SECURITY ACCESS CONTROL REPORT

Metro Rail Transit Consultants
DMJM/PBQD/KE/HWA

January 1985

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd.)

LIST OF TABLES

Section 1

INTRODUCTION

The SCRTD's primary objective in developing an access control system for the Metro Rail project is to provide a secure, dependable, cost-efficient system that can be effectively managed and maintained by the Southern California Rapid Transit District (SCRTD).

In addressing any large-scale keying and access system, overall criteria must be developed for evaluating each and every access point within the system. This evaluation results in a classification which aids in the determination of the level of security that will be applied to each individual access point.

It is important to remember that police patrols, locked doors, and intrusion alarms are a deterrent to crimes by outside perpetrators. They are much less of a deterrent to the dishonest system employee. The employee works within the system, knows the policy and procedures of the system, and has working access to many or most areas of the system. Statistics indicate that most company losses by theft are of an internal nature. Thefts by outside perpetrators are easily identified as there is usually evidence of the illegal entry left behind. This is not so with internal theft where the loss is not discovered until the property is needed or inventory is taken. Thus, the access requirements identified herein consider both security from external and internal standpoints.

This report is presented both as a proposal for establishing access criteria and levels of access, and as an analysis of electronic card control access versus a grand master hard key system.

1.1 PURPOSE

The purpose of this report is to provide a basis for the design and development of a control access system for the Metro Rail Project.

1.2 SCOPE

This Security Access Control Report focuses on the SCRTD Metro Rail Project and is not intended to be an overall security assessment of SCRTD. This report addresses two major types of unattended access control systems and their application to the Metro Rail Project. It also considers the advantages and disadvantages of the various schemes and recommends an approach for the Metro Rail Project. Other alternative access control systems were considered as not being appropriate due to cost or reliability issues and are not addressed in this report. Identification of every access point within the Metro Rail Project and the type of access control utilized will need to be accomplished on a station-by-station basis and is also not within the scope of this report.

1.3 ORGANIZATION OF THIS REPORT

Following the Introduction, Section 2 identifies the recommended criteria for determining access levels. This is the first step in developing an access control system. Section 3 describes the types of access control systems available and the capabilities of each. Section 4 analyzes the electronic access control system and the hard key system. It also focuses on existing access control systems at other transit properties and addresses the general problems that are inherent in access control. Section 5 presents a conceptual plan for a hard key grand master keying system for the Metro Rail Project. Section 6 presents a similar conceptual plan for the card access system. Section 7 presents a rough estimate of product costs for the electronic access control system and the hard key removable core system. Section 8 describes the reliability and maintainability factors of electronic access control. Section 9 completes this report with conclusions and recommendations on access control for the Metro Rail Project.

Section 2

LEVELS OF ACCESS

2.1 CRITERIA FOR SECURITY LEVEL AND ACCESS RESTRICTION

Three levels of security access restriction have been established in the security design criteria for the SCRTD Metro Rail Project. It is believed that by adhering to these various levels of access and properly classifying Metro Rail areas for control, a secure, economic, and reliable control system can be achieved. The security levels are:

A. Critical Access

Critical access areas are those areas that can be extremely hazardous, essential to the system's safe operation, or require restricted access due to the nature of the equipment or value of the product within the area. The critical access points will be supplied with intrusion detection devices. Access will be limited to relevant disciplines.

B. Sensitive Access

Sensitive access areas are those areas that are secured to preserve the integrity of the equipment. These areas will be limited to authorized access only.

C. Moderate Access

These areas are readily available to Metro Rail employees for general operations and administration of the Metro Rail System. Employee access will be on an as-needed basis and public access will be on a controlled basis.

2.2 ROOM SECURITY CLASSIFICATION

The matrix, shown in Table 2.1, identifies the recommended classification for each area in the Metro Rail System based on the criteria found in Section 2.1 of this report. This matrix should be used by the Metro Rail Project security planners and designers for the design of the System's security control. Also, this matrix forms a basis for further evaluation of alternate access control systems.

Table 2-1

RECOMMENDED SECURITY LEVELS

STATIONS	SECURITY LEVEL	YARD & SHOPS	SECURITY LEVEL	CENTRAL CONTROL	SECURITY LEVEL
Traction Power substation	Critical	Communications Room	Critical	Communications Room	Critical
Auxiliary Power	Critical	Train Control Bungalows	Critical	Control Room	Critical
Train Control	Critical	System Stores	Critical	Police Dispatch	Critical
Communications	Critical	Machine Shop	Sensitive	Station Monitors	Critical
Batteries	Critical	Tool Room	Critical	Tape Storage	Critical
Main Entrances	Critical	Electronic Repair	Critical	Train Control Equipment	Critical
Fare Vending Equipment	Critical	Train Control	Critical	Battery Room	Critical
Electrical	Critical	Traction Power S/S	Critical	Standby Generator	Sensitive
Incoming Electrical Service	Critical	Auxiliary Power	Critical	Mechanical Equipment	Sensitive
Storage	Sensitive	Welding Shop	Sensitive	Electrical Equipment	Sensitive
Fare Gates	Sensitive	Battery	Sensitive	Elevator Equipment	Sensitive
Mechanical	Sensitive	Tool Carts	Sensitive	Administrative Offices	Moderate
Fan	Sensitive	Heavy Repair Shop	Sensitive	Lunch/Training Room	Moderate
Emergency Fan	Sensitive	Wheel Shop	Sensitive	Locker/Toilet Rooms	Moderate
Chiller	Sensitive	Elevator Machine Room	Sensitive	Custodial Room	Moderate
Air Supply Unit	Sensitive	Electrical Equipment	Sensitive		
Smoke Exhaust	Sensitive	Telephone Equipment	Sensitive		
Under Platform Exhaust	Sensitive	Mechanical Equipment	Sensitive		
Under Platform Exhaust Plenum	Sensitive	Automotive Repair	Sensitive		
Ejector	Sensitive	Carpentry Shop	Sensitive		
Sump Pump	Sensitive	Air Brake Shop	Sensitive		
Emergency Equipment	Sensitive	Air Conditioning Shop	Sensitive		
Elevator Equipment	Sensitive	Parts Cleaning	Sensitive		
Staff/Security	Sensitive	Offices	Moderate		
Custodial/Trash	Moderate	First Aid Room	Moderate		
Toilet	Moderate	Shielded Room	Moderate		
		Rest Rooms	Moderate		
		Locker Rooms	Moderate		
		Outside Entrances	Sensitive		

NOTE: The above classifications may vary depending on final design configurations or change in the functional evaluation of a particular room.

Section 3

SECURITY ACCESS CONTROL APPLICATIONS

Presently there are three types of access control that can be applied, either singularly or in combination, to the Metro Rail facilities. The three types of access control are discussed below.

3.1 HARD KEY

The hard key approach (use of conventional locks and keys) to a large system such as the Metro Rail is applied in a master key hierarchical configuration that allows predetermination of exactly which areas a particular key will access. The ability to change lock combinations in the most economical and time-efficient manner, which will be necessary in the event of lost or stolen, unauthorized duplication of keys, or a major strike, necessitates that the locks have removable cores. This provides a simplified method of rekeying without the use of specialized tools. The use of removable cores, which is necessary in a large system, also increases vulnerability to manipulation or lock picking. In general, a hard key system is considered a method of keeping out the honest public or employee, not a system to control internal theft.

3.2 INTRUSION ALARMS

Intrusion alarms are installed on doors as a support to the lock and key system so that forced or improper entry is annunciated. False alarms are common due to environmental conditions, component failure, and improper shunting by those gaining access. All alarm activations must be responded to by Security personnel, whether an actual or false alarm, in order to maintain the integrity of the intrusion devices.

3.3 CARD ACCESS

Present-day electronic access control systems use a special coded card, or employee identification (ID) card, that is inserted in a door reader to qualify access, shunt the alarm, and activate the door lock. The supervisory control host computer encodes the access ID cards for designated entry points and times of access. Where exiting the area does not require monitoring, an exit switch is used on the inside of the room to allow for limited-time exiting.

To ensure a fail-safe access, a simple nonremovable core lock is usually installed with a single key accessing all locks. This single key is maintained by Security.

Section 4

CARD ACCESS VS. HARD KEY

4.1 CARD ACCESS

Experience and opinions of organizations that have utilized both electronic card access and a hard key system indicate that electronic card access provides a more secure access control system. It allows the ability to monitor the system at any time. Status of the system's integrity is always immediately available. Record is made of all authorized, unauthorized, or attempted access. In the event that entry by a particular card key is no longer desired, entry can be rejected by inputting the necessary data into the host computer. This usage limitation of a single card key is almost immediate and at relatively no cost. The card key, after it is recovered, can be reactivated through the host computer and reissued for use.

A. Advantages

Some of the major advantages of electronic card access control are the following:

- Intrusion alarms can be bypassed when authorized entry is performed.

- The device can report unlocked as well as open doors in conjunction with monitoring intrusion alarms.

- All access times and which card made access can be reported.

- All unauthorized attempts at entry are reported.

- The device can record what particular key card made attempted entry and at what time.

- The device can lock out any or all key cards at any time.

- The door locks can be programmed to release in case of fire, loss of power, or at any time determined by the host computer operator. Some doors need to remain locked during most emergencies. These particular doors will have a door release override which will prevent any undesired releasing of door locks.

- All events occurring in the System can be documented by hard copy printout.

- In addition to assigning access to particular doors by holders of certain badges (level of access), higher security can be obtained by placing badge readers inside selected secured areas and requiring badges be read to gain exit (same logging feature).

- A further level of security can be applied by placing a 10-digit key pad (similar to a telephone tone pad) adjacent to selected badge readers, assigning personal identification numbers (PIN) to employees, and requiring entry of the PIN on the key pad prior to reading of the badge to gain entry.

- The changing, addition, or deletion of access privileges can be accomplished rapidly at any time from the control console. If required, access privileges can also be established on a basis of day of the week, time of day, or both.

- The controlled access system, as described, may also be used as a "time and attendance system" (employee time clock) allowing employees to report directly to their assigned work locations, requiring only the addition of a badge reader and controller at locations where clocking-in/out is desired.

- All cards, whether magnetically encoded or encoded in some other fashion, are available in styles that may be laminated with employee photos, etc., for visual identification purposes.

- More difficult to duplicate card than conventional hard key system.

B. DISADVANTAGES

- Higher cost for initial installation.

- Repair and maintenance will require electronic technician.

- Magnetically encoded cards may be affected by electromagnetic interference in the transit stations. However, there are electronic card access systems which employ methods other than magnetically encoding cards.

4.2 MASTER HARD KEYING SYSTEM

Any extensive hard keying system used on the Metro Rail will, during any given year, have many lost, damaged, and unauthorized duplicated keys. This is a serious maintenance and security problem which has proven to be a nemesis.

A. Advantages

- For initial installation, it is the lowest cost security system available.

B. Disadvantages

- An investigation must be conducted whenever a key is reported lost or stolen. An investigation must be undertaken which determines the extent of security breach and whether or not the affected lock combinations have to be changed. A decision must be reached within a reasonable time in all lost key cases. This is expensive in terms of manpower and resources.

- Stamping "DO NOT DUPLICATE" on keys means that it may cost more to have them duplicated by an unauthorized person. Realistically, it is not possible to know how many keys are duplicated. In organizations which conduct a documented biannual inventory of keys where verification is made by serial number, title, and location, it has been noted that many employees have duplicated keys and that ex-employees' keys have not been returned. There are many unexplained losses from facility rooms, resulting in aspersions being cast upon honest employees who have valid access. Employees can not be held accountable for company property without a tight security system.

- A separate shunt key is required for every door with an intrusion alarm to deactivate the alarm.

- An intrusion alarm used in conjunction with a hard key system usually only detects entry -- not intrusion. The discrimination between authorized and unauthorized entry can only be done through communications between the observer of the detection alarm monitor and the person entering. Therefore, real-time support is required to determine forced or improper entry.

4.3 ACCESS SITUATIONS AND RESPONSES

There are certain basic situations in an access control system that must be considered when making a decision on the type of access control that will be applied to any facility. Table 4-1 presents access situations and responses for an electronic access control system and a grand master hierarchical hard key system.

4.4 EXAMINATION OF OTHER TRANSIT PROPERTIES

Conversations with transit police officials in Atlanta, Baltimore, and Washington, DC, resulted in a general consensus that the hard key approach using a grand master key hierarchical configuration does not provide a desired degree of security. The main reasons cited were problems with the size of the system, loss of keys, unauthorized duplication of keys, and the indiscriminate allocation of keys. This results in considerable change-out of locks and replacement of keys in an effort to regain security. Validating key status and recovery of the keys has proven to be a monumental task.

A. Atlanta

Atlanta has a hierarchical, grand master, hard key system. Transit police officials feel that the weaknesses of the hard key system are in the large number of change-outs of the cores, recombinating the cores, purchase of keys, and the fact that the core control key can access any door regardless of the combination by just replacing the core. Loss or unauthorized duplication of the core key invalidates the

Table 4-1

SUMMARY OF ACCESS SITUATIONS AND RESPONSES

SITUATIONS	RESPONSES	
	Card Access	Key Access
Computer Down	Building Control Takes Over	----------
Disgruntled Employee Resigned - Takes Key or Card	Voids Card Access in 30 Seconds	Change Appropriate Lock Cores
Fire	Automatically Releases Any or All Locks	Panic Bars Override Locks
Missing Property or Damage	Records Who Was in Room and When	Security Status Unknown-All Key Holders Suspect
Lost Key or Card	Voids the Access Card Immediately	Decision Must Be Made-Change Cores or Replace Key
Intrusion Alarm Sounded	Identifies Who Made Access and If Access Was Made	Does Not Know If Access Was Made and If So, by Whom
Alarm Reset	Authorized Access Shunts Alarm	Alarm Shunt Key Needed
Unauthorized Access	Records All Access or Attempted Access and Time	No Record Available
Change-Out Cost	Replacing of Cards Only	Replacing of Key Cores and Recombinating Cores
Employee Strike	Voids Any or All Access Cards Immediately	Replace or Recombinate All Cores
Times of Access	Can Restrict Times of Access	No Control Available

total system. They feel the system does not satisfy their needs. The keying system is under the control of the transit police.

B. Baltimore

The Baltimore Transit System uses a hard key, hierarchical, grand master keying system. The transit police feel that the keying system is completely inadequate. Everyone seems to end up with a master key. The alarm panels in the station attendants' booths consistently have four or five alarms activated during the day due to employees tripping the alarms while making their rounds. Due to the frequency of false alarms, the alarms are responded to only when stations are closed. This invalidates the function of the security system because an intrusion alarm must be responded to on a hard key system to verify authorized entry. They feel that their system does not satisfy the needs of security. Transit police have no control of the keying system.

The vending equipment is equipped with a hard key system and alarm. Due to the internal money losses from the vending equipment, the transit police have required that <u>any</u> entry into the vending equipment requires the presence of a transit policeman. This requirement has cost the transit police approximately 45 to 60 labor-hours per week. The responses to the vending equipment are rotated among approximately 20 police officers. The transit police are usually the first ones on the scene after being notified by the fare collection people of a problem with a particular vending machine. The transit police respond to approximately 20 calls to vending equipment a day. At this time, the transit police report their losses from vending equipment as nil.

Baltimore is planning the installation of an electronic card keying system in their new headquarters building.

C. Washington

The Washington Transit System uses a quickset combination type of hard key system. There is not a stationwide master master key. Separate keys are required for the battery rooms and train control room in the stations. Entry to various rooms within the station requires numerous keys. The Washington transit police feel that their hard key system is extremely inadequate.

The Washington transit police do not have control of the keying system. They feel that a greater responsibility for the integrity of the system would be assumed by the transit police if the control of the keying system, as well as breaches of security, were both under the jurisdiction of the transit police.

The transit police state that their vending equipment is being pilfered constantly. The security built into the vending equipment, which is accessed by a hard key, is completely vulnerable to anyone who works with the equipment. This includes the built-in audit control.

Washington uses the electronic card access access system by "card key" in their headquarters building and their revenue room. They have approximately 25 card readers that they maintain themselves. The Washington transit police strongly recommend the use of a card keying system with vending equipment.

Section 5

HARD KEY PLAN CONCEPT

5.1 GENERAL

Each employee has a specific function. The job classification will determine what rooms the employee must access in order to do the job. The employee must also have access to every door leading to the job site.

Every room in the Metro Rail System will be classified according to its specific or related functions. An employee is issued a single key that is made to access only those rooms that are necessary for job performance.

To assist in determining the various levels of access, the system functional areas are depicted within a grand master keying plan (see Appendix A). (The grand master keying system can be reduced in size depending on the number of doors that may be controlled by electronic card access.)

A. There should be three master keys: AA for all Central Control locks, AB for all station locks, and AC for all yard and shops locks. All lock cylinders will be subject to a grand master key (AAA).

B. There will be a restricted factory-supplied keyway. Metro Rail transit police should control the supply of key blanks.

C. The system standard lock cylinder will be a removable core type, grand mastered, and keyed as shown in Appendix A. The allocation and control of removable core keys is an administrative policy decision.

D. By using a single assigned operating key, employees will have access to whatever rooms are necessary for accomplishing their respective assignments. For example, a train control maintainer would be able to open the doors with a single C key to the train control room in each station, the yard tower, the equipment room at Central Control, or doors on the path leading to these areas. Transit police may be issued master keys that will access all doors in the facility.

E. A security switch is any power or control switch that requires controlled access. Security switches and other locks, such as for entrances and toilets (which are subject to many key codes and designated S1, S2, or S3 as defined in Appendix B), will not have a specific key. These locks have been distinctly classified since several classifications of personnel must have access at various entrance points with assigned keys.

5.2 HARDWARE

The basic hardware would consist of:

- Key Cutting Code Machine - Capable of accurately cutting keys to their original bitting depth utilizing an inserted plastic card.

- Combinating Kit - Parts and tools necessary to recombinate any lock core in the system.

- Core and Key Marking Block - A device which holds a core or key for stamping with letter and number dies.

- Letter and Number Dies Set - For marking cores and keys.

- Tubular Key Cutter - Capable of duplicating, decoding, or cutting to code all three sizes of tubular keys.
- Code Book - Numerically listing all combinations presently in use and/or available.
- Core and key control cabinet.
- Lock cylinders of removable core type.
- Cylinder Cores - Control key removable and interchangeable.
- Key blanks.

Section 6

CARD ACCESS SYSTEM

A card access control system is activated by specially encoded cards (similar to bank automatic teller and thrift charge cards).

The basic encoded card entry access system generally consists of:

- Electric Door Strike - Mounted in place of a regular door strike.

- Card or Badge Reader - Vandal-resistant and mounted alongside the door or gate to be controlled.

- Door Controller - Mounted inside the secured area, usually on the wall above the controlled door.

- Multiplexer - Located in a central communications interface location, such as a station ATC & C room.

- Validation Equipment - Located in a central security control area such as the CCF.

- Control Console - Located in the central security control area.

- Hinge Intrusion Detector Junction Box - Located as denoted in Appendix D (installed at critical access doors regardless of type of keying system).

Appendix C shows the basic configuration of a controlled access system using encoded cards. Functionally, the encoded card or badge is read by the badge reader; and the door controller checks for a valid company badge ID, formats the data, adds the door identification, and passes the data to the validation equipment by way of the multiplexer.

The validation equipment checks the badge ID and door ID against a look-up table and, if the badge data is valid for the particular door, it commands the controller to release the electric door strike for entry. The validation equipment logs the badge ID, door ID, date, and time of entry to memory for later transmission to the control console and host computer for printout and permanent file. Entry attempts using noncompany badges, invalid company badges, valid company badges not valid for a particular door, and forced entry or entry using a tumbler key are reported immediately to the control console for action by Security personnel. (See Appendix D for sketch of controlled access system door hardware depicting single and double door control.)

The card key system shall be integrated with the emergency communications system to ensure proper coordination during fire and other emergencies. In the event of a malfunction that could prevent the card access from functioning (i.e., a bad selenoid), a simple nonremovable core lock is installed with a single key for unlocking the door. This single key is maintained by Secruity.

The area most subjected to vandalism is at station entrances. The card reader is vandal-resistant, and is surface mounted using special vandal resistant screws which require a special (not commonly available) tool for placement or removal.

The reader is equipped with intrusion detection between the housing (cover) and the mounting plate, and between the mounting plate and the wall. These detectors provide annunciation of housing removal and/or prying the mounting plate away from the wall. In addition, access to the read mechanism or wiring inside the housing does not provide access to the latch release mechanism. The latching device wiring is totally contained within the secured area.

Section 7

COST COMPARISONS

The following cost figures are based on the recommended critical access areas (Table 2-1). There are approximately 165 access points for the Metro Rail Project, which includes the stations, Central Control, and yard and shops.

7.1 CARD ACCESS CONTROL

The cost figures for electronic access control are rough estimates (ROM) of list cost furnished by the MRTC System Design Division.

Table 7-1 outlines estimated equipment costs (including electric strikes, door controller, and badge reader) based on:

- Eight controlled doors per station (18 stations)
- Twelve controlled doors or gates in the Yard
- Nine controlled doors in the CCF.

7.2 GRAND MASTER HARD KEY SYSTEM

The figures in Table 7-2 were obtained from Major Lock Supply, Inc., Anaheim, California, and are list cost of Falcon Locks. This includes equipment necessary to maintain the system. The number of doors used in the estimated equipment cost (165) are the same number of doors used in the cost estimate for electronic access control (Section 7.1).

Table 7-1

ELECTRONIC SYSTEM COST ESTIMATE

Description	Cost
8 Doors/station @ $940/door, $7,520/station	$135,360
9 Doors at CCF @ $940/door	8,460
12 Doors in Yard @ $940/door	11,280
1 Multiplexer/station @ $2,250	40,500
1 Multiplexer at CCF @ $2,250	2,250
1 Multiplexer at Yard @ $2,250	2,250
2 Validation units at CCF @ $10,500	21,000
1 Mini Computer @ $30,000	30,000
Software package	22,000
TOTAL EQUIPMENT*	$273,100

Additional doors @ $1,000 each up to 256 doors, plus $2,250 for every 16 doors.

The backup hard key locking system, if added, would be $30 per door. For 165 doors, this added cost would be approximately $4,950.

*For MOS-1, the total equipment cost would be reduced to $135,590.

Table 7-2

HARD KEY SYSTEM COST ESTIMATE

Description	Cost
Lock cylinder @ $20 each	$ 3,300
Deadbolts @ $31 each	5,115
Combinated cores @ $17 each	2,805
Key code machine	1,400
Combinating kit	95
Core and key block	38
Letter and number die set	27
Replacement cores and key blanks	2,227
TOTAL EQUIPMENT	$15,578

*For MOS-1, the total equipment cost would be reduced to $5,555.

Section 8

RELIABILITY AND MAINTAINABILITY OF ELECTRONIC ACCESS CONTROL

8.1 EXISTING ACCESS CONTROL SYSTEMS

The following organizations, which utilize card access as part of their controlled access system, were assessed as to their justification for installing card access and the reliability and maintainability factors associated with the card access system.

A. Southern California Gas Company

The Southern California Gas Company (SCGC), which has a fairly extensive card access system that has been in operation for 4 years, presented the following evaluation.

1. Justification

The SCGC representative stated that their use of card access was justified because of the various management applications that are available with card access control. Most of these applications are listed in Section 4. Some of their access points are programmed to unlock and lock at specific times. They are able to maintain the integrity of the card access system, which is not the case with the hard key system. The SCGC representative stated they do not have any statistical data on property loss but believes that losses from theft have gone down considerably.

2. Maintenance Factors

The SCGC utilizes 128 card readers, 3 CRTs, 3 printers, 7 expanders, and 1 central processing unit.

The system is maintained under a yearly contract that is based on the number of readers and other pieces of equipment. Their present maintenance contract for 1984 is $29,500. A survey of maintenance records revealed the following service calls during 1984:

Type of Problem	Number of Calls
Repair loose wire	1
Printer cleaned	1
Replace reader cartridge	8
Replace door strike	1
Replace lock	1
Readjust access time on door No. 1	1
Replace Alarm Monitor Board	1
Power out due to construction	1
Replace alarm	1
Replace transformer	1
Problem with phone lines	1
Replace CRT	1
Reader not registering	1
System power down	2
Replace alarm	1

B. Southern California Rapid Transit District

The Southern California Rapid Transit District (RTD) has utilized card access within their data processing section. This system has been in effect for approximately 2-1/2 years. Their representative presented the following evaluation:

1. Justification

The data processing section was considered a very critical area and the existing hard key system presented inadequate control. The management controls offered by a card access system were the determining factors to install card access.

2. Maintenance Factors

The SCRTD utilizes 21 card readers, 5 cameras, 3 monitors, 1 CPU and 1 printer. There are 294 active cards. With the turnover of employees, approximately 50 cards a year are issued. New cards cost approximately $3.00 apiece. The maintenance of the system is under a yearly contract which is presently $250.00 a month. SCRTD stated that most of their problems with the card access system have been with poor workmanship in the construction and installation of the doors and door jambs. Some of the problems also rest with the quality of installation of the card access system. There appears to be little problem with the card access hardware.

C. Reference Data on Reliability and Maintainability

Data and particular references are presented below. The data is based on a controlled access system that includes a door controller, badge reader, multiplexer, and validation unit.

Data

Mean Time Between Failures:	2,496 hours
Mean Time to Repair:	2 hours

References

RADC-TR-75-22. Non-electronic Reliability Notebook. January 1975.

MIL-HDBK-217D. Reliability Prediction of Electronic Equipment. 15 January, 1982.

Section 9

CONCLUSIONS AND RECOMMENDATIONS

9.1 CONCLUSIONS

A grand master hard key system has many inherent problems that affect the integrity of the keying system security. It will be a considerable task to maintain the System and the maintenance cost will be considerable over a period of time. Breaches of the hard key system are much easier than the electronic access control System and resultant losses by theft can exceed any initial installation cost of any access control system. In the Metro Rail System, where employees will travel to many stations to perform their jobs, the electronic access control system will also provide a record of access by time and location and by which particular employee. The employees' time of access may also be restricted. When evaluating the total cost of hard key versus electronic access control, electronic access control is initially more costly, but is more secure and easier to maintain. When evaluating the cost to provide electronic access control to a particular room, the cost can be easily justified because of the importance or the potential loss that could be incurred should the security be breached.

9.2 RECOMMENDATIONS

A. Control

There are a great number of structures in the rail transit system, all basically uniform in organization and function. They are generally unstaffed with many critical and sensitive areas. This places a greater responsibility on the transit police for integrity of the system. It is recommended that the rail transit keying system be under the control and management of the transit police since they are responsible for the security of the Metro Rail System. This will assure greater attention to the proper utilization of the keying system. The maintenance of the system should be accomplished by other elements of SCRTD using established SCRTD work order procedures.

B. Electronic Access

At a minimum, electronic access control should be applied to all areas defined as critical except vent shafts and other emergency exits leading directly to the surface. Consideration should be given to providing electronic access control for areas classified as sensitive.

Due to the relatively high electrostatic and electromagnetic fields in which many Metro Rail employees will be working (i.e., near contact rail along guideways, in traction power substations, and repairing traction motors) the use of traditional magnetic stripe or similarly encoded cards should be carefully evaluated before being specified. These types of cards are susceptible to damage to the encoded information on the card from high magnetic and radio frequency fields. Card systems are available using laser and infrared scanning techniques which are more resistant to damage from external sources.

The cost for magnetic or laser scanned systems are basically equal. The readers utilize different electrical techniques for reading the cards, but interface to the door controller is electrically identical in both cases.

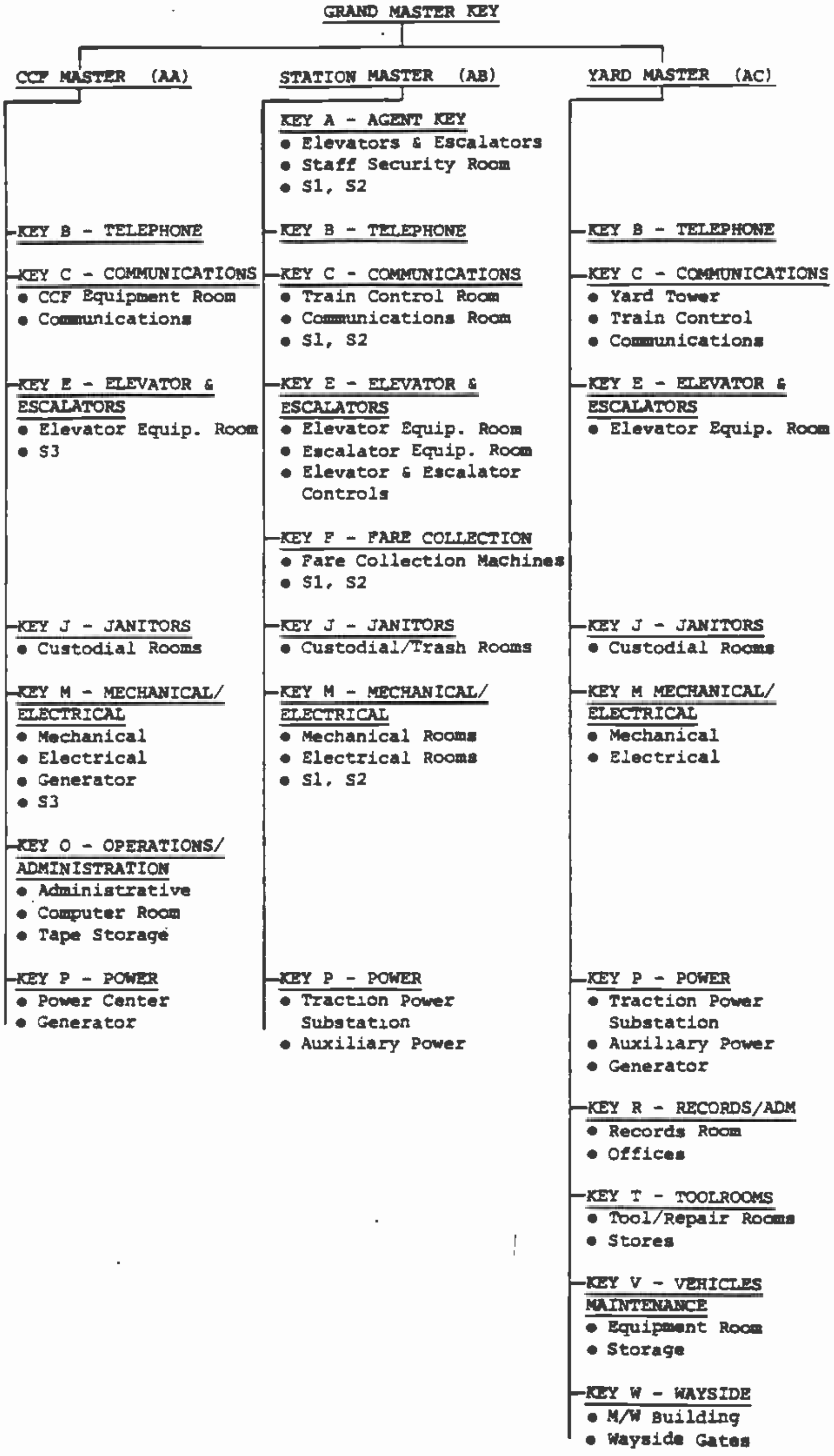
C. Installation

During the construction period, all areas using a hard key system should have a removable core lock cylinder of approved quality installed. This will ensure a quick and efficient change-out using removable cores.

APPENDIXES

Appendix A

GRAND MASTER KEYING PLAN FOR THE SOUTHERN CALIFORNIA METRO RAIL SYSTEM



GRAND MASTER KEY

- CCF MASTER (AA)
  - KEY B - TELEPHONE
  - KEY C - COMMUNICATIONS
    - CCF Equipment Room
    - Communications
  - KEY E - ELEVATOR & ESCALATORS
    - Elevator Equip. Room
    - S3
  - KEY J - JANITORS
    - Custodial Rooms
  - KEY M - MECHANICAL/ ELECTRICAL
    - Mechanical
    - Electrical
    - Generator
    - S3
  - KEY O - OPERATIONS/ ADMINISTRATION
    - Administrative
    - Computer Room
    - Tape Storage
  - KEY P - POWER
    - Power Center
    - Generator
- STATION MASTER (AB)
  - KEY A - AGENT KEY
    - Elevators & Escalators
    - Staff Security Room
    - S1, S2
  - KEY B - TELEPHONE
  - KEY C - COMMUNICATIONS
    - Train Control Room
    - Communications Room
    - S1, S2
  - KEY E - ELEVATOR & ESCALATORS
    - Elevator Equip. Room
    - Escalator Equip. Room
    - Elevator & Escalator Controls
  - KEY F - FARE COLLECTION
    - Fare Collection Machines
    - S1, S2
  - KEY J - JANITORS
    - Custodial/Trash Rooms
  - KEY M - MECHANICAL/ ELECTRICAL
    - Mechanical Rooms
    - Electrical Rooms
    - S1, S2
  - KEY P - POWER
    - Traction Power Substation
    - Auxiliary Power
- YARD MASTER (AC)
  - KEY B - TELEPHONE
  - KEY C - COMMUNICATIONS
    - Yard Tower
    - Train Control
    - Communications
  - KEY E - ELEVATOR & ESCALATORS
    - Elevator Equip. Room
  - KEY J - JANITORS
    - Custodial Rooms
  - KEY M MECHANICAL/ ELECTRICAL
    - Mechanical
    - Electrical
  - KEY P - POWER
    - Traction Power Substation
    - Auxiliary Power
    - Generator
  - KEY R - RECORDS/ADM
    - Records Room
    - Offices
  - KEY T - TOOLROOMS
    - Tool/Repair Rooms
    - Stores
  - KEY V - VEHICLES MAINTENANCE
    - Equipment Room
    - Storage
  - KEY W - WAYSIDE
    - M/W Building
    - Wayside Gates

Note: Refer to Appendix B for explanation of Locks S1, S2, and S3.

Appendix B

SECURITY AND BYPASS SWITCH LOCKS

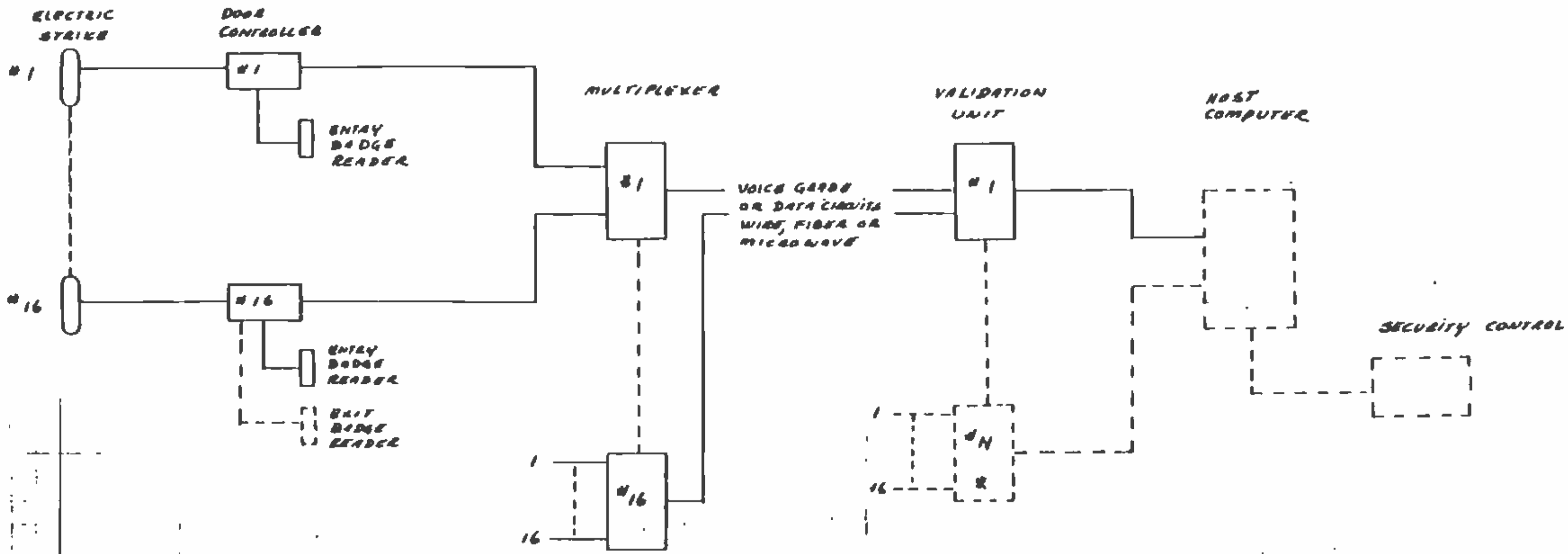
When a lock is subject to four or more different key codes, such as at station entrances, toilet rooms, and end of platform gates, the lock will have an "S" designation, as follows:

	Designation	Function
S1	Subject to Keys A/C/E/F/M/P	For use at station entrances and station elevators.
S2	Subject to Keys A/C/E/F/J/M/P/W	For use at station toilets emergency exits, and end of platform gates.
S3	Subject to Keys C/E/J/M/O/P	For use on OCC elevators and lobby doors.

METRO RAIL TRANSIT CONSULTANTS
DMJM / PBQD / KE / HWA

CONTROLLED ACCESS
SYSTEM
TYPICAL BLOCK DIAGRAM

DESIGNED BY C. Coco	DATE 08-01-84
	SHEET NO



* NUMBER OF VALIDATION UNITS DEPENDS ON NUMBER OF DOORS IN MULTIPLES OF 256 & SIZE OF HOST COMPUTER.

DOOR CONTROLLER	1/DOOR
MULTIPLEXERS	1/16 CONTROLLERS OR 1/STATION (WHICHEVER IS LESS)
VALIDATION UNIT	1/256 DOORS OR 1/16 MULTIPLEXERS

Appendix C

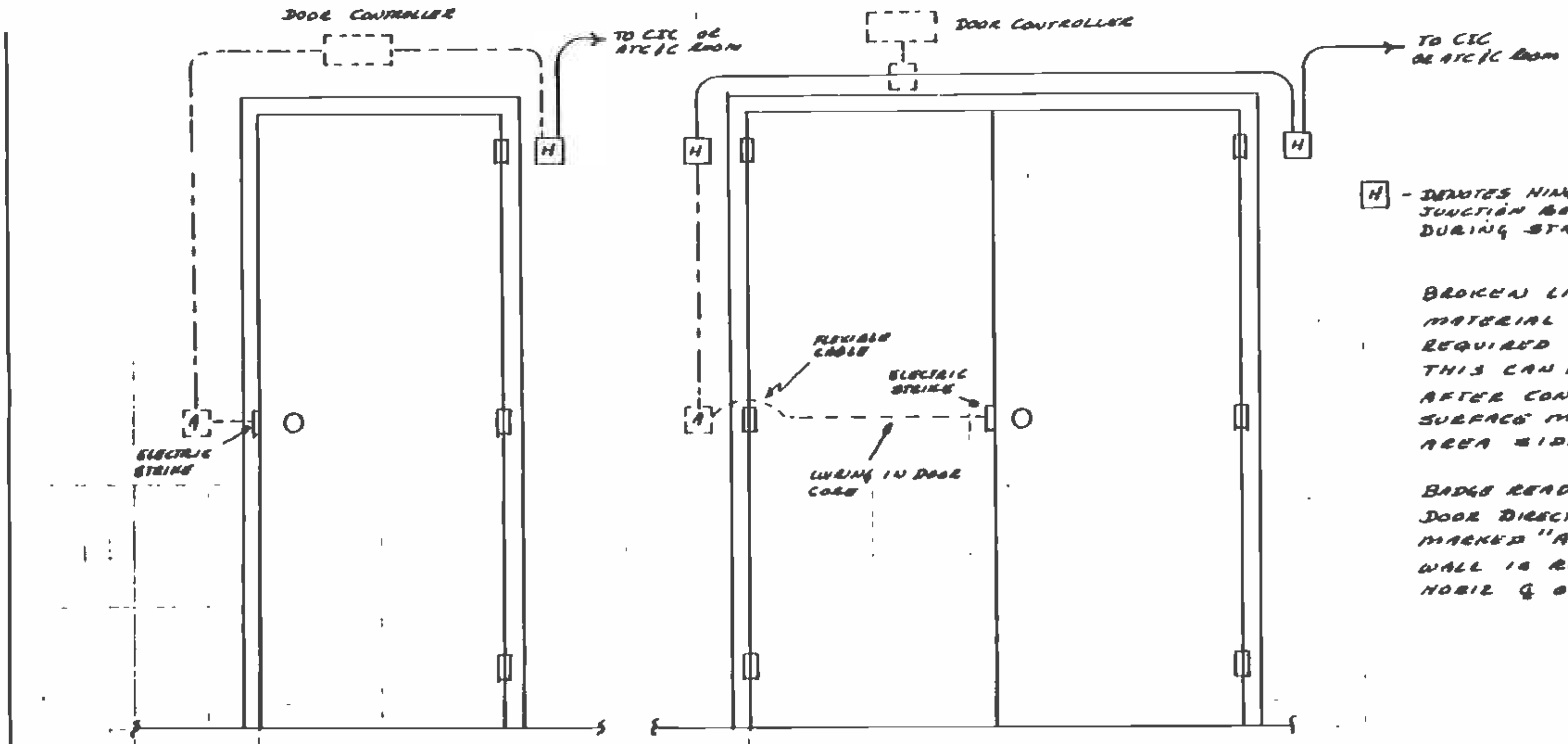
TYPICAL BLOCK DIAGRAM FOR CARD ACCESS SYSTEM

METRO RAIL TRANSIT CONSULTANTS
DMJM / PBQD / KE / HWA

CONTROLLED ACCESS
SYSTEM
DOOR HARDWARE

SHEET NO

C. Cain 08-01-86



DOORS VIEWED FROM SECURE SIDE

H - DENOTES HINGE INTRUSION DETECTOR JUNCTION BOX TO BE INSTALLED DURING STATION CONSTRUCTION.

BROKEN LINES INDICATE MATERIAL & EQUIPMENT REQUIRED FOR ACCESS CONTROL. THIS CAN BE INSTALLED AFTER CONSTRUCTION AS SURFACE MOUNTED ON SECURE AREA SIDE OF DOORS.

BADGE READER MOUNTS OUTSIDE DOOR DIRECTLY OPPOSITE "J" BOX MARKED "A". 5/8" HOLE THROUGH WALL IS REQUIRED AT VERT & HORIZ ℄ OF "J" BOX "A".

Appendix D

DIAGRAM OF DOOR HARDWARE FOR CARD ACCESS SYSTEM