

ACCESS ANYWHERE

ACCESS CONTROL SYSTEM

SOFTWARE MANUAL

VERSION 6

FOR Windows 9x, NT, 2000, XP



Quick Start

UP AND RUNNING IN 2 MINUTES

1. Place Installation Disk In Floppy Drive & Type: HDSETUP
2. Double Click The AC3.MDB Icon When It Appears On Your Desktop

3. Welcome Menu Will Appear

- Click The PC-P2 Icon
- Click The Report Manager Icon
- Exit The Welcome Screen



The system should now be On-Line and if each device you have defined in your security level is communicating properly, the word SUPERVISED (located on the ACTION WINDOW status bar) will change from red to light blue after one minute. To check the status of each device by module code, hit Esc and select Routine 5. Each device you have defined is displayed. Any device not communicating displays in red.

PROGRAM A CARD

1. Double click the Access Central icon and select Cardholder Database
2. Enter a name, a card number, and assign it to a security level
3. Click the PROGRAM THIS CARD button

That's It

To observe card transactions, return to the PC Central ACTION WINDOW (Esc) and present a card to one of the readers.

To observe alarm inputs, you must first go to the MEMORY Routine ("M" Hot key) and define alarm text in order to activate and observe alarms.

About the *Access Central* Software Package

Access Central is comprised of three programs. When you click your AC3.MDB Desktop Icon, you will be able to load all three at once.

1. AC3.MDB

This is the Microsoft Access Program that you will use to program and maintain the access control system. It resides in your TC85DIR subdirectory and loads when you click the AC3.MDB shortcut icon on your Windows Desktop.

Note: The setup program places the AC3.MDB icon on your Windows Desktop (c:\windows\desktop). If your Desktop is actually a second party Desktop and not the actual Windows Desktop, you must move the icon to the Desktop you are using.

2. LOG.MDB

This is the MS Access program called Report Manager, and it must be running at all times (on your Windows Task Bar) to capture incoming access control transactions that you want to view. You will also be able to run activity reports.

3. PC-P2

This is the background program that controls all the access control system field devices, and makes the actual decisions to grant or deny access. It runs in RAM memory so that it can respond instantly to all field events. Because it resides in RAM memory, it is fast and can unlock a door 70 milliseconds after the card is presented, if the card is valid for entry. It can also respond to alarm events with the same speed. When you run this program from the Access Central Welcome Screen, it will load on your Windows Task Bar. You must keep this program running at all times, and you must be certain that you have only one PC-P2 icon on your Task Bar. It should be noted that PC-P2 also maintains a log of all events independent of Report Manager. So if Report Manager is not running, you will still always be able to view and print out activity reports.

It is possible to program cards directly into PC-P2. In fact doing so is a very fast method of initializing a system. You can program all cards, or ranges of card numbers instantly into preliminary security levels so that the access control system can go on-line immediately without having to enter all the cardholder data into Access Central first. Then you can take the time to populate your Access Central database with the names and personal information of each of your cardholder while their cards continue to operate the system. When your Access Central Database is fully populated, you may then replace your preliminary programming with your finished database.

While most programming functions may be done using the Microsoft MS Access

Database (Access Central), there are a few system parameters that must be entered into PC-P2.

1. Alarm Text Descriptions. Alarm points will not report unless text is assigned to them.
2. Holidays. Must be entered if Security Levels use the Holidiay parameter
3. Anti-Pass-Back Modes, Nesting, Tenant Space Allocation for parking
4. Space Counters
5. Optional software for Card Use Debiting, and V.I.P. tracking

If you desire, you may run your Access Central System entirely from PC-P2, and not use the MS Access program. You can run it out of Windows 95/98, or you can run it in a 100% DOS environment. For complete instructions on how to do this, please refer to the PC-P2 Operating Instructions later in this book.

Access Central For Windows 95/98

Microsoft Access version 97 or higher must be pre-installed on your computer.

Installing Access Central With Existing Systems

If you have an existing Toye system installed in the TC85DIR sub-directory, you can import all of your existing data into the latest version of Access Central.

There are three options for importing data from older systems.:

1. Use the built-in Macro (F11 key) called (ImportP2 Programming) This will immediately populate your cardholder database with new records based on cards already programmed into the system. The ***Access Central*** cardholder database will contain each person and the levels to which they have been assigned. All level definitions and system parameters will also be imported, and the new system will be ready to run.
2. You may populate your ***Access Central*** database from the dBase III file built into **PC-P2**. Use the Macro: (Convertdbf)
3. You may populate your new ***Access Central*** database from an earlier version of ***Access Central*** using the Macro: (Convertmdb)

Getting Started

Three basic steps are necessary to initialize the system .

1. Define at least one entry point
2. Define at least one security level in
3. Program at least one cardholder.

That's it. If the field bus is connected to your PC's serial port properly, the access control system will go on-line.

Loading Access Central

With "PC" Central running, simply double click the AC3 icon, and a Welcome

screen will appear. Load PC-P2 and Report Mnager, and close the Welcome screen.

Your program may or may not load with the *Access Central* Toolbar displayed. To display the correct Toolbar, Select View/Toolbars from the pull down menu. Scroll down to *Access Central* and place a check in the box. Be sure there are no other Toolbars that are checked.

Tool Bar Buttons

Tool Bar buttons are provided for quick access to the most frequently used functions.

Real Time Events

When you click this button, a Dynamic Display of incoming card and alarm events will be displayed as they occur. You click on an incoming cardholder's name to jump to that cardholder's database record. If you can also filter all records to show just the transactions of one cardholder by highlighting the name, right mouse click, and select filter by selection. You can also change the display order to anything you want, and remove the filter with another right mouse click.

Menu

Displays the Main Switchboard Menu

Cards

Displays the Cardholder Database

Binoculars

When you click in any field (except cardholder memory number), you can search for any other record.

Manual

Displays the entire contents of the Software Instruction Manual. You can use keyword search to locate the topics you want to find.

Unlock

Instantly unlocks any door

Locate

Use this button to locate any cardholder record based on: memory number, name, vehicle, license plate number, make or color of car.

Release Info

Shows the paramters of your system.

CARDHOLDER DATABASE

Note: The cardholder record form contains subforms for entering vehicles and security levels. These subforms reflect only the information about that particular record. So if you use the search utility in either subform, you will be seeking information pertaining only to that record. If you want to find a cardholder's record based on a license plate number, you must use the Locate Tool Bar button.

To program a card into , you must minimally enter a name, a valid card memory number (which may differ from the number shown on the outside of the card), and security level assignments. Once entered, you can program the card by clicking on the PROGRAM THIS CARD button. Only those levels displayed will be programmed. If you have previously programmed the card into other levels by using Direct To Memory Programming, they will be erased, and only those levels reflected here will be applicable to this card.

You can change the TAB order of your form so that the cursor jumps only to the fields you wish to populate with data. To do this, select FORM DESIGN from the View Menu, and then select Tab Order.

Open Report Or Search For Another Record

You can view the cardholder data in a columnar format. You can change the order of the displayed records, and you can filter records to be displayed by highlighting any value. If you want to display all cardholders currently programmed into level 5, just highlight the 5, and do a filter by selection (right click). *Microsoft Access* provides many tools for searching, filtering, and displaying data. Most of these capabilities can be explored without reading any manuals.

Nine Digit Social Security Number Systems Only

There is a special version of our **Access Central** Interface for nine digit systems. To enroll cardholders, you must begin by entering a nine digit number. The first record is a sample record, but you may type over the sample information to enroll your first cardholder. At the bottom of the record there is a field called: Internal Memory Location. You will notice that this number increases consecutively as you add new records. Each system is specifically configured for a certain number of cardholders, and you can see what that capacity is by clicking on the ABOUT button. You must not attempt to enter records that exceed this capacity.

At any time, you may reuse a memory location previously occupied by a voided card. To void a cardholder, simply type the word VOID, and click the PROGRAM THIS CARD button. Now you may enter a new cardholder into this Internal Memory Location. Be sure to remove the word VOID, and be sure to reassign new levels to the new cardholder.

Note to Johnson Controls Metasys Users

The Internal Memory Location Number located at the bottom of each record is the decimal number that will be reported to Metasys. When you program this number into the PMI software, it will become available for Metasys-wide reports, Process Groups, and HVAC Interlocks.

READER AND MODULE DEFINITIONS

In order to view transaction records and perform module programming, you must define each hardware device in the system . Use the assigned two digit module

code, and the text description you want.

DEFINE LEVELS

Cardholder Security Levels

To simplify the selection of appropriate levels for cardholder programming, Access Levels you define in may be fully described in *Access Central*. The descriptions you make are displayed on each cardholder record form in the Level Library. When you assign a level to a cardholder, this description will automatically be displayed. For a level to be valid, it must have at least one reader, one day of the week, and one start and stop time.

Reader Module Level Definitions

While Security Levels define the status of cardholders, Command Levels define the status of Command Modules. Each Command Module Level can be defined to perform one of the following commands:

- Timed Unlock
- Timed Alarm Shunt
- Timed Keypad activation

For entry points equipped with only a Keypad, a Command Level must be defined in order to activate it for use. If a Keypad Level is not currently active, the Keypad will not permit access. This insures against off-hour tampering.

Keypad Operation

Keypad Only

For entry points with a Keypad and no card reader, it is necessary to both create a Command Level to activate the Keypad as described above, and a Security Level To authorize Keypad use just as you would for cardholders. You must then program the active Keypad numbers into this Security Level. When an individual enters a valid Keypad number into the Keypad, entry will be granted.

A Keypad transaction begins with the star key (*), followed by the Keypad number, and ending with the pound key (#).

Keypad Or Card

If the Command Module firmware is set up to accept either the use of a Card or Keypad Code, the instructions above for *Keypad only* apply.

Card Plus Keypad

When the Command Module firmware is set up for Card Plus Keypad you must first enter a valid Keypad number when a Keypad Command Level is active. If a Keypad Command Level is not active, access will be granted based only on a valid card.

A detailed explanation of the Keypad option is contained in the Component Installation Instruction Manual.

CAUTION

Never disable a command level that is currently active by removing its module location code, unless that module is defined in another level. Doing so will prevent the module from receiving a command to secure. In other words, if a door is unlocked, it will not re-lock until commanded to do so. Removing a location code from an active level will terminate communication to that module unless it is also defined in another level.

To disable a level that is currently active (relay(s) pulled in), first replace the current day with any another day of the week. Wait two minutes to insure that the secure command has been transmitted to the module. After two minutes, modules codes may be removed.

To define or change a command, you must select a Command Level number, and then choose either “U” for UNLOCK, “A” for Alarm, or “K” for KEYPAD ENABLE. When choosing UNLOCK, the defined command will both UNLOCK, and shunt the ALARM during the programmed period.

If ALARM is chosen, only the alarm will shunt during the programmed time period.

Any command can be changed from one type of command to the other by simply hitting “A”, “U”, or “K”.

A command definition can include up to 127 entry points, one or more days of the week, and a specified time interval.

For increased security, the computer checks every programmed module once per minute to insure that its output relay is in compliance with the programmed parameters. When programmed commands are initiated, they will be transmitted to their respective modules on the minute.

Transaction Activated Levels (Elevator)

Selective programming of individual cardholder access to authorized floors can be accomplished with the 16 relay Output Module. The Output module may be used for either continuous time programmable output commands, or for momentary activation in response to authorized cards.

For elevator control applications, when a card is inserted into the card's reader, all the relays applicable to that cardholder's authorization LEVEL will activate for a period of time pre-selected at the Output Module. When that time period expires, the Module will assume the relay matrix that was set before the Transaction activated event.

The time selected should give the cardholder time to select a floor button. A separate timer adjustment screw is provided for each bank of 8 relays. If the button pressed matches an active relay, then the elevator control logic should provide the cardholder access to that floor. This system provides relay outputs only, and interfacing to actual elevator control circuitry should be coordinated with the manufacturer of the elevator equipment.

An output relay should be dedicated for each controlled floor per reader. For example: One elevator car with a reader serving 10 floors requires 10 relays. If two elevator cars access the same 10 floors, then 20 relays should be dedicated. If more than one elevator car has access to the same relay, a possible contention could exist when there are simultaneous card insertions in both cars. If this is not considered to be a problem, then up to 16 readers can be programmed to address the same relay.

You may combine Transaction activated Levels And Time Programmed Levels when certain floors are required to have free public access, and other floors require card activation.

Up to 63 Output Modules may be used providing 1008 relays each with a unique code. A relay output code is a four digit number consisting of the two digit Module code plus the specific two digit relay number indicated along the terminal strip. Any Module code may be selected from 00 to 3F except for the code 20 which cannot be used.

Transaction Activated Levels are used to define the various access categories of floor authorization in which cardholders will be programmed. There are 100 possible Transaction Activated Levels. The levels dedicated to elevator control must be numbered between 801-900.

Programming these levels is similar to Access LEVEL Definitions used for entry control.

A Transaction Activated Levels is defined as follows:

- One Reader/Command Module Location Code (One elevator car except as noted)
- One or more days of the week
- A time parameter
- One to 78 Output Relay codes (Floors).
- A start and stop date if required

As stated earlier, each car should have exclusive outputs, however there is no problem applying many different levels to the same Outputs. For example, a single output for a given floor may be included in a master level for top executives, and also included in a level intended for more restrictive cardholder use. Any cardholder may be assigned to one or more levels, or all the levels.

After at least one Elevator LEVEL is defined, individual cards may then be programmed using FUNCTION 3.1.

Transaction Activated Levels Triggered by Alarm Inputs

As discussed earlier under Alarm Text, Transaction Activated Levels may be triggered by unused card numbers sent from incoming alarms. This feature is useful when specific alarm inputs must pulse specific relays for alarm panels, zoned alarm dialers or CCTV controllers. Setting up Transaction Activated Levels which are triggered by card numbers defined in alarm text is performed exactly as described above for elevator levels. Remember to choose memory numbers that are not assigned to cards, otherwise the use of those cards will trigger the output defined in the alarm text.

I/O Module Levels

I/O Modules include 16 Relay Output Modules, 16 Input Alarm Modules, and Multi-Point I/o Modules. These levels can be defined to determine the status of the modules by time and day. When relays should be pulled in, or alarms shunted. Output LEVEL Definitions apply to the 16 relay Output Modules. These levels are handled exactly like the Remote Command Definitions used for Command Modules, except that a four digit number is used to define these levels instead of two. If both 16 Relay Output Modules, and Programmable 16 Input Alarm Modules are used on the same system, care should be taken not to duplicate module codes (See hardware installation instructions).

Output Levels defined for Relay Modules simply activate and deactivate the relays when programmed to do so. Output Levels defined for the Programmable 16 Input Alarm Modules deactivate or shunt the alarm inputs when programmed to do so. There are up to 100 available LEVELS numbered from 1-100.

An Output LEVEL consists of the following:

- One or more output address (Up to 78)
- One or more days of the week
- A time parameter
- A start and stop date if required

When each of these three parameters are entered, the command will be transmitted at the next one minute update. Every output in the system which is defined in at least one LEVEL, is automatically updated once per minute on the minute to insure maintenance of the programmed status in the event of a remote power interruption. Only locations programmed into properly defined levels (active or inactive) will receive the update, so a location should not be removed from an active level (relay pulled in or alarm shunted) unless it is also programmed into an inactive level, otherwise it will not receive a command to change states.

Routine 5. ALARM MODULE LEVELS: Programmable Shunting

Alarm Module Levels apply to the 16 Zone Alarm Input Modules with codes ranging from 00-3F for a total of 1008 shuntable alarms. Module code 20 is not usable.

These levels simply deactivate (shunt) alarm inputs when programmed to do so. Alarm Module Levels are handled exactly like Output Module Levels. If both 16 Relay Output Modules, and Programmable 16 Input Alarm Modules are used on the same system, care should be taken not to duplicate module codes (See hardware installation instructions).

An Alarm Module Level consists of the following:

- One or more input addresses (Up to 78)
- One or more days of the week
- A time parameter
- A start and stop date if required

When each of these three parameters are entered, the command will be transmitted at the next one minute update. Every input in the system which is defined in at least one LEVEL, is automatically updated once per minute on the minute to insure maintenance of the programmed status in the event of a remote power interruption. Only locations programmed into properly defined levels (active or inactive) will receive the update, so a location should not be removed from an active level (alarm shunted) unless it is also programmed into an inactive level, otherwise it will not receive a command to change states.

If an Alarm Level expires when its input is open (in alarm), that alarm will be annunciated, and will display as an open alarm.

MAKE I.D. BADGE

Because *Microsoft Access* supports linked or embedded photos, the ability to include photographs in the database or to create a first quality photo I.D. card is virtually a free bonus of the system. You may use any low cost consumer digital camera such as the Casio QV-10A.

You may place a photo onto the cardholder form using any of three methods. You can create a link (BMP or PCX files only) to an existing photo, you may copy a photo image from your application into the Windows clipboard and paste it, or you may drag and drop a photo from your photo imaging application. To make the choice, simply right mouse click the photo area of the form.

Which ever method you use, the original size of the photo is not important since *Access* will re-size it to fit the I.D. badge form provided the proportions of the photo showing just head and shoulders is maintained for each image. If the photos you take are not confined to a portrait showing only head and shoulders, you can rotate and crop the image in your application, then copy and paste it into your cardholder database.

There are two ways to make a badge; print directly on the surface of a plastic I.D. card using a Fargo printer, or create a fully laminated I.D. card using the following process:

To make the badge, you will need the following equipment and supplies

1. Table top roll laminating machine and carriers
2. High resolution Inkjet printer (Epson 720 DPI)
3. Special Image Transfer Paper
4. Scissors

The complete process requires the following operations:

1. Load the Special Image Transfer Paper into the printer.
2. Print the desired employee record from the Access Print I.D. form.
3. Using your scissors, trim out the image to a width that will fit through your laminator.
4. Position the clear overlay over the image so that it frames the I.D. badge the way you want it.
5. Place the image and overlay into the laminating carrier pinching it together securely so it won't shift.
6. Tear the clear overlay away from the paper.
7. Place the clear overlay (now with I.D. image) onto the badge blank and run it back through the laminator.

This process permits a center core of any thickness, and back overlays with pressure sensitive adhesive for attachment to access cards. In addition, the badge blanks may be ordered with badge clip slot pre-punched.

Mass Program Cards At Once

Use this utility to program every cardholder into your database at once. This utility would be useful for initializing a database where no cardholders had been programmed when the record was populated. You might also use this utility to make sure that the *Access Central* database matches what's in in case you have combined Direct To Memory Programming and *MS Access* Programing. To do this, first use P2's direct To Memory Programming to void all cards in all levels. Save it, then select Update System form *Access Central*. This process can take several minutes depending upon the speed of your computer and the number of

cardholders to program. It can take as much as a second or so per record.

REPORT MANAGER

Transaction activity may be viewed and printed using Report Manager. When this program is running, it captures and stores system activity. It can only report activity that occurs while it is running. If Report Manager is not running, there is still a log record containing activity that is accessible from the PC-P2 background program.

TIME MANAGEMENT REPORT

This utility creates a report based on "IN" and "OUT" time calculations. You must designate which entry points are entrances, and which are exits for the purposes of this calculation. Select "Define Entry Points" to make these designations. The default report contains a column for Revenue Time which is the actual time rounded up to the next 30 minutes. For Time & Attendance applications, you can ignore this column, or delete it Report Design.

You can run the report by individual, or by groups. If you want the report to be grouped by department number, or by tenant group, simply place unique descriptors on each cardholder's text, such as Dept 123. When you run the report, simply enter this unique string.

Access Central Database Properties

All tables, queries, forms, reports, macros, and modules are contained in a single database. You may name or rename this database as desired, but you must not rename any of the data contained in it. All definitions and properties are available for user modifications utilizing the full capabilities of Microsoft Access, however Toye Corporation is only able to provide support for those features it has included in the mdb file.

You may explore the database structure at any time by hitting the F11 key. Following is an overview of this structure:

Tables

Tables are the basic raw building blocks of a database. The tables you find here are used in combination with other tables to create meaningful information. One of the tables (tclog.dta) has an arrow indicating that it is linked to an outside table. It assumes that the tclog.dta table is in a subdirectory named: c:\tc85dir. If this file is located elsewhere, the import definition must be modified in Linked Table Manager.

Queries

Queries combine information from one or more tables or other queries to create relational data. For example, when you display transactions, the information comes from two different tables; `tclog.dta`, and entry points.

Forms

Forms are created to display the information from tables, or from queries.

Reports

Reports format data when they require formatting or calculations, such as the Time Management Report.

Macros

Macros perform sequential tasks. For example, the macro name "autoexec" initializes the program so that the Access Central Main Switchboard Menu appears when you load the program. Other macros allow you to clear all of your tables in case you want to start from scratch. There are three macros defined to import data from external sources in order to automatically populate the Access Central Cardholder Database. They are:

ImportP2Programming. This utility can be used if your is already programmed with cardholders. It will extract the names and security level assignments of each cardholder, and create a record in Access Central

ConvertDBF: This utility is designed to import data from previous versions of where the data is contained in the built-in dBase III utility.

ConvertMDB: This utility is designed to import data from earlier versions of Access Central

Modules

Modules contain the actual Visual Basic Code needed to link with Access Central. The module named *Global* sets the directory paths, so if your software is not running in `C:\tc85dir`, you will need to change the path statement in this code module. It only appears once at the top.

PC-P2 Operating Instructions

PC-P2 is comprised of three main software components; `SR.COM`, `P2.EXE`, and `MP.EXE`. All three are loaded together from `PC.BAT`.

SR.COM is a program always running in the computer's background memory. It is responsible for managing communication with all the access control system hardware devices that are connected to the computer's serial port. In addition to managing communications, `SR.COM` maintains all system programming files in

memory so that access decisions can be made instantly without disk access. When a card is presented to a reader, the reader receives the go or no go signal virtually in milliseconds directly from SR.COM.

P2.EXE is the human interface used to program SR.COM and to display system transactions as they occur. P2.EXE is a DOS based program that will run under Windows 95 full screen or in a graphical window. In a Windows 95 environment, P2.EXE must be running in either the foreground or minimized on the task bar for proper operation.

All basic system definition parameters (except cardholder programming) must be performed using P2. These include Security Level Definitions, Alarm Definitions, Time Programmable Outputs, Elevator Levels, Holidays, and Unlock Schedules.

MP.EXE is a search and report utility designed to provide instant displays or reports of system activity, and to set up import parameters for customers desiring to maintain cardholder programming from an external dBase file. Several specialized parking and space count management reports are also included in MP.EXE. This program is initiated by hitting the "H" Hotkey, and is especially useful to users not using the Microsoft Access Interface.

Cardholder Programming Choices

There are two cardholder programming methods from which to choose:

- Direct To Memory Programming using P2. (**M** Hotkey)
- A built-in dBase III cardholder programming utility (**B** Hotkey)

Direct To Memory P2 Programming

Sometimes it makes sense to initialize a system by programming cardholders directly into P2. It takes only a few seconds to validate cards or ranges of card numbers to get the system functioning immediately. With that accomplished, the Microsoft Access database can be populated at a more leisurely pace. Once all the individual cardholder records are entered into the Microsoft Access database, you can erase the direct To Memory Programming and replace it with your new Microsoft Access database.

Built In dBase Utility

Many customers prefer the simplicity and versatility of dBase. Using dBase, it is easy to use employee records from a preexisting database, or a database located on a network. The built-in dBase utility is especially useful for customers who prefer to work out of DOS environment.

Overview

Your Computer's Configuration

Your computer must be equipped with a serial communication port. All software is COM port specific, and must be specified when ordering (COM1 is the default). For Windows 95 users, *Microsoft Access 7* or higher must be pre-installed on the computer along with Windows 95. For DOS only users, you need DOS 6 or higher.

The ANSI.SYS driver must be installed in your CONFIG.SYS file in order to use the dBase Management and the Hard Disk Management History features (**H** Hotkey). This can be added with a text editor, or you can create a new CONFIG.SYS file using a simple DOS command. The file ANSI.SYS is usually located in the directory C:\WINDOWS\COMMAND. The statement to be added to Config.sys is:

```
DEVICE=C:\WINDOWS\COMMAN\ANSI.SYS
```

BACKING UP DATA

Data crucial to your specific system is contained in all files with the extensions: .BAS or .DTA. It is wise to maintain a floppy backup of these files in the event of a computer failure. If you are backing up your transaction data on a regular basis, there is no need to maintain a separate backup of TCLOG.DTA which is the large file used for transaction storage. Should you experience a computer failure, or you wish to move your system to another computer, simply use the original installation program to start up the system, and then copy all the .BAS and .DTA files from your backups into the TC85DIR sub-directory.

DEFINING YOUR PC-P2 SYSTEM

The software program permits the user to custom define all access control parameters. These parameters are called SECURITY LEVELS. A SECURITY LEVEL is a convenient way to define the common access status of a group of cardholders. For example, LEVEL #1 might be for executives. Any person assigned to LEVEL #1 would have access to all doors at any time day, night and holidays (day 8). Instead of laboriously programming executives into each and every door individually, the operator need only assign the card once to LEVEL #1. LEVEL #2 might be defined for first shift production employees. That LEVEL would designate certain authorized entry points, a start time, a stop time, and the applicable days of the week, such as Monday through Friday but not on holidays. If a cardholder's access status does not fit one of the predefined levels, then you can program the card into a combination of levels which will create the exact access status you desire.

Security Levels can be created for specific date ranges in case you want to automatically validate a group of cards on a specific date and time, and then automatically void those cards at another date and time. This feature might be useful for controlling access to temporary groups such as contractors.

While Security Levels define the access authorization for cardholders. The same

kind of levels are used to define the desired status of field modules. These are called Module Levels. There are Module Levels available to program relays, alarm shunt periods, elevator outputs, and keypad activation times. Like Security Levels, Module Levels can be programmed for specific date ranges also. A parking lot gate could automatically be opened on a specific Sunday for a special event for example.

To examine these levels, press the "L" key from the ACTION WINDOW, or select FUNCTION 5 from the FUNCTION MENU.

PROGRAMMING CARDHOLDERS INTO THE SYSTEM

Internal Programming

The "M" hot key takes you to the Internal Programming Routines. Changes you make here go directly to the background operating system the moment they are entered on the keyboard, and take effect immediately.

There are a number Internal Programming techniques that cannot be performed efficiently by *Microsoft Access* or a dBase program such as block voiding or validating a specific range of card numbers. If for example you want to instantly preprogram a group of cards to be valid in Level 1, and another group of cards in Level 2, you can perform this operation in seconds. With certain precautions, you can take advantage of the simplicity and convenience of *External Programming*, and the flexibility and immediacy of *Internal Programming*.

THE FIRST STEP

To begin, make copies of the Level Definition Work Sheet included with this manual. Fill out a work sheet showing the descriptions of your entry points. To the left of the description, enter the two digit location code. This code is the Remote Command Module code already selected during installation. The Component Installation Manual shows how to set the Module Codes.

Next, create a few hypothetical levels. These will be common access categories shared by several individuals. If you want certain cardholders to enjoy virtual carte blanche access, you might want to define a master level and describe them as Grand Masters, or Executive Management. Each such group needs to be assigned a level number.

Now enter your Levels on the main work sheet showing appropriate module codes, applicable days of the week, and start and stop times. If a particular Level defines more than 12 readers, use additional lines to define that Level.

With entry points and access level categories defined, the information can now be compiled for easy entry into the computer. Press the "L" hot key from the ACTION WINDOW, or select Function 5 from the FUNCTION Menu. Select Routine 1 to Define Levels.

THE SECOND STEP

With at least one level defined, one or more cards can be programmed into these levels, or into any combination of levels using *Access Central*, or the Internal Programming Routines ("M" hot key).

NOTE: The sequential card serial number stamped on the outside of the card may not necessarily be the number encoded in or on the card. Always use the random number (Memory Number) shown on the Card Log for programming purposes unless you are sure that the outside serial number is in fact the same as the one actually encoded in the card.

LAN NETWORKING

It is possible to control all functions of the access control system from any LAN work station. These functions include programming changes, and remote monitoring and printout.

The most desirable configuration for LAN networking is to use a dedicated PC for access control configured with a network card. This PC would run the access control program, and a commercial program called Close-Up LAN. The software package includes both a *host* program, and a *viewer* program for up to 64 work stations. No special software is required for the access control system to work with Close-Up LAN.

WORKING WITH THE SOFTWARE

The ACTION WINDOW is designed to provide single screen monitoring and control of every important element of access control management. The blue **Status Bar** at the top constantly displays the following information:

Type Of Transactions being displayed (selectable by hitting Escape once)

- *Current System Activity*: (all transactions: access, alarms, and counters.)
- *Access Transactions & Alarms* only.
- *Counter Activity* only.

Supervision Status

Blue means all devices are communicating properly. Red means that one or more devices are not communicating properly. To display the status of all devices, hit Escape and select Supervision Status.

Anti-Pass-Back Status

There are numerous APB modes from which to choose including Timed, In-Exit, Hard, and Soft. The selected mode is constantly displayed. To change APB modes, hit the "F" Hot Key, and select Routine 4.

Date

Displays the current date from the computer's internal CMOS clock

Daylight Savings Time Icon

If selected, the system will automatically adjust the time twice a year for daylight savings time changes. If this feature is enabled, a sun icon is displayed. To change

the Daylight Savings Time mode, hit the "F" Hot Key and select Routine 1. Time

The time displayed is taken directly from the computer's CMOS clock which is located on the mother board. It is updated 18 times per second. The time can be adjusted through the access control program

Hot Key Bar

The brown Hot Key Bar immediately below the Status Bar provides one touch access to the most used system functions. Many of these **FUNCTIONS** contain sub-menus which display the **Routines** available for that **FUNCTION**. To examine a basic system **FUNCTION**, hit the appropriate Hot Key, or hit the "F" Hot Key to display a list of every **FUNCTION**. *You may always return to the ACTION WINDOW by hitting Escape.*

SOFTWARE FUNCTIONS: as they appear on the Function Menu.

"U" : UNLOCK a Door or Raise A Gate Instantly ("U" Hot Key)

This function provides instantaneous release of any door or gate by keyboard command. The U command operates the Command Module's main relay for the amount of time selected on the main timer adjustment "pot". The shunt relay will also be activated for the time selected on the shunt timer adjustment "pot".

The U command also operates the main relay on a Dual I/O module, but not the shunt relay. The U command does not operate relays contained on the 16 relay output module.

P : PASSWORD Protection

This function protects specific system Functions from unauthorized use. Any combination of ten characters may be used for a password. The selected passwords can be saved along with other data on the hard disk so password protection is unaffected by re-booting. It is best to wait until all system parameters are programmed before selecting passwords and saving them.

Passwords are mutually exclusive so that any combination of **FUNCTIONS** may be protected by any password. In addition, each password can include the ability to program cards into restricted levels. Restricted levels provide an additional password layer so that persons whose password enables them to program cards in unrestricted levels cannot also program cards in restricted levels.

If you unintentionally select Restricted Levels, and a program a card, that level becomes restricted. To Un-Restrict that Level again, simply go to Level Definitions, and remove all the days of the week from that Level, and reenter the days again. Do a Save upon exiting.

Note: The Restricted Level feature works only when Internal Memory Program-

ming is utilized.

There are four levels of passwords available. Knowledge of the Master password is required to change other passwords. The Password Function is used to:

1. Define each Password (visible or invisible)
2. Define which Functions are to be protected by each password.

Knowledge of the master password provides access to any menu item (Function). Knowledge of other passwords provides access to only those menu items protected by that password.

Passwords are “case” sensitive which means that if an upper case character is selected initially, a lower case character cannot be substituted when entering the password.

Always test the selected passwords before saving them. Once tested, use FUNCTION 3.3 to store them on the hard disk.

If You Forget The Password

1. Exit to DOS
2. Type: `C:\xxx\DEBUG C:\TC85DIR\DEFS.BAS`
XXX= The sub-directory containing DEBUG.COM
3. Press the ENTER key
4. At the Debug prompt (minus sign), type:
FCS: 107 186 00

Note the colon symbol and the spaces

5. Press the ENTER key
6. Type the letter: **W** and then press ENTER
7. Type the letter **Q** and then press ENTER
8. Re-boot the computer

This will clear all the passwords.

Note: You may want to copy these instructions and put them in a secure location, and then black out this section with a felt marker to prevent system tampering.

1 : TIME & HOLIDAY Definitions

Routine 1. Set Date and Time

Setting the time is not necessary with systems equipped with correctly set perpetual clocks. If the perpetual clock is incorrect, or an instant time change is desired, use Function 1. to change the time.

Routine 2. Holiday Definitions

The enhanced software provides for holiday exceptions for its security and

command levels. This means that you can automatically override a level or a command that might ordinarily be good on Thursdays, but if Thursday happens to be a holiday such as Thanksgiving, the computer will reject access to any level not good for Day 8, (Holiday) authorization. Any level you wish to remain active on holidays must include day 8.

At the Holiday Screen, enter the date of all company holidays, and on those days, only LEVELS designated for Day 8 will be active. Holidays may be entered in any order up to the year 2099. To remove a date from the screen, simply reenter it.

Routine 3. Automatic Daylight Savings Time

When enabled, this feature automatically changes the system clock for the new time. The actual time of change is displayed on the screen and may vary depending on locale. If your PC automatically adjusts for Daylight Savings Time, do not enable this feature.

2 : HARD COPY Options

Note: If you use this utility to print transactions as they occur while also using Access Central, you must load Access Central prior to turning on the printing feature in PC-P2.

The line printer may be programmed to print an ongoing hard copy report as follows:

Current Mode »» 0 = Print Nothing

1 = Print Valid ACCESS Transactions only

2 = Print ACCESS Exceptions & Alarms

3 = Print All ACCESS Transactions & Alarms

4 = Print COUNTERS only

5 = Print COUNTERS & Valid ACCESS Transactions

6 = Print COUNTERS, ACCESS Exceptions & Alarms

7 = Print Everything

The hard copy log shows each transaction by day, date, time, location, system code, memory code, and various transaction status symbols. If the printer is on-line, it will also record Unlock Commands.

The following are special status codes that indicate each type of transaction exception:

- A** Hard Anti-Pass-Back violation, no access granted
- a** Soft Anti-Pass-Back violation, access was granted
- S** Wrong system code, access was not granted
- Invalid card, access was not granted
- K** Keypad violation, access was not granted
- *** **Alarm**
- N** Hard Nesting violation

D Debit card violation (out of uses)

Transactions without one of the above symbols are valid card transactions which do not involve exceptions.

3 : MEMORY Programming & Verification ("M" Hot Key)

Routine 1. PROGRAM Card MEMORY is used to program individual cards into their respective Security LEVELS. When programming cards, it is possible to enter more than one level so that cards can be simultaneously programmed into multiple levels. In addition, you can program all cards into selected levels at once, or a range beginning with one number and ending with another.

Software options are available to accommodate 4 , 5, and 9 digit numbers. When entering individual memory codes for programming, type the full number of digits. If you have the 9 digit software, you can use numbers that have fewer than 9 digits as long as you precede them with the appropriate number of zeros.

Routine 2. LOAD Card MEMORY from Disk, transfers all data contained on the disk into the computers memory.

Routine 3. SAVE Card MEMORY on Disk, transfers the contents of the computer's memory onto the disk. **Always use this Routine following changes to the program.** You do not need to use this Routine to save changes to cardholder text, or when using dBase Memory Management.

Routine 4. List LEVELS per Card provides a listing of all LEVELS in which a given card is programmed.

Routine 5. List CARDS per Level provides a listing of all Cards assigned to a given level.

Routine 6. Cardholder TEXT permits the entry of names or other text to be printed out with every card transaction. Simply enter the cardholder's memory code found on the card log, and enter the person's name and/or other information.

Routine 7. ALARM TEXT allows you to identify incoming system alarms with up to 32 text characters. Until text is assigned to an input, that alarm point is not activated and will not report. Assigning at least one character of text to an input activates the alarm. These alarm inputs may originate from Command Modules, 16 Input Modules, or Dual I/O Modules.

The system is capable performing a combination of functions based on incoming alarms. Some of these functions are triggered by the text information you enter. You can use any input to perform any of the following functions:

- Display, annunciate, archive, and print as Open & Secure Alarms
- Trigger a BATch file (such as one defined to display an alarm graphic).
- Activate a relay on a Transaction Activated Output Module
- Increment or decrement a Counter (see space counting)
- Toggle between the Transaction and Counter Status screens
- Cause the "PC" to emit a continuous high pitched "Warble" until acknowledged by an operator.

Alarm Descriptions

Up to 32 characters of text may be entered for each alarm. This text will be displayed and logged each time the input changes state. The actual display will also include either the text: ALARM OPEN, OR Alarm Secure.

Alarm inputs may originate from a Command Module, a Dual I/O Module, or a 16 Input Alarm Module. For monitoring alarms originating from a Command Module or Dual I/O Module, simply enter the two digit Module code followed by 71 or 72 depending upon which input you are monitoring. To define text originating from a 16 Input Module, enter the two digit module code followed by the two digit input. When using both Command Modules, and Dual I/O Modules, you must not duplicate Module Codes since they are essentially the same type of device. You may however assign these same two digit module codes to 16 Input Modules without conflict.

ALARM BATch.FILE OUTPUT

This feature allows incoming alarms to cause the computer to execute predefined BATch files. A BATch file may be defined to load another program such as Procomm for example. Procomm would be configured to dial a pocket paging service to annunciate alarms.

Batch files can also be defined to display custom graphic or text screens that will appear automatically when there is an alarm. A commercial paint program can be used to create the graphics. For example, to display a graphic saved in the PCX format (16 colors 640x480) named FRNTDOOR.PCX, simply copy the graphic file into the TC85DIR sub-directory, and create a Batch file with the following command line:

```
SHOWPCX FRNTDOOR.PCX
```

The program SHOWPCX has already been installed in this directory during installation of the access control program.

Batch files can be created using any text editor such as DOS EDIT. You can use different names for each Batch file such as ALARM1.BAT.

The Alarm Bat file feature can be applied to any alarm input, and that input can be automatically turned on and off in software using the shunt features described earlier. This restricts BAT.FILE responses only to specified times.

To cause a specific a alarm to execute a BATch file, simply place an asterisks (*) in the first character position of the alarm text. The next 8 characters should contain the path and name of the BATch.file. Do not use the extension .BAT. For example:

***ALARM1**

This assumes that you have placed ALARM1.BAT in the access control working sub-directory: TC85DIR.

You may add any additional text you wish to describe the actual alarm IE:
***ALARM1 BUILDING 3 FRONT DOOR**

When adding additional text after the BAT file name, begin in position 10 or 11 to avoid any conflict regarding the name of the BAT file.

Note: the ALARM BAT.FILE feature works only when the Access Control program is running in the foreground. If any alarms come in after exiting to DOS, they will be stored and executed in order once the foreground program is loaded. This insures that no alarms can be lost while the system is processing another BATch.FILE.

Transaction Activated Alarm Output

Incoming alarms can be programmed to pulse one or more relays contained on the 16 Relay Output Module. This is accomplished by selecting an available system memory number, and entering it into the Alarm Text field preceded by a back slash. For example, if you want a certain alarm to pulse an output relay, you simply select an unused system memory number, and enter it anywhere in the alarm text field as follows: \1234. You must then create a Transaction Activated Output Level, and then program number 1234 to be valid in that level.

You may combine both an Alarm BATch file and Transaction Activated Alarm Output from the same alarm input if you want to both display an alarm graphic and create a relay output. For example:

***ALARM1 BUILDING 3 FRONT DOOR \1234**

Screen Switching

For parking operators who want attendants to be able to view system transactions and the status of Space Counters without allowing them the use of a computer keyboard, Screen Switching can be performed with a simple push button tied to any

input such as a nearby exit reader.

Simply place a semicolon (;) in the first character position of text for that input. Since this alarm input will probably be used exclusively for screen toggling, you may want to assign additional text to this input for logging purposes. Example:

; EXIT BOOTH 1 SCREEN TOGGLE

ALARM WARBLE

Any alarm can be programmed to warble by placing a caret symbol (^) in the first character of the alarm text. To do this, press the M hot key to select Memory Functions. Select Routine 7, Alarm Text. Enter the alarm code. Place a caret symbol in the first text position so that it reads:

^ ALARM TEXT

The caret symbol triggers the warble, and the text that follows defines the incoming alarm.

You may also want the incoming alarm to trigger a BATch file. If so, place the name of the BATch file next to the caret symbol beginning in the second text position. If you want to trigger the BATch file without setting off the warble, use an asterisk instead of a caret symbol.

Routine 8. PROGRAM Cards in RESTRICTED LEVELS. A Security Level automatically becomes Restricted if one or more cards is programmed into it. This feature is useful if more than one person has card programming authority, and you need to prevent unauthorized individuals from programming cards into certain levels.

To unrestricted a level that has been restricted, simply select Level Definitions and remove all of the days defined for that level, and then reenter them. That level will now be unrestricted.

If you are using the restricted level programming feature, be sure to password protect dBase Memory Management, and Level Definitions so that restricted levels cannot be overridden by unauthorized individuals.

Routine 9. Program Card Use Debiting (Optional Software)

This optional software module allows you to specify the number of uses each designated cardholder may have of one or more specified readers. When cardholders are programmed for use in readers subject to debiting, they will be denied access if the value of their account is zero. Other cardholders not programmed for debiting are unaffected. Cardholders subject to debiting may use readers not designated as debit readers if they are programmed accordingly.

To initialize Card Use Debiting, simply enter the readers to be subject to debiting, enter the cardholders, and assign a number of uses.

4 : ANTI-PASS-BACK Definitions & Space Counters

Routine 1. Anti-Pass-Back Definitions

Any reader in the system may be defined as an entry point or an exit point for the purposes of detecting multiple entries by a single card. If the Anti-Pass-Back feature is enabled, a card will be denied passage if an attempt is made to use it for a second entry if it has not first passed through an exit reader, and vice versa. For Anti-Pass-Back to be enabled, you must define at least one entrance reader, and one exit reader.

Timed-Anti-Pass-Back

Timed Anti-Pass-Back is designed to control entrance tailgating where there are no on-line exit readers. In addition, the Timed Anti-Pass-Back feature may be used for automatic once per day resynchronization with or without on-line exit readers.

When timed Anti-Pass-Back is enabled, all cards are resynchronized at the time interval specified. You may select a resynchronization interval from 1 minute to 2400. For resynchronization every 15 minutes, simply enter 15. For once per hour, enter 60. For automatic resynchronization once per day at 1 AM, simply enter 0100. To disable Timed Anti-Pass-Back, enter 0.

If Timed Anti-Pass-Back is to be used without an exit reader, you must select a bogus exit reader location in order to initiate Anti-Pass-Back.

The icon header will show T-APB for Timed Anti-Pass-Back, and D-APB for Daily resynchronization. The icon will also show whether APB is enabled on entrances, exits, or both.

Hard and Soft Anti-Pass-Back

When any reader module code is entered as either an entrance or exit location, all cards using that reader automatically become subject to anti-pass-back detection. If anti-pass-back is disabled, “soft” anti-pass-back will be in effect which means that violations will be logged as exceptions, but passage will not be denied. If anti-pass-back is enabled, “hard” anti-pass-back will be in effect denying passage to violators. It is possible to invoke “hard” anti-pass-back at exits, and “soft” anti-pass-back at entrances, or any combination.

Valet and Special Anti-Pass-Back Exceptions

Specific cardholders can be programmed to be exempt from anti-pass-back control. Simply select FUNCTION 5.3, and define the highest available level. Transaction Activated levels are not subject to Anti-Pass-Back control, so any cardholder programmed into these levels will be exempt. Transaction activated levels require

an Output to be defined. Enter 2001 for the output code.

Hard Nesting

Nesting is the term used to describe enforcement of special area parking. The nest is the special area into which designated vehicles are to park. Nesting software is designed to detect vehicles which fail to park in the special area, but instead remain in a premium area. The software permits the selection of a grace period (up to 255 minutes) within which nested vehicles must vacate the premium parking area.

Two forms of nesting are available. Soft nesting simply allows the operator to display or print a list of vehicles which have violated the nesting parameters. Soft nesting reports are generated using Function 9, Hard Disk Management.

Hard nesting actually denies use of the card for exiting the premium area if the nesting grace period has been exceeded. In order to avoid a hard nesting violation, the vehicle must enter the nest, or exit the parking facility within the grace period. If the grace period is exceeded, the card will not operate any nest entrance reader, and will not operate any premium area exit reader.

For the purpose of nesting enforcement, any reader that permits entry to the premium area is considered an ENTRANCE reader. Any reader that can be used to exit the premium area is considered an EXIT reader. Therefore, the entrance to the nest must be defined as an EXIT reader. The nest exit reader must be defined as an ENTRANCE reader.

For systems with hard nesting, the highest security level is used as a special nesting level. If the system has 100 Security Levels, Level 100 is used to define the nesting level. The use of a level to control nesting permits the operator to designate specific times and days when hard nesting will be active. There may be certain days, times, or holidays that may not be subject to hard nesting. Security Level Definitions are defined using Function 5, Routine 1.

Any ENTRANCE READER, and any EXIT READER to be used in conjunction with nesting must be so defined using Function 4, Routine 1, Anti-Pass-Back Definitions. Hard, Soft, or Override Anti-Pass-Back may be invoked without affecting hard nesting. In either mode, hard nesting will prevail.

Any cardholder to be subject to hard nesting must be programmed into the nesting level (Function 3.1). This makes it convenient to program any card in the system in or out of hard nesting.

Reviewing the steps:

1. Select Function 4.1 and enter as an entrance reader any reader that places the vehicle into the premium area. Enter as an exit reader any reader that exits the premium area. A reader that provides access to the nest is an exit reader. Select

the nesting grace period.

2. Select Function 5.1, and define the highest level. Under Location, ENTER ONLY EXIT READERS. Select the days and times hard nesting is to be invoked. In addition to this nesting level, you must also define at least one normal security level which contains both entrance and exit readers.
3. Select Function 3.1 and program any cardholder to be subject to nesting as valid in the nesting level, and the normal security level.
4. Select Function 3.3 and save the result of your programming.

To quickly override Hard Nesting, simply select Function 5.1 to enter the nesting level, and then remove the current day.

Capacity/Limitations

Hard Nesting is accomplished by calculating the time lapse between an exit request and an entrance transaction. The transaction data on which the calculations are made are contained in a memory buffer with a total capacity of 1,000 entrance transactions. For Hard Nesting to work properly, the total number of entrance transactions can not exceed 1,000 transactions per grace period. To calculate this capacity, divide 1,000 by the minutes in the grace period. A grace period of 10 minutes would provide a capacity of 100 entrance transactions per minute, or almost 2 per second. A 15 minute grace period would accommodate a capacity of about 67 entrance transactions per minute or more than one per second. Higher memory buffer capacities are available on special order, and are subject to the limitations of the host computer.

Routine 2. SPACE COUNTING

Any input can be used for space counting provided the source is a dry contact. Counters can be defined to increment, decrement, or count differentially. Differential counters provide output relay responses to a zero count to active lot full signs etc.

The standard Space Counting software includes 80 counters with inputs for 12 up counts, and 12 down counts each. Special optional software is available for additional counters. Each counter can trigger up to 12 relays in response to a zero count. Any counter can use input addresses also utilized in any other counter, making it possible to define many different counts from the same inputs. For example, by using two inputs, in and out, you could define at least three different counters. A spaces available counter, an occupancy counter, and a cumulative counter.

Each counter can be identified by the user with up to 48 characters of text. A counter set up screen provided under FUNCTION 4.2 to define counters and to enter text descriptions. A dynamic display screen is provided to show the status of all counters at a glance. In addition, all counter activity is logged to the hard disk for

future reference and reports. An added feature is a daily report designed to provide hour by hour counter activity for reconciliation purposes.

HOW IT WORKS

You can specify which inputs should increment the counter, and which inputs should decrement the counter. An input is any alarm monitor point. Each Reader has two, each Alarm Module has 16, and each Dual I/O Module has 2.

The set up screen also lets you select outputs should you want a relay to pull in when a count reaches zero. Any relay (Card Readers or Relay Output Modules) can be specified to activate in response to a zero count. The relay will remain pulled in until the count increases to one.

Both alarm monitor points (XX71 and XX72, where XX equals the module code) are usable as inputs to the counter. When specified as a counter input, they can also function as alarm inputs as well.

The Command Module Output Relays are both usable as Zero Count Outputs. When a relay is specified as an output, it will pull in when the counter reaches zero or below. The relays will immediately drop out when the counter advances above zero.

For the purpose of space counting output definitions, the main relay is considered XX72 and the shunt relay is considered XX71.

For a complete explanation of how to view and printout past counter activity, see Hard Disk Management functions.

IMPORTANT: If you do not want the shunt relay (XX71) to activate when the main output relay (XX72) is pulled in, you must cut the diode located at the lower left side of the Command Module. Cutting this diode will insure independent operation of both relays.

Counter Definitions

Space counters are defined in Function 4.2. Up to 12 input sources can be defined to increment the counter, and the same number to decrement it. Inputs defined for one counter can also be used as inputs to another counter.

Up to 12 outputs can be defined as a result of a counter reaching zero. Outputs defined in one counter can be used as outputs for other counters.

Vehicle Space Counting

For differential counting based on spaces available, exit inputs should be defined

to count up, and entrances inputs should be used to count down. To initialize the counter, simply enter the number of available spaces into the respective counter definition screen when the lot is empty. Vehicles entering will reduce the available spaces, and vehicles exiting will increase the available spaces.

For occupancy counting where the count reflects the number of vehicles present, simply use entrance inputs as up counts, and exit inputs as down counts. To initiate the counter, set it at zero when no vehicles are present.

For accumulative counting, define an input to count up.

Caution: It is possible to use Space Counters to unlock one or more doors based on any alarm input. This is done by setting the counter to a value of 1, and defining the doors to be unlocked as Zero Count Outputs. Never utilize this feature when life safety is an issue, or if emergency egress is the intent. In an emergency, power or communications problems may prevent the computer from sending the unlock command. Always use mechanical emergency exit devices to insure egress in an emergency.

Routine 3. IN-OUT Location Definitions (Optional V.I.P. Tracking Software)
V.I.P. Tracking is an optional software module that allows you to specify one or more individuals whose IN-OUT status is constantly monitored. When this option is utilized, all cardholders who are assigned to Level 1 will be displayed on a special V.I.P. Tracking screen when they are present.

Use Routine 3 to indicate which readers are to be regarded as entrances, and which readers are exits.

5 : SECURITY LEVEL & OUTPUT RELAY Definitions

Routine 1. SECURITY LEVEL Definitions

This function is the key to the system's ability to manage access authorization conveniently. Access levels may be defined by simply entering the desired location(s), applicable week day(s), and time parameters. After LEVELS have been defined, individual cards, or all cards can be quickly programmed into one or more of these levels.

Each LEVEL is independent of all other LEVELS (there is no hierarchy between levels). The number of available levels is determined by the size of the memory.

A work sheet is provided to assist in defining access levels. These parameters can be modified at any time.

Programming cards into the Levels you define can be password protected. A second layer of password protection may be added to certain levels so that programming can be restricted. This capability is designed for users who may have two different

operators. For example, a hospital may want all its security levels restricted so that parking personnel who must also perform programming functions for parkers cannot program cards in or out of security levels. A level automatically becomes restricted when any card is programmed into it using the restricted level option.

Once levels have been defined, they must be saved to avoid loss in the event of power failure.

Routine 2. COMMAND MODULE LEVELS:

While Security Levels define the status of cardholders, Command Levels define the status of Command Modules. Each Command Module Level can be defined to perform one of the following commands:

- Timed Unlock
- Timed Alarm Shunt
- Timed Keypad activation

For entry points equipped with only a Keypad, a Command Level must be defined in order to activate it for use. If a Keypad Level is not currently active, the Keypad will not permit access. This insures against off-hour tampering.

Keypad Operation

Keypad Only

For entry points with a Keypad and no card reader, it is necessary to both create a Command Level to activate the Keypad as described above, and a Security Level To authorize Keypad use just as you would for cardholders. You must then program the active Keypad numbers into this Security Level. When an individual enters a valid Keypad number into the Keypad, entry will be granted.

A Keypad transaction begins with the star key (*), followed by the Keypad number, and ending with the pound key (#).

Keypad Or Card

If the Command Module firmware is set up to accept either the use of a Card or Keypad Code, the instructions above for *Keypad only* apply.

Card Plus Keypad

When the Command Module firmware is set up for Card Plus Keypad you must first enter a valid Keypad number when a Keypad Command Level is active. If a Keypad Command Level is not active, access will be granted based only on a valid card.

A detailed explanation of the Keypad option is contained in the Component Installation Instruction Manual.

CAUTION

Never disable a command level that is currently active by removing its module

location code, unless that module is defined in another level. Doing so will prevent the module from receiving a command to secure. In other words, if a door is unlocked, it will not re-lock until commanded to do so. Removing a location code from an active level will terminate communication to that module unless it is also defined in another level.

To disable a level that is currently active (relay(s) pulled in), first replace the current day with any another day of the week. Wait two minutes to insure that the secure command has been transmitted to the module. After two minutes, modules codes may be removed.

To define or change a command, you must select a Command Level number, and then choose either “U” for UNLOCK, “A” for Alarm, or “K” for KEYPAD ENABLE. When choosing UNLOCK, the defined command will both UNLOCK, and shunt the ALARM during the programmed period.

If ALARM is chosen, only the alarm will shunt during the programmed time period.

Any command can be changed from one type of command to the other by simply hitting “A”, “U”, or “K”.

A command definition can include up to 127 entry points, one or more days of the week, and a specified time interval.

For increased security, the computer checks every programmed module once per minute to insure that its output relay is in compliance with the programmed parameters. When programmed commands are initiated, they will be transmitted to their respective modules on the minute.

Routine 3. OUTPUT MODULE LEVELS: Transaction Activated Transaction Activated Levels for Elevators

Selective programming of individual cardholder access to authorized floors can be accomplished with the 16 relay Output Module. The Output module may be used for either continuous time programmable output commands, or for momentary activation in response to authorized cards.

For elevator control applications, when a card is inserted into the car’s reader, all the relays applicable to that cardholder’s authorization LEVEL will activate for a period of time pre-selected at the Output Module. When that time period expires, the Module will assume the relay matrix that was set before the Transaction activated event.

The time selected should give the cardholder time to select a floor button. A separate timer adjustment screw is provided for each bank of 8 relays. If the button

pressed matches an active relay, then the elevator control logic should provide the cardholder access to that floor. This system provides relay outputs only, and interfacing to actual elevator control circuitry should be coordinated with the manufacturer of the elevator equipment.

An output relay should be dedicated for each controlled floor per reader. For example: One elevator car with a reader serving 10 floors requires 10 relays. If two elevator cars access the same 10 floors, then 20 relays should be dedicated. If more than one elevator car has access to the same relay, a possible contention could exist when there are simultaneous card insertions in both cars. If this is not considered to be a problem, then up to 16 readers can be programmed to address the same relay.

You may combine Transaction activated Levels And Time Programmed Levels when certain floors are required to have free public access, and other floors require card activation.

Up to 63 Output Modules may be used providing 1008 relays each with a unique code. A relay output code is a four digit number consisting of the two digit Module code plus the specific two digit relay number indicated along the terminal strip. Any Module code may be selected from 00 to 3F except for the code 20 which cannot be used.

Transaction Activated Levels are used to define the various access categories of floor authorization in which cardholders will be programmed. There are 100 possible Transaction Activated Levels. The levels dedicated to elevator control must be numbered between 801-900.

Programming these levels is similar to Access LEVEL Definitions used for entry control.

A Transaction Activated Levels is defined as follows:

- One Reader/Command Module Location Code (One elevator car except as noted)
- One or more days of the week
- A time parameter
- One to 78 Output Relay codes (Floors).
- A start and stop date if required

As stated earlier, each car should have exclusive outputs, however there is no problem applying many different levels to the same Outputs. For example, a single output for a given floor may be included in a master level for top executives, and also included in a level intended for more restrictive cardholder use. Any cardholder may be assigned to one or more levels, or all the levels.

After at least one Elevator LEVEL is defined, individual cards may then be programmed using FUNCTION 3.1.

Transaction Activated Levels Triggered by Alarm Inputs

As discussed earlier under Alarm Text, Transaction Activated Levels may be triggered by unused card numbers sent from incoming alarms. This feature is useful when specific alarm inputs must pulse specific relays for alarm panels, zoned alarm dialers or CCTV controllers. Setting up Transaction Activated Levels which are triggered by card numbers defined in alarm text is performed exactly as described above for elevator levels. Remember to choose memory numbers that are not assigned to cards, otherwise the use of those cards will trigger the output defined in the alarm text.

Routine 4. OUTPUT MODULE LEVELS: Time Program Activated

Output LEVEL Definitions apply to the 16 relay Output Modules. These levels are handled exactly like the Remote Command Definitions used for Command Modules, except that a four digit number is used to define these levels instead of two. If both 16 Relay Output Modules, and Programmable 16 Input Alarm Modules are used on the same system, care should be taken not to duplicate module codes (See hardware installation instructions).

Output Levels defined for Relay Modules simply activate and deactivate the relays when programmed to do so. Output Levels defined for the Programmable 16 Input Alarm Modules deactivate or shunt the alarm inputs when programmed to do so. There are up to 100 available LEVELS numbered from 1-100.

An Output LEVEL consists of the following:

- One or more output address (Up to 78)
- One or more days of the week
- A time parameter
- A start and stop date if required

When each of these three parameters are entered, the command will be transmitted at the next one minute update. Every output in the system which is defined in at least one LEVEL, is automatically updated once per minute on the minute to insure maintenance of the programmed status in the event of a remote power interruption. Only locations programmed into properly defined levels (active or inactive) will receive the update, so a location should not be removed from an active level (relay pulled in or alarm shunted) unless it is also programmed into an inactive level, otherwise it will not receive a command to change states.

Routine 5. ALARM MODULE LEVELS: Programmable Shunting

Alarm Module Levels apply to the 16 Zone Alarm Input Modules with codes

ranging from 00-3F for a total of 1008 shuntable alarms. Module code 20 is not usable.

These levels simply deactivate (shunt) alarm inputs when programmed to do so. Alarm Module Levels are handled exactly like Output Module Levels. If both 16 Relay Output Modules, and Programmable 16 Input Alarm Modules are used on the same system, care should be taken not to duplicate module codes (See hardware installation instructions).

An Alarm Module Level consists of the following:

- One or more input addresses (Up to 78)
- One or more days of the week
- A time parameter
- A start and stop date if required

When each of these three parameters are entered, the command will be transmitted at the next one minute update. Every input in the system which is defined in at least one LEVEL, is automatically updated once per minute on the minute to insure maintenance of the programmed status in the event of a remote power interruption. Only locations programmed into properly defined levels (active or inactive) will receive the update, so a location should not be removed from an active level (alarm shunted) unless it is also programmed into an inactive level, otherwise it will not receive a command to change states.

If an Alarm Level expires when its input is open (in alarm), that alarm will be annunciated, and will display as an open alarm.

6 : ON-LINE Mode

When initializing a new system, you must define at least one security level, and program at least one card into that level in order to place the system in the On-Line Mode. Be sure to save all programming (FUNCTION 3.3 or FUNCTION 5.6).

7 : OFF-LINE Mode

The use of this function will instantly prevent access to entry points where Module switch #9 is "off". Modules with switch #9 set to "on" will accept only those cards that contain the facility code encoded into that module. The instant Unlock feature will continue to operate when the system is in the Off-Line mode.

8 : MONITOR Transactions & Display Active Alarms (ACTION WINDOW)

Routine 1 : Display Current System Activity

Routine 1 provides a dynamic display of the 22 most recent system transactions. This includes access transactions, open alarms, secure alarms, and space counter changes.

Invalid cards are displayed in red and are annunciated with two low pitched beeps. A code is displayed indicating the reason for denial.

Alarms are annunciated with three high pitched beeps and are displayed in white on a red bar. When secured, they are displayed in green.

The following are the codes that will be displayed on the transaction screen following the time of day for violations and exceptions:

- A** Anti-Pass-Back violation, access denied
- a** Anti-Pass-Back violation, access granted
- C** Carpool violation, access denied
- c** Carpool violation, access granted
- N** Nesting violation, access denied
- n** Nesting violation, access granted

- s** Wrong system code, access was not granted
- Invalid card, access was not granted
- k** Keypad violation, access was not granted
- *** Alarm

Transactions without one of the above symbols are valid card transactions where access was granted.

Routine 2. Display Active Alarms.

Routine 2 provides an instant “snap shot” of all active (unsecured) alarms such as open doors. The exact time of the check is displayed, and a hard copy can be made by using the computer’s print screen key.

Routine 3. Purge Active Alarms

Routine 3 permits a purge of the computer’s active alarm buffer. This allows you to clear the screen of alarms that are already acknowledged but which are not secured.

Routine 4. Purge Current Transaction Screen

Routine 4 permits a purge of the current transaction screen.

Routine 5. Supervision Status

Routine 5 displays the module codes of all devices which have been defined in any Command or Security Level, or any counter input. In addition, any alarm text entered will trigger supervision of the originating module. Any device displayed on the screen will be supervised (polled) once per minute, and each device must report back to the computer immediately in order to avoid a supervision error.

Any device not responding will display in red, and the word "Supervised" located on the status line of each screen will also turn red indicating that the device did not acknowledge its poll.

During very busy or high traffic periods, it is not uncommon for a device to occasionally skip an acknowledgment while it is tied up processing card transactions or alarm inputs. If one particular module continues to flash for more than three minutes, this is an indication that the reader is actually off-line, and the condition should be checked. Supervision may be enabled, or disabled from Function 8.5 by pressing the F7 key.

6 : Monitor Space Counters

The status of each counter is displayed dynamically as they change. This screen shows the counter number and text assigned to that counter.

7 : Display Only Access Transactions & Alarms

This command causes the activity display on the ACTION WINDOW to show all transactions except counts.

8 : Display Only Counter Activity

This command causes the activity display on the ACTION WINDOW to display only counter changes. If more than 16 counters are defined, the screens may be scrolled to show the additional counters.

9 : Display Occupancy (requires optional V.I.P. Tracking software)

If your system includes the V.I.P. tracking option, this screen will display in alphabetical order all cardholders programmed into Level 1 who are currently present.

The occupancy count shown at the top of the screen reflects all occupants, not just those being tracked. Space Counter 1 is reserved for this count and may be manually adjusted using Function 4, Routine 2, Space Counting.

9 : HARD DISK MANAGEMENT Functions ("H" Hot Key)

Note: If you have Access Central running, you must close Report Manager, and the Real Time Events window to run this utility.

This FUNCTION provides the following utilities:

- Display and print achieved transactions by any search or filter criteria
- Export archived data to a dBase file
- Backup selected archived transactions to another file
- Search cardholder text file
- Import cardholder name, number and levels from another dBase file
- Setup utilities for dBase Memory Management
- Display a list of "Who is In"

- Soft Nesting Reports
- Display and print Space Counter archived transactions
- Run a daily 24 Hour Space Counter reconciliation report

Each time a transaction of any kind occurs, it is stored temporarily in a RAM memory transaction buffer, and if the access control program is running in the foreground, those transactions are cleared and written to the hard disk every 5 seconds. If the program is running only in the background, those transactions will remain in the RAM buffer until the foreground program is loaded. If more than 800 transactions occur before the foreground program is reloaded, the latest transactions will automatically overwrite the earliest.

When in the foreground program, all system transactions are written to a file named TCLOG.DTA. The standard file size is 10,000 transactions, or 125,000 transaction if specified initially. For users with much larger disk capacity, any size achieve file may be specified. TCLOG.DTA is a continuous circular file designed to permit current transaction to automatically overwrite the oldest transactions. Thus, the decision as to how often to back up transactions is dictated by the nominal traffic on the system. Within this program, you can backup any time: daily, weekly, monthly, or not at all.

It is important to note that while the Hard Disk Management program is running, on-going systems transactions are temporarily stored in a buffer and not on the disk. It is therefore advisable to return to the ACTION WINDOW when the current search has been completed.

CONDUCTING A SEARCH

The opening screen is used to set the search parameters for past transactions stored on the hard disk. Answer the prompts as follows:

- Include Access Transactions?
- Include Alarm Transactions?

Answering Y (yes) to both will produce a search of all transactions without regard to specific Alarm or specific Cardholder criteria that may be entered. For this reason, always answer yes to one or the other, but not both when specific search parameters are desired. For example, if you are searching a particular door, or a particular person, be sure not to include Alarm Transactions in the search. Conversely, if you are searching for particular alarms, do not include Access Transactions in the search.

SEARCH PERIOD

For a new system with few transactions, it is best to begin with the date of the first transaction, and some future date. To insure that your first searches will not be limited by time, enter 00:00 and 24:00 as the start and stop times. If the time and

date are left blank, the search will automatically apply to transactions that have occurred during the last fifteen minutes.

SPECIFIC ALARM POINTS

Enter an alarm location code if you want your search to exclude all but transactions from that alarm point.

LIMITING THE SEARCH BY ACCESS TRANSACTION STATUS

The "-" sign limits the search to access transactions that were denied because the cardholder was not valid in a level applicable to the attempted entry.

- "A" limits the search to cards denied due to Anti-Pass-Back violations.
- "K" limits the search to cards rejected because of an incorrect Keypad P.I.N. code or a failure to use a code during an active Keypad Level.
- "S" limits the search to cards rejected because of wrong system codes. When an "S" occurs, it could possibly be due to the use of a card from another system, or due to an improperly inserted or damaged card. If numerous "S" transactions occur from any one reader, it is probably an indication that the reader is in need of calibration.

If left "blank" the search will be limited to only valid authorized transactions.

- "V" is for all transactions not limited by any exceptions.

SEARCHING BY READER LOCATION

Enter a reader module location code to limit the search to transactions from that one location. If you want to search for transactions from 2 or more specific readers, you may do so by conducting the search from the Transaction Audit screen (F7).

SEARCHING BY MEMORY CODE

For cardholder searches by memory code.

SEARCHING BY TEXT

Searches may be conducted by exact match, or by random character string. If the character location of the text being searched is unknown, choose N (no) for Exact Match, and the program will find every entry with the specified characters no matter where in text they may be. For example, entering the characters "on" will produce a list of transactions that might include:

Don Jackson
Billy Johnson
Bonnie Badilla
Bob Pearson

If exact match is specified, nothing would be found unless the characters "on" were typed @ positions 10 and 11. The computer would then find Jackson and Pearson only because the other two have names with other characters in positions 10 and 11.

If department numbers always occupy the first four characters, than a search of all department 1234 activity would not accidentally pick up transactions for someone in department 5678 but whose license number is ABC1234. If you did not specify an exact match, then that transaction would be included.

INITIATING THE SEARCH

Once the search parameters have been specified, press Function key 6 or 10 and select the file to be searched. As noted on the Input/Output screen, transactions stored to the hard drive use the file name: TCLOG.DTA. If you are searching a file that has been backed-up to floppy, simply specify the drive and file name.

The actual search provides an opportunity to concurrently display, print out, and/or to store the search on a floppy. In addition, you can send the data to a dBase file that has been predefined to accept the data.

If periodic backups are saved to the same disk and to the same file, the newest information will write over the previous file. This is a quick way of keeping your backup current. The backup file name can simply remain on the screen as a default.

dBase EXPORT

dBase Export is a utility that lets you populate a predefined dBase file with transactions recorded by the access control system. Transferring the transactions will append the existing D-Base file.

The information to be transferred can be selected and filtered just like any other search. Therefore it is a good idea to view the search before actually making the transfer.

The first step is to define a dBase file into which you want to transfer the transactions. The following are the fields together with the field lengths:

FIELD CHARACTERS DESCRIPTION FIELD LENGTHS

DAY	2	DAY OF THE WEEK
DATE	8	DATE
TIME	8	TIME
STATUS	1	VOID, VALID, ALARM
MOD	2	MODULE CODE
FAC	4	FACILITY CODE
MEM	4 OR 5	MEMORY NUMBER

ALARM	4	ALARM ADDRESS
ALARM_STAT	12	ALARM STATUS
NAME	32	CARDHOLDER TEXT

You may label your fields in the dBase file with any name you desire. Normally all fields will be defined as "character fields" even though they may contain numbers. Consult your dBase manual for field types.

For fuel dispensing applications, the FAC field is used to record the number of fuel units dispensed. Therefore it is a good idea to define that field as a "numeric field" in the dBase program so that calculations can be made.

After a dBase file is defined, enter the access control program and select FUNCTION 9. Set the search criteria and view the results of the search to insure that is what you want exported. After viewing the initial search, press the F6 key (I/O). Select Y (yes) for "Write to dbase File:"

While the cursor is on the "Y", select F6 to bring up screen S024. Here is where you tell the program what you have named each field. Simply enter the field names you have selected for your dbase file.

To initiate the export functions, simply press the F10 key. The program will now populate your dbase file, and if data already exists in this file, it will append it.

SEARCHING THE TEXT DATA BASE

Press the F3 key from the Management Package opening screen to search the computer's current text data base.

This feature permits a rapid text search and displays and/or prints a list of cardholders in memory code order of all entries matching the entered search criteria. If no search criteria is entered, then every entry containing at least one text character is displayed. If cardholder memory codes have been entered without text, they will not be displayed.

TRANSACTION AUDITING (F7 Key)

Nesting Enforcement-Cardholders Present

Transaction auditing provides instant reports of controlled parking "nesting" violations, and will provide instant verification of cardholders present. In both cases, the controlled areas must be equipped with card readers at both entrance and exit locations.

NESTING ENFORCEMENT

Nesting is a term which refers to special rate parking areas. Nesting enforcement is a method used to assure that special rate parkers actually park in the special rate

area (nest), and not in regular parking areas.

The program is designed to audit the length of time a parker remains in a regular parking area. If the time exceeds the customer's specified grace period, it is assumed that the special rate parking criteria has been violated.

A parker must exit the regular parking area by entering the special rate area (nest), or exiting the entire parking facility before the grace period in order to avoid detection as a nesting violator.

Designating Special Rate Parkers In The Data Base

Cardholders subject to special rate restrictions should be identified by a word or a symbol typed into the text data base. Always use the same character location for this designator. For example, a "*" in the first character position could delineate a special rate parker. If there are several categories of special rate parkers, other characters could be used as well. Be careful not to use the designated character for other none restricted parkers. In other words, if the character "W" is used in the first character position to delineate a certain group of parkers, any cardholder with a "W" in the first position would be assumed to be a special rate parker, like "William Smith".

Entrance-Exit Definitions

For the purposes of Nesting Enforcement only:

An entrance location is any gate which permits entry into the regular parking area. It could be a gate from outside the parking lot, or it could be a gate leaving a special rate area (nest) which enters the regular parking area.

An exit location is any gate that exits the regular parking area. It could be the main parking lot exit, or it could be a gate which permits entry to the special rate area.

RUNNING A NESTING ENFORCEMENT REPORT

To set the parameters for a nesting report, enter the date of the report, or leave blank for today's activity. For time, it is best to specify the start time as 0000, and the end time 2400.

Enter the grace period in minutes. This period can be changed at will, and should be adjusted to reflect a reasonable transition time from the main entrance to the special rate area. One way to establish this figure would be to run several reports using different grace periods to determine a typical transit time. If 5 minutes picks up too many violations, try 10 etc.

The Access Transaction Status should be left blank.

Text string to search should contain the designated special rate parking character symbol such as "*". You can also enter the name of any cardholder if you want to check for nesting violations of just that person.

Enter YES "Y" to exact match.

Finally, enter the reader module code of the Entrance Locations, and the Exit Locations.

These parameters will remain unless changed, providing instant verification of nesting violations with only a few key strokes.

To run the report, press the F10 Function Key, set the prompts, and hit the F10 key again.

To inspect the entire pattern of a nesting violator, simply hit the F5 Key which returns you to the Transaction Management screen. Enter the person's name, then hit F10 to see that person's complete entry/exit record.

CARDHOLDERS PRESENT

It is possible to quickly establish which cardholders are in a facility provided both entrances and exits are controlled with card readers.

From the TRANSACTION AUDITING main screen, simply use a grace period greater than the number of minutes remaining in the work day, such as 600. If a cardholder has not exited before that time, his name will appear.

dBase IMPORT

This utility lets you import cardholder information from another dBase file. Although the Import utility contained in this program is limited to the industry dBase III standard, most other database programs include a conversion utility that can save the data to dBase so that it can be imported into the access control program.

The access control software is able to import all information necessary to completely program individuals into the system. This includes card number, name, and security level assignments.

To use the dBase Import feature, select FUNCTION 9 from the Function Menu or "B" from the ACTION WINDOW. Then press the F3 key (CARD). Select F7 (import).

Now simply enter the path and name of your dBase. Enter the name of the field from which the card memory number is to be imported, and the name of the field from which the cardholder's name is to be imported. If you would also like to program cardholders into specific security levels, enter the name of the fields that

contain these levels. Press F10 to start the import.

If you are maintaining your cardholder database in an external database program, you can configure the access control system to automatically import the data whenever changes are made. See Dbase Memory Management.

SPACE COUNT REPORTS (F8)

Each time the status of a counter changes, the new count is logged to the hard disk (TCLOG.DTA). The day, date, time, counter number, counter status, and counter text description are recorded. This data can be retrieved in two ways, a daily (hour by hour) printed report, or a display of chronological log entries which can be displayed or printed by counter, and/or specified dates and times. Thus, the status of any counter can be recalled at a future date, displayed, printed, or written to a disk file.

Daily Report

When you select the F8 key the first time, the daily (hour by hour) set up screen is displayed. Each column may be defined to display a specific value. For example, COL 1 might display the highest count within each hour, or the "high water mark" for that hour. COL 2 might simply reflect the up counts. There are four available values, and each of the four may be displayed in different ways:

If you want the highest value of the counter within each one hour period, you may enter either:

HIGHEST, or MAXIMUM

If you want all the up counts that occurred within each one hour period, you may enter either:

UP COUNT, INCREMENTS, or ENTRIES

If you want all the down counts that occurred within each one hour period, you may enter either:

DOWN COUNTS, DECREMENTS, or EXITS

If you want to know what the value of a counter was at the beginning of any one hour period, enter either: STARTING, or BEGINNING COUNT

To run the printed report, simply enter the report date and hit the F10 key to execute. This is a printed report only, and cannot be displayed.

If you have entered text descriptions in the counter setup FUNCTION 4.2) and you have saved these descriptions (FUNCTION 3.3), they will automatically be displayed on the setup screen.

Counter Status Log Reports

To retrieve counter activity from the hard disk log, select FUNCTION 9, and hit

the F8 key twice. Enter the start time and date, and the stop time and date of the activity you want to review. Select the counter you want to examine, or leave it blank to view the chronological status of all counters. You may view the report, print it, or send it to a disk file.

D: dBASE MEMORY MANAGEMENT Functions ("B" Hot Key)

(Not available for 9 digit systems)

There are two ways to program and maintain the access control cardholder database; *internally* by using the programming utilities located in FUNCTION 3, or *externally* from a dBase file. When you use internal programming, changes you make go directly from the keyboard into the "PC"s memory as you make them. When you use a dBase program, the changes you make take place in an external database and are actually imported into the access control system when you exit the dBase program. With certain precautions, you may program the system both *internally* and *externally* without restriction.

This section explains exactly how the dBase Memory Management feature works. If you are using both the *internal* and *external* programming utilities, it is extremely important to understand how they both function with respect to one another.

External Programming: Pressing The "B" key from the ACTION WINDOW takes you to a dBase screen where you can enter and maintain your cardholder database. This built-in database contains fields that you can relabel to reflect the information about each cardholder that you would like to maintain in the system. You have the option when exiting this database to allow the data to be imported and saved to the access control system automatically. You can use the same database to program the Smart Cartridge program as well.

If you have your own dBase III compatible database program, you can configure the system so that the dBase Memory Management feature takes you directly to your dBase program. You also have the option when exiting that database to allow the data to be imported and saved to the access control system automatically.

If you choose not to maintain the access control system from your own dBase program, you still may import the data into the access control system by using the import utility located in FUNCTION 9, F3, F7.

The built-in database is an actual dBase program containing the basic functions necessary to enter data, search, add, and delete records. It is not intended to emulate a full featured database program containing high end dBase functions. But, because it is in fact a dBase III compatible program, you can easily perform high end dBase functions using any of several available commercial programs such as dBase III, and Clarion Report Writer. These third party programs let you index, sort, filter, and create displayed and printed reports based on any combination of

parameters.

To illustrate the simplicity and power of such utilities, this program includes three database reports created in Clarion Report Writer. Once you have populated your database with cardholder information you can try these reports. Instructions follow later in this section.

It is very important to recognize that the dBase Memory Management feature is intended to provide convenient access to dBase records, and to automate the process of importing and saving this data into the access control system in one step. It is in fact an *external* dBase file that is not an interactive part of the access control program. For this reason, data contained in the dBase file may not necessarily reflect the programming status of the access control program if both *internal*, and *external* programming functions are utilized.

You may for example want to initialize your access control system quickly by validating every cardholder in one or more levels using the *internal* programming routines. This gets the system going immediately giving you plenty of time to begin the process of entering individual cardholder data. Once you have entered all the cardholder information into the dBase program, you can now import it into the access control system, but you will first need to clear the system's memory so that after the import, it reflects only the programming parameters contained in the dBase file.

This operation takes only seconds to do:

Enter FUNCTION 3.1 or hit the "B" Hot Key. Select Routine 1, F2 for All Levels, F3 for all cards. Type VOID to remove every card from the system.

Now enter dBase Memory Management, answer yes to import upon exiting. When you exit the dBase file, the *internal* memory will be programmed to match every record in the database. Any cardholder not in the dBase file will be void.

The dBase Memory Management feature performs the following import functions for each record:

1. Program a card to be VALID in every security level. (Type VALID in the *All field*)
2. Program a card to be VOID in every security level. (Type VOID in the *All field*)
3. Add or delete any combination of 10 security levels at a time. (*Level fields*). The *All field* must be blank.

The All field (VOID OR VALID) is intended for instant action. If you want to remove a card instantly without modifying the cardholder's record, typing VOID in that field will remove the card from the system regardless of what other levels might be entered above it. The same is true for the use of VALID. Once a card has been voided from the system, it is strongly recommended that you use the Delete

Key

Setting Up The Access System to Accept Imported Data

In order for the access system to import data from an external dBase file, it needs to know the names of the fields containing the data. If you are using the built-in database, the setup screen already reflects the correct information so you can begin entering data immediately by selecting dBase Memory Management. If you are using your own database, you must change the Import setup screen to reflect your file name and field descriptions. To set this up, select FUNCTION 9, F3, F7 Import. The setup screen shows the information required for the built-in default database.

S031 CARD TEXT INFORMATION

dBASE File Import Parameters

Name of dBASE File: **CARDS.DBF**

dBASE Field Name for:

Internal Card Memory Code. **MEMORY_NO**Card Text..... **NAME**

Card Level Programming (up to 10 names)

01... **COM1LVL01** 06... **COM1LVL06**02... **COM1LVL02** 07... **COM1LVL07**03... **COM1LVL03** 08... **COM1LVL08**04... **COM1LVL04** 09... **COM1LVL09**05... **COM1LVL05** 10... **COM1LVL10**All Levels VALID/VOID.... **COM1ALL**

Shown in bold are the actual field names in the database from which the access control program extracts the data. If you are using another database with a different file name, and different field names, then you need to change this setup screen to reflect those names.

If you are using the same database to program both the "PC" system software, and the Smart Cartridge Software, you can define the Smart Cartridge set up screen exactly as above if the two memory configurations are identical. If the Smart Cartridge software has different security level definitions, then you must use different level fields for the Smart Cartridge. The built-in database contains additional fields for this purpose, and they must be defined in the Smart Cartridge software under FUNCTION 9, F3, F7.. They are labeled COM2 LVL01-COM2LVLE10. The ALL field is labeled COM2ALL. You can modify the display form to reflect these changes using DOS Editor. The display form is located in the access control directory, and is named CARD1.FOR.

When both the PC and Smart Cartridge software are managed from the same database, the import will occur separately from each program. In other words,

when you are in the PC program, only the PC records will be imported. To be sure that the Smart Cartridge database receives the information, you need to bring up that program, select FUNCTION D:, answer yes to import, and then exit FUNCTION D in order to import the data into the Smart Cartridge program.

Once the configuration information is correct, you may now return to the ACTION WINDOW and select **D: dBASE MEMORY MANAGEMENT Functions**. You will be asked at this point whether or not you want the data you add or change to be automatically imported into the access control system. If you select no, the automatic import will not occur when you Escape out of dBase Memory Management. If you respond with a "Y", your dBase file will be imported into the access controls system in its entirety.

The manner in which the data fields are laid out may be modified by using any text editor. Current versions of DOS contain a text editor. You may rearrange the location of fields, and you may change the field labels. The name of the default form is CARD1.FOR. If you plan to edit this display form, it is best to load it in DOS Editor, and then save it as CARD2.FOR so that you can experiment without changing the default form. The F2 key allows you to select which display form to use, so you can create as many different forms as you wish to make data entry and interrogation more convenient..

Using dBase Memory Management

The following explains the use of the Function Keys located at the bottom of the screen:

FUNCTION KEY F1: Cancels any changes you have made to the data that has not been saved. If no changes have been saved, this key exits dBase Memory Management.

FUNCTION KEY F2: Select the name of the database to be viewed, and the display form. The default database will be CARDS.DBF. The default display form is CARD1.FOR.

As previously noted, you can modify the field names on any form by using a text editor. When you display the form in a text editor, you will notice two references to each field. The first is the name you wish displayed for that field, and the name in brackets is the name of the field as defined in the database. The name you wish displayed for a field shows on the form, and the location on the form that the field name appears will be substituted for the actual data you have entered into the field. For example, the form will show NAME: [NAME]. The field name in the brackets tell the database where to display the data you have entered. The word NAME simply provides the label for the data. You can edit the word name and replace it with CARDHOLDER if you wish. The new form when viewed by a text editor would appear like this: CARDHOLDER: [NAME]. The field name stays the same.

FUNCTION KEY F3: Takes you to the first record in the database, or if you are using the F9 filter feature, it takes you to the first record that meets the filter criteria.

FUNCTION KEY F4: Allows you to DELETE and UN-DELETE a record. If the record is deleted, the data it contains will be ignored by the access control system, but the record will still be visible for future reference and can be found in a search. If you delete this record because the individual to whom it belonged is to be cancelled permanently, you can use the same record for someone new. It is advisable to delete records that have been voided. This will increase the import processing time since the system will not have to repeat the voiding process every time an import occurs.

FUNCTION KEY F5: Takes you to the previous record, or if you are using the F9 filter feature, it takes you to the prior record that meets the filter criteria.

FUNCTION KEY F6: Takes you to the next record, or if you are using the F9 filter feature, it takes you to the next record that meets the filter criteria.

FUNCTION KEY F7: Takes you to the last record in the database, or if you are using the F9 filter feature, it takes you to the last record that meets the filter criteria.

FUNCTION KEY F8: Creates a blank record into which you can add a new cardholder.

FUNCTION KEY F9: Takes you to a blank record into which you can enter filter values. If you place the cursor in the VEHICLE field, only records in that field will be filtered. If you enter FORD, you will be taken to the first record in the database with the word FORD in that field. If you hit the F6 Key, you will be taken to the next record that meets the criteria and so on. To cancel the filter, hit F9, and again select F9 for all.

So locating records in your database is simple. You can find a record by virtually any search value you choose. If you want to pull up a record for card serial number 8974, simply select F9:, and enter 8974 in the serial number field.

FUNCTION KEY F10: Should be used to save changes and additions as you make them. The F10 KEY is also used to execute a search after having entered a filter value.

Adding Records To Your Database

To add cardholder records, you can type over an existing record if it is no longer in the system, or hit FUNCTION Key F8 to add a new record.

1. The NAME field contains 32 characters. Whichever 32 characters you place in this field will be displayed on the transaction log each time the card is used.
2. The MEMORY NUMBER FIELD **51** the encoded number to be used by

Index

A

About Access Central 5
About PC Central 6.1 3
ACTION WINDOW 33
Action Window 14
Alarm Batch File 19
Alarm Descriptions 18
ALARM GRAPHICS 19
ALARM MODULE LEVELS: Programmable
 Shunting 32
ALARM OUTPUTS 20
ALARM SHUNTING 32
ALARM TEXT 18
ALARM WARBLE 18, 20
ANSI.SYS 11
ANTI-PASS-BACK 21
 EXCEPTIONS 22
 HARD AND SOFT 22
 TIMED 21
ANTI-PASS-BACK STATUS 14
Automatic Loading 5

B

BACKING UPDATA 12
Badge Making Equipment 9
Built In dBase Utility 4

C

CARD NUMBER TO PROGRAM 13
Card Numbers Exceeding 65,5535 50
Card or Keypad Dual Code Option 49
CARD PROGRAMMING 17
CARD TEXT 35
CARDHOLDER DATABASE 7
CARDHOLDER TEXT 18
CARDHOLDERS PRESENT 40
CCTV controllers 31
Changing path statemet 11
Changing tlog path 10
COMMAND MODULE LEVELS 26
Command Module Switch Settings (4120) 50

D

DAYLIGHT SAVINGS TIME 14, 16
DBase EXPORT 37
DBase IMPORT 41
DBASE MEMORY MANAGEMENT 42
 ADDING NEW RECORDS 47
 REPORTS 47
 SETUP 44

DEFINE ENTRY POINTS 8
DEFINING A SYSTEM 12
DESCRIBE LEVELS 8
Direct To Memory P2 Programming 4
Display Active Alarms 33
Display Current System Activity 33, 34
Display Only Access Transactions & Alarms 34
Display Only Counter Activity 34

E

ELEVATOR LEVELS 30
EXIT to DOS 48

F

FORGOTTEN PASSWORDS 15, 16
Forms 10

G

Garbled Text 11
Getting Started 6
GRAPHICS 19

H

HARD COPY Options 17
HARD DISK MANAGEMENT 35
HISTORY 35
 CONDUCTING A SEARCH 35
HOLIDAY Definitions 16
Hot Key Bar 14

I

Installing Access Central With Existing
 Systems 5
Internal Programming 12

K

Keypad Operation 26

L

LAN NETWORKING 13
Level Definition Work Sheet 13
Linking ID Photos 8
LIST CARDS PER LEVEL 18
LIST LEVELS PER CARD 18
Loading The Microsoft Access Interface 6

M

Macros 11

MAKE I.D. BADGE 8
MEMORY Programming & Verification 17
Metasys 8
MODULE LEVELS 12
Modules 11
Monitor Space Counters 34
MONITOR Transactions 33
MP.EXE 4
MS Access Central Database Properties 10

N

NESTING 22
NESTING, SOFT 39
New System Installation 5
Nine Digit Social Security Number Systems 7

O

OFF-LINE Mode 33
ON-LINE Mode 33
OUTPUT MODULE LEVELS: Time Program
Activated 31
OUTPUT MODULE LEVELS: Transaction
Activated 30

P

P: PASSWORD Protection 15
P2.EXE 4
PASSWORD
FORGOTTEN 16
PRINTING 17
PROGRAMMING CARDHOLDERS INTO THE
SYSTEM 12
The first step 13
Programming Choices 4
Purge Active Alarms 34
Purge Current Transaction Screen 34

Q

Queries 10

R

READER SUPERVISION 14
Reports 11
Restricted Levels 15
RESTRICTED SECURITY LEVELS 21

S

SCREEN SWITCHING 20
SECURITY LEVEL & OUTPUT RELAY
Definitions 25
SECURITY LEVEL Definitions 26
SECURITY LEVELS 12
SETUP 2

SOFTWARE FUNCTIONS MENU 15
Software Installation 5
SPACE COUNT REPORTS 41
SPACE COUNTING 24
SR.COM 3
SUPERVISION 14
Supervision Status 34
Supervisor First Option 49
System Requirements 3

T

Tables 10
TASK SWITCH 48
TCLOGDTA 12
Three ways to program 4
TIME & HOLIDAY Definitions 16
TIME MANAGEMENT REPORT 10
Timed Alarm Shunt 26
Timed Keypad activation 26
Timed Unlock 26
TRANSACTION ACTIVATED OUTPUTS 20
TRANSACTION AUDITING 39
TRANSACTION DISPLAY 14
TRANSACTION EXCEPTION CODES 33
Trouble Shooting
Scrambled Text 11

U

"U": UNLOCK a Door or Raise A Gate
Instantly 15
UPDATE PC CENTRAL 9

V

V.I.P. Tracking 25, 34
VIEW ACCESS TRANSACTIONS Or
ALARMS 8

W

WHO'S IN 40

Y

Your Computer's Configuration 11

Toye Corporation
20916 Itasca St.
Chatsworth, CA 91311
(818) 882-4000