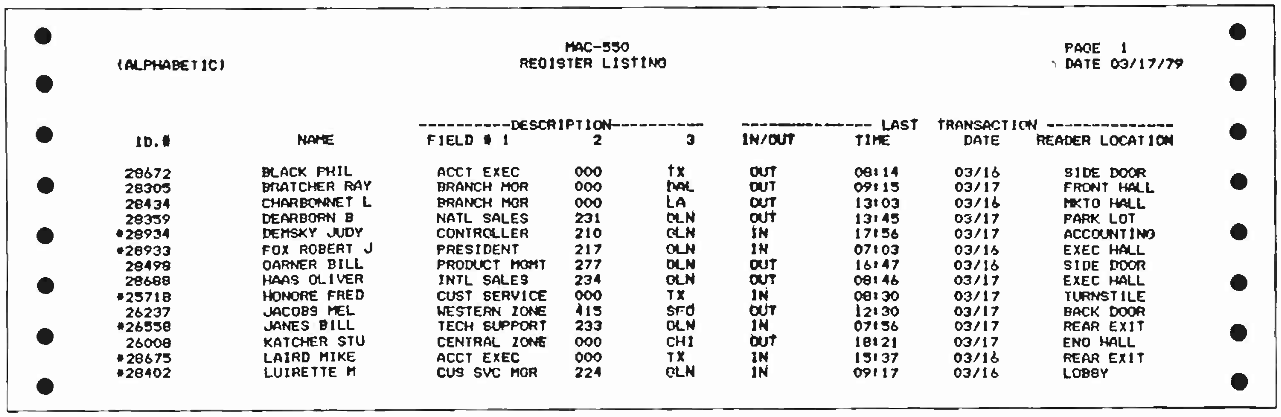
The Alarm Definition File provides for an English text definition of each alarm message received from the MAC530/540. The user can determine which of the alarm points are to be displayed in real time on the CRT and to be acknowledged. All alarms are logged in the transaction and alarm history file and identified as alarms.

Transaction/Alarm File. – A file of the most recent transactions is maintained. The size of this file will vary as a function of the number of readers (and CCM's), the number of active ID's and the overall transaction activity.

Alarm History File. – An alarm history file is maintained from which alarm history reports can be displayed and printed.

DISPLAY FORMAT

A typical format for data displayed is as follows:



```
                                    MAC-550                                          PAOE  1
(ALPHABETIC)                    REOISTER LISTINO                                   DATE 03/17/79

                                ----------DESCRIPTION----------   --------------- LAST  TRANSACTION --------------
   ID.#          NAME           FIELD # 1          2         3    IN/OUT      TIME        DATE    READER LOCATION

   28672      BLACK PHIL         ACCT EXEC        000       TX     OUT       08:14       03/16     SIDE DOOR
   28305      BRATCHER RAY       BRANCH MOR       000       DAL    OUT       09:15       03/17     FRONT HALL
   28434      CHARBONNET L       BRANCH MOR       000       LA     OUT       13:03       03/16     MKTO HALL
   28359      DEARBORN B         NATL SALES       231       OLN    OUT       13:45       03/17     PARK LOT
  *28934      DEMSKY JUDY        CONTROLLER       210       OLN    IN        17:56       03/17     ACCOUNTINO
  *28933      FOX ROBERT J       PRESIDENT        217       OLN    IN        07:03       03/16     EXEC HALL
   28498      OARNER BILL        PRODUCT MOMT     277       OLN    OUT       16:47       03/16     SIDE DOOR
   28688      HAAS OLIVER        INTL SALES       234       OLN    OUT       08:46       03/17     EXEC HALL
  *25718      HONORE FRED        CUST SERVICE     000       TX     IN        08:30       03/17     TURNSTILE
   26237      JACOBS MEL         WESTERN ZONE     415       SFO    OUT       12:30       03/17     BACK DOOR
  *26558      JANES BILL         TECH SUPPORT     233       OLN    IN        07:56       03/17     REAR EXIT
   26008      KATCHER STU        CENTRAL ZONE     000       CHI    OUT       18:21       03/17     ENO HALL
  *28675      LAIRD MIKE         ACCT EXEC        000       TX     IN        15:37       03/16     REAR EXIT
  *28402      LUIRETTE M         CUS SVC MOR      224       OLN    IN        09:17       03/16     LOBBY
```

STANDARD FEATURES

English Text Transaction Logging. – The numeric characters generated by the MAC530/540 are converted, by the MAC550, into English text output at the time of occurrence.

Authorized System Control Authority. – Multiple levels of operator access are an integral feature of the MAC550 System. *Master level control authority* is required for access to restricted files or for program revision.

Display/Printout All Personnel. – All personnel in the system may be displayed in alphabetical or numerical order. The displayed/printed data may contain various items such as: ID number, name, last reader used, time and date of use, department, cost center, telephone extension, and/or other user defined data.

Alarm Alert and Acknowledge. – Whenever an alarm occurs, the operator is immediately alerted by an audio and/or flashing alarm indication on the CRT. The alarm persists until an acknowledgement has been performed.

Track by ID or Reader – The System will track, display, and/or print in English text all activity for any ID or Reader, including name, number, reader locations, date and alarm definition.

AVAILABLE OPTIONS

Time and Attendance Program. – This program monitors and controls the collection, subsequent processing and formatting of Time and Attendance data. This information may be used as input for payroll preparation. Special provision is made for supervisory inputs concerning excused time, etc.

Following are examples of reports that may be generated by the operator:

- Hours worked by employee for the day or shift and cumulative time for the day, shift or pay period.
- Employees that did not clock in during the day or shift.
- Exceptions (i.e. individual clocked in but not out, out but not in, etc.)
- Adjustments to employees' records for the pay period.
- Over/under exception report of individuals who worked more or fewer hours than required for pay period.
- Monthly summary report.
- All individuals in facility.
- All individuals who have not reported to work for the day or shift.
- All individuals who have been in but are currently out of facility.
- Pay period summary for any designated employee.

Flex-R-Time Option.-- This option provides the capability for an individual to query the system and to display pertinent Time and Attendance/ID related information such as:

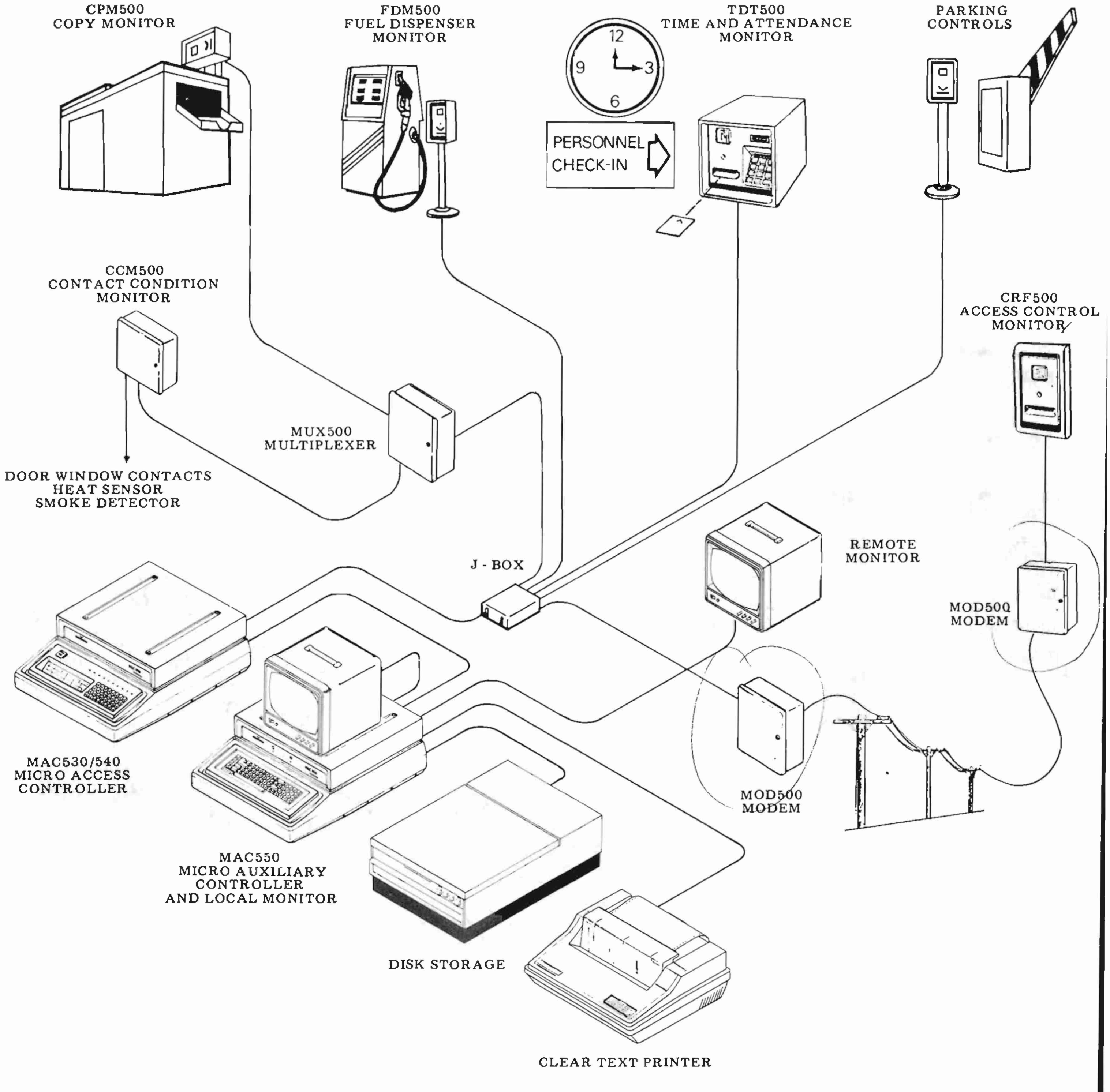
- Total hours and minutes worked today (for this shift).
- Total hours and minutes worked during pay period.
- Number of hours and minutes still to be worked today (or shift).
- Number of hours and minutes still to be worked this pay period.
- Total number of hours and minutes of overtime worked today (for this shift).
- Total number of hours and minutes of overtime worked during this pay period.

Copier Usage Reporting. -- This program will collect, summarize, and display/printout various copier usage reports such as: daily, weekly and monthly reports on copier usage by individual, department or cost center, including such pertinent data as job number, client number, etc.

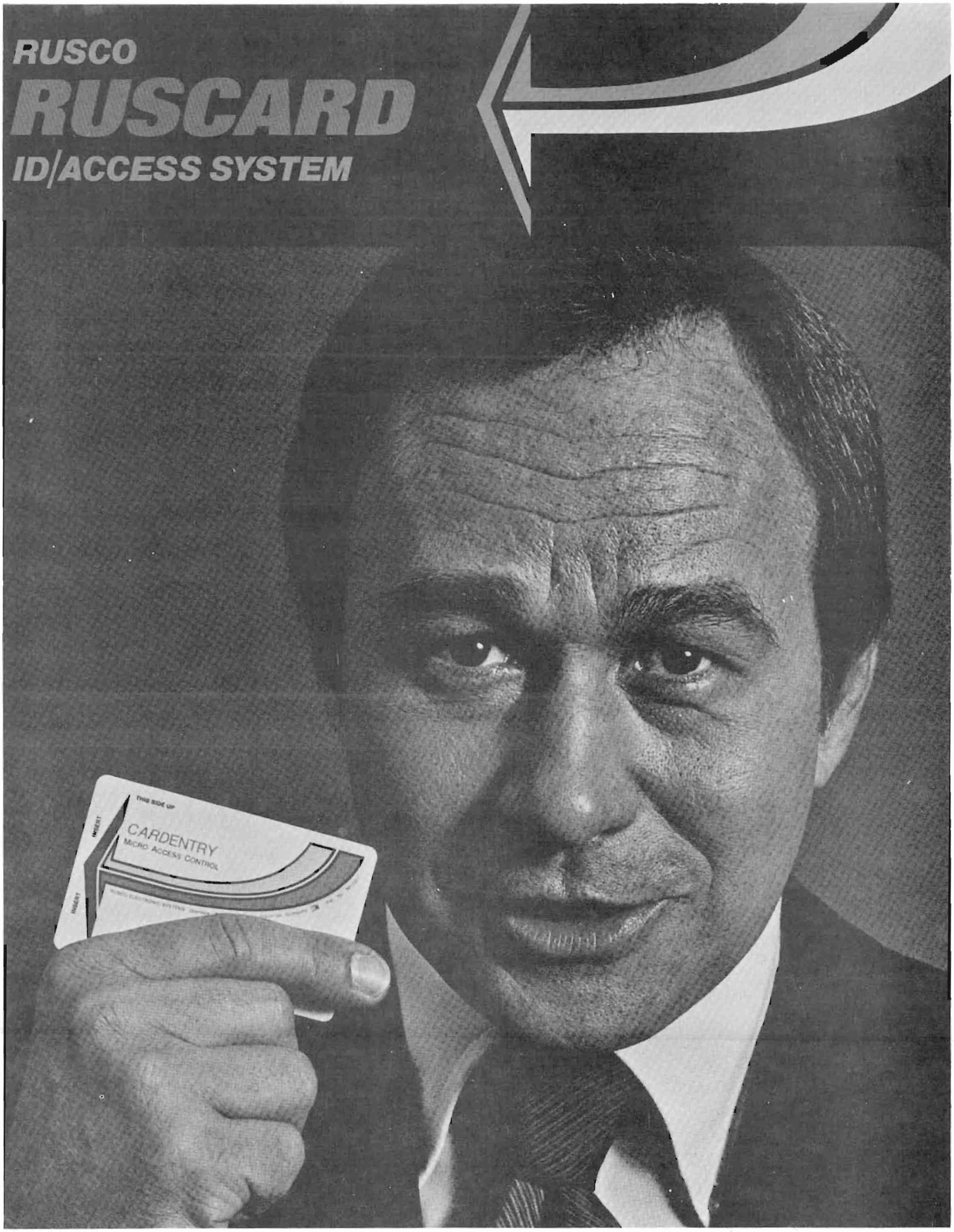
Fuel Usage Reporting. – This option allows the collection of data from fuel dispenser monitors and provides reports on consumption by vehicle, individual, department (or cost center), dispenser and fuel type. Mileage calculation can be generated based on odometer readings input at the time of fuel dispensing.

Doctors Registry Reporting.-- This software package has been tailored to the unique requirements of a busy hospital environment. It provides current data concerning the presence or absence of doctors in the hospital complex, their location and the time/date of departure or arrival. Other relevant information such as telephone number, specialty, messages for individual doctors (i.e., "call your office"), can be displayed at one or more locations in the hospital complex.

TYPICAL IDENTIFICATION AND REPORTING NETWORK



Page 4



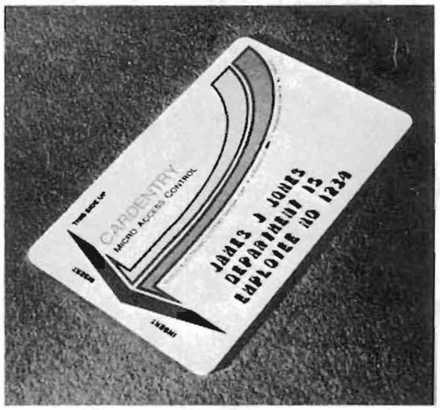
RUSCO

RUSCARD

ID/ACCESS SYSTEM

The "key" to better access control and monitoring systems

For over a decade, Rusco has been a major force in the development and perfection of card access control systems. Much of this leadership can be attributed to the unique advantages of the Ruscard,® Rusco's versatile, credit card-sized ID/Access Card. There are many types of ID cards, and many types of access cards, but only the Ruscard® has all these capabilities:



Embossing and Tipping

Unlike many access cards, the Ruscard may be embossed with up to three lines (x 25 characters) of fixed or variable information. The embossed information may then be used with any standard credit card imprinter to create machine-readable vouchers or other documents.

The raised characters may be "tipped" in a variety of colors to enhance appearance and readability.

Electronic ID

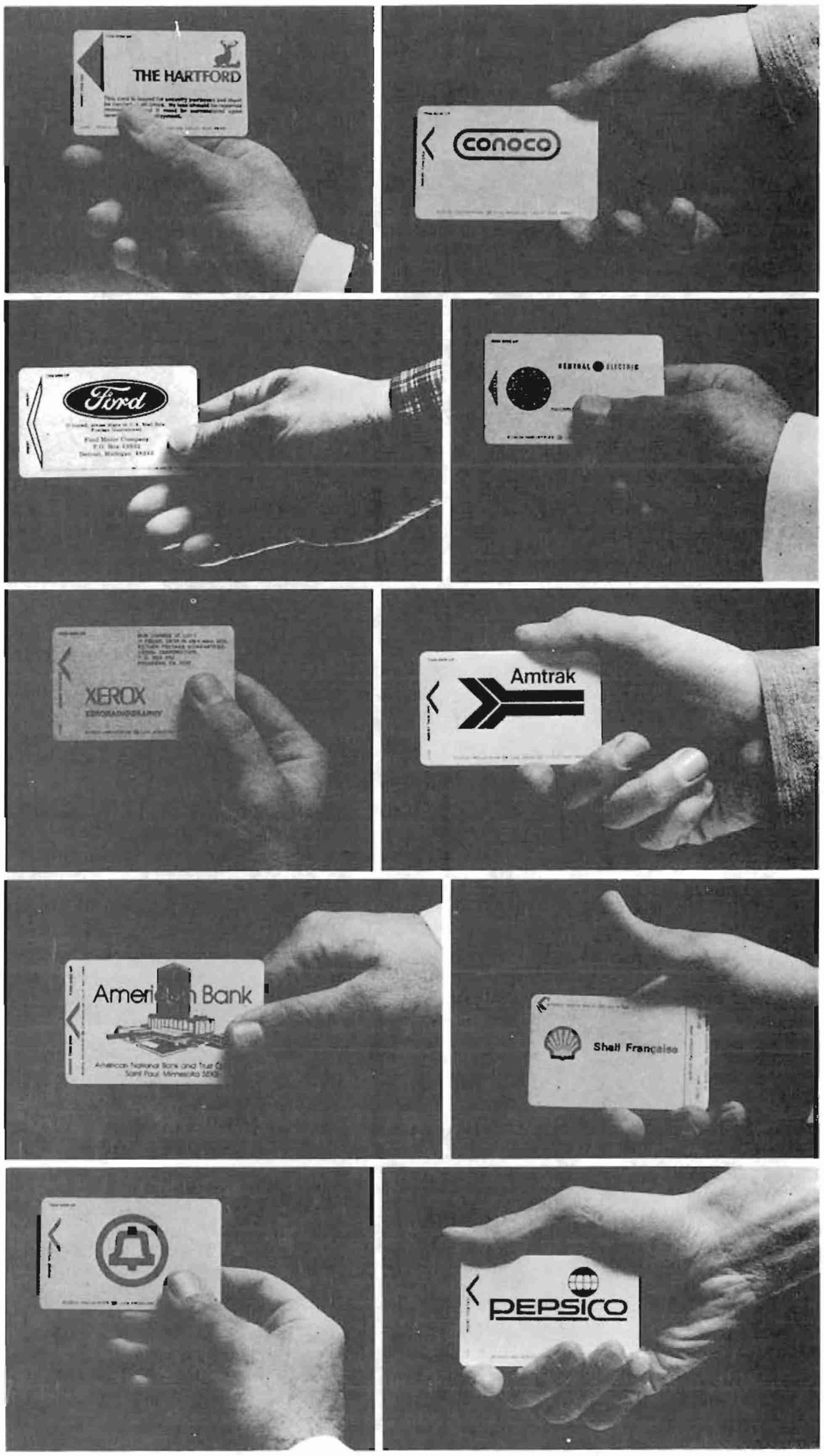
The Ruscard's scrambled, invisibly encoded "bits," when decoded by a mating Rusco CARDENTRY™ reader, form unique digital identifiers for both the individual card *and* the particular CARDENTRY installation it belongs to. Both these identification codes are available for examination by the system to determine access authorization status.

Unlike conventional "mag stripe" cards, the Ruscard's code-bearing core is buried inside the card, where it is both invisible and protected from scratches and abrasion. The sensing method used to read the card code is completely static (i.e., the Ruscard is stationary, and need not be dragged across a read head), eliminating an additional element of unreliability.

Photo ID

The Ruscard is completely compatible with most available Photo ID systems. Cards may be supplied with either a flap or a pouch on the reverse side. The identifying photo and any other desired information is sealed to the rear of the card, forming a durable, virtually tamper-proof ID/Access badge.

Ruscards may be slotted to accept straps and clips for attaching the badge to clothing.



Corporate/ Institutional ID

Custom-printed Ruscards with your organization's logo or design form an impressive, morale-boosting form of identification that your members or employees will be proud to carry and show. They can also serve to immediately identify an individual as belonging to your organization, even from a distance.

Custom Ruscards are available with full-color printing on one or both sides, using your own design or one developed by Rusco's art department. Standard Ruscards may be ordered either blank or with the CARDENTRY design.

SECURITY AND CONFIDENTIALITY

The only place Ruscards are manufactured and encoded is in Rusco's own plant, which has received bank security approval for credit card manufacture. Ruscard encoders are not available anywhere else. Ruscards are manufactured by a unique, patented process, and encoded to your specifications. A single master list of ID numbers is shipped with your cards; the only backup copy of this list remains in our vault.

How secure is the Ruscard?

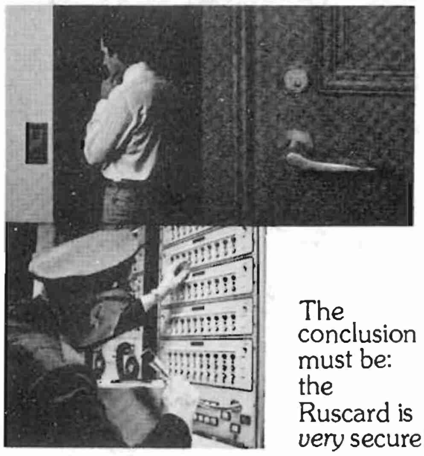
A mathematical investigation was undertaken to determine the probability of deciphering the code on a given Ruscard. In order not to reveal any important details of the encoding scheme, only the results are presented here.

Since the code bits on the Ruscard are scrambled differently for each CARDENTRY installation, and there are many unused "decoy" bits interspersed with the actual data, the first task in decoding the card is to pick the correct bits *and arrange them in the correct order.* The odds of successfully guessing the correct arrangement are less than one chance in

1.5×10^{39}, which when written out is 1,500,000,000,000,000, 000,000,000,000,000,000, 000,000

Furthermore, once the code *sequence* is known, there are roughly 25 million different combinations of system and card codes possible.

What these numbers mean is that, even if a determined individual could "read" the bits on a Ruscard (which requires special equipment), he would still face truly astronomical odds in attempting to interpret the information.



The conclusion must be: the Ruscard is *very* secure!

CARDENTRY Equipment and the Ruscard

All Rusco CARDENTRY access control devices utilize the same basic Ruscard. However, due to differences in encoding format and hardware capability, cards used with one series of equipment are generally not compatible with CARDENTRY readers of a different series (unless first re-encoded by Rusco).

Regardless of which CARDENTRY system they are used with, all Ruscards have identical "mechanical" properties (i.e., embossing capability, photo ID pouch, etc.)

Rusco's CARDENTRY line covers the entire spectrum of card access control equipment, from inexpensive "off-line" readers to the highly sophisticated, programmable System 500, which utilizes distributed microprocessor architecture to provide the industry's most complete and flexible access control and monitoring capabilities.

CARDENTRY equipment can be used to operate door locks, elevator controls, data terminals, fuel pumps, office copiers, and Park-O-Matic® vehicle control gates. In addition, it can provide activity logging on paper or magnetic media, and interfaces with auxiliary alarm systems, fire & smoke detectors, and virtually any other device for which a change of state can signal an alarm condition.

For more information on the Ruscard or CARDENTRY access control systems, contact your local Rusco sales office or the address given below.

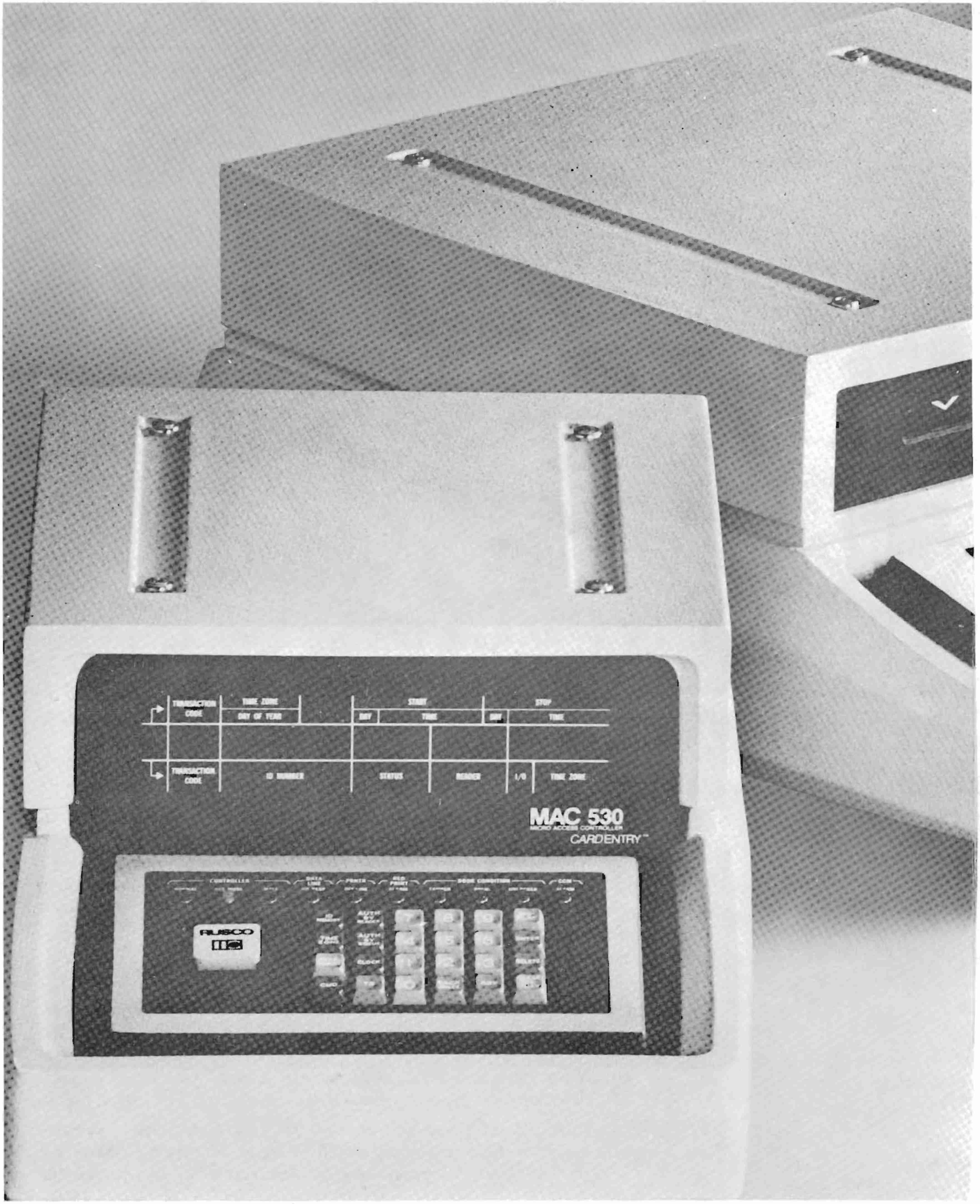
RUSCO
ELECTRONIC SYSTEMS
A division of **ATO**
P.O. Box 5005, 1840 Victory Blvd.
Glendale, CA 91201
(213) 240-2540, Telex: 696318

Sales & service in major U.S. cities and countries throughout the world.

RUSCO

MAC 530/ MAC 540

MICRO ACCESS CONTROLLERS


TRANSACTION CODE
TIME ZONE
DAY OF YEAR
START
DAY
TIME
STOP
DAY
TIME
TRANSACTION CODE
ID NUMBER
STATUS
READER
I/O
TIME ZONE
MAC 530
MICRO ACCESS CONTROLLER
CARDENTRY™
CONTROLLER
DATA LINE
PRNTR
RED PRINT
DOOR CONDITION
COM
RUSCO
ID MEMORY
TIME ZONE
CMD
AUTH BY BLOCK
AUTH BY GROUP
CLOCK
ENTER
DELETE

Rusco
CARDENTRY
Micro Access Controllers

– Centralized, on-line access microcontrol for up to 20,000 people at up to 256 widely separated locations.

The MAC530 and MAC540 consoles contain the control, memory, and monitoring functions of Rusco's state-of-the-art CARDENTRY System 500. Utilizing powerful distributed microprocessor technology, they form the basis for a reliable, flexible access control and operations monitoring system.

In conjunction with Rusco's proprietary Ruscard,® the MACs control who goes where, when in any facility, and collect the data necessary to insure the security of personnel, equipment, and information.

Owing to their flexible architecture and software configurability, both MACs may be equipped with a wide variety of options and special application capabilities. The MAC's logic is instructed and interrogated through simple keystroke programming, which allows changing, verifying, or deleting a cardholder's access privileges in seconds.

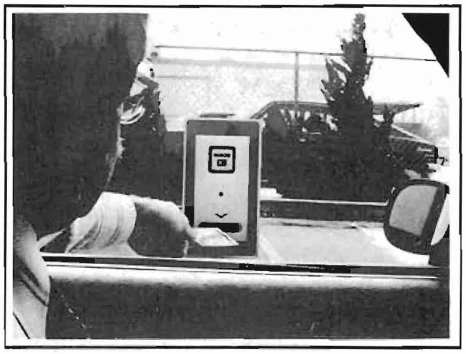
Activity logging options include printed records of all system transactions, as well as magnetic media storage for further computer processing of data gathered by the system.

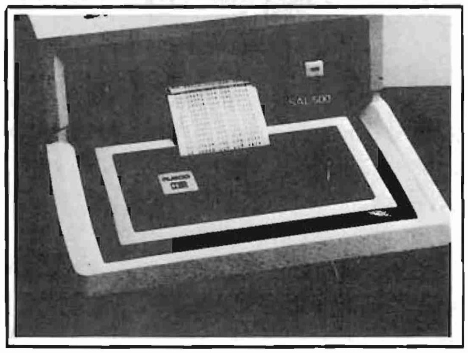
ILLUSTRATION

Excerpts from a typical System 500 log.

The following hypothetical sequence of operations illustrates some of the functions the MAC can perform in a typical manufacturing environment.

Activity shown is for a typical business day, but the MAC's automatic functions may be programmed on completely different time schedules for each day of the week, if desired.

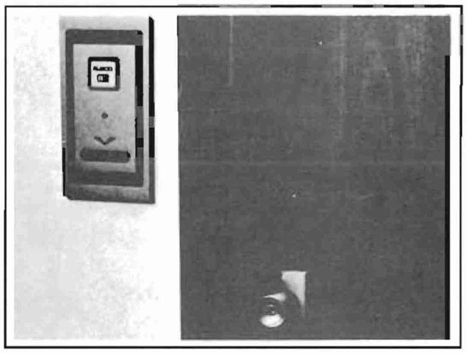


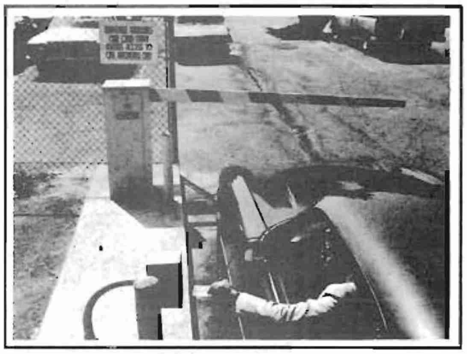


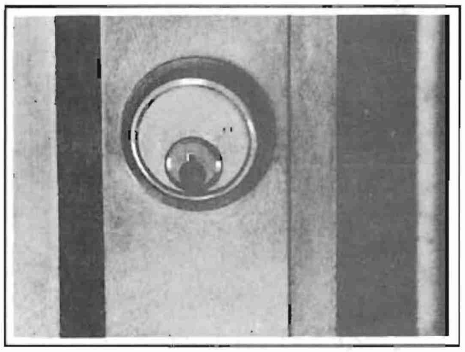
07:00 MAC unlocks gate on main employee parking lot so early-arriving employees may enter with their Ruscards. **07:30** MAC raises main parking lot gate to avoid traffic jams as traffic of arriving employees picks up. New "time zone" begins, allowing supervisory personnel to enter plant with their Ruscards and begin preparing the day's activity.

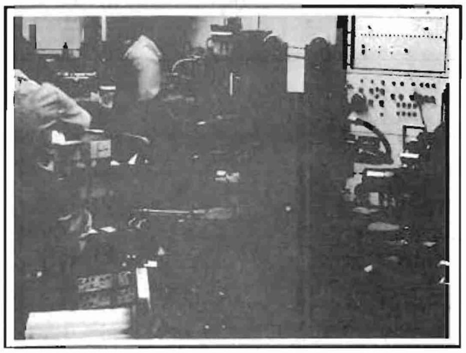
07:45 MAC enables employee entrance. As each employee enters, his/her arrival time is recorded on magnetic tape. **07:52** Early-arriving secretary attempts to use office copier for personal copying, finds her Ruscard will not operate machine until business hours begin. **08:00** MAC opens lobby entrance to building, enables office equipment for authorized use, opens doors in heavily used hallways.

08:05 MAC lowers parking lot gate so late employees must use their Ruscards to enter (They are not penalized, but the act of using the card serves as a reminder of their tardiness.) **08:40** Line supervisor queries MAC for a list of all employees in her department who failed to report for work, as an aid in scheduling jobs. **09:25** Warehouse hand several miles away needs access to special locked storage area (not normally included in his access privileges). He telephones central security officer, who keys "unlock" command into MAC. Command is transmitted via phone lines to remote warehouse, logged.









11:12 Level in a critical supply tank drops abnormally low. Contact Condition Monitor detects this and signals MAC, which sounds alarm and prints out type of condition and location.

12:10-12:22 New employee takes self-guided "tour" of plant, trying his Ruscard at every reader location. Where his status level specifies "no access," attempt is logged in red. Where access is permitted, the location and time are logged in black.

14:55 Programmer enters computer center machine room and door sticks slightly ajar. After 8 seconds, Ruscard reader signals MAC, which turns on warning light and logs location of condition. Security officer telephones computer room to have door closed fully. **14:56** MAC receives "door closed" signal from computer room, logs transaction.

17:00 Employees begin leaving, "punching out" with Ruscards. Parking lot exit gate is raised. Front office door returns to card control. **17:20** Elevator switches from free access to card control of destination floor. **17:40** Security officer requests a MAC printout of all personnel remaining in building.

18:00 Night watchman arrives and receives instructions from departing security officer.

19:00 Watchman begins tour. MAC has been programmed with a sequence of times and Ruscard reader locations where he is expected to insert his Ruscard. (Failure to stay on schedule sounds a general alarm.) **19:30** MAC unlocks meeting room doors for regularly scheduled employee meeting.

20:00 Parking gates lower, return to card control. **21:00** Meeting over, meeting room doors re-locked by MAC. **21:15** "Clean-up committee" leaves now-locked meeting room. To avoid triggering alarm when leaving secured areas, Exit pushbuttons are provided to bypass alarm system door switches momentarily. Night watchman in security office notes printout caused by operation of exit button, but realizes no action is required.

PRINCIPLES OF OPERATION

Access Control

When a cardholder inserts his or her Ruscard in a CARDENTRY System 500 reader, a complicated chain of events is set in motion.

1. Insertion of the Ruscard activates the reader's built-in microprocessor, which senses the digital code stored in the card's embedded memory core.

If the Ruscard does in fact belong with *this specific* CARDENTRY system, the reader will unscramble the card code "bits" into a System Code and a Cardholder ID Number (Note that if the card does *not* belong with the system, the reader's output will be "garbage").

2. The reader then transmits the System Code and Cardholder ID Number to the MAC. For distances up to 2 miles, communication may be over 2 wire pairs; longer distance transmission requires a dedicated full-duplex voice channel (such as a leased phone line) with a System 500 Modem at each end.

3. The card data are received by the MAC, checked for transmission errors, and the access decision process begins.

First, the System Code is verified, as a double check on the validity of the card.

Then, the MAC begins scanning its memory in an attempt to find the Cardholder ID Number. If the number is located, indicating that the card is valid, its assigned "status level" is then examined.

A status level is a collection of cardholders with the same access privileges. It is defined by a list of instructions keyed into the MAC specifying when access is permitted *at each reader location* in the system. Any cardholder's status level may be assigned or changed via the MAC keyboard.

4. If the cardholder's status level specifies access at the reader location at the current time of day and day of week, the MAC processor issues a "GO" command to the reader (otherwise, a "NO GO" command is issued).

4a. At the same time, if the System is equipped with a logging device (printer, mag tape, etc.) a transaction record is formatted and transmitted to the device. The transaction record contains the reader location, time of day, cardholder ID number, cardholder status level, and a transaction code indicating the type of transaction.

5. The reader receives the MAC command. If the command is "GO" the reader closes a set of internal contacts for an adjustable time period (up to 15 seconds). Simultaneously, a green "GO" light on the reader faceplate lights.

6. If the application is door control, the reader's contacts are connected to an electric door strike which releases the lock and allows entry.

Note that the MAC makes four separate tests before granting access: correct System Code, valid Cardholder ID No., valid status level, and authorized time zone. Failure of any of these tests will cause denial of access, and will generate a transaction record in red ink on the SAL500 logger (if included), identifying the time, location, and Cardholder ID No., and specifying the reason for denial of access.

Even in a large, extremely busy CARDENTRY system, the entire decision process from card insertion to MAC response normally takes less than a second.

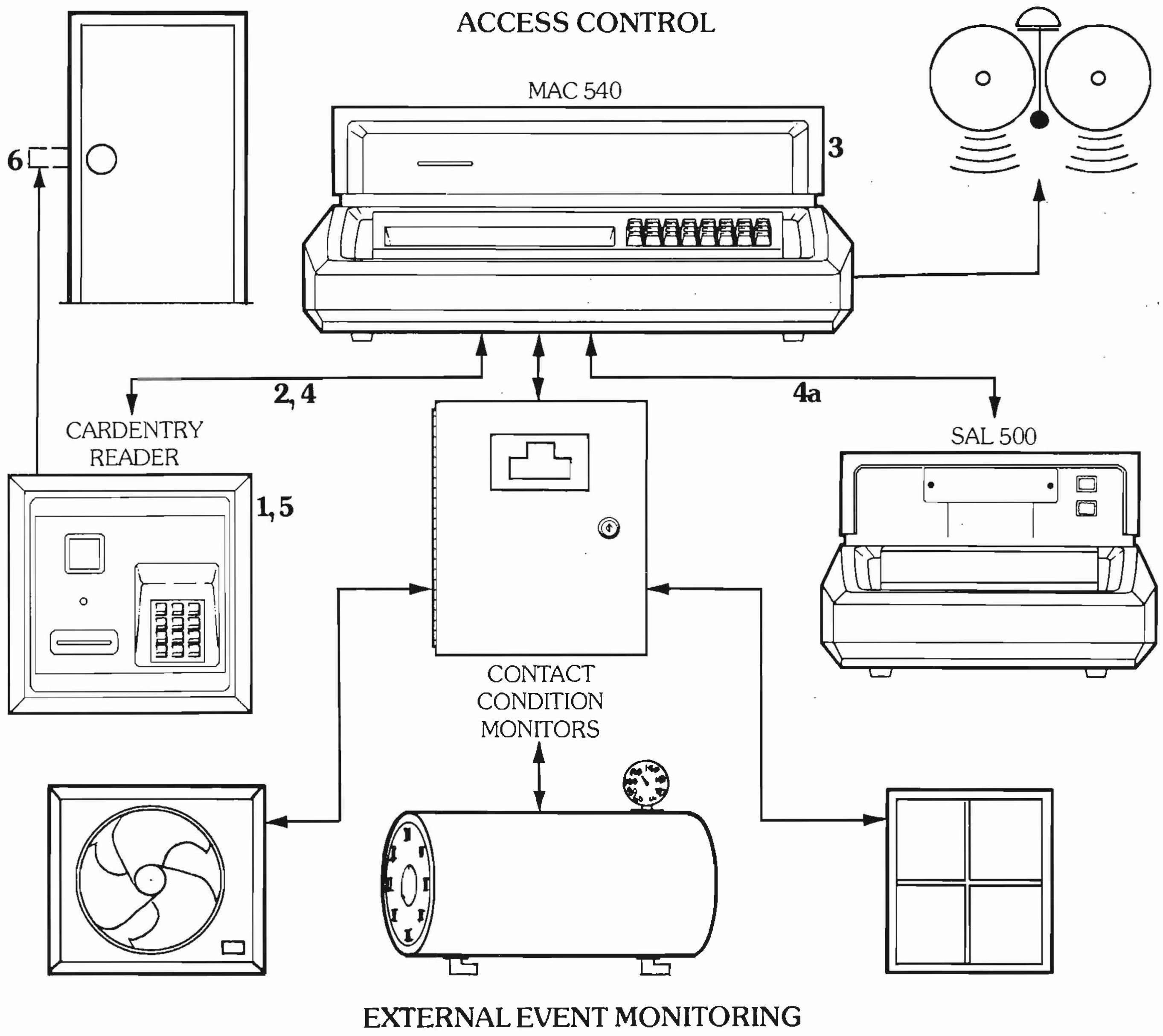
External Event Monitoring

Standard System 500 interface devices enable the MAC to serve as a centralized monitoring unit for any of a wide variety of events and conditions, which may or may not be related to access control or security.

This capability is provided via Contact Condition Monitors (CCM's), which connect to the MAC in the same manner as a Ruscard reader. Each CCM continuously monitors the state of up to 20 sets of external contacts, and immediately informs the MAC when any change is detected.

Upon receipt of a CCM alarm, the MAC creates a transaction record identifying the time and location of the event, and whether the contact is now opened or closed. Simultaneously, a warning light and audio alarm in the MAC are energized (optional on MAC530).

Typical applications for CCM's include fire & smoke detectors, door and window alarm switches, high pressure warnings, power failure warnings, equipment overload indicators, etc.



Self-Monitoring Features

To assure system integrity and reliability, the various components of the CARDENTRY System 500 are designed to monitor each other and detect operational faults.

Even when not presented with an access request, the MAC "polls" each Ruscard reader and CCM continuously to receive a status report. Failure by a device to respond generates an alarm; hence failures in terminal devices or in communication links are detected immediately.

Readers also report the status of controlled equipment, such as "door locked," "door held open" (after an authorized access) and a variety of other conditions.

Note also that if a reader's communication link or the MAC itself should fail, an exclusive Rusco option allows the reader to *automatically* switch to a local, off-line mode of operation. In this patented "degraded mode," which is transparent to users, the reader checks Ruscards for the correct System Code, and thus maintains security until the entire system is back on-line.

System Capacity

The MAC530 may be ordered with memory and I/O facilities sufficient to handle from 4 to 32 CARDENTRY readers, from 16 to 64 cardholder status levels, from 250 to 2,000 cardholder ID numbers, and from 16 to 127 time zone intervals.

The larger MAC540 offers even greater expandability, with options for up to 256 readers, 256 status levels, and 20,000 cardholder ID numbers.

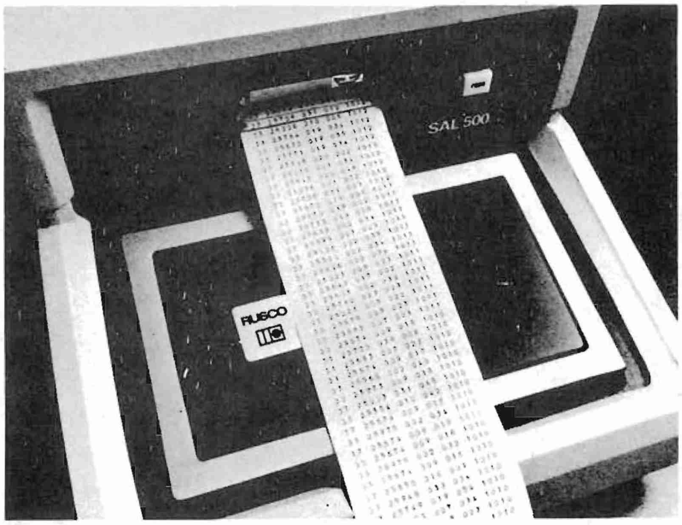
OPTIONAL CAPABILITIES

The straightforward access control and event monitoring capabilities already described comprise only the most basic operations of System 500. With installation of the appropriate "firmware," the MAC530 and MAC540 may be provided with a variety of optional features to meet special needs.

The options described below are only a sampling of those available. Rusco continues to add capabilities as need develops, so it is advisable to consult a sales office for information on additional features and options.

Logging Facilities

Recording of system transactions is an important feature of most System 500 configurations. The most common output device for "stand-alone" systems is the SAL500 activity logger, which provides a printed transaction log, with black ink for authorized transactions and red ink for abnormal or alarm conditions.



Where input of transaction data into a computer for additional processing and analysis (e.g., automatic payroll, parking lot billing, etc.) is desired, three options are available. The direct output option provides an RS-232C port which is plug-compatible with industry-standard mini and mainframe computer interfaces or with data communication modems.

Off-line recording of system transactions is available on compatible magnetic tape and diskette recorders offered by Rusco.

Anti-Passback

The Anti-Passback option allows the controller to define each CARDENTRY reader as "In" (used when entering the premises) or "Out" (used when leaving). Whenever a cardholder passes through an In door, a notation is made in the MAC memory; likewise when he exits through an Out location. The MAC is programmed to prevent use of any Ruscard for two successive "In" or "Out" transactions.

This feature prevents a cardholder from passing through a controlled turnstile or parking gate, then passing his card back to another person to use for entering.

Single Use

Single Use is an extension of the Anti-Passback feature, whereby all cardholders may be set to "Out" status, either manually or once a day at a pre-programmed time.

Thereafter, cardholders are limited to a single use of their Ruscards at an "In" location. This option has been used to limit employees with meal privileges to one cafeteria access per meal period.

Manual Reader Override

(Standard on MAC540)

This option provides the necessary logic for an authorized MAC operator to key in commands for transmission to remote CARDENTRY readers or CCM's.

Commands include functions such as Unlock Door, Lock Door, Release Lock Momentarily, and Report Status.

Automatic Reader Override

Any of the commands available with the Manual Reader Override option (above) may be transmitted automatically to selected terminal devices at pre-programmed times with this option.

A typical use for this option would be to unlock an entrance during work shift changeover, place it under card access control during each shift, and lock it at the close of the working day.

Automatic commands are stored via MAC keyboard entries, and may be changed at any time by an authorized MAC operator.

Red Print Alarm

This option (standard on the MAC540) provides a "Sonalert" audio alarm and indicator light which are energized whenever an "abnormal" system transaction occurs. It also includes a momentary contact closure for actuating an external alarm.

Alarm indication continues until the condition is acknowledged by the appropriate keyboard input.

Red Print Select

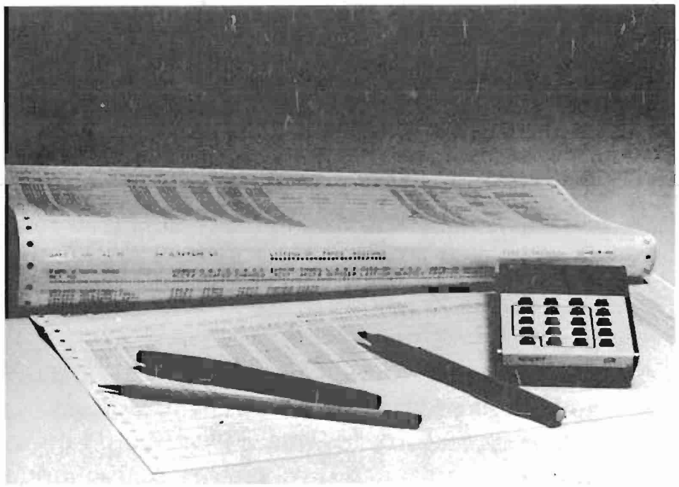
In some systems, it may not be desirable to print all abnormal transactions. This option provides the capability of selecting any combination of the following alarm categories for printing on the SAL500 logger:

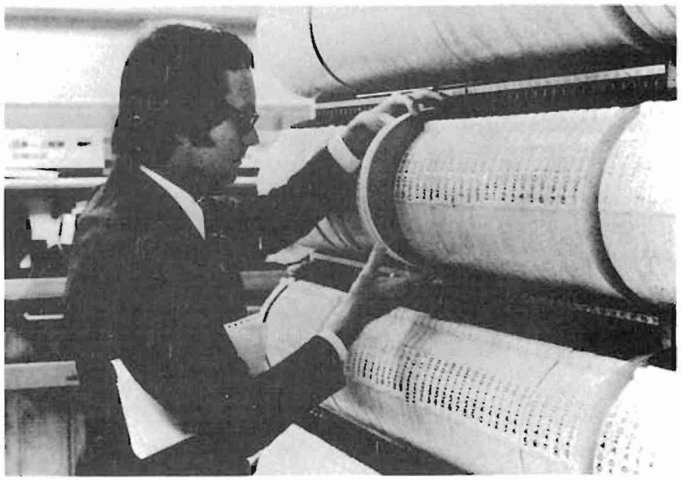
Card alarms (i.e., invalid System Code, wrong time zone, etc.)
Reader alarms (Door Open, Tamper, etc.)
CCM alarms (change in the status of an external sensor).

Selective Print

This option allows certain selected transaction records to be output to a second SAL500 printer. Data which may be selected (via MAC keyboard input) for logging include:

All activity for a single cardholder ID number
All activity for a given status level
All activity for a selected reader location.





Memory Listing

(Standard on MAC540)

With this option, the MAC operator can request any of 13 different breakdowns of the information stored in the MAC's memory. Listings are generated on the second, optional SAL500 printer, and include information such as:

All cardholder ID numbers currently "In" the premises
All ID numbers in a given status level that are currently "Out"
All status level and time zone assignments for a specified reader.

Recall Buffer Memory

This option provides additional MAC memory and firmware for storing the last 128 system transactions. The MAC operator may select any combination of the following four types of transactions for storing:

Valid transactions
Reader alarms
Card alarms
CCM alarms

(see "Red Print Select" option)

Optionally, the Recall Buffer may be segmented into four blocks of 32 transactions each, one for each of the four types of transactions listed above.

All buffers operate in a "wraparound" mode, whereby only the most recent 32 (or 128) transactions are retained. Older data are lost as new transactions are written into a full buffer.

The contents of the buffers may be printed out on the second SAL500 logger whenever desired by entering the appropriate MAC keyboard command.

APPLICATIONS PACKAGES

Equipment Usage Monitoring

The same CARDENTRY reader that controls access to a piece of equipment can also record the amount of usage per access.

Likely applications for this feature include such things as office copiers, computer data terminals, and fuel dispensing stations. Besides the obvious advantages of better cost accounting and elimination of unauthorized use, there are important security benefits. Copy machine control, for example, can solve the problem of a disaffected employee staying after hours to copy secret company files.

The only requirements on the equipment are that it must be able to be turned on and off electrically, and be capable of supplying a "count" signal to the CARDENTRY reader. In the case of a fuel pump, the count would correspond to tenths of gallons; for a copier, each pulse would correspond to one copy; for a computer terminal, minutes of usage might be counted.

To operate a monitored device, a Ruscard is inserted in the reader slot and left there for the duration of usage. The card insertion is logged, and if its status is OK, the equipment is enabled. When usage is completed, the cardholder removes his card, causing the reader to transmit the total usage count to the MAC. This count, along with other identifying information, is entered in the system log.

Data Collection

The data collection package allows authorized cardholders to transmit numeric information to the MAC for entering in the system log.

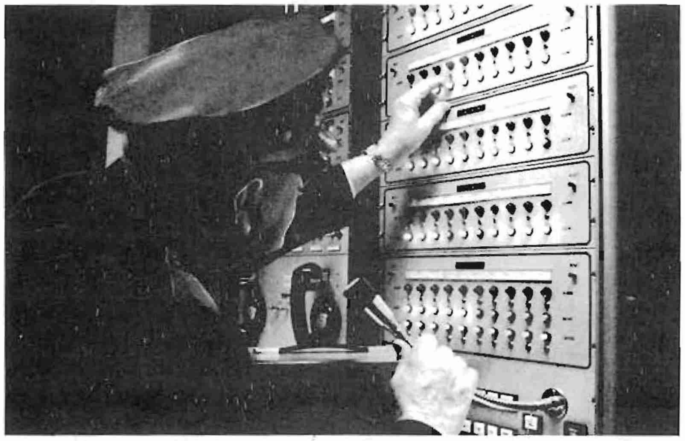
This option requires use of a Rusco Data Entry™ Reader which is equipped with a telephone-type keyboard for numeric entries of up to 9 digits.

A typical use of the data collection feature would be keeping track of information usage in a library. When a cardholder left the library, he would key in the catalog number of the book (or tape, or microfilm) being checked out. This information would be logged, and could be used for computer-prepared usage reports.

Watchman's Tour

A CARDENTRY system can "follow" a night watchman as he makes his tour around an installation.

Via the MAC keyboard, a sequence of reader locations and times is entered in memory. This sequence becomes the watchman's "tour," and the MAC will expect his ID card to be inserted in each specified reader at the specified time (plus or minus a small tolerance). If a deviation from the preprogrammed time schedule is detected, the MAC activates an external alarm device (which may be an automatic dialer to summon police, etc.)



For high-security applications, the watchman's tour may be changed as often as desired—even every night. Since, in this case, not even the watchman knows his route until he goes on duty, the possibility of "stakeouts" is eliminated.

Doctor's Register

Where important personnel come and go frequently, and it is desirable to know of their presence or absence at all times, the MAC may be interfaced with a lighted "call board" such as found in hospitals. Whenever a cardholder passes through an entrance reader, the MAC will turn on the light corresponding to that individual; whenever an exit reader is activated, the light is extinguished.

In this way, the problem of absent-minded doctors or executives forgetting to sign in and out is solved.

Open-Ended Capability

At the heart of the MAC530 and MAC540, and of every System 500 Ruscard reader, lies an extremely powerful Motorola 6800 microprocessor, with the ability to sense and respond to its environment under program control. Since the flexibility of programming is virtually limitless, so in fact is the flexibility of the system.

With this in mind, Rusco applications engineers will be pleased to discuss any special requirements you may have for additional functions and capabilities not detailed in this brochure.

MAC SPECIFICATIONS

Rusco Micro Access Controllers are highly reliable, solid state devices, designed for minimum down time and maximum maintainability.

A standard feature of all MACs is a standby battery pack which will preserve the user's data in memory for up to 72 hours of AC power outage, saving the time and bother of re-entering the information.

Cardholder ID numbers and their associated access privileges may be keyed in one at a time, or blocks of cards may be entered at once with the "mass load" feature.

MACs provide front panel indicator lights for various operational modes and conditions, and a pushbutton keyboard and LED numeric display for examining and modifying data in memory.

The MAC 540 is equipped with its own built-in Ruscard reader for limiting access to its control functions. The MAC530 uses a key switch for operator authorization.

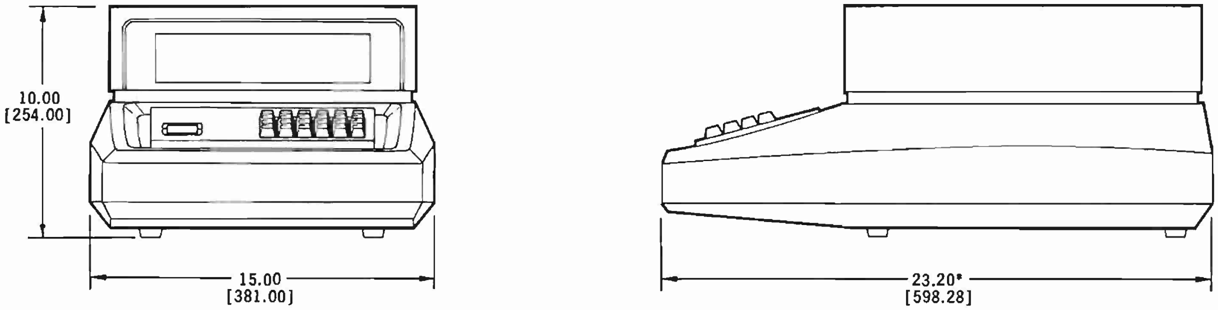
Power consumption of both units is 11VAC @ 4A, or 230VAC @ 2A (switch selectable). If desired, external 12V backup batteries may be provided for extended blackout protection. Both MACs are available as free-standing desktop consoles, or in rack-mount versions for standard 19" EIA racks.

Rusco Cardentry System 500

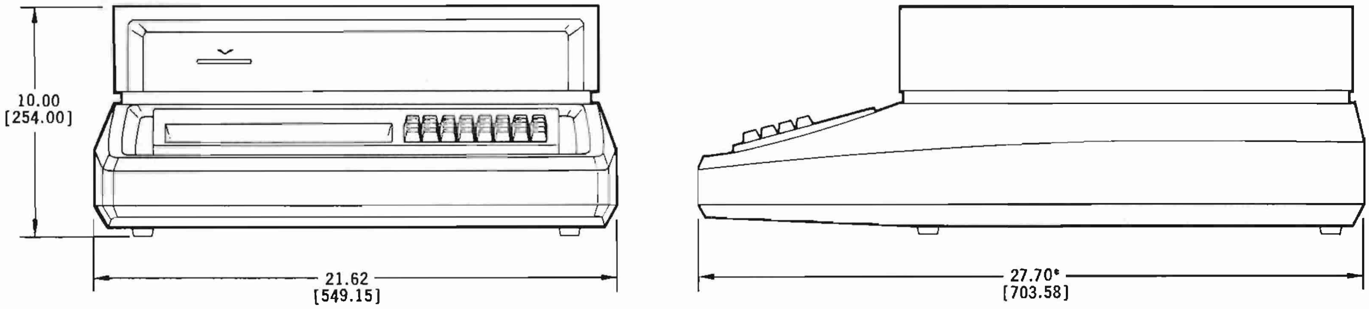
SPECIFICATIONS AND DIMENSIONS

SYSTEM 500 CONTROLLERS AND ACTIVITY LOGGER

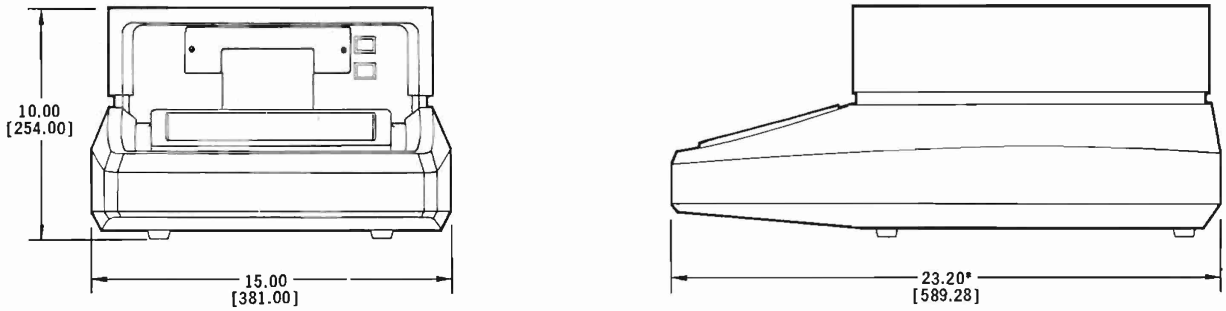
MAC530
microaccesscontroller



MAC540
microaccesscontroller



SAL500
systemactivitylogger



RES | RUSCO
ELECTRONIC
SYSTEMS
A DIVISION OF ATO

1840 VICTORY BLVD. • P.O. BOX 5005 GLENDALE, CALIFORNIA 91201 • TELEX 696318 • (213) 240-2540

SYSTEM 500 SPECIFICATIONS

GENERAL

The CARDENTRY access control system shall be as manufactured by Rusco Electronic Systems and shall include a centrally located Micro Access Controller; (specify quantity) remote access control card readers; (specify quantity) Ruscard access cards; and a System Activity Logger. The following optional equipment shall also be required: (if required, specify the quantity of each item) Multiplexers, Modems, and Contact Condition Monitors.

MAC530 SPECIFICATIONS

The central Controller shall be the all solid state microprocessor based, MAC530 Micro Access Controller as manufactured by Rusco Electronic Systems, and shall be a (specify one: stylized table top Controller or 19-inch rack mount style).

The Controller shall be capable of controlling (specify quantity: 4, 8, 16 or 32) remote card readers and shall have a random access memory bank capable of storing (specify amount: 250, 500, 1000 or 2000) ID Numbers from encoded Ruscards. The Controller shall have provisions for programming (specify quantity: 16, 32 or 64) Status Levels and (specify quantity: 16, 32, 64 or 127) Time Zone Intervals.

MAC540 SPECIFICATIONS

The central Controller shall be the all solid state microprocessor based, MAC540 Micro Access Controller as manufactured by Rusco Electronic Systems and shall be a (specify one: stylized table top Controller style or 19-inch rack mount style).

The Controller shall be capable of controlling (specify quantity: 16, 32, 64, 96, 128, 192, or 256) remote card readers and shall have a random access memory bank capable of storing (specify amount: 1000, 2000, 4000, 8000, 12,000, 16,000 or 20,000) ID Numbers from encoded Ruscards. The controller shall have provisions for programming (specify quantity: 16, 32, 64, 96, 128, 192, or 256) Status Levels and (specify quantity: 64 or 127) Time Zone Intervals.

GENERAL CONTROLLER SPECIFICATIONS

(The remainder of these specifications are common to both the MAC530 and MAC540 Controllers).

The Controller shall control remote card readers by comparing the system code and unique ID Number stored within each individual Ruscard, and the place and time of entry with the controller system code, and the list of acceptable ID Numbers which is stored with their authorized places and times of entry in a random access electronic memory.

When a card is used at a Reader location, access is granted only if the system code is valid, the ID Number is found in memory and it is authorized for that location for the current time period. If all conditions are met, a signal shall be sent to the Reader location to activate the appropriate access control device. A printout of the card ID Number, access point, card status level, and time of day shall be printed for each Reader transaction. If any of the above conditions are not met, the Controller shall not activate the access control device but shall print out the same information with an indication of why the access was denied. All valid entries shall be printed in black and invalid access attempts shall be printed in red.

The ID memory shall always be in full capacity; voiding (deleting) an ID Number shall not void a memory location—it shall be possible to program another ID Number in the place previously occupied by a voided number. There shall be no preassigned memory addresses for ID Numbers.

The Controller shall maintain a digital calendar and clock for controlling and indicating all time-related functions. This data may be displayed at any time and shall consist of day of year, day of week and time of day in hours and minutes (24-hour day). Time zones shall be used for controlling access by time. A time zone shall consist of one or more intervals with each interval comprised of a start day and time and a stop day and time. Each interval shall be accurate to the minute. It shall be possible to assign more than one interval to a single day within one time zone. Up to 16 intervals may be used to define a single time zone.

All vital memory in the Controller shall be maintained for at least 48 hours after a power failure. After power has been restored, the Controller shall bypass the time zone test for granting access until the clock has been reset.

The MAC540 Controller shall contain a card reader which shall be used for restricting programming operations to authorized personnel only. An authorized cardholder must insert his card before he shall be abie to change any programmable functions or Controller memory. It shall be possible to use this reader to test Ruscards or the System.

The MAC530 shall contain a special security lock switch for restricting programming operations. This key-operated switch must be open before any changes can be made to any programmable functions or to Controller memory.

Line monitor supervision shall be an integral function of the Controller and card reader communication. Each time a reader is polled by the Controller, the reader shall respond with a message. The Controller shall provide a visual indication and shall cause an alarm message to be printed if a compromising of a communication line occurs.

The Controller shall have all controls and indicators available on the front of the Controller. A keyboard shall be provided for entering functional and numerical information into the Controller. A digital display shall provide a visual readout of the information stored in the Controller memory and shall be used when entering keyboard data. Whenever data is to be entered via the keyboard, the display shall display dashes (—) in the display fields requiring data. As each keyboard entry is made, the dash shall be replaced by the keyboard entry. A total data entry may be verified by visual inspection of the display before the data is stored in memory.

The operation and programming of the Controller shall be by means of simple keyboard entries. The keyboard shall provide means of validating or invalidating card numbers or status levels and shall also provide means for adding, deleting or changing the status level or time zone assignments for readers.

Consecutive ID Numbers, with the same status level, may be mass-loaded into memory by a single set of keyboard entries. Likewise, consecutively numbered reader assignments may be mass-loaded into memory when their assigned status levels and time zones are the same.

All entries for card ID Number shall be made using the ID Number only with no separate memory addressing or tables required.

Any data that has been programmed into memory may be recalled for display without disturbing the stored data. The Controller shall be capable of searching for and displaying ID Numbers, reader, status, and time zone assignments.

CONTROLLER OPTIONS

RED PRINT SELECT

The red print select option shall provide a means of printing a category of red print functions. Without this option all red functions will be printed. The red print functions shall be divided into three categories:

1. Card Alarms
2. Reader Alarms
3. Contact Condition Monitor Alarms

Any combination of these alarm categories may be selected for printing.

RED PRINT ALARM

This option shall provide an audio alarm (sonalert) and a visual display for indicating alarm conditions. The audio alarm shall sound only when a red print occurs — that is if CCM Alarms only are selected for red print, the audio alarm shall sound only for CCM Alarms.

A display for each of the following alarms shall be provided.

1. Data Line — No Response
2. Door Open
3. Door Unlocked
4. CCM Alarm
5. Reader Tamper Switch

The audio alarm and visual indicator shall remain ON until manually reset. The audio alarm may be silenced by command from the keyboard.

A single momentary contact closure shall be available at the rear of the Controller for signaling any external alarm device that a red print has occurred.

ANTI-PASSBACK

The Controller shall be capable of performing an anti-passback function which allows card readers to be defined as IN readers, OUT readers or other readers. In addition it shall be possible to program each cardholder (ID Number) as IN the facilities, OUT of the facilities, or undefined.

The Controller shall store in memory the cardholder's present IN/OUT status (attendance code) and shall be capable of displaying or printing this upon request. Once programmed IN, a cardholder must use his card at an OUT reader before his card will be granted access to any IN reader. As he exits through the OUT reader, the Controller shall program his ID Number with an OUT attendance code. A cardholder always shall have access to any "other" reader as defined by his status level.

An ID Number may be initially programmed into memory with an "undefined" attendance code. Once the cardholder uses his card in an IN or OUT reader, the Controller shall set his attendance code accordingly.

SINGLE USE OPTION

The Controller shall have the capability of programming every ID Number to an OUT condition, either manually at anytime, or automatically once a day at a preset time. This option shall allow "single use" applications when used with IN readers only.

As an example, IN readers shall be used to grant access to. a cafeteria, where each employee is limited to a single use during the lunch period. Once the cardholder has accessed the cafeteria, his card no longer shall have access to the cafeteria until his ID Number is programmed OUT, for example at midnight each day.

READER OVERRIDE CONTROL

It shall be possible to transmit commands from the Controller to remote access card readers. These commands may be initiated manually by means of keyboard entries or automatically under time zone control. This reader override control shall enable doors .to be unlocked momentarily, for granting a single entry, or unlocked for long time intervals, when card entry is not required. This option shall also provide for sending commands to IDEK card readers for changing the mode of operation.

SELECTIVE PRINT

It shall be possible to program the Controller to present only selected data for printing to an optional System Activity Logger. The selective print shall be by ID Number, Status Level, or Door (Reader) Number. Selection shall be made on a single number basis.

Selectlve Print Functions

ID Number — Print all activity for ID No.__________

Status — Print all activity in Status Level__________

Reader — Print all activity at Reader No.__________

MEMORY LISTINGS

The Controller shall be capable of searching its memory and providing the following memory listings to an optional System Activity Logger. It shall be possible for the Controller to output a memory listing to one logger, while at the same time it is outputting normal card transaction data and alarm data to another logger.

ID Number Listings

All ID Numbers in memory
All ID Numbers in a selected Status Level
All ID Numbers with IN Attendance code
All ID Numbers with OUT Attendance code
All ID Numbers IN with a selected Status Level
All ID Numbers OUT with a selected Status Level

Reader Listings

All Status Levels and Time Zones for a selected Reader
All IN Readers
All OUT Readers
Reader Number Definition Listing
Reader Override Memory Listing

Status Listing

All Readers and Time Zones for a selected Status Level

Time Zone Listing

All intervals for each Time Zone

RECALL BUFFER MEMORY

The Controller shall contain a buffer memory with the capacity of storing the last 128 transactions. The Controller shall be capable of displaying these transactions, one at a time, or outputting them to an optional System Activity Logger.

Single Buffer

Any one of the data formats listed below may be selected for storing into the full 128 transaction buffer.

Segmented Buffer

As an option the transaction buffer can be divided into four 32 transaction buffers. These segments shall be used as follows:

Segment	Type of Data Stored
1	CCM Alarms
2	Reader Alarms
3	Card Alarms
4	Valid Card Transactions

OUTPUT CHANNELS

The Controller shall have two optional output channels with RS-232-C logic and voltage discipline and ASCII character format. These channels shall allow the Controller to transmit to external devices the same data that is printed by the System Activity Loggers, (viz, card transaction and alarm data on output No. 1 and selective transactions and memory listings on output No. 2).

OPTIONAL PERIPHERAL INTERFACES

It shall be possible to add interfaces to allow the Controller to record data on magnetic tape, diskettes or other computer peripherals.

In addition it shall be possible to add an RS-232-C I/O channel which will allow an external device to communicate to the Controller using the keyboard instruction set and receive the same data being displayed by the Controller.

SYSTEM ACTIVITY LOGGER

The System Activity Logger (SAL) shall provide the hard copy printout of the system transactions and alarms. A transaction or alarm condition shall be printed as a single line on 3½-inch wide fan-fold or roll paper. The MAC540 Controller shall buffer a maximum of 64 transactions (16 transactions for the MAC530) so that its operation is not degraded by the printing speed.

The System Activity Logger shall be connected to the Controller with only two twisted pairs of wire (normally 22 AWG gauge). Direct connections may be made between the Logger and Controller up to a maximum of 2 miles.

The logger shall print all valid card transactions in black. All invalid card transactions and all reader and contact condition monitor alarms shall be printed in red. The Controller shall provide for the selection of:

RED PRINT ONLY — (Alarms and invalid cards only)

RED AND BLACK PRINT — (All Transactions)

Each card transaction shall have the following data printed: Transaction code, ID Number, Status Level, Reader Number and Time of Day. Once each hour, on the hour, the logger shall print the day of year, day of week and time. A unique transaction code shall be printed for identifying each type of valid, or invalid transaction and alarm condition, (such as; invalid system code, invalid status level, invalid IDEK code, door open detect, door unlocked, etc.).

An alarm light shall be provided on the Controller which shall indicate when the System Activity Logger has been disconnected or is inoperative. This light may be reset only by personnel authorized to program the Controller.

(Optional)

A second SAL shall be provided for printing selective transactions and memory listings. This logger shall be identical to the first SAL however, no transaction buffering shall be required.

CARDS

Cards shall be as manufactured by Rusco Electronic Systems. They shall be capable of accepting binary coded bits in a scrambled pattern as a unique identification code stored within the cards which can be read by Rusco Electronic Systems equipment. Cards shall be 3⅜" x 2⅛" x .032" and shall be highly resistive to wear or environmental deterioration. Cards shall be capable of being printed on any area of the card, front or back; of being embossed with up to three lines of variable or fixed data; and of being produced as photo ID cards. Cards shall be capable of being used on any standard credit card imprinting device to produce machine readable documents.

The ID Number shall be sequentially encoded on each card. All cards for a system shall be encoded with the same system code. The combination of the system code and the ID Number shall be unique to a single card and that combination shall never be duplicated.

BASIC READERS

The System 500 reader shall be directly compatible with both versions of the System 500 Controller (MAC530 and MAC540). The reader shall be solid state in design and shall not employ any codeboard or mechanical locking mechanisms. All electronics shall be contained within the reader assembly — no additional interface box shall be required.

The System 500 reader shall read two encoded sets of numbers, a system code and an individual identification number from the Ruscard and transmit both sets to the Controller for an authorization determination. The Controller shall be programmed only to accept cards with the particular system code common to all cards for that system, before it will examine the identification number which shall be different for each card. Ruscards encoded with different system codes yet having valid identification numbers will not pass the access authorization test.

Two twisted pairs of wire (normally 22 AWG gauge) shall be required for connecting the reader to the Controller. Direct connections may be made between each reader and the Controller up to a maximum of 2 miles. Additionally, up to 16 readers may be connected to a multiplexer (maximum distance of 2 miles) which, in turn, shall be connected to the Controller by two twisted pairs of wire up to a maximum of 2 miles.

Line monitor supervision shall be an integral function of the reader and Controller communication scheme. Each time a reader is interrogated by the Controller, the reader must respond with an acknowledge message, an alarm message or a data message. If the Controller does not receive any reply it will print an alarm message. When the degraded mode option is added, a reader shall operate as an off-line stand-alone reader when a loss in communications has been detected. On-line operation shall be restored automatically when normal communications resume.

All System 500 card readers shall provide a single-pole double-throw (SPDT) relay contact output for indicating authorized access. These contacts are normally used to unlock the door by switching externally supplied power to an electric door strike. The contacts shall be rated for 3 amps maximum, at 115V AC or 28V DC. The operate time for this relay shall be adjustable from 1 to 15 seconds by the variable time delay (VTD) circuit.

A green "GO" or acknowledge light shall be contained on the faceplate of all System 500 readers. This light shall be illuminated for the duration set by the variable time delay circuit when an authorization command is received from the Controller.

If an UNLOCK (reader override option) command is received from the Controller, the output relay shall latch and remain in that condition until a LOCK command is received. The acknowledge light shall remain illuminated during this period, indicating that the door is unlocked.

Two styles of housings shall be available for the basic reader: Flush mount and Surface/Pedestal mount.

All reader housings shall provide front access to the reader assembly. Each unit shall be secured by a key lock which shall be hidden from view by an aesthetically designed faceplate.

The front access flush mount reader assembly shall comprise a rough-in box for mounting the reader in a 4-inch thick wall, the reader assembly, and a reader faceplate which mounts flush against the wall surface. The reader may be mounted either vertically or horizontally.

The surface/pedestal mount housing shall provide a stylish enclosure for the reader assembly for use at glass door installations, other situations requiring surface mounting. A threaded coupling may be attached to rear surface for connecting this housing to a post or pedestal. This housing may be mounted either vertically or horizontally.

IDEK READERS

The System 500 IDEK reader shall provide the highest level of security, for entry access control. This reader shall require the use of a valid Ruscard plus a keyboard entry of the proper 4-digit personal code before access is granted.

The following sequence must be completed successfully before access is granted:

1) Ruscard is inserted in reader

2) 4-digit personal code is entered on keyboard

3) Reader compares keyboard entry with 4 scrambled digits of the ID Number on card

4) Reader transmits the following data to Controller:

   a) System code read from card

   b) ID Number read from card

   c) Keyboard entry valid or invalid

5) Controller makes normal authorization tests and, if all are valid, returns an "access granted" command to reader.

6) If the keyboard entry is no good, or if any of authorization tests are invalid, the Controller will print red message and an "access denied" command to reader.

The IDEK reader shall operate in either CARD ONLY or CARD PLUS KEYBOARD mode. The mode of operation may be set manually at the reader or (optionally) by the Controller (either manually or automatically under time zone control). The Controller command shall override the local reader setting.

A code scrambling network shall be provided so that any combination of the 5-digit identification code encoded on the card may be established as the 4-digit personal code for keyboard entry. This scrambled code may be different for each IDEK reader in the system, providing a further selectivity in access control. The scrambled code may be changed by the customer at any time without re-encoding cards.

The IDEK reader shall consist of a basic reader assembly and a 12-key telephone-type keyboard mounted on an attractive faceplate. This assembly shall be furnished with a rough-in box for flush mounting in a 4" deep wall, or in a hooded fully enclosed housing for surface mounting. A threaded coupling may be attached to the rear of the surface mount housing for pedestal mounting. Both assemblies shall be accessible from the front and shall be secured by a key lock which is hidden by a stylized faceplate.

Duress Alarm

This IDEK reader option shall provide a contact closure which indicates entry under duress conditions. If a cardholder is being forced to enter his personal code by an unauthorized person, he may indicate this fact by pressing the duress key (*) as he is entering his code. A duress alarm relay contact at the reader shall momentarily close (3 seconds) to indicate this condition.

A valid personal code must be entered before the duress key will operate the contact. This shall prevent false alarm signals from being generated by someone mischievously pressing the duress key as he walks by the IDEK reader.

Error Monitor

This IDEK reader option shall monitor and count each incorrect keyboard entry. After a predetermined number of consecutive invalid attempts at entering a personal code, the error monitor relay contact, at the reader, will momentarily close (3 seconds). A selector switch shall provide for setting the allowable number of invalid attempts from 1 to 8.

Audio-Visual Alarm

The audio-visual alarm option for the IDEK reader shall be provided in separate housing and consist of an audible alarm (sonalert), a light, reset pushbutton, a silence switch to disable the audible alarm, and an output terminal strip. When connected to either or both Duress Alarm and Error Monitor options, this option shall provide audio and visual alarm for either alarm condition. The alarm shall remain sounding (and light on) until the reset pushbutton is depressed. A set of alarm contacts shall be provided for additional applications by the customer.

ELEVATOR READER

The System 500 Elevator Reader shall provide on-line individual access control for elevators. The functions of status, time zone and individual control are accomplished in the same manner by the MAC540 Controller. Each elevator floor location shall be treated by the Controller as a separate reader location. A maximum of 100 floors can be controlled.

An elevator reader and floor selector shall be required for each elevator to be controlled. The reader shall be installed in the elevator car and the floor selector in the elevator machine room. Only two twisted pair of wires are required between the reader and floor selector and between the floor selector and MAC540 Controller.

The elevator reader shall consist of a basic card reader and a 12-key telephone-type keyboard. An individual must insert his Ruscard and then tap in the floor number desired. The Controller shall consider each floor number as a separate door location and perform the necessary authorization tests. If all tests are valid the Controller shall send an "access granted" command to the floor selector. The proper floor selector relay shall be operated momentarily which enables the elevator circuits to send the elevator to the selected floor. The acknowledge light on the elevator reader also shall be lighted momentarily.

BASIC READER OPTIONS

DEGRADED MODE

The Degraded Mode option shall allow an on-line reader to automatically function in a stand-alone, off-line mode when it has lost communications with the Controller. Normal on-line operation shall be restored automatically when full communications with the console is restored. Security shall be maintained in degraded mode by granting access only to those cards which have the correct system code.

When degraded mode is used with an IDEK reader, the cardholder must also enter the proper personal code before access is granted, if the "card plus keyboard" mode is selected.

A system may incorporate readers both with and without degraded mode.

ALARM SHUNT/DOOR OPEN DETECTION

The Alarm Shunt option shall provide a reader with the capability of permitting an authorized entry without breaking an external alarm circuit. This option shall provide an alarm shunt relay which operates prior to the door open relay. The shunt relay shall keep the alarm circuit intact momentarily when an authorized cardholder is granted access through a secured door by the Rusco System.

The shunt relay may be adjusted to remain operated for 2 to 32 seconds. If the door is held open for longer than the preset time, the external alarm circuit shall be broken. If the door is forced open, the alarm circuit shall be broken immediately.

Door Open Detect shall initiate a Controller printout in the event that a door is held open for longer than a pre-set time. A second printout shall occur when the door is closed after being held open too long. The Alarm Shunt variable time delay of 2 to 32 seconds shall establish the Door Open Detect time. Door monitor contacts shall be required to indicate door status. This option shall operate independent of any card transactions at the Reader. The System Activity Logger shall provide a printout each time a door open detect alarm occurs. Additionally, a "Door Open" display lamp is lit on the Controller front panel.

TAMPER SWITCH OPEN

The specified System 500 card readers shall be furnished with a tamper switch. This switch shall be mounted inside the reader and shall provide an alarm contact whenever access to the reader is attempted by removal of the faceplate. This tamper alarm switch shall cause the reader to transmit an alarm message to the Controller which will cause a red printout and turn on the "tamper switch" display.

COLD WEATHER PACK

The specified System 500 card readers shall be equipped with a cold weather pack option where ambient operating temperatures are below 35°F. This option shall consist of a thermostatically controlled internal heater and a weather flap behind the card slot to enable the reader to operate to —25°F ambient temperature.

NO-GO OUTPUT OPTION

A NO-GO output relay shall be provided on the specified readers. This relay shall operate when an "access denied" Controller command is received by the reader. Duration of closure shall be determined by the "Door Unlock" variable time delay (1 to 15 seconds).

CONTACT CONDITION MONITOR

The Contact Condition Monitor (CCM) shall permit the System 500 to have additional capability to record the opening and closing of electrical contacts which could be used to monitor, for example, heat sensors, smoke sensors, door and window openings and perimeter alarm devices.

A basic CCM shall be capable of monitoring 10 "Form A or B" dry electrical contacts and shall be expandable to monitor a total of 20 contacts. A CCM with either 10 or 20 contact monitoring capacity utilizes one reader location in a system.

Whenever a CCM detects any change (open or closed) in the condition of any of the contacts, a message shall be transmitted to the Controller which shall initiate a red printout. The printout shall include the time of the condition change, the location of the CCM (reader number), the location of the contact (contact number) and a transaction code to indicate whether the contact opened or closed.

The CCM shall be of solid-state design and shall be isolated electrically from the alarm contacts and the Controller. The CCM may be connected directly to a controller or to a multiplexer or modem by two twisted pair of wires.

MULTIPLEXER

The Multiplexer (MUX) shall provide for expanding the output capability of a Rusco Controller. A Multiplexer shall allow up to 16 Readers and CCMs to be connected to a single Controller channel by means of only two twisted pair of wires. A MUX may be located up to 2 miles from the Controller and the Readers may be located up to 2 miles from the MUX. Additionally the MUX may be connected to a modem and phone line to provide unlimited distance between a Controller and 16 Readers.

The MUX shall be a solid-state design and shall be available as an 8-Reader or 16-Reader capacity unit.

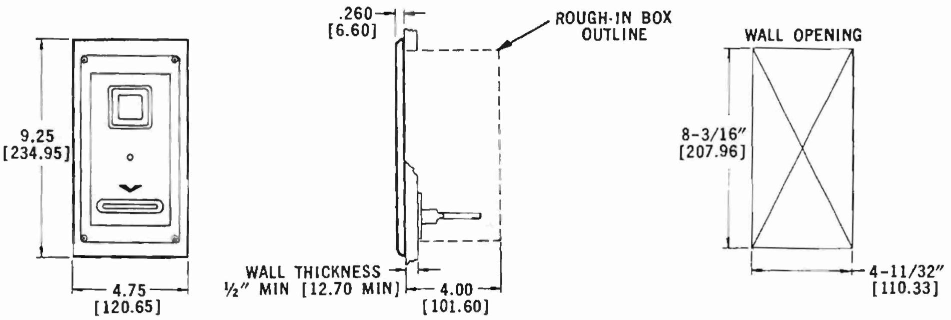
MODEM

The Modem shall provide the Rusco Electronic System 500 with the capability of communicating over leased voice grade telephone lines. The phone lines shall be type 3002, 4-wire, full-duplex circuits. The Modem shall convert the 20 mA. current input signals to Frequency-Shift-Keyed (FSK) signals of 1200 and 2200 Hertz frequency. At the receiving end, the Modem shall reconvert received FSK signals back to 20 mA. current outputs compatible with the Rusco System. Data transmission rate shall be 600 Baud.

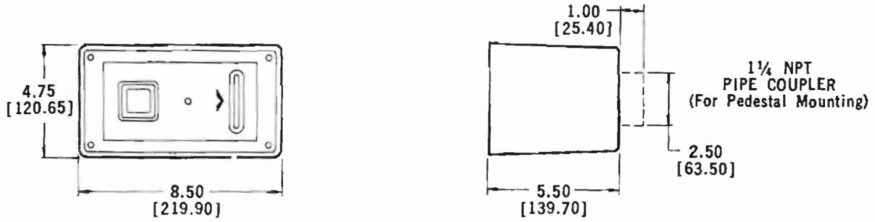
Modems shall be required in pairs, one at the Controller end and the other at the remote end of the phone line. The remote modem may be connected directly to a single Reader or CCM or to a Multiplexer for operating with a maximum of 16 Readers or CCMs.

SYSTEM 500 CARD READERS

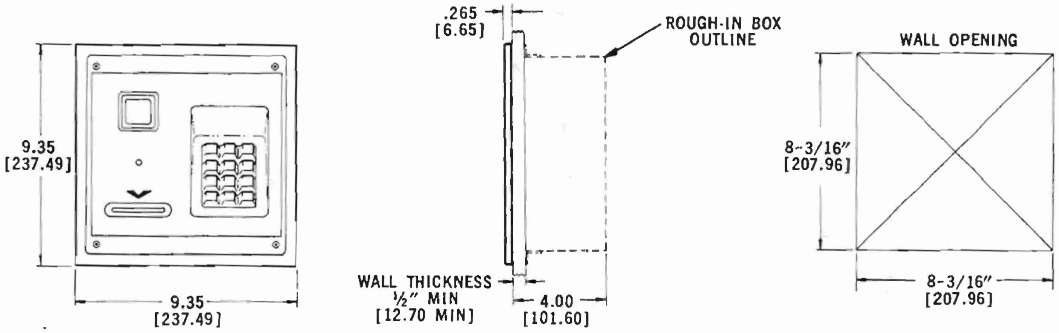
CRF500 reader – flush-mounted



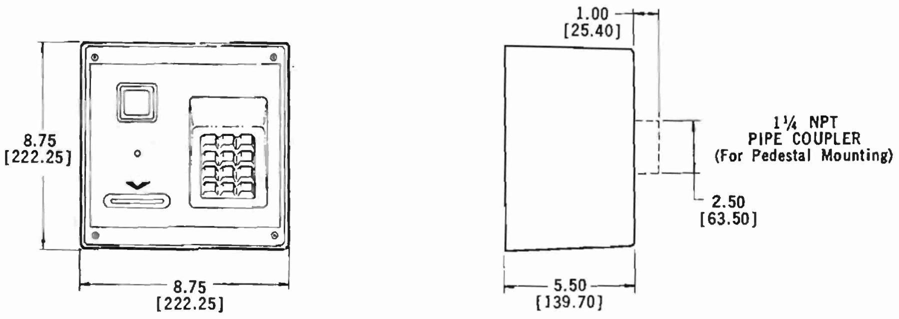
CRS500 reader – surface-mounted
CRP500 reader – pedestal-mounted



IDF500 idek reader – flush-mounted
ERF500 elevator reader – flush-mounted



IDS500 idek reader – surface-mounted
IDP500 idek reader – pedestal-mounted
ERS500 elevator reader – surface-mounted

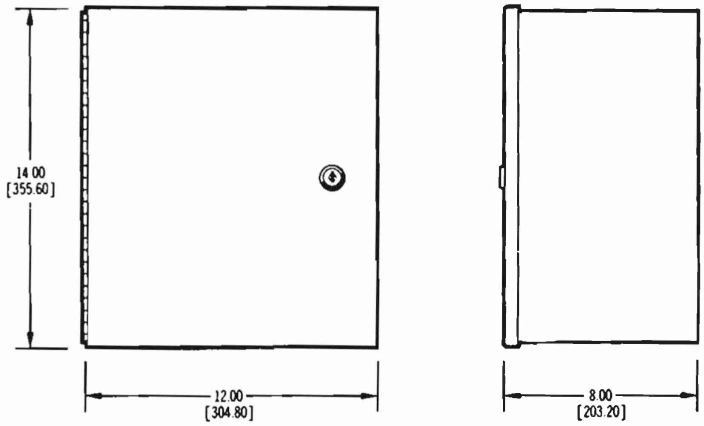


CARDENTRY SYSTEM 500 OPERATING SPECIFICATIONS

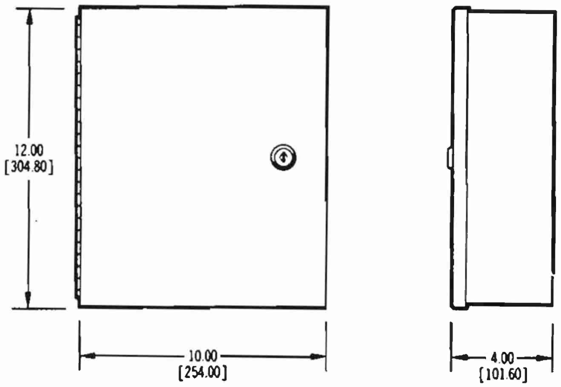
ITEM	AMBIENT TEMPERATURE	HUMIDITY	POWER REQUIREMENTS	OUTPUT	WIRING METHOD	MAXIMUM DISTANCE	COMMENTS
MAC 530 CONTROLLER	32 TO 120 F [0 TO 48.9 C]	95% NON-CONDENSING	115VAC, 50 60 HZ, 4 AMP 230VAC, 50 60 HZ, 2 AMP	8 CHANNELS — 20 mA CURRENT LOOP, OPTICALLY ISOLATED	2 TWISTED PAIR TO THE CHANNEL DEVICE	2 MILES MAX. ±22 AWG. WIRE (MAX LOOP RES ≤ 360 OHMS)	A CHANNEL DEVICE CAN BE ANY ONE OF THE FOLLOWING A) READER B) FLOOR SELECTOR C) CCM D) MODEM E) MULTIPLEXER
MAC 540 CONTROLLER	32° TO 120 F [0 TO 48 9 C]	↕	115VAC, 50 60 HZ, 4 AMP 230VAC, 50 60 HZ, 2 AMP	16 CHANNELS — 20 mA CURRENT LOOP OPTICALLY ISOLATED	2 TWISTED PAIR TO THE CHANNEL DEVICE	↕	A CHANNEL DEVICE CAN BE ANY ONE OF THE FOLLOWING: A) READER B) FLOOR SELECTOR C) CCM D) MODEM E) MULTIPLEXER
SYSTEM 500 CARD READER	32 TO 120 F [0 TO 48.9 C] OR -25° TO 120° F [-30.7 TO 48.9 C] WITH COLD WEATHER PACKAGE	↕	12 VAC. 50 60 HZ, 1 0 AMP	FORM C (SPDT) DRY CONTACT CLOSURE 3 AMPS MAX., 115VAC OR 28VDC MAX.	2 TWISTED PAIR TO A CONTROLLER, MUX OR MODEM	↕	A READER CAN BE CONNECTED TO ANY ONE OF THE FOLLOWING A) CONTROLLER B) MULTIPLEXER C) MODEM
SYSTEM 500 ELEVATOR READER	32° TO 120 F [0° TO 48.9 C]	↕	12 VAC. 50 60 HZ, 1 0 AMP	SEE FLOOR SELECTOR (BELOW)	2 TWISTED PAIR THRU TRAVEL CABLE TO FLOOR SELECTOR	↕	A FLOOR SELECTOR IS REQUIRED FOR EACH ELEVATOR READER.
SYSTEM 500 FLOOR SELECTOR	↕	↕	115VAC, 50 60 HZ, 1 0 AMP 230VAC, 50 60 HZ, 0.5 AMP	A DRY CONTACT CLOSURE PER FLOOR, FORM A (SPST) 2 AMPS MAX. 600 VOLTS MAX.	2 TWISTED PAIR TO A CONTROLLER, MUX OR MODEM	↕	A FLOOR SELECTOR CAN BE CONNECTED TO ANY ONE OF THE FOLLOWING A) CONTROLLER B) MULTIPLEXER C) MODEM
SYSTEM 500 CONTACT CONDITION MONITOR	↕	↕	115VAC, 50 60 HZ, 0.5 AMP 230VAC, 50 60 HZ, 0 25 AMP	CONTACT SENSING OUTPUTS 10 mA CURRENT LOOP	2 TWISTED PAIR TO A CONTROLLER, MUX OR MODEM 1 TWISTED PAIR TO EACH REMOTE CONTACT	↕	A CCM CAN BE CONNECTED TO ANY ONE OF THE FOLLOWING A) CONTROLLER B) MULTIPLEXER C) MODEM
SYSTEM 500 MULTIPLEXER	↕	↕	115VAC, 50 60 HZ, 0.5 AMP 230VAC, 50 60 HZ, 0.25 AMP	8 OR 16 MUX CHANNELS 20 mA CURRENT LOOP ISOLATED, PER MUX DEVICE	2 TWISTED PAIR TO A CONTROLLER OR MODEM 2 TWISTED PAIR TO EACH MUX DEVICE	↕ 2 MILES MAX. ±22 AWG. WIRE (MAX LOOP RES ≤ 360 OHMS)	A MUX DEVICE CAN BE ANY COMBINATION OF 8 OR 16 A) READERS B) FLOOR SELECTORS C) CCM
SYSTEM 500 MODEM	↕	↕	115VAC, 50 60 HZ, 0.5 AMP 230VAC, 50 60 HZ, 0.25 AMP	FREQUENCY SHIFT KEYED (FSK) SIGNALS DATA RATE IS 600 BAUD	DEDICATED VOICE GRADE, FULL DUPLEX TELEPHONE LINE	UNLIMITED	MODEMS ARE REQUIRED IN PAIRS. LOCAL MODEM CONNECTS MAC 530 OR MAC 540 TO PHONE LINE AND REMOTE MODEM CONNECTS PHONE LINE TO A CARD READER, FLOOR SELECTOR, CCM OR MULTIPLEXER.
SYSTEM 500 SYSTEM ACTIVITY LOGGER	32° TO 120 F [0° TO 48.9 C]	95% NON-CONDENSING	115VAC, 50 60 HZ, 1.0 AMP 230VAC, 50 60 HZ, 0.5 AMP	TWENTY-ONE COLUMN PRINTOUT ON 3½" WIDE PAPER—FAN-FOLD OR ROLL	2 TWISTED PAIR TO MAC 530 OR MAC 540 CONTROLLER	2 MILES MAX. ±22 AWG. WIRE TO CONTROLLER	ONE LOGGER IS REQUIRED FOR PRINTING CARD TRANSACTIONS AND ALARMS. A SECOND LOGGER IS REQUIRED FOR SELECTIVE PRINTING AND MEMORY LISTINGS

SYSTEM 500 ACCESSORIES

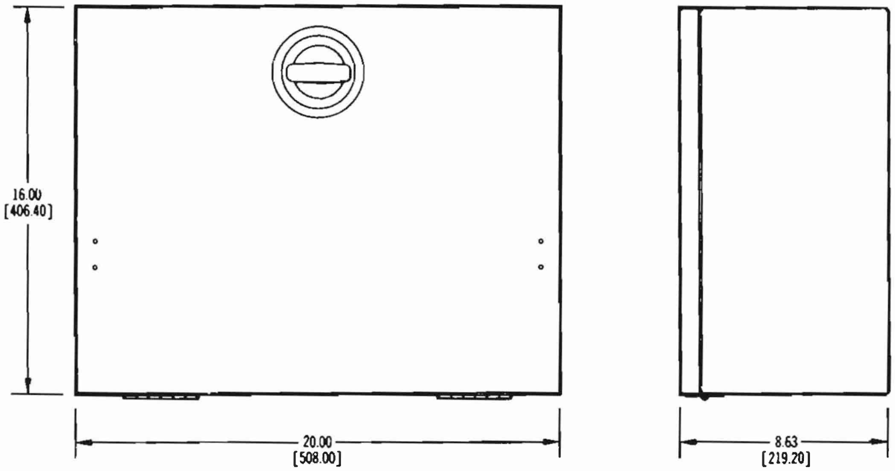
MUX500 multiplexer/ CCM500 contact condition monitor



MOD500 modem

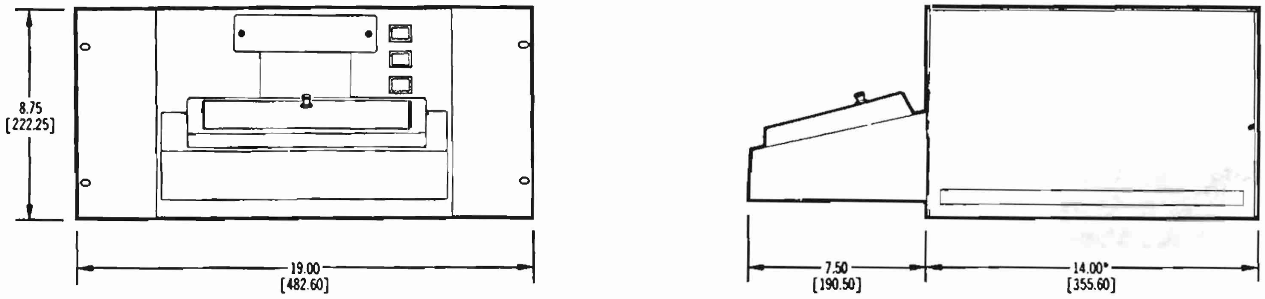


FLS500 floor selector/FSX500 floor selector expander

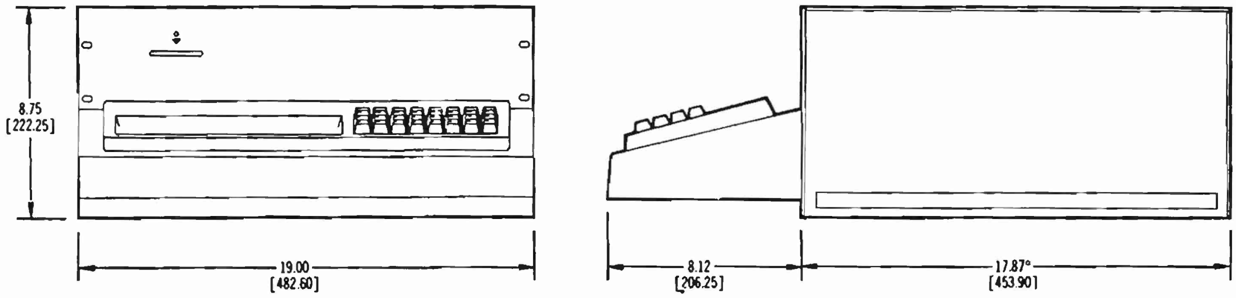


RACK MOUNTING

MAC530** microaccesscontroller/ SAL500 systemactivitylogger



MAC540 microaccesscontroller



RUSCO ELECTRONIC SYSTEMS SALES & SERVICE CENTERS

SALES OFFICE	TELEPHONE NO.
Albany	(518) 459-6593
Atlanta	(404) 325-1025
Boston	(617) 543-4891
Charlotte, N. C.	(704) 535-4120
Chicago	(312) 833-0720
Cincinnati	(513) 771-6297
Cleveland	(216) 835-4288
Dallas	(214) 690-3640
Denver	(303) 758-9233
Detroit	(313) 553-9320
Hartford	(203) 633-8379
Houston	(713) 777-5254
Indianapolis	(317) 788-4649
Kansas City	(913) 649-3704
Los Angeles	(213) 725-1411
Milwaukee	(414) 784-6850
Minneapolis	(612) 894-8040
New Orleans	(504) 835-0713
New York	(201) 343-7100
Philadelphia	(215) 331-5313
Pittsburgh	(412) 884-7540
Portland	(503) 225-0028
Rochester	(716) 473-1830
San Antonio	(512) 692-0141
San Diego	(714) 297-5173
San Francisco	(415) 858-1000
Seattle	(206) 575-1350
St. Louis	(314) 231-8622
Tampa	(813) 248-4955
Washington, D.C.	(703) 821-3763

RES RUSCO ELECTRONIC SYSTEMS
A DIVISION OF ATO

HEADQUARTERS
P.O. Box 5005
1840 Victory Blvd.
Glendale, CA 91201
(213) 240-2540
Telex: 696318

Rusco Electronic Systems reserves the right to change this product and its specifications at any time without notice to improve its design or performance.

Patents issued and pending.

APPENDIX J

Vikonics Specifications

VIKONICS T.M.
SYSTEMS DIVISION

Using Technology Creatively
For Control Systems You Can
Depend on Today
— and Tomorrow.

TAC-1000

TOTAL ACCESS CONTROL SYSTEM

The Systems Division of Vikonics, Inc., a precedent-setting authority in the field of Advanced Security Control Systems, now bring you TAC-1000™ our latest and most advanced proprietary access control and alarm system.

The controller, the heart of the system, is a uniquely designed microcomputer, and its characteristics distinguish it from all others.

One TAC-1000™ controller can accommodate up to 128 magnetic card-readers and up to 1024 contact alarm points.

One of its distinguishing features is a front panel CRT display which communicates with the operator in English.

This easy to operate, low-cost system can function as a stand-alone security system or as a satellite to larger security systems and large main frames through standard serial communication lines.

PROGRAMMING

Programming functions are accomplished by means of 16-special-function pushbuttons located on the front panel.

TIME ZONES

Eight time zones per day are available. Each time zone is programmed with a start and stop time for each day of the week.

ACCESS LEVELS

TAC-1000™ offers up to 128 individually programmable access levels. Each access level can include any number of doors.

CARD INFORMATION

Each card to be used is programmed at the controller with identification number, access level and time zone.

MASTER CLOCK

Optional internal crystal controlled clock, which affords continuous operation in event of power failure, allows TAC-1000™ to keep a perpetual calendar, including year, month, day of month, day of week and time of day.

ACCESS CONTROL

Magnetic Card Readers may be installed at any entry point and as much as 1.5 miles away. The readers have a system code protection feature which assures card is the proper one for your system, then allows transmission of card number to controller for processing.

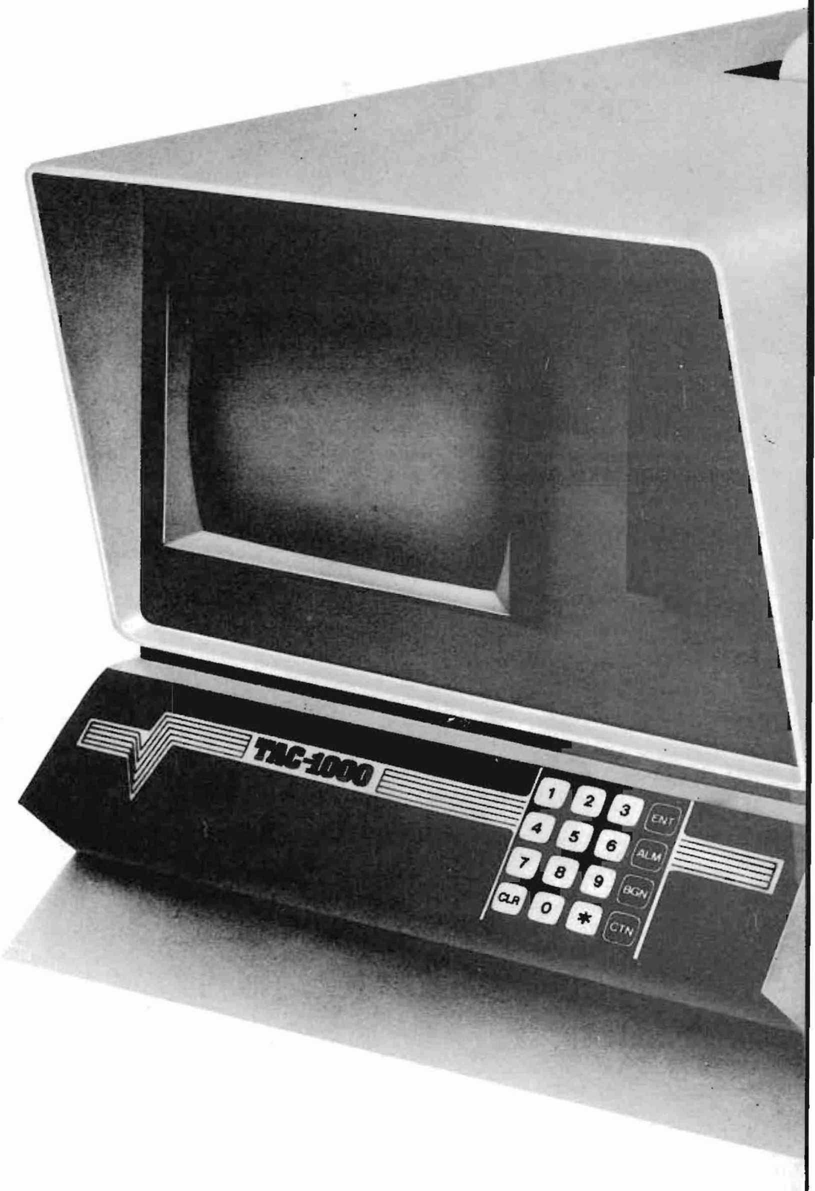
MULTIPLEXER

For remote locations up to 3 miles from controller, a multiplexer can be used. Each multiplexer can handle up to 16 card readers and alarm monitors in any combination. The multiplexer may be located up to 1.5 miles from controller and the readers or monitors may be up to 1.5 miles from the multiplexer. Hence, maximum distance is 3 miles.

For greater distances telephone lines driven by modems can be used.

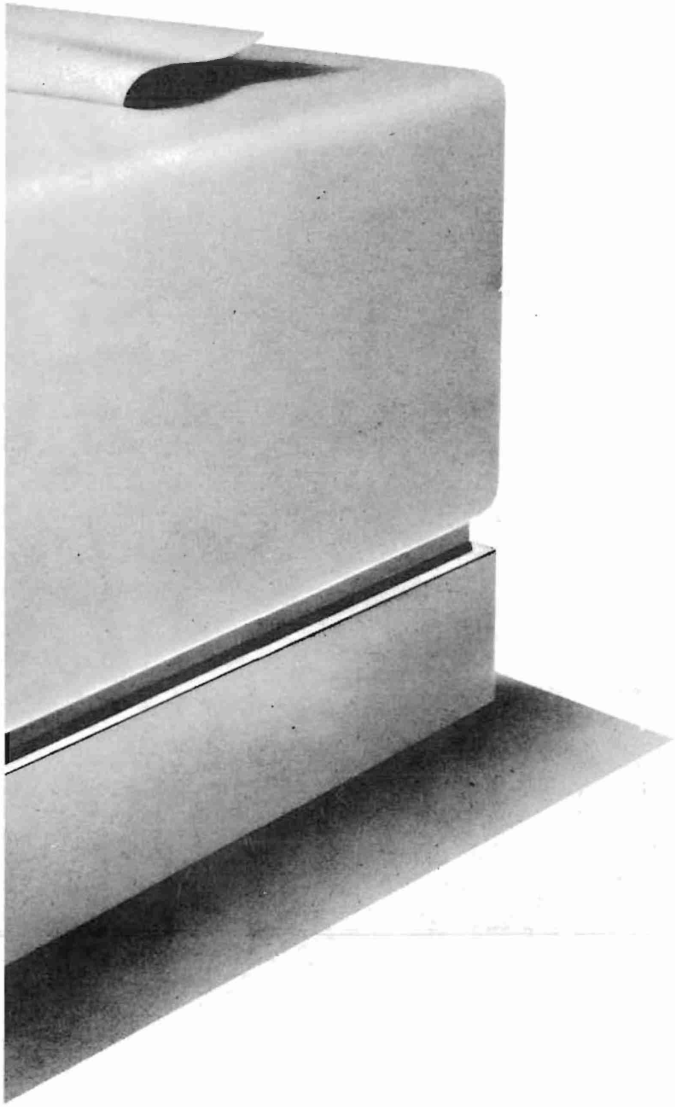
RESPONSE TIME

Maximum 1.5 second response time to all events under the worst case conditions.



"THE" ACCESS CONTROL SYSTEM

TAC-1000



FLOPPY DISK

Computerized data storage (floppy disk) allows for:

- permanent record storage
- communication with other systems
- on-line playback of history reports

CRT DISPLAY

The TAC-1000™ Controller features a front panel CRT display which interacts with the operator in English. It allows the system to guide the operator through each procedure with simple step-by-step instructions.

PANEL PASSWORD

To program the system, the operator must use a valid password entered on the keyboard.

ALARM MONITORING

Each magnetic card reader can accept 4 external alarm contacts. Also available are devices called alarm monitors which accept 8 alarm contacts.

OPTIONAL EQUIPMENT

PRINTER

An 80-column alpha numeric printer provides apermanent paper record of all door accesses, alarm signals, and operator actions. All printouts are in understandable English.

LINE SUPERVISION

TAC-1000™ offers, as an option, full electrical line supervision to insure line integrity in ultra-high security applications.

KEY PAD CARD READER

TAC-1000™ offers Card Readers with a Key Pad. Each Card has a unique 4 digit code. 4 LED's are included in the face plate to identify "Insert Card," "Enter Code," "Entry Granted" and "Entry Denied." One state will light as appropriate.

SPECIFICATIONS

CENTRAL CONTROLLER

Voltage:	105 to 125 or 210 VAC
Frequency:	47 to 440 Hz
Power:	200 VA @ 120 VAC or 200 VA @ 220 VAC
Size:	18" Deep x 16" High x 17" Wide
Weight:	60 lbs.
Operating Temp:	0 ° c. to 70 ° c.
Pushbuttons:	16
Displays:	1 CRT Display Plus Remotes

MASS STORAGE

Type:	Single or dual floppy disk drive
Speed:	16,000 characters/sec.
Capacity:	80,000 characters/disk

CCTV ALARM PRIORITY SWITCHER

99 Cameras x 99 Monitors Maximum

CAPACITY

Card Readers:	128
Alarms:	1024
Relay Outputs:	2048
Card Numbers:	4,000
Time Zones:	8
Access Levels:	128

OPTIONS

MAP DISPLAY

256 Points Up to 4 Displays

PRINTER

Type:	Thermal
Speed:	45 char/sec.
Columns:	80

Vikonics Inc.

23 East 26th Street, New York, N.Y. 10010 (212) 685-7660 TELEX: 420-398

RACAL
The Electronics Group

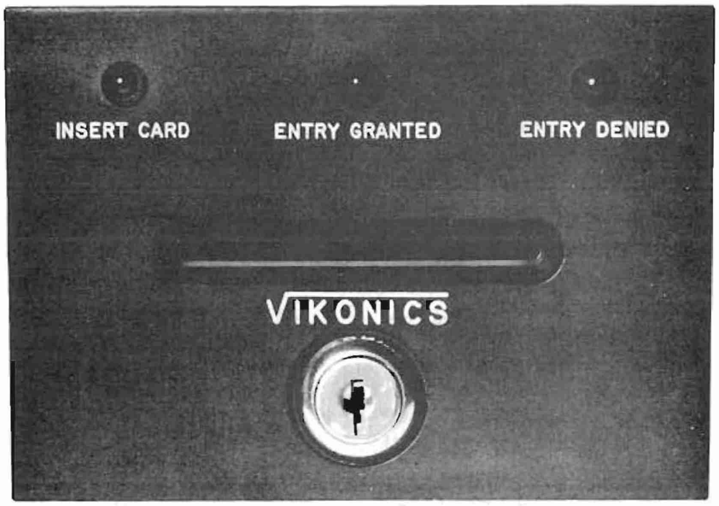
VIKONICS™

New Product Specifications

STANDARD CARD READER

Model VS—1020

The VIKONICS, Model VS-1020, standard Card Reader can control doors or other Access points. A card may be inserted when INSERT CARD is flashing. Once inserted, the Card Reader indicates either ENTRY GRANTED or ENTRY DENIED. The Card Reading cartridge is completely solid-state. A magnetically encoded, plastic encased, durable credit card size card is used. The entire system is designed for rapid response. The VIKONICS VS-1020 is virtually maintenance free and is easily installed.



FEATURES

Fully compatible with programmable Central Computer.

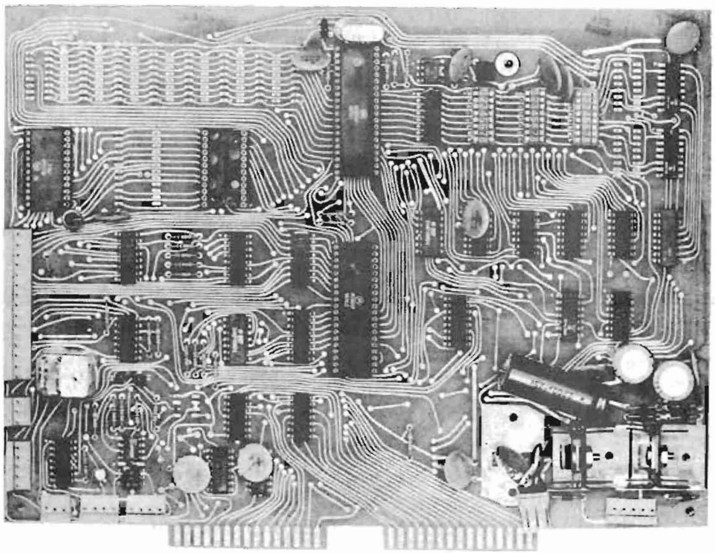
High speed data communications assures rapid response.

Heavy duty face plate lock prevents tampering.

Heavy duty ⁵⁄₁₆" milled aluminum housing.

Decorative, Flush or Surface Mounting.

Card Reader Electronics (Intelligent Interface) is tamper-proof and is placed in a secure location.



For Information Write:

Vikonics Inc.
23 East 26th St. • New York, N.Y. 10010 • (212) 685-7660 • Telex: 420-398

RACAL
The Electronics Group

SPECIFICATIONS:

Finish: Black baked enamel, scratch resistant surface.

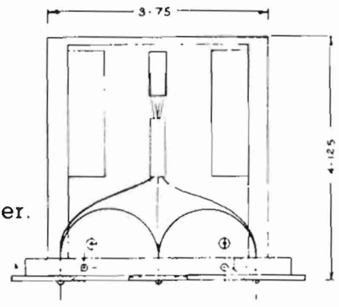
Temperature: 0-75 degrees C.

Mounting: Flush, Surface or Post

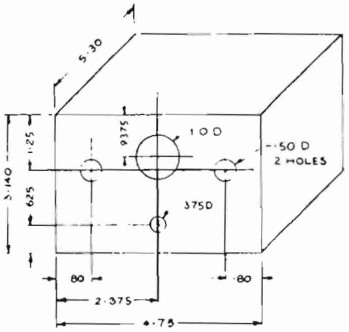
Connectors: 12 Pin Reader data and power+4 Pin LED data power.

Input Voltage: 5 volts at 15Ma.

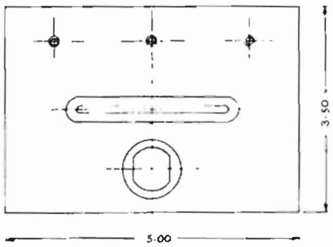
Response Time: Off-line—max 10ms
On-line—max.
1.5 seconds



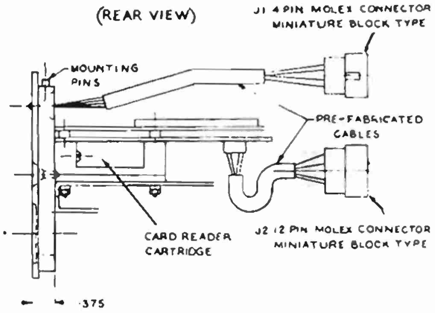
TOP VIEW



VS-1020 BACK BOX
(REAR VIEW)



CARD READER
FACEPLATE



SIDE VIEW

CONTROLLER INTERFACE

To insure total security, VIKONICS Interface circuits are mounted in a secured location near the Card Reader. They are housed in "NEMA" box or in a standard VIKONICS enclosure for indoor use. In both cases, enclosures are tamper-proof. In the stand-alone mode, the Card Reader and its interface can function without the Computer Controller.

INTERFACE SPECS

8 VAC a 11Ma, 8 VAC at 50Ma
and 16 VAC at 45Ma

Temperature: 0-75 degrees C.

Communication: Serial Asynchronous data at 1200 BAUD.

Connectors: 8 Molex Connectors, 2-each one 30 Pin edge.

PROGRAM FLEXIBILITY

Optional Push-button override for exit or door egress

Optional Local Audible Alarm and Reset.

Automatic Off-Line

Stand-Alone Capability

HOUSING:

"NEMA" type 4, 16"x16"x6" or VIKONICS 13"x11"x3"

APPENDIX K

Schlage Specifications

Access Control & Alarm Monitoring Systems

Schlage Electronics—The proven concept in proximity card access control and alarm monitoring

Effectively control and monitor access, and you've reduced security considerations to manageable proportions. Effective access control, however, must not only provide maximum protection, but should be convenient for authorized access and practical in cost. A big challenge, but one that we believe has been squarely met by the electronics technology and the systems approach developed by Schlage Electronics.

Thousands of successful applications—in business, industry, government and residential facilities—provide the working proof, day in and day out, that the Schlage Electronics access control system is both the most advanced and the most logical security concept on the market today.

Schlage Electronics is a Schlage Lock Company, a leader in security hardware for over 50 years, and a member of the world-wide family of Ingersoll-Rand International.

How It Works

The Schlage system operates by proximity. A hidden sensor reads a credit-card-size command card and transmits signals to a control unit, which regulates access, and if desired, to a printer, which records access and attempts.

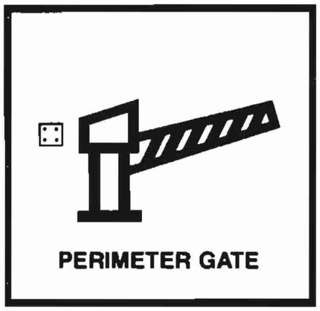
There are no conventional keys, key holes, card slots or push buttons. The system can be completely concealed, which in itself contributes to added security as well as aesthetics.

Access is gained by placing an authorized command key within 4 inches of a concealed sensor conveniently located near the access point. If the user is authorized for that door, or gate, at that time, the door will unlock. At the same time, the system can print the date, time, key code and the access location. Unauthorized attempts, while they will not unlock the door, may also be recorded and printed in red ink with an additional status code indicating the reason for rejection. Some systems have the additional capability to monitor a number of contact points and alarm conditions which may arise from unauthorized tampering, forced entry, and doors open too long.

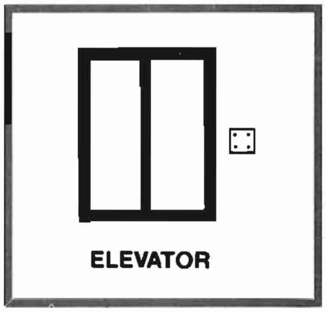
You program the system to suit your needs—by individual command key, by access point, by time. Any command key can be voided immediately or access status modified by simple entry of data on a standard keyboard terminal.

Proximity Access Control Systems with . . .

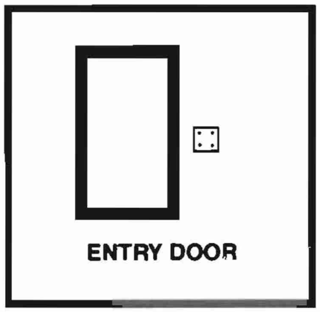
- Computer-controlled efficiency
- Alarm monitoring and processing
- Programming and reporting capabilities



PERIMETER GATE



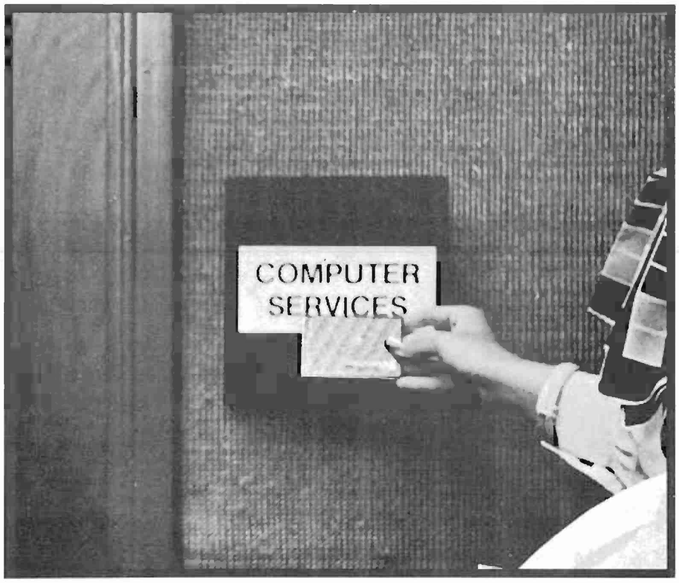
ELEVATOR



ENTRY DOOR

AUTOMATIC DOOR

Schlage Electronics units are commonly used to control private parking gates, to control access to plants, computer rooms, and even apartments and dormitories to provide a convenient, low-cost **first level** of security with minimal equipment.



Nothing to vandalize or "attack"

The ideal access control system protects itself while it's protecting you. The Schlage Electronics access control system has become known as "The Hidden Alternative." There need be no visible mechanism at the point of entry. The sensor is a small flat encapsulated unit which can be completely concealed within a wall, plaque-mounted on the surface, or attached behind glass or in the door itself.

A single coaxial cable connects the sensor to the control unit which may be located in an interior secure zone. Installation of both sensors and connecting cable—which represents about a third of the wiring necessary for some systems—is not only concealed, but simple, fast and inexpensive.

Flexibility

Schlage offers practical access control ranging from a single access point control to a computerized system covering hundreds of access points and thousands of users.

Schlage Electronics units are commonly used to control private parking gates, to control access to plants, computer rooms, and even apartments and dormitories to provide a convenient, low-cost **first level** of security with minimal equipment.

At more advanced levels, the Schlage system is **modularly expandable** and can be integrated into existing or planned security and environmental systems requiring control of hundreds of access locations. Schlage systems can also monitor remote points; open and close contact switches; locate and record alarms or events.

A "User Oriented" System

The Schlage proximity system has achieved a high degree of user acceptance. The small command key fits easily in pocket or purse, or may double as a lapel ID badge, and can activate the access point without removal from pocket or purse or when hands are otherwise full. Because there are no key holes, card slots or push buttons to operate, the Schlage proximity system is fast.

Schlage Electronics Access Control Systems Feature . . .

- Options to control both ingress and egress with a single sensor.
- Anti "passback" capabilities.
- Individual card recognition and voiding capabilities.
- Self-contained unlocking power for electrical locking hardware.
- Flexibility in mounting sensors.
- Standby power capabilities for both locking devices and memory retention.
- Manual switch-controlled lockout or unlocking.
- Flexibility to be integrated with other building or life/safety systems.
- Tamper-resistant control units.
- Variable door unlock time.
- Alarm shunt capabilities.
- Contact point monitoring.
- Card authorization by time zone control.
- Hard copy and/or visual display of data transactions.
- 5-year warranty on command cards.

A partial list of satisfied Schlage customers includes:

New York Telephone
Northeastern Telephone and Telegraph
Foster Grant
Avis Rent-A-Car
Amfac
County of Santa Clara, California
Sambo's
Hallmark Card Shops
XEROX
University of Massachusetts
Ford Foundation
Convair, General Dynamics
Memorial Hospital, Houston
Coca Cola Co.
Texaco, Inc.
Fireman's Fund Insurance Co.
El Paso Natural Gas Co.
County of Nassau, New York Bureau
of Security
Hillsboro Community College, Florida
Playboy Club
Thomas J. Lipton, Inc.
Fort Wayne, Indiana Police Department
State of Illinois Office Building
Boston, Mass. City Hall
Pacific Northwestern Bell Telephone Co.
Western Conference of Teamsters
Del Monte Corporation
Union Bank
Iowa Mutual Insurance
General Electric Co.
Southern Bell Telephone Co.
U.S. Department of Transportation
General Services Administration
Honeywell, Inc
Westinghouse Electric Corp.
Southern Pacific Communications Co.
Ingersoll-Rand Co.
Ramada Inns
Dr. Pepper Co.
WTVT-TV
General Motors Corp.
Pacific Telephone Co.
Teachers Credit Union
Wildwood Apartments
Standard Oil of California
ITEL
PPG Industries, Inc.
Midas International
Towers Key Club
Southwestern Bell Telephone Co.
Escondido, California Police Department
South Jersey Port Corp.
Cooper Laboratories
Alexandria Hospital
Mellonics Systems Development Div.
Winston Churchill Schools

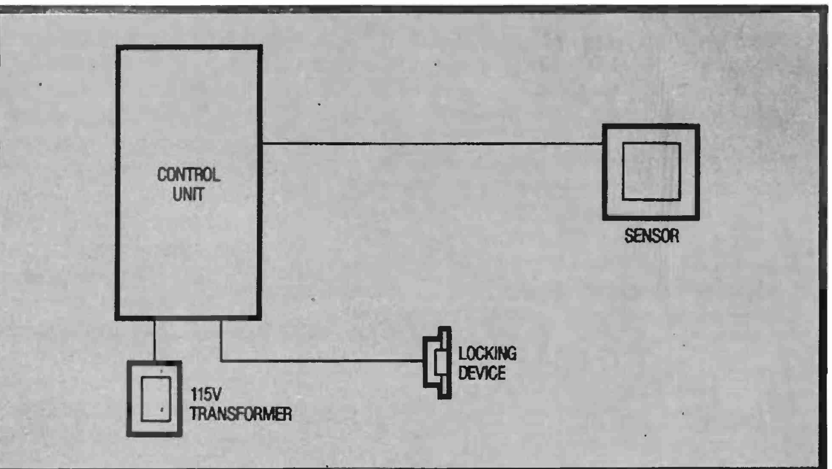
Schlage Electronics Systems Selection Chart

FEATURE	MODELS							
	114	**214**	**224**	**234**	**414**	**708**	**732**	**514**
INDIVIDUAL KEY CODE RECOGNITION	No	No	No	No	Yes	Yes	Yes	Yes
DOOR QUANTITY	1	1–10	1–10	1–10	1–8	1–8	1–32	1–256
ACCESS LEVELS	N/A	N/A	N/A	N/A	255	N/A	32	128
KEY CODES	3	1	6	10 individual 2 master	1500	*8000	*8000	5000
TIME ZONES	3	No	3	No	8	N/A	8	8
ALARM SHUNT	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ALARM MONITORING	No	No	No	No	No	Yes	Yes	Yes
PRINTER	No	No	No	No	Yes	N/A	Yes	Yes
CRT	No	No	No	No	No	N/A	Yes	Yes
BATTERY STANDBY	Option	Yes	Yes	Yes	Yes	Option	Option	Option
ANTI-PASSBACK	No	No	No	No	Yes	Yes	Yes	No
FAIL SOFT (DEGRADED MODE)	N/A	N/A	N/A	N/A	Yes	Yes	Yes	Yes
LOCK POWER	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VARIABLE DOOR UNLOCK	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

*For greater key codes, contact factory

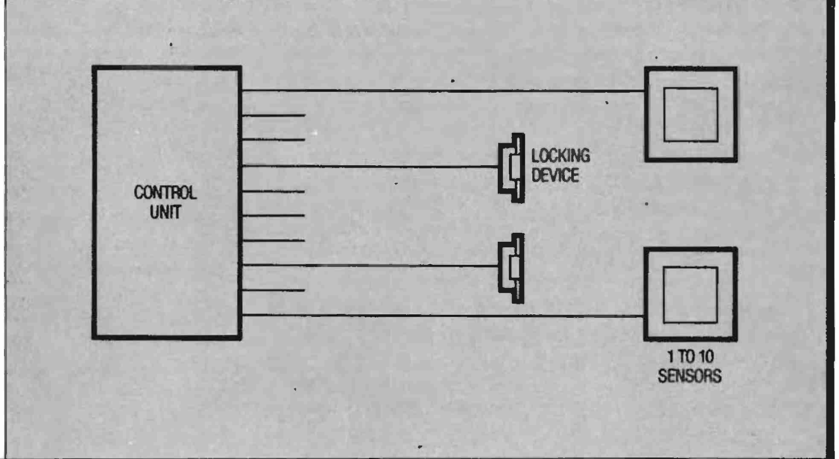
MODEL 114

Model 114 is designed to securely and conveniently control the locking hardware for a single door, gate or turnstile. A complete system consists of Schlage Command Keys, a sensor, a transformer, and a control unit. Features include three time zones, three code levels, alarm shunt and invalid key relay and standby output power.



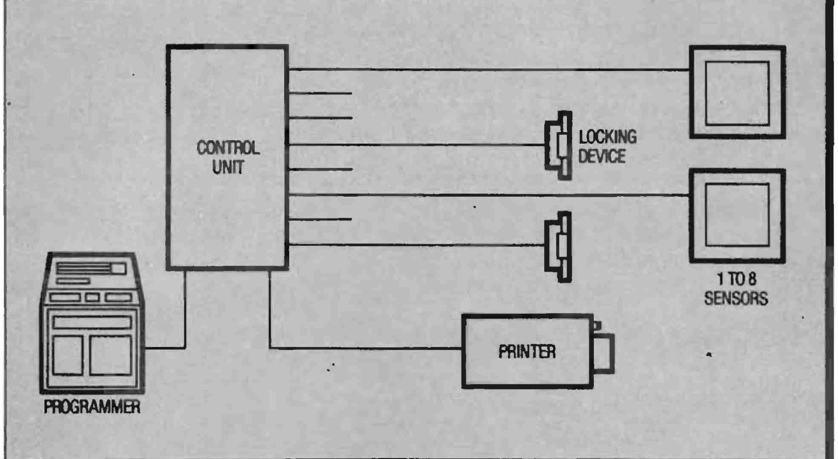
200 SERIES

Models 214, 224, and 234 are designed to securely and conveniently control the locking hardware for up to ten doors, gates or turnstiles. A complete system consists of Schlage Command Keys, sensors, and a control unit. Model 214 can be ordered with one key code valid for all ten doors. Model 224 can be ordered with one to six key codes, individually switch selectable for each door. Model 234 can be ordered so that each door is controlled by its own unique key code, plus a master and grandmaster key capability. Features include battery standby, lock power and alarm shunt capabilities.



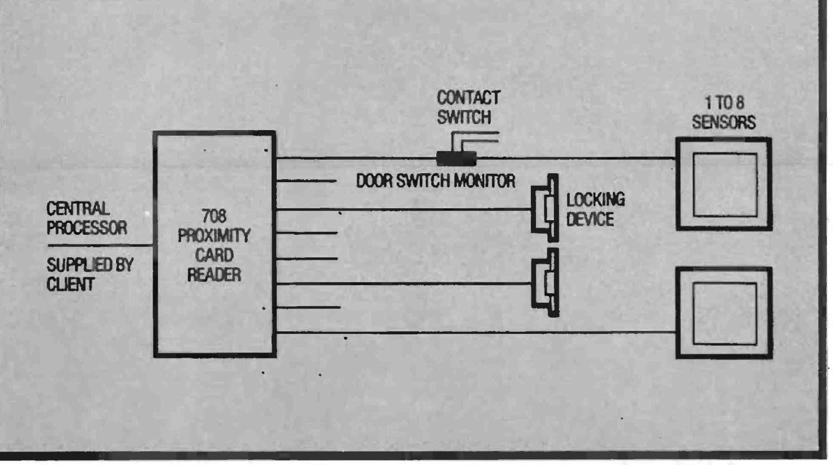
MODEL 414

Model 414 is designed to control—securely and conveniently—up to eight doors, gates or turnstiles and over 1,000 employees—by individual key code recognition, time of day, door and anti-passback status. A complete system consists of Schlage Command Keys, sensors (one for each door), control unit, system programmer and optional printer. Features include battery standby for memory and locks, lock power and alarm shunt capabilities.



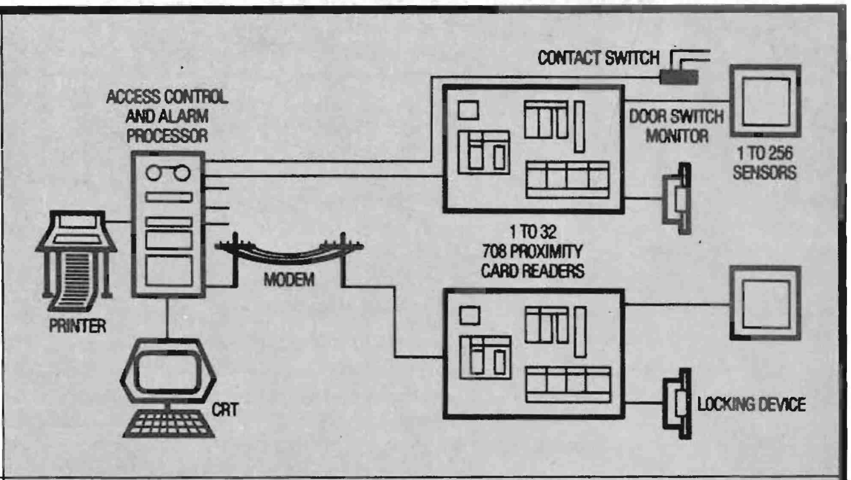
MODEL 708

The Model 708 Proximity Card Reader is designed to be part of a distributed access control and alarm processor system. The SE 708 reads the key code, door status, and sensor number and transmits the data to a central processing control unit via a full duplex ASCII data channel. The SE 708 receives commands from the central processor which may be door unlock instructions or other requests for action and response. Features include fail soft mode, lock power and complete set of self diagnostics.



MODEL 514

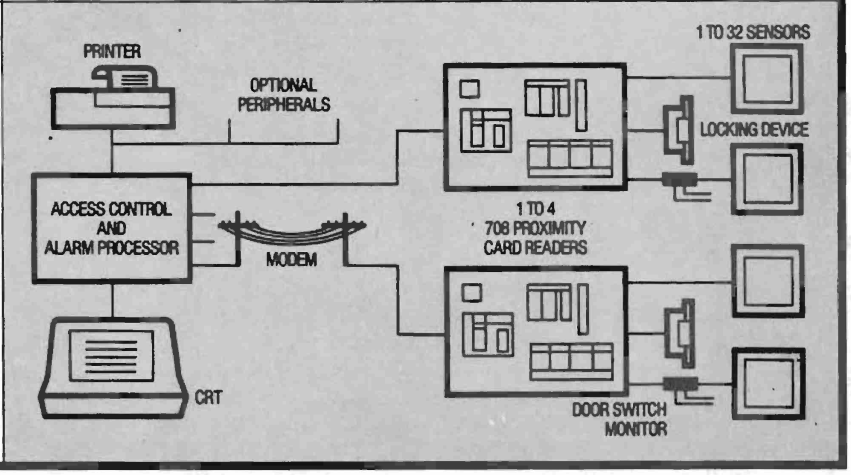
The Schlage Electronics Model 514 Access Control and Alarm Monitoring System is designed to control securely and conveniently up to 256 entrances and up to 5000 employees. Access is controlled by individual employee card code, by time of day and by authorized access levels. System 514 is comprised of a set of individually coded command keys (user cards), a central control unit, proximity card readers (Model 708), and remote monitoring terminals. Features include history recall and report generation.



MODEL 732

The Schlage Electronics Model 732 Access Control and Alarm Monitoring System is designed to control securely and conveniently up to 32 entrances and 8000 employees.* Access is controlled by individual employee card code, by time of day and by authorized access levels. System 732 is comprised of a set of individually coded command keys (user cards), proximity card readers (Model 708), a central control unit, an operator's terminal (CRT), and one or more printers. Features include English text printout, magnetic tape storage and alarm monitoring.

*See factory for larger key code requirements.



NOTE: Drawings of components do not represent proportional size relationships.

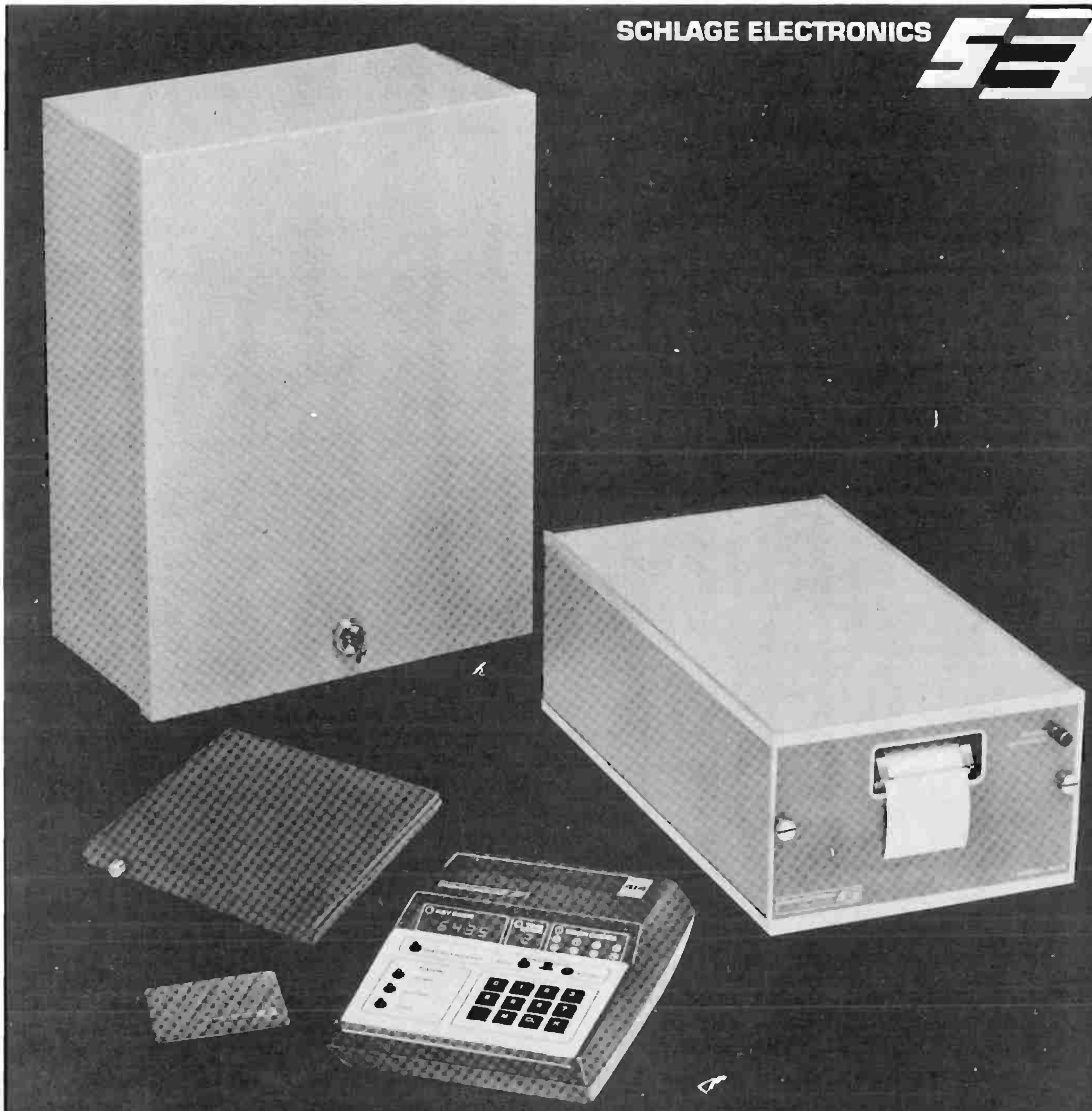
While there are standard models of Schlage Electronics access control systems, each designed to perform within specific parameters, the Schlage Electronics capability is best reflected in the "systems approach," uniquely applying the technology to your particular requirements. Authorized Schlage Electronics dealers worldwide are specially trained to install and service electronics access control systems and are backed by products listed by Underwriters Laboratories. We invite your confidential inquiry.

Call TOLL-FREE (800) 538-1755.
In California call (408) 736-8430.

SE SCHLAGE ELECTRONICS
1135 East Arques Avenue
Sunnyvale, California 94086
(408) 736-8430

International representatives—Europe: MAFSA, 12 Cadogan Place, Belgravia, London SW1, England, (01) 235-9658. Japan: Ingersoll-Rand, Japan Ltd., Kowa Building No. 17, 2-7 Nishi-Azabu 1-Chome, Minato-Ku, Tokyo 106 Japan, (403) 0641. Far East: Ingersoll-Rand Far East, 19th Floor, Lap Heng House, 50 Gloucester Road, Hong Kong, 5-270183. Canada: Esden Ltd., 1967 Leslie St., Don Mills, Ontario M3B 2M3, (416) 441-4100. South America: Crafting Services, S.R.L. Division Accesos Electronicos de Seguridad, Lavalle 1171, P.B. 1354 Buenos Aires, Argentina. Australia: Westinghouse Security Systems, 49-51 Wellington St., Windsor 3181, VIC, $319 1222, Australia. New Zealand: Harding Signal Ltd., P.O. Box 36007, Lower Hutt, New Zealand.

SCHLAGE ELECTRONICS



SE/414

Electronic Access Control System

SCHLAGE ELECTRONICS

Model 414 Electronic Access Control System

Hold a valid Schlage Electronics Command Key within inches of a sensor near your door...the door unlocks... and simultaneously the employee number (key code), door number, date and time of entry are permanently recorded. You get individual electronic recognition...with absolute security and reliability. This "proximity operation" represents the ultimate in user convenience, security and ease of installation, by removing card slots, key holes and pushbuttons. In other words, there's nothing to attack.

Schlage Model 414 Electronic Access Control System

is designed to control—securely and conveniently—up to 8 doors, gates or turnstiles and over 1,000 employees —by employee recognition, time of day and door. A complete system consists of Schlage Command Keys, sensors (one for each door), control unit, system programmer and optional printer.

Command Key is an electronically coded card. By simply bringing it within 2 to 6 inches of a sensor located near the door to be unlocked, the system is actuated almost instantaneously.

Sensor is a 7.5 inch square "Lexan" plaque, mounted adjacent to the door being controlled and connected to the control unit by a single coaxial cable. When a Command Key is presented, the Sensor "senses" the key code and sends it to the control unit for validation.

Control Unit contains the electronic circuitry, the authorized key code memory and power supplies for the locking hardware. If the Command Key being presented is authorized for that door, at that time, a signal is sent to unlock the door's electrically actuated lock or relay. If the Command Key code is not authorized, the system will prohibit access—and, if desired, an alarm will sound. The control unit may be mounted in a secure location anywhere within a thousand feet of the doors to be controlled.

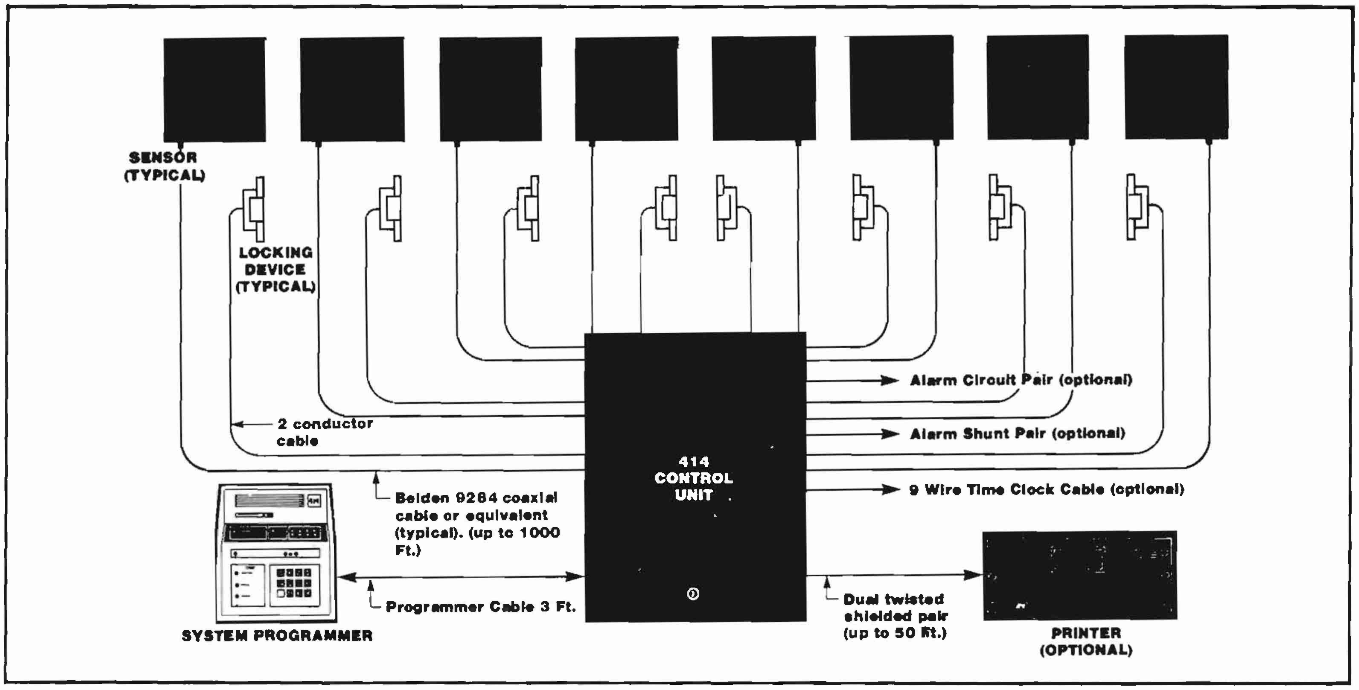
System Programmer enters authorized key codes, time codes, and door codes into the system or voids key codes previously entered. Operation of the programmer is as simple as using a hand-held calculator. When not in use, the programmer is easily removed for safe secure storage.

Printer provides a print out of all accesses and attempted accesses, recording key code, date, time of entry, and the door number. Invalid access attempts print out in red with an additional code number identifying why the attempt was invalid. This provides total information on all accesses and attempted accesses to your premises.

MAJOR FEATURES

The Model 414 Electronic Access Control System:

- Controls personnel access for up to 8 doors, gates or turnstiles.
- Has a memory capacity for over 1,000 individual key codes.
- Provides individual key code validation and positive "rule out" or voiding with no loss of memory capacity.
- Assigns access authorization by door (or doors) to each individual key code.
- Provides 255 access levels through the ability to assign any combination of doors to any key code.
- Assigns authorized time code to each individual key code. Up to eight time zones are defined and controlled by external time clock or manual switches.
- Is programmed through an easy to use system programmer, which may be removed and secured when not in use.
- Provides a selectable "Anti-Passback" capability tc prevent employees from passing back the card to other employees. This feature is switch-selectable and programmable by door.
- Contains built-in door unlocking circuitry to simplify installation and eliminate the need for power outlets to be installed at each door.
- Provides a selectable "fail-soft" operating mode. This feature is switch-selectable by door.
- Contains built-in battery standby power for both system and lock operation in the event of a line power outage.
- Allows control of both ingress and egress (if desired) with a single sensor at each door.
- Provides for selecting desired door unlocked time from 1 to 30 seconds.
- Provides for adjusting alarm shunt time from 5 to 30 seconds.
- Provides for adjusting the alarm time from 5 to 30 seconds.
- Provides a capability to manually unlock or lockout all doors through use of a single switch in the control unit.
- Provides a print out of all access activity, with the option of printing out only invalid access attempts and suppressing print out of all authorized accesses.
- Allows sensor to be installed in walls, on plate glass surfaces, or on external surfaces by using a vandal-resistant "Lexan" encapsulated sensor.

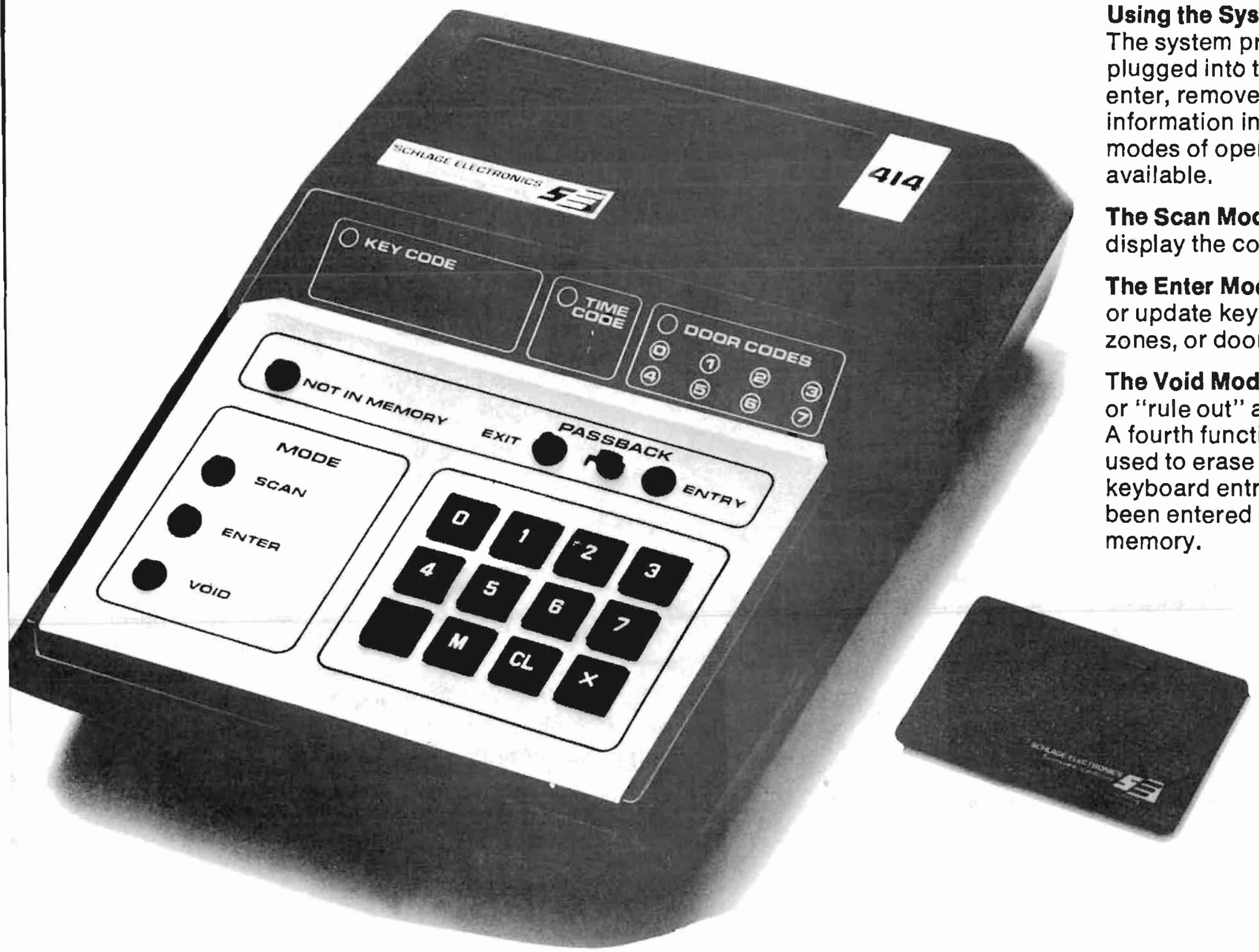

SENSOR (TYPICAL)
LOCKING DEVICE (TYPICAL)
2 conductor cable
Belden 9284 coaxial cable or equivalent (typical). (up to 1000 Ft.)
Programmer Cable 3 Ft.
SYSTEM PROGRAMMER
414 CONTROL UNIT
Alarm Circuit Pair (optional)
Alarm Shunt Pair (optional)
9 Wire Time Clock Cable (optional)
Dual twisted shielded pair (up to 50 Ft.)
PRINTER (OPTIONAL)

Simplicity and Security in one Easy to Install System.

System Programming

Prior to installation the user must determine and define the number of individual employees, the doors each is allowed to enter, and up to 8 time zones that can be used to regulate access.

Security log sheets are provided with the system on which are entered the name of each employee or user, his assigned key code, the doors he is authorized to enter, and the number of the time zone governing that employee's access.



Using the System Programmer: The system programmer is plugged into the control unit to enter, remove, or update access information in memory. Three modes of operation are available.

The Scan Mode is used to display the contents of memory.

The Enter Mode is used to enter or update key codes, time zones, or door authorizations.

The Void Mode is used to void or "rule out" a key code.
A fourth function key, Clear, is used to erase an incorrect keyboard entry before it has been entered or cleared from memory.

TECHNICAL SPECIFICATIONS

System Interconnections

Sensor to Control Unit: Single coaxial cable, up to 1,000 ft. (305 m), Belden 9284 or equivalent, with male F-56 or F-56A connectors.

System Programmer to Control Unit: Single cable 3 ft. (.9 m) in length, supplied with System Programmer.

Printer to Control Unit: Single shielded dual twisted pair cable 50 ft. (15 m) in length, supplied with printer.

Locking Devices to Control Unit: Two conductor cable, up to 1,000 ft. (305 m) in length. Contact your Schlage Electronics dealer for proper wire size for various length cable runs.

Command Key: The command key is credit-card size. Each key is electromagnetically encoded with a unique code which identifies the user whenever it is used to gain access. Each command key has a twelve character, alphanumeric identification number. The command keys do not deteriorate with age and can be reasonably flexed without damaging them. Command keys are warranted for 5 years.

Sensor: A transmit/receive antenna designed to concentrate energy within a few inches of the sensor surface. "Lexan" plaque 7.5 in. square by .67 in. thick (18.03 cm. x 1.7 cm.). The sensor attaches to the control unit via high quality CATV coaxial cable up to 1,000 ft. (300 meters) in length. Sensitive circuits within the sensor detect code data in command keys and transmit the code data to the control unit.

CONTROL UNIT:

Control Unit: Contains electronic circultry, memory, power supplies, alarm relay, alarm shunt relay, and terminals for door unlock power cables, sensor coaxial cables, time clock cable, printer cable, and alarm and alarm shunt wiring. The electronic assembly is mounted on a swing-out removable chassis, which is removed during mounting of the control unit enclosure.

Alarm Relay and Alarm Shunt Relay: Each provides one set of N/O and N/C relay contacts for connection to existing alarm system. Contacts are rated at 115V, 2 ampere resistive load.

Lock Power Output: Pulsed DC providing 32 VDC impulses of 10 millisecond duration 1 to 5 times a second, with a sustaining voltage of 6 volts nominal between pulses. Pulsed operation is designed to provide positive door unlocking even under conditions of heavy door wind loading or warped doors. Locking devices should be rated for 12 or 16 VDC operation and require not more than three amperes of current for an individual device or 15 amperes total load for up to 8 doors.

Systems Power: 115 VAC, 50 or 60 Hz to control unit. 220 VAC available on special order. Total system power consumption is less than 30 watts exclusive of unlocking power with batteries fully charged. If batteries are completely discharged, up to 80 watts will be required for a short period.

Timing:

Command Key response times:

Minimum: 150 milliseconds.

Average: 600-700 milliseconds (4 simultaneous requests).

Maximum: 1.2 to 1.4 seconds (8 simultaneous requests).

Door unlock period: Variable from 1 to 30 seconds.

Alarm period — Invalid access attempt: Variable from 5 to 30 seconds.

Alarm shunt period upon valid access: Variable from 5 to 30 seconds.

Standby Power System. Uses two 4½ ampere hour gell cell batteries with regulated charging. The system will operate for at least eight hours with approximately 100 lock actuations in the event of a power line outage. Memory will be protected for an additional sixteen hours, or for a total power outage period of 24 hours.

Enclosures: 14 guage steel with locked removable cover, anti-tamper switch, blue enamel. Dimensions: 16 in. L x 12 in. W x 8⅝ in. D (41 cm L x 31 cm W x 22 cm D). Weight: 39 lbs. (18 kg).

SYSTEM PROGRAMMER:

Used to enter, void out, or change allowed key codes, time zones, and door authorizations. Plugs into socket in control unit after removing control unit cover. Dimensions: 9 in. L x 6¾ in. W x 2¼ in. D (22.9 cm L x 17.1 cm W x 5.7 cm D). Weight: 1½ lbs. (.68 kg).

Keyboard: Contains eight numeric keys marked 0 through 7; and four function keys: **Write Key (red), Mode Select Key** marked **M, Clear Key** marked **C,** and **Execute Key** marked **X.**

DISPLAYS:

Data Entry: 3 display lights, indicating next data to be entered: **Key Code, Time Zone, Door Codes.**

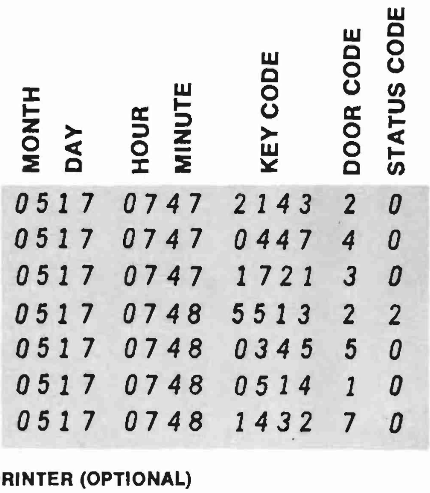
Key Code: 4 digits

Time Zone: 1 digit.

Door Authorizations: 8 display lights, one per door.

Mode Indicators: 3 display lights indicating current operating mode: **Scan, Enter, Void.**

Anti-Passback: 2 display lights: **Entry, Exit.**



MONTH	DAY	HOUR	MINUTE	KEY CODE	DOOR CODE	STATUS CODE
05	17	07	47	2143	2	0
05	17	07	47	0447	4	0
05	17	07	47	1721	3	0
05	17	07	48	5513	2	2
05	17	07	48	0345	5	0
05	17	07	48	0514	1	0
05	17	07	48	1432	7	0

PRINTER (OPTIONAL)

Printer requires 115 VAC 60 Hz power and requires approximately 40 watts. It receives data from the control unit over a shielded dual twisted pair cable up to 50 ft. (15 m) in length. Dimensions: 16 in. L x 8½ in. W x 5¼ in. D (40.6 cm L x 21.6 cm W x 13.3 cm D). Weight: 16 lbs. (7.27 kg).

Paper: The printer uses either fan-fold or roll paper with the paper storage located within the printer.

Print Drum: Each column of the 18-column print drum contains the characters 0 through 9.

Controls: The power switch and print controls are located behind the front panel. The paper advance pushbutton is located on the front panel.

Inhibit Switch: A key switch is mounted on the rear panel of the instrument. When placed in the "ON" position, the printing of valid accesses is inhibited. When in the "OFF" position, all data received by the printer is printed. Valid entries are printed in black ink; invalid attempted entries are printed in red ink.

ENVIRONMENTAL SPECIFICATIONS

All model 414 components will operate in ambient air having a relative humidity of 0-95%. Ambient temperature limits for model 414 components are as follows:

- **Door Sensors:** —50° F to 180° F. (—45.6° C to 82° C.)
- **SE Command Keys:** —50° F to 120° F. (—45.6° C to 49° C.)
- **414 Control Unit:** 20° F to 120° F. (—7° C to 49°C.)
- **414 System Programmer:** 20° F to 120° F. (—7° C to 49° C.)
- **Model 5010 Printer:** 20° F to 120° F. (—7° C to 49° C.)

SCHLAGE ELECTRONICS

A Schlage Lock Company • 1135 E. Arques Avenue
Sunnyvale, California 94086 • (408)736-8430
Call toll-free (800) 538-1755 • In Calif. call (408)736-8430

International representatives—Europe: MAFSA, 12 Cadogan Place, Belgravia, London SW1, England, (01) 235-9658. Japan: Ingersoll-Rand, Japan Ltd., Kowa Building No. 17, 2-7 Nishi-Azabu 1-Chome, Minato-Ku, Tokyo 106 Japan, (403) 0641. Far East: Ingersoll-Rand Far East, 19th Floor, Lap Heng House, 50 Gloucester Road, Hong Kong, 5-270183. Canada: Esden Ltd., 127 Sunrise Ave., Toronto, Canada M4A 1A9, (416) 751-5722. South America: Crafting Services, S.R.L. Division Accesos Electronicos de Seguridad, Lavalle 1171, P.B. 1354 Buenos Aires, Argentina. Australia: Westinghouse Brake and Signal Co., Stephenson St., Spotswood, Victoria 3015, Australia. New Zealand: Harding Signal Ltd., P.O. Box 36007, Lower Hutt, New Zealand.

APPENDIX L

IBM Specifications

IBM

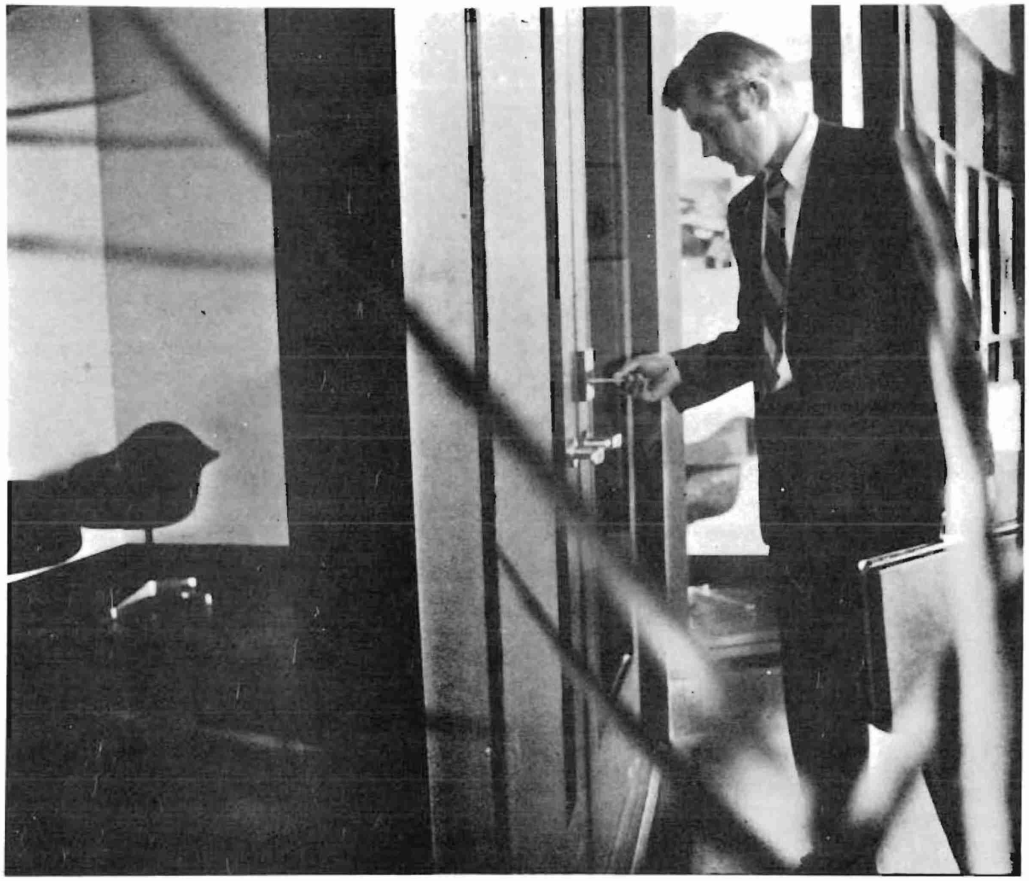
FIELD
DEVELOPED
PROGRAM

Program Number 5798-NQJ

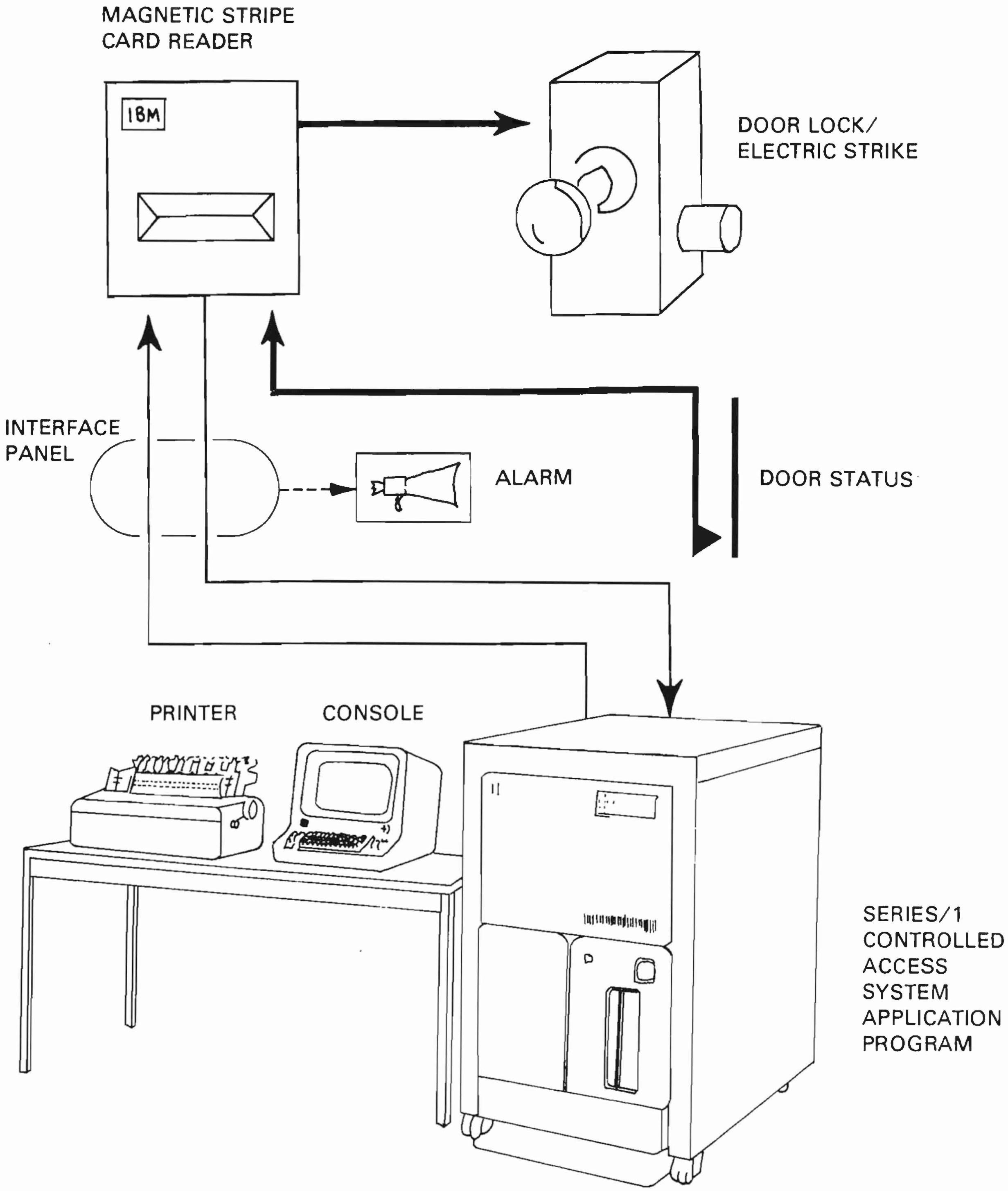
GB30-1175-1

March 21, 1978

IBM Series/1 Controlled Access System—1



Series/1 Controlled Access System-1 is a standalone computer-based access control system. The system uses an IBM Magnetic Stripe Card Reader, and cryptographically encoded, wallet size, magnetic stripe identification cards or badges to monitor and control entry and/or exit for a facility or restricted area. These IBM Magnetic Stripe Card Readers may be mounted in or near doors, turnstiles, gates, elevators, etc. in both indoor and outdoor environments.


MAGNETIC STRIPE
CARD READER
IBM
DOOR LOCK/
ELECTRIC STRIKE
INTERFACE
PANEL
ALARM
DOOR STATUS
PRINTER
CONSOLE
SERIES/1
CONTROLLED
ACCESS
SYSTEM
APPLICATION
PROGRAM

The system is designed to permit entry only to personnel who are currently authorized to enter the specific area. Access to as many as 63 points may be controlled by this system. Each of these points to which a badge reader is connected may be assigned to one of fifteen (15) access control classes or groups. Additionally, the basic system allows each of up to 1,000 individual magnetically encoded badges to be assigned to one or more of these classes or groupings. Up to 4,000 badges may be assigned, without program modification, by expanding the system storage capacity. The Controlled Access System-1 uses the IBM 4974 Bidirectional Printer for recording system activity, including: access data, invalid entry attempts, and monitoring violations, with time and date indicated for later audit or transcription purposes. Changes entered from the operator's console which affect badge, door, or time of day control information are recorded on diskette.

In addition to determining if a badge is valid in an area to which entry is being attempted, the Controlled Access System-1 maintains a list of cards that have been stolen or lost, notifies security personnel of unauthorized badge entry attempts, provides an emergency function to lock or unlock any one or all doors in the controlled system, provides the capability for immediate console operator validation or invalidation of each individual card, and also provides capability to detect and alarm if doors are opened or left open unintentionally for a greater than specified time.

Simple operation of the system is provided through use of the IBM 4979 Display Station as a keyboard console. The console operation is designed with menu selection and prompting so as to require very minimal training, even for the novice, to become comfortable and competent in operating the system. Indoor and outdoor models of the IBM Magnetic Stripe Readers (RPQ's — DO8140, DO8141, DO8142, DO8242, and DO8246) are supported by the system, thus providing for both 22-column badge or "Mr." Credit Card size badge (ID card) use and a variety of readers to meet specific installation requirements. This FDP, Controlled Access System-1 for the IBM Series/1, and the other systems components provide the user with an economical solution to his growing needs for greater and more flexible access control as a part of his overall security program.

HIGHLIGHTS

- Controls access authorization by door and security classification of the individual.
- Controls up to 63 separate entrances or devices, each with a magnetic stripe reader.
- Allows the assignment of 1000 unique identification numbers for determining the control and activity of any individual (up to 4,000 optionally without program adjustment.)
- The program is personalized by the customer to his specific user requirements and configurations by simple console display menu selection and abbreviated data insertion.
- On-line user education via display station screens provides quick reference information on all system functions.
- Simple keyboard display console commands to: validate, invalidate, change status of individual badges, or change status of one or more doors.
- Uses either 22-column or "Mr" credit card size magnetic stripe badges, including an option for pictures.
- Reads ten characters from ANSI 4.13 and 4.16 (ABA) Track II, cryptographically encoded magnetic stripe cards.
- Provides an optional printed log of entries by time of day, date, door, and badge number.
- Provides door monitoring for unauthorized opening and door sensing for proper closure after a valid access has occurred.
- Provides simple operator keyboard display console menu selection of display screens for operating and controlling system.
- Alerts security personnel of attempts to enter controlled areas without authorization.
- Latches and/or releases the doors in case of emergency, by console commands, thus allowing doors to remain closed or open to meet situation.
- Allows manual loading of predetermined setups of class and badge validations for evening, shift or weekend operating mode.
- Automatically checkpoints (i.e. saves user-entered data) every hour or when badge or door assignment data is updated, and/or monitoring and sensing assignment data is updated.
- Manual checkpoint capability is provided.
- Display console always indicates date and time, updated every 30 seconds.

- Individual doors may be assigned to one of fifteen (15) access classifications or groupings. The assignment may be changed from the operator's console to meet special situations.

- Continues to examine the status of a door with an outstanding monitoring or sensing alarm and alerts the operator when the alarm has been secured.

SYSTEM DESCRIPTION

The Series/1 Controlled Access System is an automated, computer-based system that works with magnetically encoded wallet-sized identification cards and magnetic stripe card readers to monitor and control doors, gates, turnstiles, elevators, etc., providing access control to restricted areas. Authorization can easily be added or deleted, activity logs maintained, door control specifications changed, and current status reports printed of the various system operating parameters, e.g., valid badges for an area, door control specifications, and lost badges. Alarm messages may be selectively printed containing current time, date, and identifying information for the particular point or function, for invalid or lost badge attempts, various door status conditions, or when a badge is inserted in a reader and it is outside the range of the system (a foreign badge.) An audible alarm also may be incorporated to alert personnel of the existence of the following alarm conditions: lost badge attempted use, a door never closed after a valid opening, and a monitored door alarm indicating an unauthorized opening of a door.

The IBM Magnetic Stripe Readers are simple electronic devices, which can be mounted on a door, wall or pedestal, and which sense the uniquely encoded data from the magnetic stripe and transmit the amplified signal by inexpensive telephone-type wires to the IBM Series/1. Some of the features of the IBM Magnetic Stripe Card Reader are: simple design that minimizes the exposure to accidental damages; possession of the card by the user all of the time, even when the card is fully inserted into the reader; asynchronous reading technique, which allows the data to be read over a wide range of insertion or withdrawal speeds.

The person desiring entrance to a controlled area inserts the card into the slot provided in the reader. If the Series/1 allows access, the door control mechanism or other device is activated and allows entry. It remains unlocked without alarming for the period of time determined by user-specified parameters.

If access is denied, the person attempting to gain entrance can insert the card again. Each time the card is inserted, the data is read and transmitted to the Series/1 for a decision and can be logged on the printer.

An interface on the card reader is provided to accept input from an optional door status switch. The switch conditions the data interface of the card reader to indicate a DOOR OPEN or DOOR CLOSED condition. Data from a card is not read if the door associated with that card reader is open. Note: if the switch is not used, the data is read at all times.

All data transmitted by the card reader and all control signals received by the card reader are over four wires. The maximum direct wire separation from the card reader to the Series/1 is five wire miles. For installations with more remote requirements, translators or modems allow distances greater than five wire miles over voice grade communications facilities.

A switching device is provided in the card reader to operate the door control mechanism. It can switch a maximum control voltage of 27V AC, one amp. This AC control voltage must be provided by the user at the card reader site.

SPECIFIED OPERATING ENVIRONMENT

PROGRAMMING SYSTEMS

This program was written using IBM Series/1 Control Program Support and assembler language. It has been assembled under the IBM Series/1 Base Program Preparation Facilities (5719-PA1) Version 1. There are no prerequisite licensed programs required to operate this program. The basic material, which provides object code on two diskettes, (one program diskette and one specification diskette), a Program Description/Operations Manual and a Physical Installation Planning Manual must be ordered. Additional copies of the program diskette (Feature Code 8700) may be ordered for use as back-up or as a convenient method of recording alternate access strategies. These diskettes may be used only on the same Series/1 CPU licensed to use this Field Developed Program.

NOTE: A separate license is required for each processor on which the license program materials will be used.

If modifications are desired, the Licensed Machine Readable Materials containing source and specifications modules and the following Licensed Programs are required as well as a Series/1 Development System. (See Development System Series/1 Configuration).

- IBM Series/1 Base Program Preparation Facilities (5719-PA1) Version 1.

- IBM Series/1 Standalone Utilities (5719-SC2)

- IBM Series/1 Control Program Support (5799-TAA) PRPQ P82508 Version 1 Modification Level 1 and its optional machine readable source material (Feature Code 3000)

- IBM Series/1 4979 Display Station Control Program Support (5799-TAE) PRPQ 82515 and its optional machine readable source material (Feature Code 3001)

- IBM Series/1 4991-201 Magnetic Stripe Badge Reader Control Program Support (5799-TAJ) PRPQ P82504

SYSTEM REQUIREMENTS

Minimum Series/1 Configuration for 1000 Badges and 31 Doors

Machine Type	Model or Feature	Qty.	Description
4955	C00	1	32K Processor
	3581	1	Diskette Attachment
	9136	1	Primary IPL
	3585	1	4979 Display Station Attachment
	5620	1	4974 Printer Attachment
	7840	1	Timers
	1560*	1	Integrated DI/DO
	4540	1	Rack Mounting Fixture
	9901	1	115 VAC Single Phase, 6' Cord
	9029	1	Application Code
4964	001	1	Diskette
	9901	1	115 VAC Single Phase, 6' Cord
4974	001	1	Printer
	9901	1	115 VAC Single Phase, 6' Cord
4979	001	1	Display Station
	9901	1	115 VAC Single Phase, 6' Cord
4997	01A	1	1 Metre Rack
	9901	1	115 VAC Single Phase, 6' Cord
	9197	1	First Rack

* Order 2 for 32-63 Readers

Notes:

1. For 4000 badge capacity, order feature 6325, quantity of 1, 16K storage addition under the 4955 machine type.

2. The 4979 Display Station and 4974 Printer Station are provided with a standard 20' signal cable. They may be extended up to 150 feet as an option.

3. Magnetic Stripe Readers, interface panel, and installation are in addition to the above system configuration requirements.

Development System Series/1 Configuration

The following minimum Series/1 system configuration is required in lieu of the minimum operational system shown above. If testing will be performed on the development machine, additional memory and sensor I/O features may be required.

Machine Type	Model or Feature	Qty.	Description
4955	C00	1	Processor (32K)
	3580	1	Disk Attachment
	3581	1	Diskette Attachment
	3585	1	Display Attachment
	5620	1	Printer Attachment
	5650	1	Programmer's Console
	7850	1	Teletypewriter Adapter
	2055	1	Teletypewriter 20' Cable
	7840	1	Timers
4962	002	1	Disk/Diskette Unit
4974	001	1	Printer
4979	001	1	Display Station
4997	01A	1	Rack Enclosure (1 meter)

A TTY-compatible terminal required to complete the configuration is the responsibility of the customer.

This FDP was developed to operate in conjunction with the following IBM Magnetic Stripe Card Readers:

RPQ D08140 - Magnetic Stripe Card Reader
RPQ D08141 - Magnetic Stripe Embossed Credit Card Reader
RPQ D08142 - Magnetic Stripe Extended Distance/External Environment Reader
RPQ D08242 - Magnetic Stripe Embossed Credit Card-Extended Distance/External Environment Reader
RPQ D08246 - Magnetic Stripe Card or Embossed Credit Card-External Environment Reader

Depending upon the reader, reverse read (i.e. read data upon card withdrawal) is supported as an optional feature.

Interfacing of the Magnetic Stripe Reader to the Series/1 requires separate central powering of the badge readers and signal isolation as well as other installation specifications noted in the Physical Installation Planning Manual. Installation guidance, the interface panel or the entire subsystem installation wiring (including the interface panel) may be contracted through IBM Sensor Based Installation Services (SBIS) or handled by the user himself using the installation planning material and specifications provided.

IRD (Information Records Division of IBM) and other vendors supply encoded cards in three varieties:

1. A solid plastic stock is provided with user-specified design and lettering.

2. Card stock may be combined with a printed or typewritten ID. This ID is then sealed into the badge with the appropriate cold or hot laminate sealer.

3. Card stock can also be used with a suitable camera which produces a photo ID suitable in size for inclusion within the badge. When cold or heat sealed, this produces a visual photo and machine readable ID. Badges can be 22-column or "Mr." Credit Card size.

CUSTOMER INSTALLATION TASKS

Successful implementation of Series/1 Controlled Access System-1 should involve careful and thoughtful planning and preparation. A total system not only includes a standard Series/1 configuration and the Controlled Access System-1 program, but also includes some number of Magnetic Stripe Readers, other controlling devices, and the necessary wiring to interface the readers.

In addition to normal Series/1 physical installation, there are several steps to consider in setting up or implementing the Controlled Access System-1:

1. Determine the needs for your facility.
   — How many doors must be controlled?
   — Which doors to be alarm monitored?
   — Are there any unique requirements?

2. Develop the physical planning (wiring and components) requirements for badge readers, door latch controls, etc.

3. Load and run the System Specifications Program to specify the facility's needs and generate badge ordering listing.

4. Order magnetic stripe badges.

5. Design, procure, fabricate, install and check out subsystem components and wiring.

6. Personalize the Controlled Access System-1 program to reflect the badge, class, and door data for your facility.

8. Educate employees, both operating and users, in the use of the system, magnetic stripe cards, and the readers, as applicable.

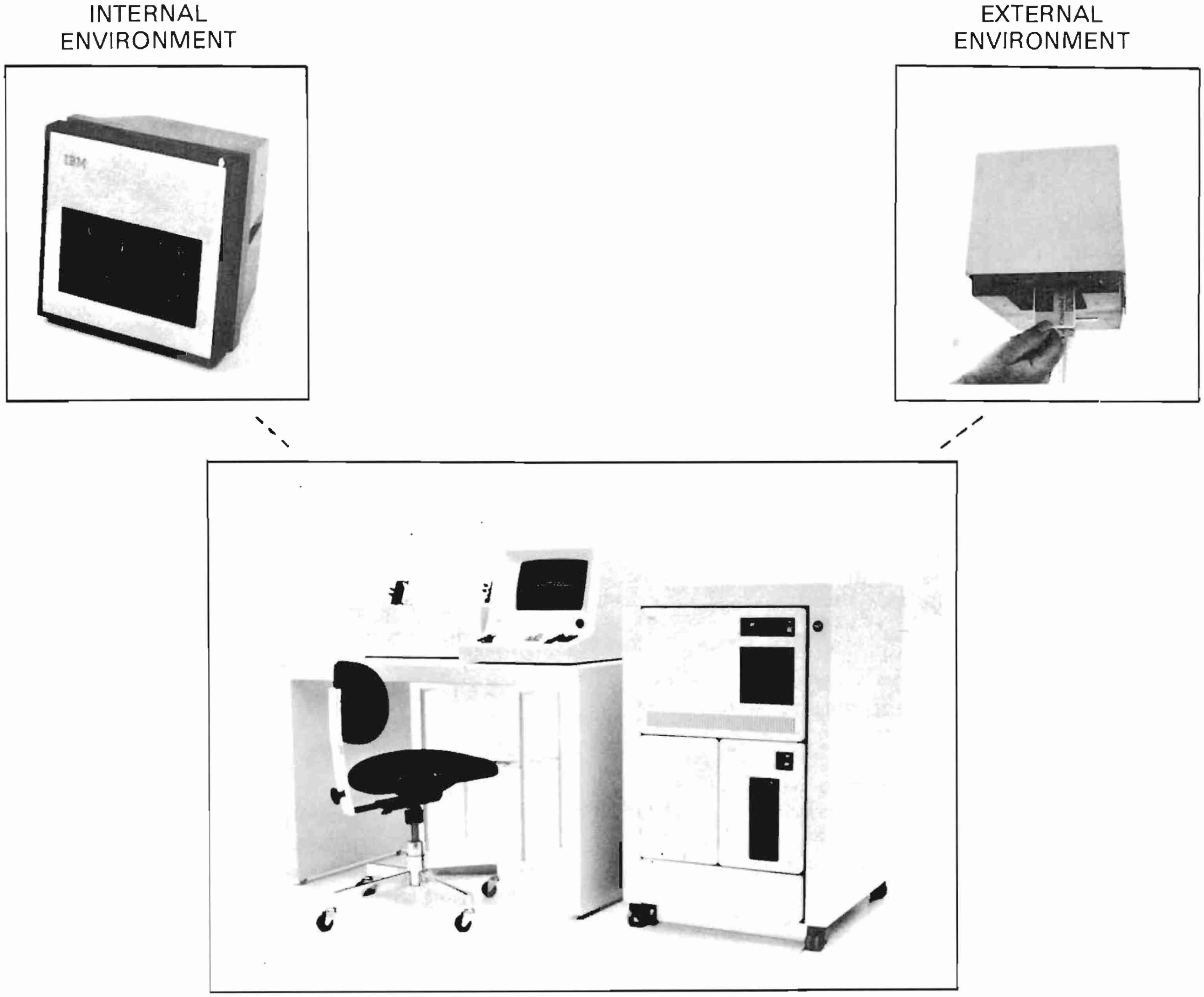
9. Create and maintain master list records of badges/cards.

The preceding steps apply to the installation of an unmodified version of Controlled Access System-1. If user-written application code is to be included, program assembly and link edit are required on a Series/1 development system configuration. See the modification section following.

A description of installation procedures is included in the Controlled Access System-1 Program Description/Operation Manual (SB30-1176) and the Physical Installation Planning Manual (SB30-1177). IBM Systems Engineering Services and Sensor Based Installation Services (SBIS) are available at a fee for guidance and assistance in implementation.

Reference Publications:

Series/1 System Summary	GA34-0035
Series/1 Physical Planning	GA34-0029
Series/1 Operator's Guide	GA34-0039
4979 Display Description	GA34-0026
4974 Printer Description	GA34-0025
4955 Processor Description	GA34-0021
4964 Diskette Description	GA34-0023



ORDERING INFORMATION

This program and its related documentation are scheduled to be available April 28, 1978. Contact your local IBM Branch Office to order this program.

BASIC MATERIAL

Unlicensed Documentation: One copy of the Program Description/Operations Manual, SB30-1176 and the Controlled Access Physical Installation Planning Manual, SB30-1177.

Licensed Machine Readable Material: One copy of the machine readable material which provides object code on two diskettes (one program diskette and one specification diskette).

To order this Basic Material use the following Specify Number:

Specify Number	Description	User Volume Requirement
9041	Diskette 1 @128 bytes/ sector	None

Additional Copies of PROGRAM DISKETTE (Object Code)

Licensed Machine Readable Material: A maximum of ten copies of the program diskette may be ordered.

In order to accommodate those customers who do not have the in-house capability to generate copies of the program diskette (object code), up to ten additional copies of the machine readable material may be ordered for backup and to permit offline storage of alternate access strategies for use on the same processor.

Distribution of the program diskette requires entry of a quantity and the feature listed below.

Feature Number	Distribution Medium	User Volume Required	Process Charge*
8700	Diskette 1 @128 bytes/ sector	None	$16/Copy

The quantity specified in the order as well as associated charges will be recorded and repeated automatically for future releases or until changed by the customer.

OPTIONAL MATERIAL
(SOURCE CODE)

Licensed Documentation: One copy of the Systems Guide, LB30-0940.

Licensed Machine Readable Material: One copy of the machine readable material containing source code.

Distribution of the Optional Material (Source Code) requires entry of the feature listed below.

Feature Number	Distribution Medium	User Volume Required	Process Charge*
3041	Diskette 1 @128 bytes/ sector	None	$93

Monthly Charge: $145

Payment Period: 12 continuous months

Unless a later ship date is requested, orders will be scheduled for shipment the Friday of the week following AAS order entry.

All monthly license charges shown are provided for information and are subject to change in accordance with the terms of the Agreement for IBM Licensed Programs.

Type	Program Number/AAS
5798	NQJ

Location license does not apply.

Installation license does not apply.

Testing period: One month

CHARGES FOR ADDITIONAL COPIES OF DOCUMENTATION

Licensed Documentation: The Systems Guide. For customers who must already be a licensee of the program, order by Feature Number from PID. For IBM Internal Use, order by Form Number only from Mechanicsburg.

Form Number	Feature Number	Price
LB30-0940	8604	$2.40

*One-time process charge includes service updates.

Unlicensed Documentation: The Program Description/Operations Manual (PDOM) and the Controlled Access Physical Installation Planning Manual (PIPM). Order from Mechanicsburg.

Form Number	Price/Copy
SB30-1176 (PDOM)	$7.80
SB30-1177 (PIPM)	$6.40

General Documentation: Order from Mechanicsburg.

Form Number		Price/Copy
GB30-1175	Availability Notice	No Charge

PROGRAM SERVICES

Central Service:
Available until April 30, 1979
Local Service: Not Applicable
Local Assistance: Not Applicable
Designated IBM Representative: Not Applicable

Warranted: No

If, within the service period, a problem is encountered which user diagnosis indicates is caused by a defect in the licensed program, documentation may be submitted to:

IBM Corporation
Series/1 Field Technical Support Center
Department 93E/002—3
P. O. Box 1328
Boca Raton, Florida 33432

Through the program authors IBM will, without additional charge, respond to a reported defect in the current unaltered release of the licensed program by issuing known defect correction information to the customer reporting the problem and/or issuing corrected code or notice of availability of corrected code. However, IBM does not guarantee service results or represent or warrant that all defects will be corrected.
All charges shown are provided for information and are subject to change.

This Program is distributed on an "as is" basis, without warranty either express or implied. Successful implementation depends solely on the customer's ability to integrate each program into his total inventory of "in-house" produced programs, including his acceptance of full maintenance responsibility. While each offering has been reviewed by IBM for its transferability and maintainability, no assurance of successful installation can be given.

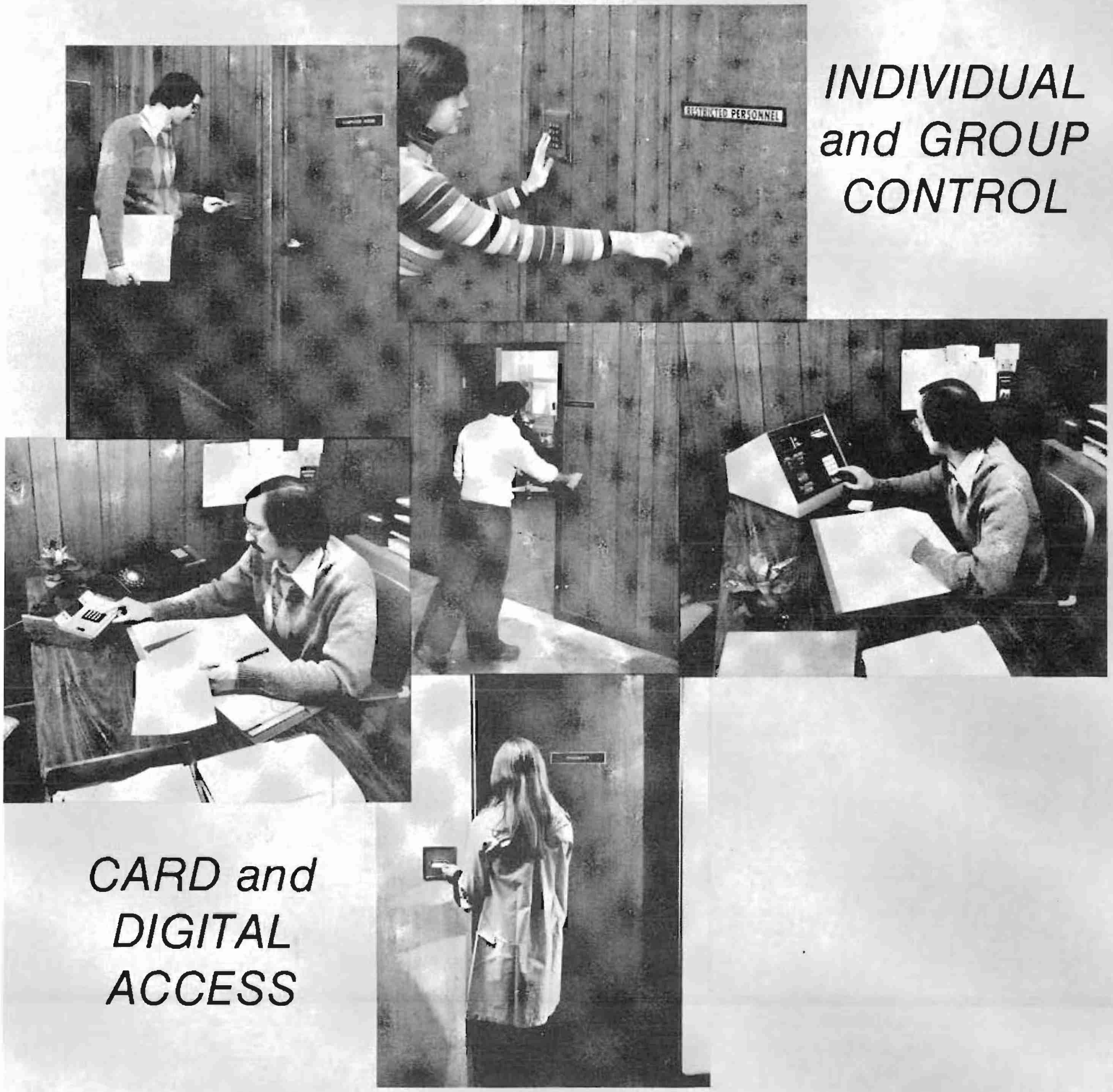
APPENDIX M

APD Specifications

APD

SECURITY SYSTEMS

division of: Automatic Parking Devices, Inc.
24700 Crestview Ct., Farmington Hills, Michigan 48018
(313) 477-2703 or, toll free, 1-800-521-9332
TWX 810-242-9369 APDSS FMHL



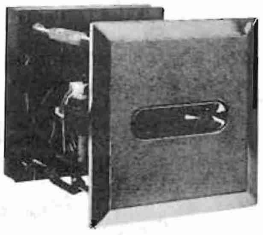
INDIVIDUAL and GROUP CONTROL

CARD and DIGITAL ACCESS

"INTEGRITY and RELIABILITY"

BSL-1000 SERIES

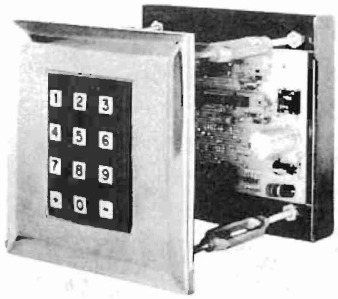
Security Lock



The BSL Card Lock is a completely solid state lock with low power operation designed for building security applications. Each BSL has 15 separate codes available which are determined by miniature code switches mounted on the unit. The flexibility of the unit allows the usage of more than one code at a time which can be used to control groups of people or individuals up to fifteen. Anti Pass Back feature available on similar unit designated as an ARL card lock.

SELECTRONIC 420

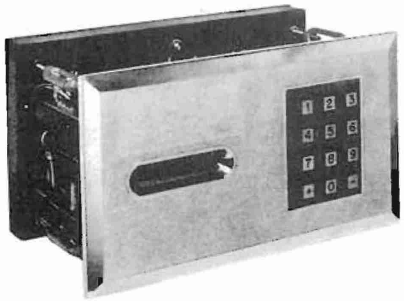
Code Combination Lock



The Selectronic 420 is a push button combination lock system which allows programming of an individual code by means of code selection switches. Codes may be changed easily to accommodate particular applications. The Selectronic 420 eliminates the necessity of carrying cards or keys yet provides a safe and reliable access system.

SELECTRONIC/ LOCK 1420

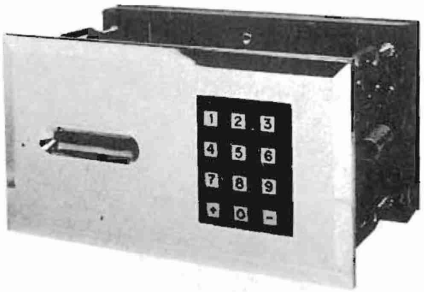
Double Security



The Selectronic Lock 1420 provides double security by combining the finest features of our Selectronic 420 and the BSL 1000 Series card locks. Access is gained by means of the correct code combination and the properly encoded magnicard being used. Codes are easily changed for either unit by a selection of switches at the rear of the unit. A selection switch is provided to allow the individual usage of the card lock and Selectronic or both independently.

IDC/484

Individual Digital & Card Combination Lock



The IDC/484 Individual 4 Digit Access Controller is used in conjunction with the ROL Card Lock or the off line and on line Memory Control units. The interfacing of these units provides maximum security in that the user must first enter his own 4 digit code number and then insert his own individual control card. The go signal is determined by a mathematical comparison between the 4 digit number and the individual code within the card.

SECURITY KARDS

The APD Security Kontrol Kards come in two basic types, magnetic and differential optics. Standard APD Kontrol Kards are readily available for prompt delivery from our factory. Special custom Kontrol Kards are available upon request. Options are: Personalized logos, I.D. photo slots so you can place photos on kards, Hole punch for key chains or bull dog clips or embossed characters and multiple coding. Contact APD for your special requirements.

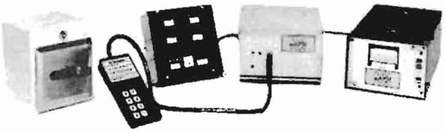
DIGITAL PRINT RECORDER

Model DP/500

The DP/500 Digital Print Recorder offers eighteen column capacity, with black printing for all valid entries and red printing for all invalid attempts. The unit prints out month & day, military time, location or station number and card number. The audit tape will give you a permanent record of all access activities within your facility. The DP/500 Digital Print Recorder can be easily interfaced with any of APD Security Systems' equipment.

ON LINE CENTRAL MEMORY

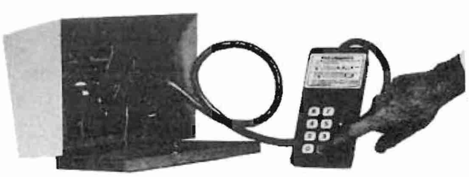
710 Series



The Memory Central is simply designed to allow total expandibility of security needs to any size. The system utilizes the APD Model 731 or 732 on line Memory Reader. Additional readers can be added to the system by using the APD Model 733 Expander. The Memory Central has a capacity of up to 8,000 kards. The kards used are the APD Optic Kards. For programming an APD Model 743 hand held Programmer is inserted in a jack located on the Memory Central front panel. Other options that can be added to the Memory System, like the Digital Print Recorder can be easily plugged into an existing socket on the rear of the housing.

PROGRAMMABLE OFF-LINE READER

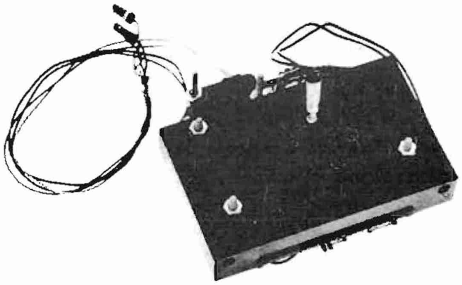
740 Series



The 740 Series Memory Kard Lock is a stand alone programmable unit capable of accepting individually coded kards. The kards used are the APD Optic Kards, which may be programmed in or out of Memory by a hand held model 743 Programmer. The 740 Series is an off-line unit which does not require any wiring back to a central unit. Many various options are available, including anti pass back, alarm shunt, time zones and printer interface. Standard capacities are 1,000, 2,000 and 4,000

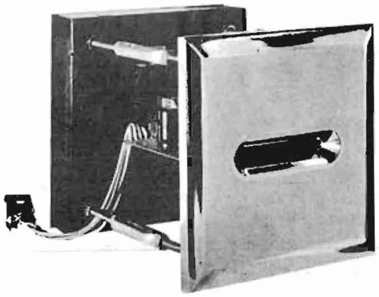
CCR-700

Common Code Reader



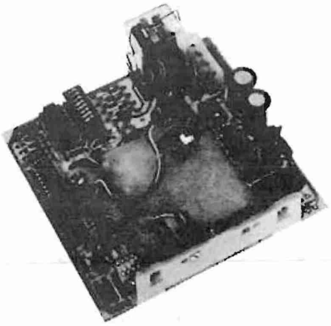
The APD CCR-700 Reader can be utilized as an inexpensive second reader when over all access is controlled by an individual programmer reader. The main function of the CCR-700 reader is to allow access to an entire group of Kards, rather than individual Kards. The Anti-pass-back option is also available with the CCR-700 unit.

ROL/SR ROL/100



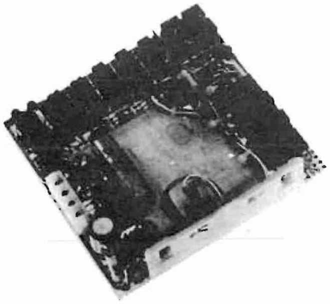
A communications reader which reads all of 4096 individual codes of a preset systems code. ROL/SR provides serial data output for interfacing to central processing unit by others. ROL/100 provides parallel data output for interfacing to central processing unit by others.

ROL/200



A solid state lock with relay dry contact outputs. Any combination of 7 codes easily selectable, plus up to 24 different systems codes available. Group control lock.

ROL/300

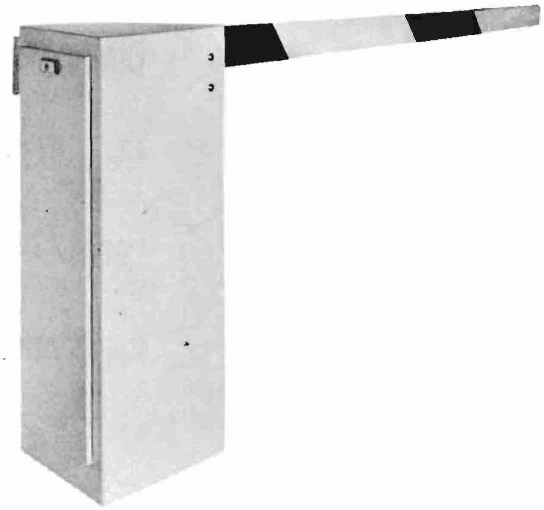


A solid state lock which has the ability to be programmed at the read lock itself. Any one of 4096 codes are selected by simply setting, the four 10 position micro dip switches to the desired number. Reads 24 bits of serial data encoded on an APD magnicard.

AVAILABLE OPTIONS

Surface or Flush Mount enclosures
Card lock stand
All weather or privacy hoods
Alarm
Cold weather
Power pack
Time zoning
Anti tamper alarm

Elevator floor control
Monthly group control
Anti pass back
Custom Kontrol Kards
Programmable security levels
Fuel Pump control
Invalid print.



A.P.D. SECURITY SYSTEMS

also handles a full line of Parking Equipment, featuring the G-89 Auto Gate (as illustrated). The Auto Gate can be used in conjunction with any Security Systems' products.

For additional information on your Security needs, please contact:

A.P.D. SECURITY SYSTEMS

24700 Crestview Ct.
Farmington Hills, MI 48018
Call: 313—477-2703

11782 Western Ave. Unit 3
Stanton, CA 90680
Call: 714—893-0550

. . . or for your nearest A.P.D. SECURITY SYSTEMS Representative:

WARRANTY

All new equipment sold by A.P.D. Security Systems is carefully inspected before shipment and is warranted against defects in material and workmanship for 90 days from date of shipment. Warranty covers repair or replacement of any part which has failed under normal usage. Fair wear and tear excepted. Transportation charges (if any) are to be paid by customer.

(Cut and Mail)

APD

Company Name: ____________________

□ Send Additional Literature

Name: ____________________

□ We are interested in a phone call

Our phone number is __________

Title: ____________________

Address: ____________________

□ We are interested in a personal visit

City: __________ State: __________ Zip: __________

A.P.D

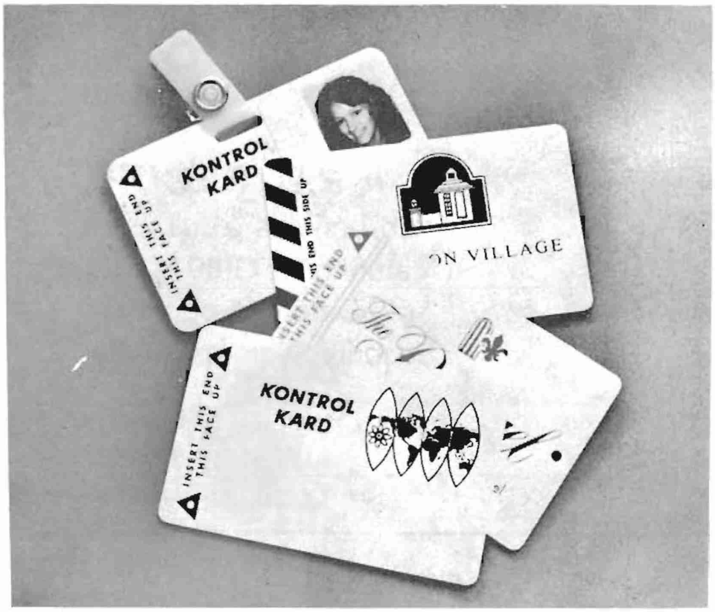
Security Kards

KONTROL KARDS

SECURITY SYSTEMS

- **Versatile**
- **Credit Card Size**
- **Security Pass**

- **Durable**
- **Identification**
- **Pedestrian & Parking Application**


KONTROL KARD
INSERT THIS END THIS FACE UP
INSERT THIS END THIS SIDE UP
ON VILLAGE
KONTROL KARD
INSERT THIS END THIS FACE UP

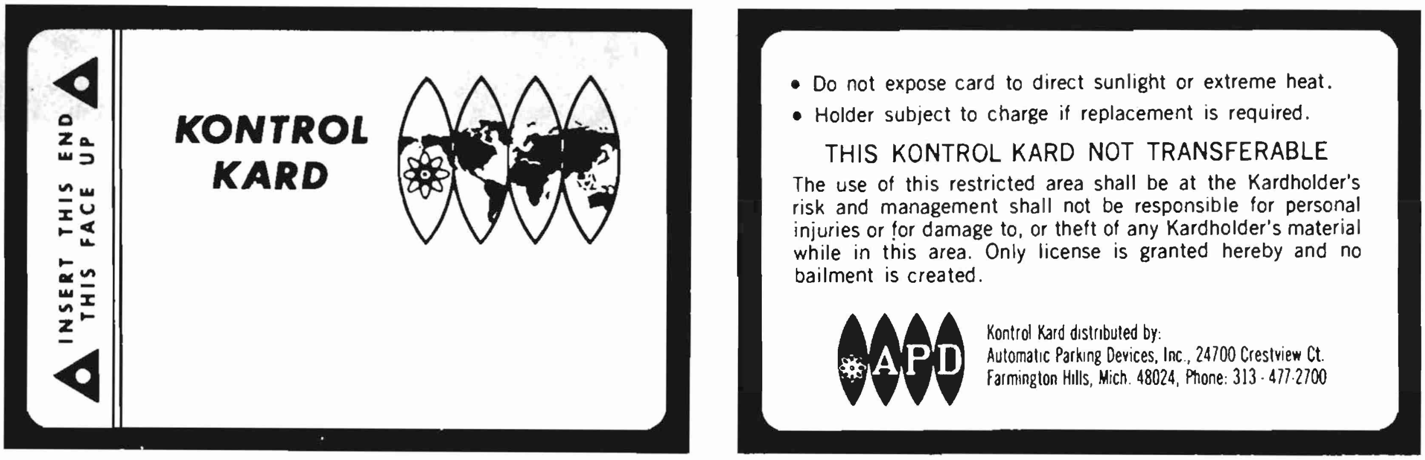
Shown with clip I.D., personalized artwork, keychain punch and personalized artwork and the standard Kontrol Kard

The A.P.D. Security Kard comes in two basic types, Magnetic and Differential Optics (Memory Card). The Magnetic card is referred to as "Magnicard". This card operates with all A.P.D. Security Systems R.O.L., B.S.L., Selectronic 1420 and ARL card readers. The card carries invisible magnetic coding that is virtually impossible to duplicate. It is embedded with a rubber bonded barium ferrite composite material which generates a strong magnetic field with a high resistance to de-magnetization. Cards are factory encoded upon order.

The Differential Optic or Memory Card operates with all A.P.D. Security Systems Memory Control units. This card contains light filters within the card. These filters allow for individual coding of the card and defy detection, duplication or alteration.

A.P.D. SECURITY SYSTEMS

24700 CRESTVIEW COURT
FARMINGTON HILLS, MI 48018   (313) 477-2703
TWX 810-242-9369   APDSS FMHL



INSERT THIS END
THIS FACE UP

KONTROL
KARD

- Do not expose card to direct sunlight or extreme heat.
- Holder subject to charge if replacement is required.

THIS KONTROL KARD NOT TRANSFERABLE

The use of this restricted area shall be at the Kardholder's risk and management shall not be responsible for personal injuries or for damage to, or theft of any Kardholder's material while in this area. Only license is granted hereby and no bailment is created.

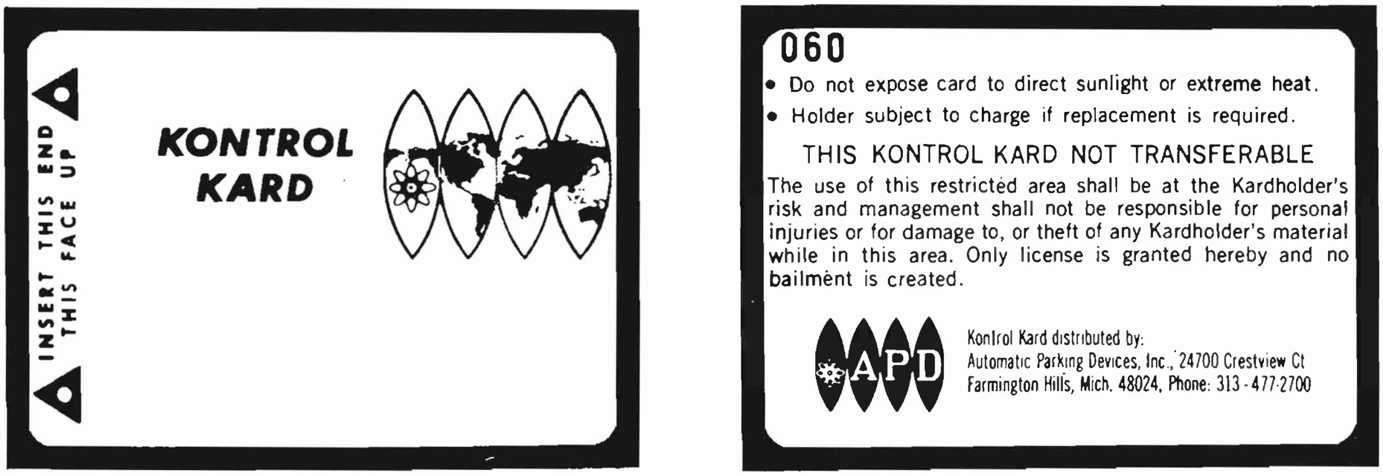
APD

Kontrol Kard distributed by:
Automatic Parking Devices, Inc., 24700 Crestview Ct.
Farmington Hills, Mich. 48024, Phone: 313 - 477-2700

Standard Magnetic control card shown actual size

PHYSICAL DIMENSIONS

CARD	WIDTH	LENGTH	THICKNESS
Magnetic Kards	2.125 in.	3.375 in.	.035 in. minimum .060 in. maximum
Optical Voider Kards	2.328 in.	3.250 in.	.025 in. minimum .040 in. maximum



INSERT THIS END
THIS FACE UP

KONTROL
KARD

060

- Do not expose card to direct sunlight or extreme heat.
- Holder subject to charge if replacement is required.

THIS KONTROL KARD NOT TRANSFERABLE

The use of this restricted area shall be at the Kardholder's risk and management shall not be responsible for personal injuries or for damage to, or theft of any Kardholder's material while in this area. Only license is granted hereby and no bailment is created.

APD

Konlrol Kard distributed by:
Automatic Parking Devices, Inc., 24700 Crestview Ct
Farmington Hills, Mich. 48024, Phone: 313 - 477-2700

Standard Memory control card shown actual size.

OPTIONS AVAILABLE

Personalized Logos
Individualized Cards
Magnetic Coding
Embossed Characters
Multiple Coding
Hot Stamping

Slotted for Clips
I.D. Photos
Multiple Colors
Signature Panels
Hole Punch for key chain
Serial Numbered

Except for the A.P.D. standard cards (illustrated on this sheet), all cards are custom made. For further information, please feel free to contact "A.P.D. SECURITY SYSTEMS."

WARRANTY

All new equipment sold by A.P.D. Security Systems is carefully inspected before shipment and is warranted against defects in material and workmanship for 90 days from date of shipment. Warranty covers repair or replacement of any part which has failed under normal usage, fair wear and tear excepted. Transportation charges [if any] are to be paid by customer.

Items illustrated on this sheet are subject to engineering design and/or appearance modifications which are production standards at time of shipment.

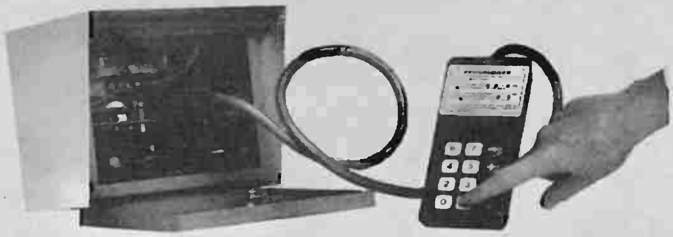
APD

SECURITY SYSTEMS

PROGRAMMABLE READER
740 SERIES

• Memory Card Lock •

- BASIC UNIT ACCEPTS UP TO 1000 INDIVIDUALLY CODED CARDS.
- MICRO-ELECTRONIC CIRCUITRY FOR SIMPLICITY AND LOW COST.
- LOW VOLTAGE OPERATION.
- OPERATES WITH DIFFERENTIAL OPTIC CARDS.



- PROVEN DESIGN—RELIABLE IN ENVIRONMENTAL EXTREMES.
- SIMPLE SURFACE OR FLUSH MOUNT INSTALLATION.
- NO WIRING TO A CENTRAL MEMORY UNIT.
- SOLID STATE DESIGN WITH NO MOVING PARTS.

The 740 Series Off Line is a card lock that can remember up to 4,000 different cards assigned to it. It is all done in one enclosure without wiring back to central control unit. You may assign, deny, re-assign, or void any card or group of cards, anytime. With an inexpensive external timer, you may allow certain cards to enter during one time period, and deny them during another, or there may be cards assigned to any time period.

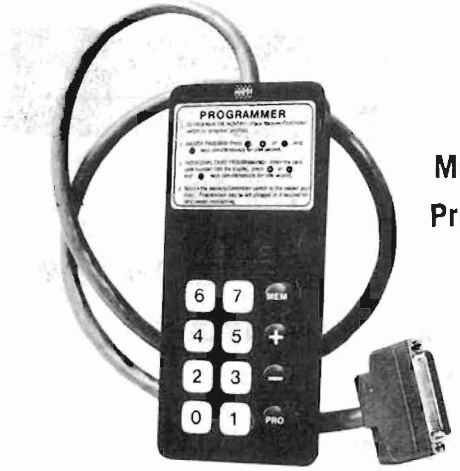
Voiding or validating cards from the 740 Series Memory Card Lock is accomplished by simply opening the front panel door, plugging in the hand-held programmer and entering the optic number on the keyboard. A bright four-digit display shows the number and its status. Just press two buttons and the card status can be changed.

The alarm shunt option allows card holders to pass in and out of alarmed areas without a special shunt key. If the door is opened by other means, the alarm will sound.

An optional unauthorized card alarm is available that will signal when a voided card has been inserted into the reader. This feature facilitates recovery of lost or stolen cards.

A.P.D. SECURITY SYSTEMS

24700 CRESTVIEW COURT
FARMINGTON HILLS, MI 48018 (313) 477-2703
TWX 810-242-9369 APDSS FMHL



Model 743
Programmer

740 CENTRAL STATION

The 740/CS is a remote program system by which, up to 250 off line memory units can be programmed from a single station and over a single twisted pair of wires. Programming is accomplished by addressing the desired memory lock to be programmed by a central station console.

Cards can now be entered or voided from memory by selecting the proper keys on the central station keyboard.

To enable the use of the Central Station, each 740 series reader must be equipped with a remote programming module. The RPM2 receives the program signals from the Central Station and acknowledges the acurate reception by energizing an audio "BEEP" at the Central Station.

**See price data sheet for available options.*

A.P.D'S MEMORY CARD

The heart of the Series 740 reader is the patented "Differential Optics" card.

The Memory Card is of wallet size and contains invisible optical coding that defies detection, duplication or alteration.

A variety of special cards are available to suit many requirements.

Cards are factory encoded upon order.

See "Security Kards" Literature sheet.

GENERAL SPECIFICATIONS

PHYSICAL DIMENSIONS	WIDTH	HEIGHT	DEPTH
Surface Mount Enclosure	12.0"	7.25"	6.25"
Flush Wall Mount Enclosure	9.5"	7.5"	adj.

Operational Temperature Range — +10°F to plus 125°F, without heater control.

Storage Temperature — Minus 25°F to plus 160°F.

ELECTRICAL SPECIFICATIONS

22-23 VDC @ 15 watts or 15-26 VAC @ 15 VA.

Output relay contacts rated @ 5 AMP, non-inductive, for inductive load switching (door strikes) use varistors cross contacts.

Battery may be stored in a cold location up to 15 months.

WARRANTY

All new equipment sold by A.P.D. Security Systems is carefully inspected before shipment and is warranted against defects in material and workmanship for 90 days from date of shipment. Warranty covers repair or replacement of any part which has failed under normal usage, fair wear and tear excepted. Transportation charges [if any] are to be paid by customer.

Items illustrated on this sheet are subject to engineering design and/or appearance modifications which are production standards at time of shipment.

APD

Digital Print Recorder

SECURITY SYSTEMS

• Black/Red Print • 18 Column Capacity • Programmable • Binary Code • Digital Logic • Events Counter • Internal Crystal Control Clock, prints time, date information • Easy visual identification • Paper Low Signal

The A.P.D. Security Systems Digital Recorder offers 18 column capacity, integral quartz clock, printing real or elapsed time and date counter.

The recorder features a printing rate of 2.5 lines per second nominal / wide variety of symbols / programmable floating decimal / "paper out" protection / programmable / black (valid) or red (invalid) print / TTL compatible, BCD input / programmable single or double spacing / systems output / automatic column blanking.

With the addition of the A.P.D. Security Systems Digital Recorder, it is immediately known as to which card was used, where, and when entry was gained or denied. For example, you have a printed record of the date, time and location of entry and card I.D., if you have a security force, the print recorder becomes your guard's partner. The recorder extends the guard's capacity by providing him with a completely automatic device that informs whether or not the entry was authorized. It also enables him to control many areas from a single location. If you don't have a security force, the print recorder provides you with information for documenting the access activities of your employees without implying restriction. The print recorder serves as a time recorder as well, giving you the exact time which a particular door was activated by a specific card.

A.P.D. SECURITY SYSTEMS

**24700 CRESTVIEW COURT
FARMINGTON HILLS, MI 48018 (313) 477-2703
TWX 810-242-9369 APDSS FMHL**

INVALID PRINT OPTION

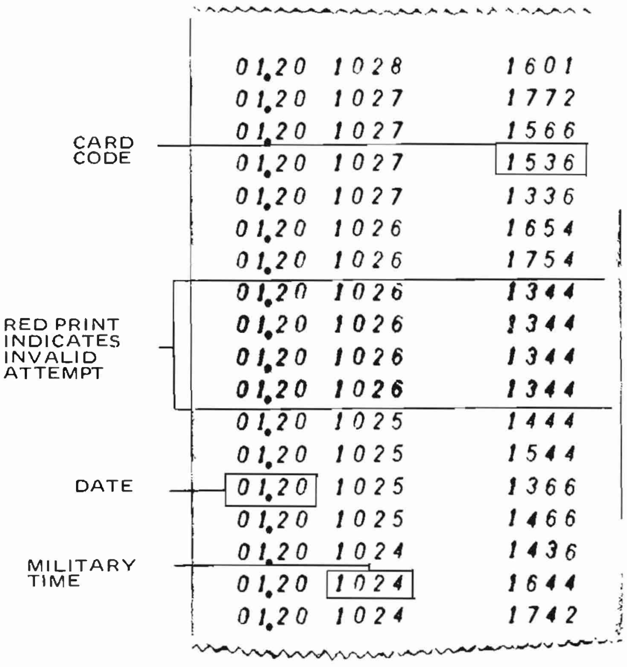
The Invalid Print Option or I.P.O., is an available option on the DP/500 Printer which allows the recording of only those attempts at entry which are denied. All valid entries are not recorded. The invalid information is printed in red and gives the same information that would normally be recorded. By simply flicking a switch the printer is put back into normal operation where all entries valid or invalid are recorded.

* *See price data sheet for available options.*

PAPER REQUIREMENTS

RP/500 Paper Tape
#3208-5004-00

EXAMPLE OF PRINTED DATA, OFF LINE:



CARD CODE
RED PRINT INDICATES INVALID ATTEMPT
DATE
MILITARY TIME

```
01.20  1028     1601
01.20  1027     1772
01.20  1027     1566
01.20  1027     1536
01.20  1027     1336
01.20  1026     1654
01.20  1026     1754
01.20  1026     1344
01.20  1026     1344
01.20  1026     1344
01.20  1026     1344
01.20  1025     1444
01.20  1025     1544
01.20  1025     1366
01.20  1025     1466
01.20  1024     1436
01.20  1024     1644
01.20  1024     1742
```

GENERAL SPECIFICATIONS

Width — 7.75" without mounting adapter

Height — 5.40"

Depth — 14.45"

Weight — 20 lbs.

Above dimensions do not include carrying handle or feet.

ELECTRICAL SPECIFICATIONS

Power Requirements — 105/125 VAC

210/230 VAC (switch on rear panel)

50 to 400 Hz, 25 Watts, nominal

INTERCONNECTION REQUIREMENTS

Output connection located on dual 25 pin connectors provided on rear of recorder.

OPERATING TEMPERATURE RANGE

0° to +50°C

WARRANTY

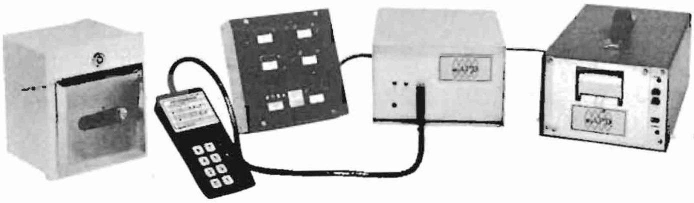
All new equipment sold by A.P.D. Security Systems is carefully inspected before shipment and is warranted against defects in material and workmanship for 90 days from date of shipment. Warranty covers repair or replacement of any part which has failed under normal usage, fair wear and tear excepted. Transportation charges [if any] are to be paid by customer.

Items illustrated on this sheet are subject to engineering design and/or appearance modifications which are production standards at time of shipment.

APD CENTRAL MEMORY 710 SERIES • On-Line System •

SECURITY SYSTEMS

- The printer option records every entry attempt. It records time, date, and location. Invalid cards are printed in red for quick recognition.
- A truly reliable centrally controlled access control system.
- The "dual memory" option eliminates multiple use of a single card. The card must be used for one entry, and one exit, in order to be valid for a second entry.



- The patented optical card readers permit speed of light data transmission. If the card is valid, the command to unlock the door occurs before the card is even to the back of the reader card slot.
- The central memory unit can accept any number of card readers with expanders.
- The Central Memory, Memory System, and Remote Off Line Memory units can be combined.

The 711 Memory Central Access System brings together a complement of the latest "State of the Art" technology in cards and electronics. Using the recent invention of Differential Optics, the Memory card makes possible the industry's highest level of security, together with unsurpassed digital data readout. The two mean high security, durability, and low cost. The read principle is a departure from the typical method of detecting the presence of, or lack of presence of a code bit (i.e., a magnetic or metallic spot). Coding is accomplished with optical filters which can only be decoded by the reader. Even having access to the precise optical filter in the card does not benefit the counterfeiter since the card contains a plurality of different filters all separately assigned to an analog value in the reader. The filters are inaccessible and invisible and are part of the plastic itself, defying duplication.

The Memory Central Electronics comprise the latest innovations in microelectric circuitry insuring simplicity and reliability. The design concept was to make memory access simple and low cost. But expandable to any size without compromise to any size system. Thus, the simplest basic system with one reader can grow to several hundred readers without modification of the basic system. Most Memory Central options, such as a printer or expander, may be added at any future time simply by plugging into an existing jack on the back of the memory controller.

A.P.D. SECURITY SYSTEMS

24700 CRESTVIEW COURT
FARMINGTON HILLS, MI 48018 (313) 477-2703
TWX 810-242-9369 APDSS FMHL

- Each central unit will accept up to 8,000 individually coded cards or badges. Each card may be voided or validated separately using the hand plug-in programmer. Groups of cards may be voided or validated according to zone or shift automatically from an external timer.

INTER-CONNECTION REQUIREMENTS

Output Relay

The output relay contains Form C contacts rated 5 amps resistive, 120 VAC with adjustable drop-out delay to 15 seconds.
Reader Power

The power supply inputs to the card reader are as follows:

+27VDC±5VDC at 120 ma maximum and +5VDC±5% at 800 ma maximum.

705 MEMORY CENTRAL

The 705 is a Memory Central with 510 card capacity and up to 8 levels of security. The system utilizes memory partitioning of any card in any combination of 8 levels. A level consists of any number of readers and is totally independent of any other level. Programming is accomplished with the use of the 743 systems programmer.

A.P.D. MEMORY CARD

The heart of the Series 711 reader is the patented "Differential Optics" memory card.

The Memory Card is of wallet size and contains invisible optical coding that defies detection, duplication, or alteration.

A variety of special cards are available to suit unusual requirements.

Cards are factory enclosed upon order.

See "Security Kards" Literature sheet.

GENERAL SPECIFICATIONS

COMPONENT	WIDTH	HEIGHT	DEPTH
Memory Central	8.5"	6"	9.5"
Expander	7"	2.5"	7"
Power Supply	2-3/8"	1-7/8"	4-5/8"
Programmer	3.250"	1.25"	7.25"
Printer	8½"	5¼"	13"

Memory Central
Operational Temperature Range—+40°F to plus 90°F

Reader Temperature —+ 10°F to plus 125°F, without heater control

Storage Temperature — minus 25°F to plus 160°F

ELECTRICAL SPECIFICATIONS

Power Requirements

1. Memory Central (711)
   24 vac/dc ± 10% 50-60 HZ(ac),
   20 watts max.
2. Remote Reader (731)
   +5 vdc ± 5%, 5 watts max.
   +26 ±4 vdc, 3 watts max.
3. Remote expander (733R)
   24 vac/dc ± 10%, 50-60 HZ(ac),
   6 watts max.
4. Local expander (733A)
   No external power required.
5. Local reader (731)
   No external power required.
6. Printer (6150)
   115 vac ± 10%, 50-60 HZ, 40 watts max.

Battery may be stored in a cold location up to 15 months.

WARRANTY

All new equipment sold by A.P.D. Security Systems is carefully inspected before shipment and is warranted against defects in material and workmanship for 90 days from date of shipment. Warranty covers repair or replacement of any part which has failed under normal usage, fair wear and tear excepted. Transportation charges [if any] are to be paid by customer.

Items illustrated on this sheet are subject to engineering design and/or appearance modifications which are production standards at time of shipment.